UNIT - IV

3.1 Quadratic Residues:

For all a, such that $(a,m)=1$, a is called a quadratic residue modulo m, if the congruence $x^2 \equiv a \pmod{m}$ has a soln

If $x^2 \equiv a \pmod{m}$ has no soln then a is called a quadratic non-residue modulo m.

Eg:

1. Let $m=11$, let us find the quadratic residues and non-residues of modulo 11

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

$x=1, a=1 \Rightarrow 1^2 \equiv 1 \pmod{11}$

$x=2, a=4 \Rightarrow 2^2 = 4 \pmod{11}$

$x=3, a=9 \Rightarrow 3^2 \equiv 9 \pmod{11}$

$x=4, a=16 \Rightarrow 4^2 \equiv 16 \pmod{11} \Rightarrow 4^2 \equiv 5 \pmod{11}$

$x=5, a=25 \Rightarrow 5^2 \equiv 25 \pmod{11} \Rightarrow 5^2 \equiv 3 \pmod{11}$

$x=6, a=36 \Rightarrow 6^2 \equiv 36 \pmod{11} \Rightarrow 6^2 \equiv 3 \pmod{11}$

$x=7, a=49 \Rightarrow 7^2 \equiv 49 \pmod{11} \Rightarrow 7^2 \equiv 5 \pmod{11}$

$x=8, a=64 \Rightarrow 8^2 \equiv 64 \pmod{11} \Rightarrow 8^2 \equiv 9 \pmod{11}$

$x=9, a=81 \Rightarrow 9^2 \equiv 81 \pmod{11} \Rightarrow 9^2 \equiv 4 \pmod{11}$

$x=10, a=100 \Rightarrow 10^2 \equiv 100 \pmod{11} \Rightarrow 10^2 \equiv 1 \pmod{11}$

Quadratic residues are 1, 3, 4, 5, 9

Quadratic non-residues are 2, 6, 7, 8, 10

3.2 Quadratic Reciprocity:

THEOREM:- 3.4:

The Gaussian Reciprocity Law:

If p and q are distinct odd primes, then

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

(or)

If p and q are distinct odd primes of the form $4k+3$, then one of the congruence $x^2 \equiv p \pmod{q}$ and $x^2 \equiv q \pmod{p}$ is solvable. and the other is not solvable. But if atleast one of the primes is of the form $4k+1$, then both the congruences are solvable or both are not solvable.

Proof:

Let S be the set of all pairs of integers (x, y) satisfying $1 \le x \le \frac{p-1}{2}$, $1 \le y \le \frac{q-1}{2}$.

i.e., $S = \left\{(x,y) / 1 \le x \le \frac{p-1}{2}, 1 \le y \le \frac{q-1}{2}\right\}$

Then the set has $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ elements. Separate S into two mutually exclusive subsets. S_1 and S_2 as follows.

$$S_1 = \left\{(x,y) / qx > py, 1 \le x \le \frac{p-1}{2}, 1 \le y \le \frac{q-1}{2}\right\}$$

$$S_2 = \left\{(x,y) / qx < py, 1 \le x \le \frac{p-1}{2}, 1 \le y \le \frac{q-1}{2}\right\}$$

no pair (x,y) in S

$\Rightarrow$ $qx = py$

(3)

There are no pairs (x,y) in S s.t $qx = py$.

If $qx = py$, then py is a multiple of q which is not possible.

Since $(p,q) = 1$, $(y,q) = 1$ $[\because 0 < y < q]$

In S_1, $qx > py$ (or) $py < qx$

$y < \frac{qx}{p}$

$S_1 = \{(x,y) / qx > py, \ 1 \le x < \frac{p-1}{2}, \ 1 \le y \le \frac{qx}{p}\}$.

Then the no. of elements in S_1 is $\sum_{x=1}^{\frac{p-1}{2}} \left(\frac{qx}{p}\right)$

$qx < py$

$x < \frac{py}{q}$

Similarly,

$S_2 = \{(x,y) / qx \not< py ; \ 1 \le x \le \frac{py}{q}, \ 1 \le y \le \frac{q-1}{2}\}$

The no. of elements in S_2 is $\sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right]$.

The no. of elements in $S = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right] + \sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right]$

$$\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right] + \sum_{y=1}^{\frac{q-1}{2}} \left[\frac{qy}{p}\right] \quad \text{---(1)}$$

now,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right]} \cdot (-1)^{\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right]} \quad [\because \text{by lemma}]$$

(power is power)

$$= (-1)^{\sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right] + \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right]}$$

$$= (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} \quad [\because \text{by (1)}]$$

2. Find the quadratic residues and non-residues of 14

H.W. i) 7 ii) 13

(continuity of page 1)

Legendre Symbol:

If p denotes an odd prime and $(a,p)=1$, the legendre symbol $\left(\frac{a}{p}\right)$ is defined as

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

Note:

1. $\left(\frac{a}{p}\right) = 0$ if $p \mid a$
2. $\left(\frac{1}{p}\right) = 1$, since 1 is a quadratic residue of all numbers.

