UNIT 10: QUADRATIC CONGRUENCE AND QUADRATIC RECIPROCITY LAW

UNIT STRUCTURE

10.1 Learning Objectives
10.2 Introduction
10.3 Quadratic Congruence
10.4 Quadratic residue
10.5 Legendre symbol and its properties
10.6 Quadratic reciprocity Law
10.7 Quadratic congruences with composite module
10.8 Jacobi symbol
10.9 Let Us Sum Up
10.10 Answers to Check Your Progress
10.11 Further Reading
10.12 Model Questions

10.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the concept of quadratic congruences
- Explain the concept of quadratic congruences and identify when an integer is a solution to a quadratic congruence modulo *n*.
- Define quadratic residues and non-residues and determine whether a given integer is a quadratic residue modulo a prime.
- Understand and use the Legendre symbol**,** including its definition, notation, and fundamental properties.
- State and apply the Law of Quadratic Reciprocity to simplify computations of Legendre symbols.
- Define and compute the Jacobi symbol, and distinguish its use from the Legendre symbol.
- Understand the Legendre symbol, compute its values, and apply its fundamental properties in problem solving.
- State and apply the Law of Quadratic Reciprocity to determine solvability of quadratic congruences modulo primes.
- Understand the Jacobi symbol, compute it using its properties, and differentiate it from the Legendre symbol.
- Apply the concepts of quadratic residues, Euler's criterion, Legendre and Jacobi symbols, and reciprocity laws to analyse and solve various types of quadratic congruence problems.

10.2 INTRODUCTION

A quadratic congruence is simply a congruence involving a square term, typically of the form

$$x^2 \equiv a(mod\ m)$$

and its solvability depends strongly on the arithmetic nature of the modulus m and the integer a.The investigation of such congruences naturally leads to the notion of *quadratic residues*, which answers the basic question: for which integers $a$does the congruence $x^2 \equiv a(mod\ m)$admit a solution? To analyze these questions efficiently, number theorists introduced powerful symbolic tools such as *Euler's criterion* and the *Legendre symbol*, which encode quadratic residuosity properties in a compact algebraic form.

One of the most remarkable achievements in number theory is the *Quadratic Reciprocity Law*, first proved by Carl Friedrich Gauss. This law reveals a surprising and elegant relationship between the solvability of two different quadratic congruences involving distinct odd primes. It not only simplifies the computation of quadratic residues but also highlights the deep symmetry underlying modular arithmetic.

This unit begins with an introduction to quadratic congruences and quadratic residues modulo primes, followed by Euler's criterion and the Legendre symbol along with its important properties. The Quadratic Reciprocity Law is then presented as the central result of the unit. Subsequently, the theory is extended to quadratic congruences with composite moduli, leading to the definition and use of the *Jacobi symbol*, which generalizes the Legendre symbol and plays a crucial role in computational number theory.

By the end of this unit, learners will gain a clear understanding of the theoretical foundations of quadratic congruences, develop the ability to determine solvability of quadratic congruences modulo primes and composite numbers, and appreciate the elegance and significance of the Quadratic Reciprocity Law in number theory.
Quadratic Congruence

10.3QUADRATIC CONGRUENCE

A quadratic congruence in one variable is of the form

$$ax^2 + bx + c \equiv 0(mod\ p)$$

where $a, b$and $c$are integers,p is an odd prime and $p \nmid a$.
Theorem 10.3.1: The quadratic congruence
$ax^2 + bx + c \equiv 0(mod\ p)$ (1)
can be transformed into an equivalent congruence of the form
$y^2 \equiv d(mod\ p)$ where $y = 2ax + b$ and $d = b^2 - 4ac$.
Proof: Multiplying the given quadratic congruence by $4a$,we get

$$4a(ax^2 + bx + c) \equiv 0(mod\ p)$$

or $4a^2x^2 + 4abx + 4ac \equiv 0(mod\ p)$

which can be written as

$$(2ax + b)^2 \equiv (b^2 - 4ac)(mod\ p)$$

Putting $2ax + b = y$ and $b^2 - 4ac = d$, the congruence reduces to

$y^2 \equiv d(mod\ p)$. (2)

Thus, solving the quadratic congruence in Eq. (1) is equivalent to solving a corresponding linear congruence together with a quadratic congruence of the form

$x^2 \equiv a(mod\ p)$ (3)

If $p|a$,then the quadratic congruence in Eq. (3) has $\equiv 0(mod\ p)$ as its only solution.

Example 1:

Consider the quadratic congruence

$$5x^2 - 6x + 2 \equiv 0(mod\ 13)$$

Now we reduce the quadratic congruence to a standard quadratic congruence.

For a quadratic congruence

$$ax^2 + bx + c \equiv 0(mod\ p)$$

We multiply both sides by $4a$ and write it in the form

$$(2ax + b)^2 \equiv (b^2 - 4ac)(mod\ p)$$

Here $a = 5, b = -6, c = 2, p = 13$.

Now, we compute

$2ax + b = 2(5)x - 6 = 10x - 6$,

and $b^2 - 4ac = (-6)^2 - 4(5)(2) = 36 - 40 = -4$

Reducing to modulo 13,

$$-4 \equiv 9(mod\ 13)$$

Hence, the given congruence is equivalent to

$$(10x - 6)^2 \equiv 9(mod\ 13)$$

Let $y = 10x - 6$

Then the congruence becomes

$$y^2 \equiv 9(mod\ 13)$$

Since $3^2 = 9$ and $10^2 = 100 \equiv 9(mod\ 13)$

The solutions are

$$y \equiv 3, 10(mod\ 13)$$

Now, we solve the corresponding linear congruences

Thus, we solve the following linear congruences:

(a) $10x - 6 \equiv 3(mod\ 13) \Rightarrow 10x \equiv 9(mod\ 13)$

$\Rightarrow x \equiv 4.9 = 36 \equiv 10(mod\ 13)$

(b) $10x - 6 \equiv 10(mod\ 13) \Rightarrow 10x \equiv 16(mod\ 13)$

$\Rightarrow x \equiv 4.3 \equiv 12(mod\ 13)$

The solutions of the given quadratic congruence

$$5x^2 - 6x + 2 \equiv 0(mod\ 13)$$

are $x \equiv 10, 12(mod\ 13)$.

Theorem 10.3.2: If the congruence

$$x^2 \equiv a(mod\ p)$$

is solvable then it has exactly two solutions.

Proof: Let x_0 be a solution of the given congruence. Then
$x_0^2 \equiv a(mod\ p)$. (1)
Obviously $(p - x_0)$ also satisfies the given congruence
$\therefore (p - x_0)^2 \equiv a\ (mod\ p)$ $[\because\ (p - x_0)^2 \equiv (-x_0)^2 \equiv x_0^2 \equiv a(mod\ p)]$ (2)

Thus,x_0 and $(p - x_0)$ are two solutions of the given congruence.
Suppose, for contradiction, that there exists a **third solution** x_1 such that
$x_1^2 \equiv a(mod\ p)$ (3)
From (1) and (3),we have

$$x_1^2 \equiv x_0^2(mod\ p)$$
$$\Longrightarrow x_1^2 - x_0^2 \equiv 0(mod\ p)$$
$$\Longrightarrow (x_1 - x_0)(x_1 + x_0) \equiv 0(mod\ p)$$

This gives that p divides $(x_1 - x_0)(x_1 + x_0)$.
This implies that either
p divides $x_1 - x_0$i.e.,$p|x_1 - x_0$

$$\Longrightarrow x_1 \equiv x_0(mod\ p)$$

or p divides $(x_1 + x_0)$ i.e.,$p|x_1 + x_0$

$$\Longrightarrow x_1 \equiv -x_0 \equiv p - x_0(mod\ p)$$

This shows that x_1 is not a distinct solution.
Thus, the congruence $x^2 \equiv a(mod\ p)$ has exactly two solutions.
Example 2:
Let us solve
$2x^2 + x + 3 \equiv 0(mod\ 5)$ (1)

The given congruence is of the form

$$ax^2 + bx + c \equiv 0(mod\ p)$$

where $a = 2,b = 1,c = 3,p = 5.$

Since $(2,5) = 1$,so, we can transform the quadratic congruence into a simpler square form**.**

Using the standard transformation

$$ax^2 + bx + c \equiv 0(mod\ p) \Leftrightarrow (2ax + b)^2 \equiv b^2 - 4ac(mod\ p)$$

We compute $2ax + b = 2(2)x + 1 = 4x + 1$

Since $(2,5) = 1$.(1) is equivalent to

$$(2x + 3)^2 \equiv 0(mod\ 5)$$

Thus solving (1) reduces to solving
$y^2 \equiv 0(mod\ 5)$, with$y = 2x + 3$ (2)

But (2) has a unique solution $y \equiv 0(mod\ 5)$
and$y = 2x + 3 \equiv 0(mod\ 5)$
$\Longrightarrow x \equiv 1(mod\ 5)$ is the unique solution of (1)
Thus, it suffices to solve the congruences of the form
$x^2 \equiv d(mod\ p)$.
Example 3: Solve the congruence

$$x^2 + 3x + 11 \equiv 0(mod\ 13)$$

Solution: We have

$$x^2 + 3x + 11 \equiv 0(mod\ 13)$$

Multiplying both sides by 4, we obtain

$$4x^2 + 12x + 44 \equiv 0(mod\ 13)$$

This can be rewritten as

$$(2x + 3)^2 \equiv 4(mod\ 13)$$

Let $y = 2x + 3$.Then the congruence reduces to

or $y^2 \equiv 4(mod\ 13)$
The solutions of this congruence are
$y \equiv 2(mod\ 13)$ or $y \equiv 11(mod\ 13)$
i.e., $2x + 3 \equiv 2(mod\ 13)$ or $2x + 3 \equiv 11(mod\ 13)$
i.e.$2x \equiv 12(mod\ 13)$or$2x \equiv 8(mod\ 13)$
i.e. $x \equiv 6(mod\ 13)$or $x \equiv 4(mod\ 13)$.
Hence, the solutions are $x \equiv 4,6(mod\ 13)$.

W CHECK YOUR PROGRESS

Q1) Solve the congruences
(a) $3x^2 + 5x + 9 \equiv 0(mod\ 11)$
(b) $x^2 + 7x + 10 \equiv 0(mod\ 11)$

10.4 QUADRATIC RESIDUE

Let p be a prime and a is an integer coprime to p.Then a is called a quadratic residue $(mod\ p)$ if and only if $x^2 \equiv a(mod\ p)$ has a solution. Otherwise$a$ is called quadratic non-residue$(mod\ p)$.
For example,$x^2 \equiv 4(mod\ 5)$ has 2 and 3 as its solutions $(mod\ 5)$.
Therefore 4 is a quadratic residue (mod 5).
Example 1: Consider the case of the prime $p = 13$.To find out how many of the integers $1,2,3,\cdots\cdots,12$ are quadratic residues of 13, we must know which of the congruences

$$x^2 \equiv a(mod\ 13)$$

are solvable when a runs through the set $\{1,2,3,\cdots\cdots,12\}$.

Modulo 13, the squares of the integers $1,2,3,\cdots\cdots,12$ are

$$1^2 \equiv 12^2 \equiv 1(mod\ 13)$$
$$2^2 \equiv 11^2 \equiv 4(mod\ 13)$$
$$3^2 \equiv 10^2 \equiv 9(mod\ 13)$$
$$4^2 \equiv 9^2 \equiv 3(mod\ 13)$$
$$5^2 \equiv 8^2 \equiv 12(mod\ 13)$$
$$6^2 \equiv 7^2 \equiv 10(mod\ 13)$$

Consequently, the quadratic residues of 13 are 1,3,4,9,10, 12 and the nonresidues are 2,5,6,7,8,11.

Theorem 10.4.1 :(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 $(mod\ p)$ if and only if $a^{\frac{p-1}{2}} \equiv 1(mod\ p)$.

Proof: Let a be a quadratic residue $(mod\ p)$and $(a,p)=1$.Then the quadratic congruence $x^2 \equiv a(mod\ p)$ has a solution (say x_0).

Thus, $x_0^2 \equiv a(mod\ p),(x_0,p)=1$ (1)

By Fermat's Little Theorem, we have

$x_0^{p-1} \equiv 1(mod\ p)$ (2)

Therefore,$a^{\frac{p-1}{2}} = (x_0^2)^{\frac{p-1}{2}}$

$$\equiv x_0^{p-1}(mod\ p)$$

$\equiv 1(mod\ p)$ [By (2)]

Conversely, suppose$a^{\frac{p-1}{2}} \equiv 1(mod\ p)$

Let r be a primitive root $(mod\ p)$.Then $1,r,r^2,\cdots,r^{p-2}$ forms a reduced residue system $(mod\ p)$ and $a \equiv r^k(mod\ p)$ for some integer k such that,$1 \le k \le p-1$.

Now we have,

$$1 = a^{\frac{p-1}{2}} \equiv \left(r^k\right)^{\frac{p-1}{2}}(mod\ p)$$
$$\equiv r^{\frac{k(p-1)}{2}}(mod\ p)$$

As r is a primitive root$(mod\ p)$,it has exponent (order) $(p-1)(mod\ p)$.This implies $(p-1)|\frac{k(p-1)}{2}$.This gives that k must be an even integer say $2t$.

Therefore $a \equiv r^{2t}(mod\ p)$.This shows that r^t is a solution of the congruence

$$x^2 \equiv a(mod\ p)$$

Corollary: Let r is a primitive root $(mod\ p)$,then r^k is a quadratic residue $(mod\ p) \Leftrightarrow k$ is even.

Theorem 11.4: If $(a,p)=1$ where p is prime, then either

$a^{\frac{p-1}{2}} \equiv 1(mod\ p)$ or $a^{\frac{p-1}{2}} \equiv -1(mod\ p)$.

Proof: By Fermat's theorem,$(a,p)=1$,we have

$$a^{p-1} \equiv 1(mod\ p)$$

This can be written as

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

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

Hence, divides either

Therefore, p divides

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

It cannot divide both simultaneously, because if it did, then their difference,

$\left(a^{\frac{p-1}{2}}-1\right)$ - $\left(a^{\frac{p-1}{2}}-1\right)=2$would be divisible by$p$which is impossible since p is an odd prime.

Therefore,

$a^{\frac{p-1}{2}} \equiv 1(mod\ p)$ or $a^{\frac{p-1}{2}} \equiv -1(mod\ p)$.

Note:

Let $a$be an integer such that $(a,p)=1$.Then $a$is a quadratic residue modulo p if

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

and a quadratic non-residue modulo $\boldsymbol{p}$ if

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

This provides a simple criterion for distinguishing quadratic residues from non-residues modulo a prime.

Example 4: Find the quadratic residue and non-quadratic residue of 13.

Solution: We have $(2,13)=1$ and

$$2^{\frac{13-1}{2}} = 2^6 = 64 \equiv 12(mod\ 13)$$
$$\equiv -1(mod\ 13)$$

∴2 is a quadratic non-residue of 13.

Also,$(3,13)=1$ and

$$3^{\frac{13-1}{2}} = 3^6 = (27)^2 \equiv 1^2(mod\ 13)$$
$$\equiv 1(mod\ 13)$$

∴ 3 is a quadratic non-residue of 13.

Example 5: Show that 3 is a quadratic residue of 23, but a non-residue of 31.

Solution: We have $(3,23)=1$ and

$$3^{\frac{23-1}{2}} = 3^{11}$$

Now, we compute modulo 23:

$$3^2 = 9,$$

$3^4 = 81 \equiv 12(mod\ 23)$,

$3^8 = 12^2 = 144 \equiv 6(mod\ 23)$,

Now,$3^{11} = 3^8.3^2.3 \equiv 6.9.3 \equiv 162 \equiv 1(mod\ 23)$

Since

$$3^{11} \equiv 1(mod\ 23)$$

3 is a quadratic residue modulo 23**.**

We have $(3,31)=1$ and

$$3^{\frac{31-1}{2}} = 3^{15}$$

Now, we compute modulo 31:

$$3^2 = 9,$$

$3^4 = 81 \equiv 19(mod\ 31)$,

$3^8 = 19^2 = 361 \equiv 20(mod\ 31)$,

Now,

$$3^{15} = 3^8.3^4.3^2.3 \equiv 20.19.9.3 \equiv 380.9.3 \equiv 8.9.3(mod\ 23)$$
$$\equiv 10.3(mod\ 23)$$
$$\equiv -1(mod\ 23)$$

Thus,

$$3^{15} \equiv -1(mod\ 23)$$

So,3 is a quadratic non-residue modulo 31**.**

10.5 LEGENDRE SYMBOL AND ITS PROPERTIES

The **Legendre symbol**, denoted by

$$\left(\frac{a}{p}\right)$$

was introduced by the French mathematician Adrien-Marie Legendre in the late eighteenth century. It provides a compact and powerful notation to describe whether an integer$a$is a quadratic residue**,** a quadratic non-residue, or divisible by an odd prime$p$.

In this section, we introduce the Legendre symbol, discuss its fundamental properties, and highlight its role in the study of quadratic residues and quadratic reciprocity.

Definition: Let p be an odd prime and a is any integer. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1\ if\ a\ is\ a\ quadratic\ residue\ (mod\ p) \\ 0\ if\ p|a \\ -1\ if\ a\ is\ a\ quadratic\ non-residue\ (mod\ p) \end{cases}$$

For example,$\left(\frac{3}{13}\right) = 1$ because 3 is a quadratic residue $(mod\ 13)$ and$\left(\frac{5}{17}\right) = -1$ because 5 is a quadratic non-residue $mod(17)$.

Theorem 10.5.1: 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) $a \equiv b(mod\ p) \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

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

(v) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$.

Proof: (i) If $a \equiv b(mod\ p)$, then both numbers behave identically modulo **p.**

Now, consider the quadratic congruences:

$$x^2 \equiv a(mod\ p) \text{ and } x^2 \equiv b(mod\ p)$$

Because $a \equiv b(mod\ p)$, both congruences have exactly the same solutions**.**

Thus, $x^2 \equiv a(mod\ p)$ and $x^2 \equiv b(mod\ p)$ are either both solvable or both are not solvable.