Problem:

1. Find $\left(\frac{7}{11}\right)$

Soln:

$a=7$, $p=11$, $\frac{p-1}{2}=5$ (10/2)

$x^2 \equiv 7 \pmod{11}$

$1^2 \equiv 1 \pmod{11}$

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

$3^2 \equiv 9 \pmod{11}$

$4^2 \equiv 5 \pmod{11}$

$5^2 \equiv 3 \pmod{11}$

$\therefore$ Q.R. of 11 are 1, 3, 4, 5, 9

Since 7 is not a Q.R. of 11 $\left(\frac{7}{11}\right) = -1$

H.W 2. Find i) $\frac{5}{11}$, ii) $\frac{2}{13}$ iii) $\frac{5}{17}$ (in the book)

THEOREM: 3.1

(3) Let p be an odd prime, a and b denote integers relatively prime to p. Then

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

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

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

(4) iv) $\frac{a^2}{p} = 1$, $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$, [illegible], if $(a,p) = 1$

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

Proof:

Given p is an odd prime and

$$(a,p) = (b,p) = 1$$

i) W.K.T (Legendre's) $\left(\frac{a}{p}\right) = \pm 1$

Case (i):

$\left(\frac{a}{p}\right) = 1$. i.e., a is a Q.R. mod p.

Then, the congruence $x^2 \equiv a \pmod{p}$ has a soln.

Let it be x_0

$$\therefore x_0^2 \equiv a \pmod{p} \quad \text{---} \quad (1)$$

Then, $(x_0, p) = 1$

$\therefore$ By Fermat's thm,

$$x_0^{p-1} \equiv 1 \pmod{p} \quad \text{---} \quad (2)$$

$(1) \Rightarrow$ $x_0^2 \equiv a \pmod{p}$

$$\left(x_0^2\right)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod{p}$$

i.e., $a^{\frac{p-1}{2}} \equiv x_0^{p-1} \pmod p$

$\equiv 1 \pmod p$ [$\because$ by (2)

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

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

case(ii):

$\left(\frac{a}{p}\right) = -1$, i.e., a is a Q.N.R modulo p.

$\therefore$ the congruence $x^2 \equiv a \pmod p$ has no soln.

i.e., the square of a number from 1 to p-1 is not congruent to a mod p.

For each j, $1 \le j \le p-1$, $\exists$ a unique i, $0 \le i \le p-1$. such that $ji \equiv a \pmod p$

$i=0$ is not possible, since $0 \not\equiv a \pmod p$

Thus, the integers 1 to p-1 can be paired off j and i s.t $ji \equiv a \pmod p$

There are $\frac{p-1}{2}$ pairs.

$\therefore 1.2.3.\ldots.p-1 \equiv a^{\frac{p-1}{2}} \pmod p$

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

By Wilson's theorem,

$(p-1)! \equiv -1 \pmod p$

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

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

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

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

case (i):

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

from (i),

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

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

on multiplying,

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

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

from (i),

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

$\because (a,p) = (b,p) = 1$

$(ab,p) = 1$

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

i.e., $\frac{ab}{p} = a^{\frac{p-1}{2}} \pmod{p}$

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

case (ii):

$$\left(\frac{a}{p}\right) = 1, \quad \left(\frac{b}{p}\right) = -1$$

then

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

from (i),

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

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

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

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

$$\therefore \left(\frac{ab}{p}\right) \equiv -1 \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

case (iii):

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

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

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

we have, $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \pmod{p}$

$\therefore \left(\frac{ab}{p}\right) = -1 = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

case(iv):

$\left(\frac{a}{p}\right) = -1$, $\left(\frac{b}{p}\right) = -1$, then $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 1$

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

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

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

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

$\therefore \left(\frac{ab}{p}\right) = 1 = \left(\frac{a}{p}\right)^{-1}\left(\frac{b}{p}\right)^{-1}$

Thus in all cases, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

iii) Given $a \equiv b \pmod{p}$

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

case(i):

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

then $x^2 \equiv a \pmod{p}$ has a soln.

Since $a \equiv b \pmod{p}$, $x^2 \equiv b \pmod{p}$ has a soln.