Therefore, in both cases we have

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

(ii) We consider the congruence: $x^2 \equiv a^2(mod\ p)$

This congruence is always solvable, because:

$$x \equiv a(mod\ p)$$

is clearly a solution.

Thus,a^2 is always a quadratic residue modulo p, which gives:

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

(iii) By Euler's criterion,

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

Applying this to ab,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{(p-1)}{2}}(mod\ p)$$

$$\equiv a^{\frac{(p-1)}{2}}.b^{\frac{(p-1)}{2}}(mod\ p)$$

$$\equiv a^{\frac{(p-1)}{2}}(mod\ p).b^{\frac{(p-1)}{2}}(mod\ p)$$

$$\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)(mod\ p)$$

Since the Legendre symbol takes the values -1 and 1,we have

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

(iv) The congruence

Since 1 is a quadratic residue of every p, we have$\left(\frac{1}{p}\right) = 1$.

Further the quantities $-\frac{1}{p}$ and $(-1)^{\left(\frac{p-1}{2}\right)}$ are either 1 or -1.

Therefore,$\left(-\frac{1}{p}\right) \equiv (-1)^{\left(\frac{p-1}{2}\right)}(mod\ p)$

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

(iv) We have

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

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

$$= \left(\frac{a}{p}\right). \quad [\because \left(\frac{b}{p}\right)^2 = 1 \text{ as } p \nmid b\ ]$$

Theorem 10.5.2: There are infinitely many primes of the form $4k + 1$ where k is an integer.

Proof: We assume contrarily that there are only finitely many primes of the form of the form $4k+1$,say

$$p_1,p_2,\cdots,p_n.$$

We consider an integer

$$N=(2p_1p_2\cdots\cdot p_n)^2+1$$

Clearly N is an integer of the form $4k+1$. Moreover, N is relatively prime to each of the primes $p_1,p_2,\cdots,p_n$, since none of them divides N.

By the Fundamental Theorem of Arithmetic, N must have at least one prime divisor; let p be such a prime. Then p cannot be any of $p_1,p_2,\cdots,p_n$. Hence, by our assumption, p must be a prime of the form $4k+3$.

From the definition of N, we have

$$(2p_1.p_2\cdots\cdot p_n)^2=-1(mod\ p)$$

Thus, the congruence

$$x^2=-1(mod\ p)$$

has a solution, which implies that -1 is a quadratic residue modulo p.

However, it is known that if p is a prime of the form $4k+3$, then -1 is a quadratic non-residue modulo p.

This contradiction shows that our assumption is false.

Therefore, there must be infinitely many primes of the form $4k+1$.

Theorem 10.5.3: If p is an odd prime, then

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

Proof: Let p be an odd prime and let r be a primitive root modulo p. Then the powers

$$r,r^2,\cdots,r^{p-1}$$

form a permutation of the reduced residue system

$$r, r^2, \cdots, r^{p-1} (mod\ p)$$

Hence, for every integer n with $1 \leq n \leq p-1$, there exists a unique integer k with

$1 \leq k \leq p-1$ such that

$$n \equiv r^k (mod\ p)$$

By Euler's criterion,

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

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

$$\equiv \left[r^{\left(\frac{p-1}{2}\right)}\right]^k$$

$$\equiv (-1)^k (mod\ p)$$

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

Therefore,

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

Now, as k runs through the integers $1,2, \cdots, (p-1)$, exactly half of the values of k are even and half are odd. Consequently, the values +1 and −1 occur equally often among $(-1)^k$.

Hence,

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

Theorem 10.5.4: (Gauss Lemma): If p is an odd integer,a is an integer such that $(a, p) = 1$ and n is number of integers in the set

$$\left\{a, 2a, \cdots, \left(\frac{p-1}{2}\right)a\right\}$$

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

Proof: Since $(a, p) = 1$, each number in $a, 2a, \cdots, \left(\frac{p-1}{2}\right)a$ is coprime to p and no two of them are congruent to each other $(mod\ p)$. So, all remainders are distinct**.**

Let $r_1, r_2, \cdots, r_{n_1}$ be the remainder on division by p such that $0 < r_i < \frac{p}{2}$ and $t_1, t_2, \cdots, t_n$ be the remainders such that $\frac{p}{2} < t_i < p$.Then, we have $n_1 + n = \frac{(p-1)}{2}$ and $r_1, r_2, \cdots, r_{n_1}, p - t_1, \cdots, p - t_n$ are positive integers less than $\frac{p}{2}$.

Now we shall show that these integers are distinct. Suppose if possible $p - t_i = r_j$ for some i and j.Then there exist integers h and k with $1 \leq h, k \leq \left(\frac{p-1}{2}\right)$ such that

$$t_i \equiv ha(mod\ p) \text{ and } r_i \equiv ka(mod\ p)$$

This gives

$$(h + k)a \equiv t_i + r_j \equiv p \equiv 0(mod\ p).$$

$$\Longrightarrow (h + k) \equiv 0(mod\ p).$$

But this is impossible because $1 < h + k \leq p - 1$.Hence, $r_1, r_2, \cdots, r_{n_1}, p - t_1, \cdots, p - t_n$ are all distinct. Thus, $r_1, r_2, \cdots, r_{n_1}, p - t_1, \cdots, p - t_n$ are simply the integers $1,2, \cdots, \left(\frac{p-1}{2}\right)$.

Therefore, there product is

$$\left(\frac{p-1}{2}\right)! = r_1 r_2 \cdots, r_{n_1}(p - t_1) \cdots (p - t_n)$$

$$\equiv r_1 r_2 \cdots, r_{n_1}(-t_1) \cdots (-t_n)(mod\ p)$$

$$\equiv (-1)^k r_1 r_2 \cdots, r_{n_1} t_1 \cdots t_n$$

But $r_1, r_2, \cdots, r_{n_1}, t_1 \cdots t_n$ are congruent $(mod\ p)$ to $a, 2a, \cdots, \left(\frac{p-1}{2}\right)a$ in some order.

Hence,

$$\left(\frac{p-1}{2}\right)! = (-1)^n a, 2a \cdots \left(\frac{p-1}{2}\right)a(mod\ p)$$

$$\equiv (-1)^n a^{\left(\frac{p-1}{2}\right)} \left(\frac{p-1}{2}\right)! \, (mod\ p)$$

$\Longrightarrow 1 \equiv (-1)^n a^{\left(\frac{p-1}{2}\right)} (mod\ p)$ [$\because \left(\frac{p-1}{2}\right)!$ is relatively prime to p]

$\Longrightarrow a^{\left(\frac{p-1}{2}\right)} \equiv (-1)^n (mod\ p)$

By Euler's criterion we have

$\left(\frac{a}{p}\right) \equiv a^{\left(\frac{p-1}{2}\right)} \equiv (-1)^n (mod\ p)$

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

Theorem 11.9: If p is an odd prime then

$$\left(\frac{2}{p}\right) = \begin{cases} 1 \ \ if \ \ p \equiv 1(mod\ 8) \ \ or\ p \equiv 7(mod\ 8) \\ -1 \ \ if \ \ p \equiv 1(mod\ 8) \ \ or\ p \equiv 7(mod\ 8) \end{cases}$$

Hence, $\frac{2}{p} = (-1)^{\frac{p^2-1}{8}}$

Proof: By Gauss Lemma, we have

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

where n is the number of integers in the set

$$\left\{2.1, 2.2, \cdots, 2.\left(\frac{p-1}{2}\right)\right\}$$

which on division by p have the remainder greater than $\frac{p}{2}$.Also the numbers in the above sets are less than p. For$1 \le n \le \frac{p-1}{2}$,$2k < \frac{p}{2}$, we have $k < \frac{p}{4}$.

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

Therefore,

$$n = \frac{p-1}{2} - \left[\frac{p}{4}\right]$$

which are greater than $\frac{p}{2}$.

Since p is an odd prime it must have any one of the forms $8k+1, 8k+3, 8k+5$ or $8k+7$.

Now,

if $p = 8k+1$, then $n = 4k - 2k = 2k$

if $p = 8k+3$, then $n = 4k - (2k-1) = 2k+1$

if $p = 8k+5$, then $n = 4k+2-(2k+1) = 2k+1$

and if $p = 8k+7$, then $n = 4k+3-(2k+1) = 2k+2$.

Thus, we see that n is even when p is of the form $8k+1$ or $8k+7$ and therefore $\left(\frac{2}{p}\right) = 1$ and if p is of the form $8k+3$ or $8k+5$, then n is odd which gives

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

Further

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

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

$$= \begin{cases} 1\ if\ \ p \equiv 8(mod\ 8) \\ -1\ if\ \ p \equiv 3(mod\ 8) \\ 1\ if\ \ p \equiv 5(mod\ 8) \\ -1\ if\ \ p \equiv 7(mod\ 8) \end{cases}$$

$$= \begin{cases} 1\ \ if\ \ p \equiv \pm 1(mod\ p) \\ -1\ \ if\ \ p \equiv \pm 3(mod\ p) \end{cases}$$

Hence,

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

Theorem 10.5.6: If p and $2p+1$ both are odd primes, then $(-1)^{\left(\frac{p-1}{2}\right)}.2$ is a primitive root of $2p+1$.

Proof: We put $q = p+1$.Since p and $2p+1$ both are odd primes, we have either $p \equiv 1(mod\ 4)$ or $p \equiv 3\ (mod\ 4)$.

If $p \equiv 1(mod\ 4)$ then $(-1)^{\left(\frac{p-1}{2}\right)}.2 = 2$.

Now $\phi(q) = q - 1 = 2p$,the order of 2 modulo q is any one of the numbers $1,2,\cdots,p$ or $2p$.

Also, we have

$$\left(\frac{2}{q}\right) \equiv 2^{\frac{q-1}{2}} \equiv 2^p (mod\ p).$$

But $q \equiv 3(mod\ 8)$,therefore $\left(\frac{2}{q}\right) = -1$.

Hence,$2^p \equiv -1(mod\ q)$.This shows that 2 cannot have order p modulo q.Also,2 cannot have order 1 and 2 because $2^2 \equiv 1(mod\ q)$ implies $\frac{q}{3}$ which is impossible.So the order of 2 modulo q is $2p$.This shows that 2 is a primitive root of q.

If $p \equiv 3\ (mod\ 4)$ then $(-1)^{\left(\frac{p-1}{2}\right)}.2 = -2$ and

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

Since $q \equiv 7(mod\ 8)$,we have $\left(-\frac{1}{q}\right) = -1$.

Also $\left(\frac{2}{q}\right) = 1$.Therefore, $(-2)^p \equiv -1(mod\ q)$.

This shows that -2 is a primitive root of q.

Theorem 10.5.7: There are infinitely many primes of the form $8k - 1$.

Proof: Suppose there are only finite number of primes of the form $8k - 1$ gives as $p_1, p_2, \cdots, p_n$.

Let $N = (4p_1p_2 \cdots p_n)^2 - 2$

Obviously N is an integer of the form $2(8n_1 - 1)$.Therefore it will have an odd prime divisor, say,p.So

$$N \equiv 0(mod\ p).$$

This implies that $x^2 \equiv 2(mod\ p)$ has a solution $4p_1, p_2, \cdots, p_n(mod\ p)$.

Therefore,

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

Hence,p must of the forms $8n_1 + 1$ or $8n_1 - 1$.Since p and $2, p_1, p_2, \cdots, p_n$ are coprime to p cannot be of the form $8n_1 - 1$.This shows that all prime divisors of N are of the form $8n_1 + 1$.This implies that N is of the form $8n_1 + 1$.This is contradiction.

Hence, there are infinitely many primes of the form $8k - 1$.

Example 3:
Evaluate $\left(\frac{504}{23}\right)$
Solution: We have

$$\left(\frac{504}{23}\right) = \left(\frac{6^2 \times 14}{23}\right)$$
$$= \left(\frac{6^2}{23}\right).\left(\frac{14}{23}\right) \qquad [\because\ (6,23) = 1]$$
$$= -1 \qquad [\because \text{ 14 is a quadratic non-residue of 23}]$$

Example 4: Evaluate

$$\left(\frac{168}{11}\right)$$

Solution: We have

$$168 = 2^3.3.7$$

$$\therefore \left(\frac{168}{11}\right) = \left(\frac{2^3.3.7}{11}\right)$$

$$= \left(\frac{2}{11}\right)^3.\left(\frac{3}{11}\right).\left(\frac{7}{11}\right)$$

$= -(1)^3.(1).(-1)$ [∵ 2 and 7 are quadratic non-residue of 11 and 3 is a quadratic residue of 11]

$= 1.$

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

Solution: Here, $a = 5$ and $p = 19$. Therefore, $\frac{p-1}{2} = \frac{19-1}{2} = 9$.

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

With respect to modulo 19, the members of S will become

$$\{5,10,15,1,6,11,16,2,7\}$$

Four of these numbers are greater than $\frac{p}{2} = \frac{19}{2} = 9.5$.

Numbers greater than 9.5 are:

$$10,11,15,16.$$

There are 4 such numbers.

Therefore $n = 4$.

W CHECK YOUR PROGRESS

Q 2. Find all the quadratic residue of 23.

Q 3. Evaluate

$$\left(\frac{1372}{29}\right)$$

Q 4. Evaluate n of Gauss Lemma for

$$\left(\frac{11}{23}\right).$$

Q 5. Evaluate n of Gauss Lemma for

$$\left(\frac{3}{31}\right)$$

10.6 QUADRATIC RECIPROCITY LAW

In this section, we shall prove the main result of this unit, namely the Law of Quadratic Reciprocity**.** This result provides an effective method for evaluating the Legendre symbol $\left(\frac{a}{p}\right)$

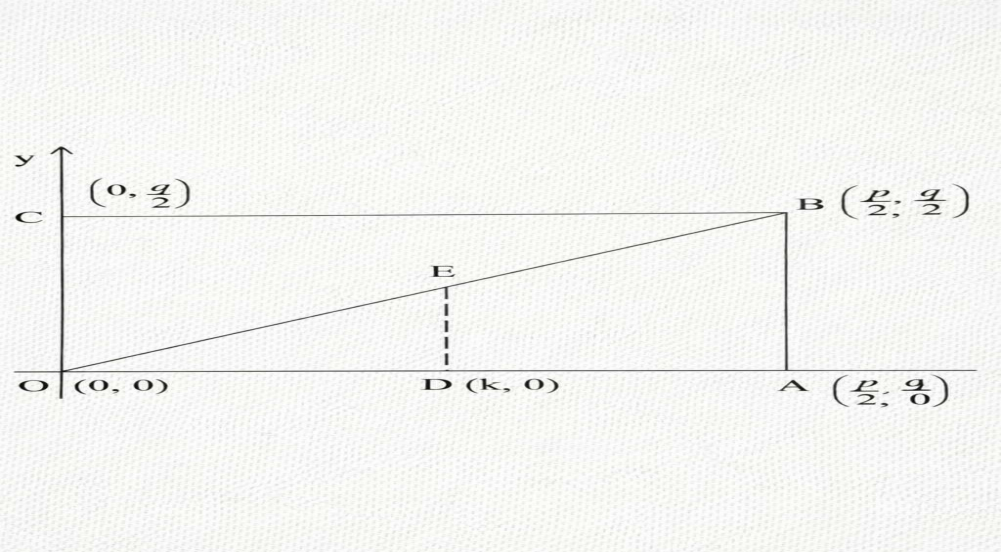
and, consequently, for determining when the congruence $x^2 \equiv a(mod\ p)$ has a solution.

Theorem 10.6.1: If p and q are distinct odd primes, then

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

Proof: We consider a rectangular region R with vertices $(0,0), \left(\frac{p}{2}, 0\right), \left(0, \frac{q}{2}\right)$ and $\left(\frac{p}{2}, \frac{q}{2}\right)$.

We **exclude the boundary** and consider only **interior lattice points**.



A lattice point (whose coordinates are integers) (m, n) inside the boundary OABC satisfies

$$1 \le m \le \frac{p-1}{2} \quad \text{and} \quad 1 \le n \le \frac{q-1}{2}.$$

We will count these lattice points. Since p and q are odd integers, the number of such points will be

$$\left(\frac{p-1}{2}\right).\left(\frac{q-1}{2}\right) \qquad (1)$$

The diagonal OB joins $(0,0)$ to $\left(\frac{p}{2}, \frac{q}{2}\right)$

Now the equation of diagonal OB is given by, $y = \frac{q}{p}x$.

We will show that no lattice point lies on the diagonal OB.

Suppose if (m,n) lies on OB, then

$$n = \frac{p}{q}m \Longrightarrow pn = qm$$

$$\Longrightarrow p|qm$$

Since p and q are distinct primes,

$$(p,q) = 1 \Longrightarrow p|m$$

But this is **impossible**, because

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

Therefore, no lattice point lies on the diagonal OB.

Let R_1 be the portion of R below OB and R_2 be the portion of R above OB.We will count the lattice points inside these two regions. We consider a point $D(k,0)$ on OA where

$$1 \leq k \leq \frac{p-1}{2}.$$

Let the perpendicular on D meet the diagonal on E. The number of lattice points lying on DE will be $\left[\frac{kq}{p}\right]$.