$\therefore \frac{b}{p} = 1$, Hence $\left(\frac{a}{p}\right) = \frac{b}{p}$

case(ii):

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

Then $x^2 \equiv a \pmod{p}$ has no soln.

Given $a \equiv b \pmod{p}$

$\therefore x^2 \equiv b \pmod{p}$ also has no soln.

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

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

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

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

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

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

c) To prove: $\left(\frac{1}{p}\right) = 1$

$1^2 \equiv 1 \pmod{p}$ is a soln. of $x^2 \equiv 1 \pmod{p}$

Thus, $x^2 \equiv 1 \pmod{p}$ has a soln.

1 is a Q.R. modulo p.

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

d) To prove: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

W.K.T. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

an odd prime is of the form $4k+1$ (or) $4k+3$

Suppose $p = 4k+1$

$p-1 = 4k \Rightarrow \frac{p-1}{2} = 2k$

$\Rightarrow (-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1$

$a = -1$

$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$; i.e., $1 \equiv a^{\frac{p-1}{2}} \pmod{p}$

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

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

Suppose $p = 4k+3$

$p-1 = 4k+2 \Rightarrow \frac{p-1}{2} = 2k+1$

$\Rightarrow (-1)^{p-1} = (-1)^{2k+1} = -1$

So $a=-1$ satisfies the congruence

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

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

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

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

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

Thus in either case, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Lemma of Gauss:

Let p be an odd prime and $(a,p)=1$. Consider the integers $a, 2a, 3a, \ldots \left(\frac{p-1}{2}\right)a$ and their least non-negative residue modulo p. If n denotes the number of these residue that exceed $p/2$; then $\left(\frac{a}{p}\right) = (-1)^n$.

Proof:

Since $(a,p)=1$, none of the no's $a, 2a, \ldots \left(\frac{p-1}{2}\right)a$ is a multiple of p.

So the least residue of all these no's are

non-zero and there are $\frac{p-1}{2}$ residues and each residue is $< p-1$.

Some of these residues are $> p/2$ and some are $<$

Let $r_1, r_2, \ldots r_n$ be the residues that exceed $p/2$ and $s_1, s_2, \ldots s_k$ be the remaining residues so that $n+k = \frac{p-1}{2}$.

r_i and s_i are all distinct and non-zero, since $r_1, r_2, \ldots r_n$, $s_1, s_2 \ldots s_k$ are least residue of $a, 2a, \ldots \left(\frac{p-1}{2}\right)a$.

They are mutually incongruent modulo p and

$$a, 2a \ldots \left(\frac{p-1}{2}\right)a \equiv r_1 r_2 \ldots r_n s_1 s_2 \ldots s_k \pmod{p} \quad \text{---(1}$$

now,

$0 < p - r_i < p/2$, $i = 1, 2, \ldots n$

and the no's $p - r_i$ are all distinct

we show that $p - r_i \neq s_j$

If possible, suppose $p - r_i \neq s_j$

$\therefore r_i + s_j = p$

Since r_i and s_j are residue modulo p of the nc $a, 2a, \ldots \left(\frac{p-1}{2}\right)a$, $\exists$ ρ and σ $\ni$ $1 \leq \rho \leq \frac{p-1}{2}$, $1 \leq \sigma \leq \frac{p-1}{2}$

and $\rho a \equiv r_i \pmod{p}$, $\sigma a \equiv s_j \pmod{p}$

$(\rho + \sigma)a \equiv (r_i + s_i) \bmod p$ $\quad \because \rho + \sigma \leq \frac{p-1}{2}$

$(\rho + \sigma)a \equiv p \pmod{p}$ $\quad \because r_i, s_j$ $\quad p \mid (\rho+\sigma)a$ or $(a,p) = 1$ $\quad p \mid (\rho+\sigma)$

$(\rho + \sigma)a \equiv 0 \pmod{p}$

This is not possible since both $e, \sigma \leq \frac{p-1}{2}$

$\therefore p-r_i$ and s_j are distinct for all i and j

i.e., $p-r_1, p-r_2, \ldots p-r_n, s_1, s_2 \ldots s_k$ are all distinct and each is $< p/2$

$\therefore$ They must be integers $1, 2 \ldots \frac{p-1}{2}$ in some order.

$$(p-r_1)(p-r_2)\ldots(p-r_n)\, s_1 s_2 \ldots s_k \equiv 1 \cdot 2 \cdots \frac{p-1}{2}$$

$$(-r_1)(-r_2)\ldots(-r_n)\, s_1 s_2 \ldots s_k \equiv 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) \pmod p$$

i.e., $(-1)^n r_1 r_2 \ldots r_n s_1 \ldots s_k \equiv 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) \pmod p$ — (4)

(1), (2) $\Rightarrow$

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

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

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

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

i.e., $a^{\frac{p-1}{2}} \equiv (-1)^n \pmod p$ — (3)

W.K.T.