Therefore, the number of lattice points lying in R_1 will be

$$\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p}\right].$$

Similarly, the number of lattice points lying in R_2 will be

$$\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kp}{q}\right].$$

Thus, the total number of lattice points lying in R

$$= \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p}\right] + \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kp}{q}\right] \qquad (2)$$

From (1) and (2), we have

$$\left(\frac{p-1}{2}\right).\left(\frac{q-1}{2}\right) = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p}\right] + \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kp}{q}\right] \qquad (3)$$

By Gauss lemma, we have

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kq}{p}\right]} \text{ and } \left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kp}{q}\right]}$$

Multiplying

$$\left(\frac{p}{q}\right).\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kq}{p}\right]}.(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kp}{q}\right]}$$

$$= (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kq}{p}\right]+\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kp}{q}\right]}$$

Using Equation (3):

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

Corollary 1: If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 \; if \;\; p \equiv 1(mod\ 4) \; or \; q \equiv 1(mod\ 4) \\ -1 \quad if \;\; p \equiv q \equiv 3(mod\ 4) \end{cases}$$

Proof: We have

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

$$= \begin{cases} 1 \quad if \;\; \left(\frac{p-1}{2}\right).\left(\frac{q-1}{2}\right) \; is \; even \\ -1 \quad if \;\; \left(\frac{p-1}{2}\right).\left(\frac{q-1}{2}\right) \; is \; odd \end{cases} \qquad \left[\because \; (-1)^n = \begin{cases} 1 \; if \; n \; is \; even \\ -1 \; if \; n \; is \; odd \end{cases} \right]$$

Now we consider the product: $\left(\frac{p-1}{2}\right).\left(\frac{q-1}{2}\right)$

(i) The product is **even** if **at least one factor is even.**

i.e., Product is even if $\left(\frac{p-1}{2}\right)$ is even or $\left(\frac{q-1}{2}\right)$ is even.

i.e., at least one of p or $q \equiv 1(mod\ 4)$

(ii) The product is **odd** if **both factors are odd.**

i.e., Product is odd if $\left(\frac{p-1}{2}\right)$ is odd and $\left(\frac{q-1}{2}\right)$ is odd.

i.e., $\boldsymbol{p \equiv q \equiv 3(mod\ 4)}$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 \quad if \;\; at \; least \; one \; of \; p \; and \; q = 4k+1 \\ -1 \; if \;\; both \; p \; and \; q = 4k+3 \end{cases}$$

$$= \begin{cases} 1 \; if \;\; p \equiv 1(mod\ 4) \; or \; q \equiv 1(mod\ 4) \\ -1 \quad if \;\; p \equiv q \equiv 3(mod\ 4) \end{cases}$$

Another Form of Quadratic Reciprocity:

If p and q are distinct odd primes, then

$$\frac{p}{q} = \begin{cases} \left(\frac{q}{p}\right) \quad if \; p \equiv 1(mod\ 4) \; or \; q \equiv 1(mod\ 4) \\ -\left(\frac{q}{p}\right) \quad if \;\; p \equiv q \equiv 3(mod\ 4) \end{cases}$$

Example 6: Show that, $\left(\frac{113}{43}\right) = \left(\frac{43}{113}\right)$.

Solution: Here 43 and 113 are both odd primes. So, the Quadratic Reciprocity Law applies.

Now we check whether each prime is of the form $4k + 1$ or $4k + 3$

For 113:

$$113 = 4 \times 28 + 1 \Longrightarrow 113 \equiv 1(mod\ 4)$$

So, 113 is of the form $4k + 1$

For 43:

$$43 = 4 \times 10 + 3 \Longrightarrow 43 \equiv 3(mod\ 4)$$

So, 43 is of the form $4k + 3$.

From the result:

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

Here, we have

$$113 \equiv 1(\text{mod}4) \text{ and } 43 \equiv 3(\text{mod}4)$$

Since at least one prime is $1(\text{mod}4)$, we use the first case:

$$\left(\frac{113}{43}\right) = \left(\frac{43}{113}\right)$$

Example 7: Evaluate $\left(\frac{59}{131}\right)$

Solution: Here 59 and 131 both are odd primes and

$$59 = 4 \times 14 + 3 \Longrightarrow 59 \equiv 3(mod\ 4)$$

$$131 = 4 \times 32 + 3 \Longrightarrow 131 \equiv 3(mod\ 4)$$

So, both primes are of the form $4k + 3$.

Therefore,

$$\left(\frac{59}{131}\right) = -\left(\frac{131}{59}\right) \qquad [\because \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \text{ if } p \equiv q \equiv 3(\text{mod}4)]$$

$$= -\left(\frac{13}{59}\right) \qquad [\because 131 \equiv 13(mod\ 4)]$$

$$= -\left(\frac{59}{13}\right) \qquad [\because 13 \equiv 1(mod\ 4)]$$
$$= -\left(\frac{7}{13}\right) \qquad [\because 59 \equiv 7(mod\ 4)]$$

Now consider 7 and 13:

$$7 \equiv 3(\text{mod}4) \text{ and } 13 \equiv 1(\text{mod}4)$$

Since one of them is $1\text{mod}\ 4$,

$$\left(\frac{7}{13}\right) = \left(\frac{13}{7}\right)$$

Thus,

$$\left(\frac{59}{131}\right) = -\left(\frac{13}{7}\right)$$

$$= -\left(-\frac{1}{7}\right) \qquad [\because 13 \equiv -1(mod\ 7)]$$

Now, we know that

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

For $p = 7$:

$$\left(\frac{-1}{7}\right) = (-1)^3 = -1$$

Therefore,

$$\left(\frac{59}{131}\right) = -(-1)$$
$$= 1.$$

10.7 QUADRATIC CONGRUENCES WITH COMPOSITE MODULE

In the earlier sections, we studied quadratic congruences of the form

$$x^2 \equiv a(\text{mod}p),$$

where the modulus $p$is a prime number. Such congruences can be effectively analyzed using tools like Legendre symbols and the law of quadratic reciprocity. However, in many practical and theoretical situations, the modulus is not prime but composite. This naturally leads us to the study of quadratic congruences with composite modulus.

Theorem 10.7.1: If p is an odd prime and a is any integer such that $(a,p)=1$,then the congruence

$$x^2 \equiv a(mod\ p^n), n \geq 1$$

has a solution if $\left(\frac{a}{p}\right)=1$.

Proof: We assume that there exists an integer $x_0$such that

Suppose the given congruence has a solution x_0.Then

$$x_0^2 \equiv a(mod\ p^n)$$

$$\Longrightarrow p^n|(x_0^2-a)$$

$$\Longrightarrow p|(x_0^2-a)$$

So,

$$x_0^2 \equiv a(\mathrm{mod}p).$$

Hence, the congruence $x^2 \equiv a(\mathrm{mod}p)$has a solution.

By Euler's Criterion:

$$x^2 \equiv a(\mathrm{mod}p) \text{ has a solution } \Leftrightarrow \left(\frac{a}{p}\right)=1.$$

Conversely, suppose $\left(\frac{a}{p}\right)=1$.Then by Euler's criterion $x^2 \equiv a(mod\ p)$.

This shows that the given statement is true for $n=1$.

Now we assume that $x^2 \equiv a(mod\ p^m)$ has a solution.

We shall show that $x^2 \equiv a(mod\ p^{m+1})$ also has a solution. Let x_0 be the solution of $x^2 \equiv a(mod\ p^m)$.Then $x_0^2 \equiv a+tp^m$ for some integer t.Obviously $(x_0,p)=1$.

Therefore, the linear congruence $x_0y \equiv 1(mod\ p)$ has a solution say y_0.

Thus,$x_0 y_0 = 1 + t_1 p$ for some integer t_1.

Let $x_1 = x_0 - t y_0 p^m . \left(\frac{p+1}{2}\right)$.

Then $x_1^2 = x_0^2 - 2t x_0 y_0 \left(\frac{p+1}{2}\right) p^m + t^2 y_0^2 \left(\frac{p+1}{2}\right)^2 p^{2m}$

$= x_0^2 - 2t(1 + t_1 p) \left(\frac{p+1}{2}\right) p^m + t^2 y_0^2 \left(\frac{p+1}{2}\right)^2 p^{2m}$

$= a + t p^m - t p^m + p^{m+1}$.(some integer)

$= a + p^{m+1}$.(some integer)

$\equiv a(mod\ p^{m+1})$.

This shows that x_1 is a solution of $x^2 \equiv a(mod\ p^{m+1})$.

Hence, by mathematical induction we have that

$x^2 \equiv a(mod\ p^n)$ has a solution for $n \geq 1$.

Theorem 10.7.2:
Let a is an odd integer. Then

(i) The congruence $x^2 \equiv a(mod\ 2)$ always has a solution.

(ii) The congruence $x^2 \equiv a(mod\ 4)$ has a solution if and only if $a \equiv 1(mod\ 4)$

(iii) The congruence $x^2 \equiv a(mod\ 2^n), n \geq 3$ has a solution if and only if $a \equiv 1(mod\ 8)$

Proof:

(i) We have

$a \equiv 1(mod\ 2)$ [$\because a$ is an odd integer]

Therefore,1 is the solution of $x^2 \equiv a(mod\ 2)$

(ii) Since a is an odd integer, we have

$a \equiv 1$ or $3(mod\ 4)$.

Also, $b^2 \equiv 1(mod\ 4)$,where b is an odd integer.

Now the congruence $x^2 \equiv a(mod\ 4)$ has a solution b if $a \equiv 1(mod\ 4)$.

Also, if $a \equiv 1(mod\ 4)$,then 1 and 3 both satisfy $x^2 \equiv 1(mod\ 4)$.

(iii) Suppose $a \equiv 1(mod\ 8)$,then we have to show that $x^2 \equiv a(mod\ 2^n), n \geq 3$ has a solution.

For $n = 3$,we have $x^2 \equiv 1(mod\ 8)$.

Obviously 1,3,5,7 satisfy this congruence. Thus, the given congruence has a solution for $n = 3$.

We assume that for some $n \geq 3$,

$$x^2 \equiv 1(\text{mod} 2^n)$$

has a solution x_0.

This means:

$$x_0^2 = 1 + t \cdot 2^n \text{for some integer } t.$$

Also, the linear congruence

$$x_0 y \equiv 1(mod\ 2)$$

has a unique solution y_0 so that $x_0 y_0 = 1 + 2t_1$ for some integer t_1.

Clearly, $x_1 = x_0 - 2^{n-1} t y_0$ is solution of $x^2 \equiv 1(mod\ 2^{n+1})$, because

$$\begin{aligned} x_1^2 &= x_0^2 - 2^n t y_0 x_0 + 2^{2n-2} t^2 y_0^2 \\ &= 1 + 2^n t - 2^n t(1 + 2t_1) + 2^{n+1} . 2^{n-3} t^2 y_0^2 \\ &\equiv 1(mod\ 2^{n+1}). \end{aligned}$$

Hence, by mathematical induction we see that

$$x^2 \equiv 1(mod\ 2^n)$$

has a solution for $n \geq 3$.

Conversely, suppose $x^2 \equiv a(mod\ 2^n)$ has a solution x_0 for each $n \geq 3$, then we have

$$\begin{aligned} & x_0^2 \equiv a(mod\ 2^n) \\ \Rightarrow\ & x_0^2 \equiv a(mod\ 8) \end{aligned}$$

As a is odd, x_0 must be odd.

Thus $x_0 \equiv 1,3,5,7\ (mod\ 8)$

or $a \equiv x_0^2 \equiv 1(mod\ 8)$.

Example 8: Show that the congruence

$$x^2 \equiv 3(mod\ 88)$$

has no solution.

Solution: We have, $x^2 \equiv 3(mod\ 88)$

$$\equiv 3(mod\ 8 \times 11)$$

If a congruence modulo a composite number mn has a solution (where m and n are coprime), then it must also have solutions modulo both m and n separately.

Therefore,

$$x^2 \equiv 3(\text{mod} 88)$$

can have a solution only if both of the following congruences have solutions:

$$x^2 \equiv 3(\text{mod } 8) \text{ and } x^2 \equiv 3(\text{mod} 11).$$

From Theorem 11.14(iii), we know:

For $n \geq 3$, the congruence

$$x^2 \equiv a(\text{mod} 2^n)$$

has a solution if and only if

$$a \equiv 1(\text{mod} 8).$$

Here:

$$a = 3.$$

But:

$$3 \not\equiv 1(\text{mod} 8).$$

So,

$$x^2 \equiv 3(\text{mod} 8)$$

has no solution.

Therefore, the given congruence has no solution.

Example 9: Does the congruence $x^2 \equiv 25(mod\ 56)$ have a solution?

Solution: The given quadratic congruence modulo 56 is solvable if and only if it is solvable modulo 7 and modulo 2^3 separately.

Thus,

$$x^2 \equiv 25(\text{mod} 56)$$

is equivalent to the simultaneous congruences

$$x^2 \equiv 25(\text{mod} 7) \text{and} x^2 \equiv 25(\text{mod} 8).$$

Since $25 \equiv 1(mod\ 8)$

So, the congruence becomes:

$$x^2 \equiv 1(\text{mod} 8).$$

From Theorem 11.14(i), we know that:

$x^2 \equiv 1(\text{mod} 8)$ always has a solution.

In fact,

$$x \equiv 1,3,5,7(\text{mod} 8)$$

are solutions.

Hence,

$$x^2 \equiv 25(\text{mod} 8)$$

is solvable.

Also, $25 \equiv 4(mod\ 7)$ and $\left(\frac{4}{7}\right) = 1$, so that $x^2 \equiv 25(mod\ 7)$ also has a solution.

Hence, the given congruence has a solution.

An important result:

Let $n > 1$ be any integer and $n = 2^k p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ be its prime factorization. Then the quadratic congruence

$$x^2 \equiv a(mod\ n), \text{ where } (a, n) = 1$$

is solvable if and only if the following system of simultaneous quadratic congruence is solvable

$x^2 \equiv a(mod\ 2^k)$
$x^2 \equiv a(mod\ p_1^{k_1})$
$x^2 \equiv a(mod\ p_2^{k_2})$
$\vdots \quad \vdots$
$\vdots \quad \vdots$
$x^2 \equiv a(mod\ p_t^{k_t})$

if and only if

(i) $\left(\frac{a}{p_i}\right) = 1$ for each $i = 1,2, \cdots, t$;

(ii) $a \equiv 1(mod\ 4)$ if $4|n$ but $8 \nmid n$ and
$a \equiv 1(mod\ 8)$ if $8|n$.

Example 10: Prove that the quadratic congruence
$x^2 \equiv 9(mod\ 120)$ is solvable.

Solution: First, we factor the modulus 120:

$$120 = 2^3 \times 3 \times 5.$$

Since these factors are pairwise coprime, we can use the Chinese Remainder Theorem (CRT).

The congruence

$$x^2 \equiv 9(\text{mod}120)$$

is equivalent to the following system of congruences:

$$x^2 \equiv 9(mod\ 2^3)$$

$$x^2 \equiv 9(mod\ 3)$$
$$x^2 \equiv 9(mod\ 5)$$

So, to prove that the original congruence is solvable, it is enough to show that each of these three congruences has a solution.

Since $9 \equiv 1(mod\ 8)$,
$x^2 \equiv 9(mod\ 2^3)$ has a solution. [by Theorem 11.14 (iii)]

Since $9 \equiv 0(\text{mod}3)$.
So, the congruence becomes:

$$x^2 \equiv 0(\text{mod}3).$$

This has the obvious solution:

$$x \equiv 0(\text{mod}3).$$

Hence,

$$x^2 \equiv 9(\text{mod}3)$$

is solvable.
Also,$9 \equiv 4(\text{mod}5)$.

So, we consider:

$$x^2 \equiv 4(\text{mod}5).$$

Clearly,

$$2^2 = 4 \equiv 4(\text{mod}5),$$

so, a solution exists.

Alternatively, using the Legendre symbol:

$$\left(\frac{9}{5}\right) = \left(\frac{3}{5}\right)^2 = 1,$$

which shows that 9is a quadratic residue modulo 5.

Hence,

$$x^2 \equiv 9(\text{mod}5)$$

has a solution.

Hence, the given congruence has a solution.

10.8 JACOBI SYMBOL

Let $p > 1$be an odd integer. Suppose the prime factorization of $p$is

$$p = p_1 p_2 \cdots p_r,$$

where $p_1, p_2, \ldots, p_r$ are odd prime numbers.

For any integer a, the Jacobi symbol, denoted by $\left(\frac{a}{p}\right)$, is defined as the product of Legendre symbols corresponding to each prime factor of p.

That is,

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

Here, each symbol on the right-hand side, $\left(\frac{a}{p_i}\right)$, is a Legendre symbol.

Properties of Jacobi Symbol

Theorem 10.8.1: Let $P > 1$ and $Q > 1$ be odd integers. Then the following hold:

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

(ii) $\left(\frac{a}{P}\right)\left(\frac{a}{Q}\right) = \left(\frac{a}{PQ}\right)$

(iii) $\left(\frac{a}{P}\right)\left(\frac{b}{P}\right) = \left(\frac{ab}{P}\right)$

(iv) $\left(\frac{a^2}{P}\right) = \left(\frac{a}{P^2}\right) = 1$

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

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

Proof:

(i) Let $p = p_1p_2\cdots p_k$. Then $a \equiv b(mod\ p) \Longrightarrow a \equiv b(mod\ p_i), i = 1,2,\cdots,k.$

Therefore, $\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right)$.

Hence,
$$\left(\frac{a}{p}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$$
$$= \left(\frac{b}{p_1}\right)\left(\frac{b}{p_2}\right)\cdots\left(\frac{b}{p_k}\right)$$
$$= \left(\frac{b}{p}\right)$$

(ii) Let $P$and Q be odd positive integers. Then for any integer a,

$$\left(\frac{a}{P}\right)\left(\frac{a}{Q}\right) = \left(\frac{a}{PQ}\right),$$

where the symbols are Jacobi symbols.

Proof: Suppose the prime factorization of P is $P = p_1p_2\cdots p_r$,
and the prime factorization of Q is $Q = q_1q_2\cdots q_l$,
where all $p_i$and $q_j$are odd prime numbers.

By the definition of the Jacobi symbol,

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

and

$$\left(\frac{a}{Q}\right) = \left(\frac{a}{q_1}\right)\left(\frac{a}{q_2}\right)\cdots\left(\frac{a}{q_l}\right).$$

Multiplying $(a/P)$and (a/Q), we get

$$\left(\frac{a}{P}\right)\left(\frac{a}{Q}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)\left(\frac{a}{q_1}\right)\left(\frac{a}{q_2}\right)\cdots\left(\frac{a}{q_l}\right)$$

$$= \left(\frac{a}{p_1 p_2 \cdots p_k q_1 q_2, \cdots, q_l}\right)$$

$$= \left(\frac{a}{PQ}\right) \qquad [\because PQ = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_l]$$

Therefore,

$$\left(\frac{a}{P}\right)\left(\frac{a}{Q}\right) = \left(\frac{a}{PQ}\right).$$

(iii) We have

$$\left(\frac{ab}{P}\right) = \left(\frac{ab}{p_1}\right)\left(\frac{ab}{p_2}\right)\cdots\left(\frac{ab}{p_k}\right)$$

$$= \left(\frac{a}{p_1}\right).\left(\frac{b}{p_1}\right).\left(\frac{a}{p_2}\right)\left(\frac{b}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)\left(\frac{b}{p_k}\right)$$

$$= \left(\frac{a}{p_1}\right).\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right).\left(\frac{b}{p_1}\right).\left(\frac{b}{p_2}\right)\cdots\left(\frac{b}{p_k}\right)$$

$$= \left(\frac{a}{P}\right).\left(\frac{b}{P}\right)$$

(iv) Let the prime factorization of P be

$$P = p_1 p_2 \cdots p_k,$$

where each $p_i$is an odd prime.

By the definition of the Jacobi symbol,

$$\left(\frac{a^2}{P}\right) = \left(\frac{a^2}{p_1}\right)\left(\frac{a^2}{p_2}\right)\cdots\left(\frac{a^2}{p_k}\right).$$

Now, for any odd prime p_i,$\left(\frac{a^2}{p_i}\right) = 1$,because a square is always a quadratic residue modulo an odd prime (when $(a, p_i) = 1$).

Using the multiplicative property of the Jacobi symbol in the denominator,

$$\left(\frac{a}{P^2}\right) = \left(\frac{a}{P}\right)\left(\frac{a}{P}\right) = \left(\frac{a}{P}\right)^2.$$

Now, the Jacobi symbol $\left(\frac{a}{P}\right)$can only take the values $\pm 1$when $(a, P) = 1$.

Therefore,

$$\left(\frac{a}{P}\right)^2 = 1.$$

So,

$$\left(\frac{a}{P^2}\right) = 1.$$

(v) We have,

$$\left(-\frac{1}{P}\right) = \left(-\frac{1}{p_1}\right).\left(-\frac{1}{p_2}\right)\cdots\left(-\frac{1}{p_k}\right)$$

$$= (-1)^{\frac{p_1-1}{2}}.(-1)^{\frac{p_2-1}{2}}\cdots(-1)^{\frac{p_k-1}{2}}$$

$$= (-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\cdots+\frac{p_k-1}{2}} \qquad (1)$$

Now, $\frac{P-1}{2} = \frac{p_1p_2\cdots p_k-1}{2}$

$$= \frac{-1+\left(1+2.\frac{p_1-1}{2}\right)\left(1+2.\frac{p_2-1}{2}\right)\cdots\left(1+2.\frac{p_k-1}{2}\right)}{2}$$

$$= \frac{p_1-1}{2} + \frac{p_2-1}{2} + \cdots + \frac{p_k-1}{2} + 2N, N \text{ being an integer}$$

$$\therefore (-1)^{\frac{P-1}{2}} = (-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\cdots+\frac{p_k-1}{2}+2N}$$

$$= (-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\cdots+\frac{p_k-1}{2}}$$

$$= \left(-\frac{1}{P}\right). \qquad [\text{ by (1)}]$$

(vi) Now,

$$\frac{P^2-1}{8} = \frac{p_1^2p_2^2\cdots p_k^2-1}{8}$$

$$= \frac{\left(1+\frac{p_1^2-1}{8}.8\right)\left(1+\frac{p_2^2-1}{8}.8\right)\cdots\left(1+\frac{p_k^2-1}{8}.8\right)-1}{8}$$

$$= \frac{p_1^2-1}{8} + \frac{p_2^2-1}{8} + \cdots + \frac{p_k^2-1}{8} + 2M, M \text{ being an integer.}$$

Now,

$$\left(\frac{2}{P}\right) = \left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_k}\right)$$
$$= (-1)^{\frac{p_1^2-1}{8}}(-1)^{\frac{p_2^2-1}{8}}\cdots(-1)^{\frac{p_k^2-1}{8}}$$
$$= (-1)^{\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\cdots+\frac{p_k^2-1}{8}+2M} \qquad [\because (-1)^{2M} = 1]$$
$$= (-1)^{\frac{p^2-1}{8}}$$

Example 11: Final the value of the Jacobi symbol $\left(\frac{32}{15}\right)$.

Solution: We have

$$\left(\frac{32}{15}\right) = \left(\frac{32}{3\times5}\right)$$
$$= \left(\frac{32}{5}\right).\left(\frac{32}{5}\right)$$
$$= \left(\frac{2}{3}\right).\left(\frac{2}{5}\right)$$
$$= (-1)^{\frac{3^2-1}{8}}.(-1)^{\frac{3^2-1}{8}}$$
$$= 1$$

W CHECK YOUR PROGRESS

Q 6. Show that $\left(\frac{43}{23}\right) = -\left(\frac{23}{43}\right)$

Q 7. Evaluate

$$\left(\frac{71}{73}\right)$$

Q 8. Evaluate the Legendre symbol $\left(\frac{461}{773}\right)$

Q 9. Show that the congruence $x^2 \equiv 9(mod\ 40)$ is solvable.

Q 10. Find the value of Jacobi symbol $\left(\frac{22}{105}\right)$.

2 10.9 LET US SUM UP

- A quadratic congruence in one variable is of the form
$$ax^2 + bx + c \equiv 0(mod\ p)$$
where $a, b$and $c$are integers,p is an odd prime and $p \nmid a$.

- Let p be a prime and a is an integer coprime to p.Then a is called a quadratic residue $(mod\ p)$ if and only if $x^2 \equiv a(mod\ p)$ has a solution. Otherwise$a$ is called quadratic non-residue$(mod\ p)$.
- Let p be an odd prime and a is any integer. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \ if\ a\ is\ a\ quadratic\ residue\ (mod\ p) \\ 0\ if\ p|a \\ -1\ if\ a\ is\ a\ quadratic\ non-residue\ (mod\ p) \end{cases}$$

- Let $p > 1$be an odd integer. Suppose the prime factorization of $p$is

$$p = p_1 p_2 \cdots p_r,$$

where $p_1, p_2, \ldots, p_r$ are odd prime numbers.
For any integer a, the Jacobi symbol, denoted by $\left(\frac{a}{p}\right)$, is defined as the product of Legendre symbols corresponding to each prime factor of p. That is,

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

Here, each symbol on the right-hand side, $\left(\frac{a}{p_i}\right)$, is a Legendre symbol.

K 10.10 ANSWERS TO CHECK YOUR PROGRESS

Answer to Q1: (a)

We have

$3x^2 + 5x + 9 \equiv 0(mod\ 11)$ (1)

Multiplying (1) by $3 \times 4 = 12$,we get

$$36x^2 + 60x + 108 \equiv 0(mod\ 11)$$

This can be written as

$(6x + 5)^2 \equiv 5(mod\ 11)$ (2)

Putting $y = 6x + 5$ in (2), we get

$$y^2 \equiv 5(mod\ 11)$$

$$\equiv (5+11)(mod\ 11)$$

$$\equiv 4^2(mod\ 11)$$

This gives, $y \equiv \pm 4(mod\ 11)$

or $6x+5 \equiv \pm 4(mod\ 11)$

or $6x \equiv (2,10)(mod\ 11)$

or $x = 4,9(mod\ 11).$

Answer to Q1: (a)

Here $p = 11$ (an odd prime) and $a = 1, gcd(a,p) = 1.$

$$\therefore 4(x^2+7x+10) \equiv 0(mod\ 11)$$

$$\Longrightarrow 4(x^2+7x+10) \equiv 0(mod\ 11)$$

$$\Longrightarrow (2x+7)^2 - (7^2 - 4.10) \equiv 0(mod\ 11)$$

$$\Longrightarrow (2x+7)^2 - 9 \equiv 0(mod\ 11)$$

$$\Longrightarrow (2x+7)^2 \equiv 9(mod\ 11)$$

Now, $2x+7 \equiv 3(mod\ 11)$

$$\Longrightarrow 2x \equiv -4(mod\ 11)$$

$$\Longrightarrow x \equiv -2(mod\ 11)[\because gcd(2,11) = 1]$$

$$\Longrightarrow x \equiv 9(mod\ 11)$$

or $2x+7 \equiv -3(mod\ 11)$

$$\Longrightarrow x \equiv 6(mod\ 11)$$

$\therefore \quad x \equiv 9\ or\ 6(mod\ 11).$

Answer to Q 2:

Let $p = 23$,which is an odd prime.

The number of quadratic residues modulo$p$ is

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

Therefore, there are 11 quadratic residues modulo 23.

The square integers less than 23 are:

$1^2 = 1\ ,2^2 = 4,3^2 = 9,4^2 = 16.$

Therefore,

$$1,4,9,16$$

are quadratic residues modulo 23.

Since the product of two quadratic residues is again a quadratic residue, we compute:

$$4 \times 9 = 36 \equiv 13(\text{mod } 23),$$
$$4 \times 16 = 64 \equiv 18(\text{mod}23),$$
$$9 \times 16 = 144 \equiv 6(\text{mod}23).$$

Thus,

$$13,18,6$$

are also quadratic residues modulo 23.

Again, using products of known residues:

$$9 \times 13 = 117 \equiv 2(\text{mod}23),$$
$$4 \times 18 = 72 \equiv 3(\text{mod}23),$$
$$6 \times 9 = 54 \equiv 8(\text{mod}23),$$
$$4 \times 3 = 12(\text{mod}23).$$

Hence,

$$2,3,8,12$$

are also quadratic residues modulo 23.

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

Answer to Q3:

We have

$$1372 = 7 \times 14^2$$

$\therefore \quad \left(\frac{1372}{29}\right) = \left(\frac{4\times(14)^2}{29}\right)$

$= \left(\frac{7}{29}\right).\left(\frac{14}{29}\right)^2$

$= \left(\frac{7}{29}\right)$

$= \mathbf{1}$

Answer to Q4:

Here,$a = 11$ and $p = 23$.

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

Therefore, the set

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

Reducing each element of S modulo 23, we obtain

$$\{11,22,10,21,9,20,8,19,7,18,6\}$$

Five of these numbers are greater than $\frac{p}{2} = \frac{23}{2}$.

Therefore,$n = 5$.

Answer to Q5:

Here,$a = 3$ and $p = 31$.

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

Therefore, the set

$$S = \{3,6,9,12,15,18,21,24,27,30,33,36,39,42,45\}$$

Reducing each element of S modulo 31, we obtain

$$\{3,6,9,12,15,18,21,24,27,30,2,5,8,11,14\}$$

Five of these numbers are greater than $\frac{p}{2} = \frac{31}{2} = 15.5.3$

Numbers greater than 15.5 are:

18, 21,24,27,30

Therefore,$n = 5$.

Answer to Q 6:

Here, we have that 23 and 43 both are odd primes and both

$$23 = 4 \times 5 + 3$$

$$43 = 4 \times 10 + 3$$

are of the form $4k + 3$.

Now, by the Quadratic Reciprocity Theorem,

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

Apply the rule to $p = 23$ and $q = 43$

Since both primes are of the form $4k + 3$:

$\frac{23-1}{2} = 11(\text{odd})$ and $\frac{43-1}{2} = 21(\text{odd})$

The product of two odd numbers is **odd**, so

$$(-1)^{231} = -1$$

Thus,

$$\left(\frac{23}{43}\right)\left(\frac{43}{23}\right) = -1$$

From the above relation,

$$\left(\frac{\mathbf{43}}{\mathbf{23}}\right) = -\left(\frac{\mathbf{23}}{\mathbf{43}}\right).$$

Answer to Q 7:

Here, 71 and 73 are odd prime numbers**.**

A basic rule of quadratic reciprocity says:

If the denominator prime is of the form $4k + 1$, then

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

Now,

$$73 = 4 \times 18 + 1$$

So, 73 is of the form $4k + 1$.

Hence,

$$\left(\frac{71}{73}\right) = \left(\frac{73}{71}\right)$$

Since Legendre symbols depend only on remainders,

$$73 \equiv 2(\text{mod}71)$$

Therefore,

$$\left(\frac{73}{71}\right) = \left(\frac{2}{71}\right)$$

There is a known result:

$$\left(\frac{2}{p}\right) = 1 \text{if } p \equiv 1 \text{ or } 7(\text{mod}8)$$

Now,

$$71 \equiv 7(\text{mod}8)$$

So,

$$\left(\frac{2}{71}\right) = 1$$

Answer to Q 8:

Both numbers are **odd primes**.

Now,

$$461 = 4 \times 115 + 1 \;\Rightarrow\; 461 \equiv 1(\text{mod}4)$$

When the numerator is $\equiv 1(\text{mod}4)$, quadratic reciprocity gives:

$$\left(\frac{461}{773}\right) = \left(\frac{773}{461}\right)$$

Now, $773 \equiv 312(\text{mod}461)$

So,

$$\left(\frac{773}{461}\right) = \left(\frac{312}{461}\right)$$

Factor 312:

$$312 = 2^3 \times 3 \times 13$$

Using multiplicativity of the Legendre symbol,

$$\left(\frac{312}{461}\right) = \left(\frac{2}{461}\right)^3 \left(\frac{3}{461}\right)\left(\frac{13}{461}\right) \qquad (*)$$

Now,

$$461 \equiv 5(\text{mod}8)$$

For an odd prime p,

$$\left(\frac{2}{p}\right) = -1 \text{if } p \equiv 3,5(\text{mod}8)$$

Hence,

$$\left(\frac{2}{461}\right) = -1 \Rightarrow \left(\frac{2}{461}\right)^3 = -1$$

Also, $461 \equiv 1(mod4)$,

$$\left(\frac{3}{461}\right) = \left(\frac{461}{3}\right)$$

Now,

$$461 \equiv 1(\text{mod}3) \Rightarrow \left(\frac{461}{3}\right) = \left(\frac{1}{3}\right) = 1$$

Since $13 \equiv 1(\text{mod}4)$,

$$\left(\frac{13}{461}\right) = \left(\frac{461}{13}\right)$$

Now,

$$461 \equiv 6(\text{mod}13) \Rightarrow \left(\frac{461}{13}\right) = \left(\frac{6}{13}\right)$$

Factor $6 = 2 \times 3$:

$$\left(\frac{6}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{3}{13}\right)$$

$$13 \equiv 5(\text{mod}8) \Rightarrow \left(\frac{2}{13}\right) = -1$$

- 3 is a quadratic residue mod 13(since $4^2 = 16 \equiv 3(\text{mod}13)$), so

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

Thus,

$$\left(\frac{6}{13}\right) = -1$$

From (*)

$$\left(\frac{312}{461}\right) = (-1) \times 1 \times (-1) = 1$$

Therefore,

$$\left(\frac{461}{773}\right) = -1.$$

Answer to Q 9:

We have,$x^2 \equiv 9(mod\ 40)$

which is equivalent to the following simultaneous quadratic congruences

$x^2 \equiv 9(mod\ 8)$ and $x^2 \equiv 9(mod\ 8)$.

Now,$9 \equiv 1(mod\ 8)$, So we consider:

$$x^2 \equiv 1(\text{mod}8).$$

From Theorem 11.14 (i), we know that:

$$x^2 \equiv 1(\text{mod}8)$$

always has solutions. In fact,

$$x \equiv 1,3,5,7(\text{mod}8)$$

all satisfy this congruence.

Therefore,$x^2 \equiv 9(mod\ 8)$has a solution.

Also,$\left(\frac{9}{5}\right) = \left(\frac{3^2}{5}\right) = 1$

Therefore, $x^2 \equiv 9(mod\ 5)$ has a solution. Hence, the given quadratic congruence has a solution.

Answer to Q 10:

We have

$$\left(\frac{22}{105}\right) = \left(\frac{22}{3 \times 5 \times 7}\right)$$

$$= \left(\frac{22}{3}\right).\left(\frac{22}{5}\right).\left(\frac{22}{7}\right)$$

$$= \left(\frac{1}{3}\right).\left(\frac{2}{5}\right).\left(\frac{1}{7}\right)$$

$$= 1.(-1)^{\frac{5^2-1}{8}}.1$$

$$= -1$$

O10.11 FURTHER READING

1. David M. Burton, Elementary Number Theory (7^{th} Edn.), McGraw Hill Education (India) Private Limited, Chennai-600116, 2018.

2. S. B. Malik, Basic Number Theory (2^{nd} revised Edn.), Vikash Publishing House Private Limited, Noida-201301, 2017.

3. George E. Andrews, Number Theory, Hindustan Publishing Corporation, New Delhi.

4. S. G. Telang, Number Theory, Tata McGraw-Hill Publishing Company Limited.

5. Hardy, G. H. And Wright, E. M., Theory of Numbers, Oxford Science Publications, 2003.

M10.12 MODEL QUESTIONS

Q1. Solve the following Quadratic Congruences:

(c) $x^2 + 7x + 10 \equiv 0(mod\ 11)$

(d) $3x^2 + 9x + 7 \equiv 0(mod\ 13)$

(e) $5x^2 + 6x + 1 \equiv 0(mod\ 23)$

Q2. Find quadratic residues $(mod\ 17)$

Q3. Find the quadratic residues of 29.

Q4. Knowing that 2 is a primitive root of 19, find all the quadratic residues of 19.

Q5. Find all quadratic residues mod 83, given that 2 is a primitive root$(mod\ p)$.

Q6. Evaluate the following Legendre Symbols:

$\left(\frac{3}{31}\right),\left(\frac{2}{31}\right),\left(\frac{3}{73}\right),\left(\frac{5}{19}\right),\left(\frac{5}{29}\right)$ and $\left(\frac{11}{23}\right)$

Q7. Let p be an odd prime, then

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

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

Q8. Let p be an odd prime > 3.Prove that

$$\left(\frac{3}{p}\right) = \begin{cases} 1 \ if\ \ p \equiv \pm(mod\ 12) \\ -1 \ if\ \ p \equiv \pm(mod\ 12) \end{cases}$$

Q9. Prove that there are infinitely many primes of the form $6k + 5$.

*** *** ***