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p \quad \text{— (4)}$$

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

(6) Problem:

1. Find $\left(\frac{7}{17}\right)$ using Gauss Lemma.

$a = 7$, $p = 17$, $\frac{p-1}{2} = 8$

Consider the integers $a, 2a, \ldots 8a$

i.e., 7, 14, 21, 28, 35, 42, 49, 56

least +ve residue modulo 17 are 7, 14, 4, 11, 1, 8, 15, 5

$21 \equiv 4 \pmod{17}$

$28 \equiv 11 \pmod{17}$

Residues $> p/2 (= 8.5)$ are 11, 14, 15; ....

$\therefore n = 3$

$\left(\frac{7}{17}\right) = (-1)^n = (-1)^3 = -1$

2. Find (i) $\left(\frac{3}{31}\right)$, (ii) $\left(\frac{5}{19}\right)$ Prev note

Soln: (ii) $\left(\frac{5}{19}\right)$

$x^2 \equiv 5 \pmod{19}$

$\left(\frac{5}{19}\right) \therefore a = 5, \; p = 19; \; \frac{p-1}{2} = 9$

consider the integers $a, 2a, \ldots 9a$

i.e., 5, 10, 15, 20, 25, 30, 35, 40, 45

The residues modulo 19 are 5, 10, 15, 1, 6, 11, 16, 2, 7

Residues $> p/2 \; (= 9.5)$ are 15, 10, 16, 11

$\therefore n = 4$

$\frac{5}{19} = (-1)^4 = 1$

$x^2 \equiv 5 \pmod{19}$ is solvable.

Greatest Integer Function:

For real x, the symbol $[x]$ denotes the greatest integer $\leq x$.

$\left[\frac{15}{2}\right] = 7, \; \left[\frac{-15}{2}\right] = -8, \; [-15] = -15$

THEOREM:

Let p be an odd prime and $(a, 2p) = 1$. Then

$\left(\frac{a}{p}\right) = (-1)^t$, where $t = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right]$. Also $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Proof:

Take the no's $a, 2a, \ldots \left(\frac{p-1}{2}\right)a$

Find the residues mod p. Let $r_1, r_2, \ldots r_n$ be the residues $> p/2$ and $s_1 s_2 \cdots s_k$ be residues $< p/2$

So that $n+k = \frac{p-1}{2}$ —— (1)

Then $\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p\left[\frac{ja}{p}\right] + \sum_{j=1}^{n} r_j + \sum_{j=1}^{k} s_j$ —— (2)

$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{n} (p - r_j) + \sum_{j=1}^{k} s_j$ [Prov. Thm

$= \sum_{j=1}^{n} s_j + \sum_{j=1}^{k} r_j - p\sum_{j=1}^{n} 1$

$= \sum_{j=1}^{p} s_j - np$ —— (3)

(2) & (3) $\Rightarrow$

$\sum_{j=1}^{\frac{p-1}{2}} ja - \sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{\frac{p-1}{2}} p\left[\frac{ja}{p}\right] - np + 2\sum_{j=1}^{n} r_j$

i.e., $(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p\left[\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] - n\right] + 2\sum_{j=1}^{n} r_j$

i.e., $(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p\left[\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] - n\right] + 0 \pmod 2$ (mul. by 2)

$\therefore (a-1)\sum_{j=1}^{\frac{p-1}{2}} j = \left[\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] - n\right] \pmod 2$

$\sum_{j=1}^{\frac{p-1}{2}} j = 1+2+1 \cdots + \frac{p-1}{2} = \frac{p-1}{2}\left(\frac{p-1}{2}+1\right) \times \frac{1}{2}$

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

$(a-1)\left(\frac{p^2-1}{8}\right) = \left[\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] - n\right] \pmod 2$ —— (4)

If a is odd, $a-1$ is even

$\therefore$ (4) $\Rightarrow \left[\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] - n\right] \equiv 0 \pmod 2$.

$$n = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] \pmod 2 \quad \text{——} (5)$$

but, $\left(\frac{a}{p}\right) = (-1)^n$, by Gauss lemma, —(6)

(5), (6) $\Rightarrow$ $\left(\frac{a}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right]}$

now, let $a = 2$, then (4) $\Rightarrow$

$$\frac{p^2-1}{8} = \left[\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{j2}{p}\right] - n\right] \pmod 2$$

Since, $2j < p$, $\forall j = 1, 2, \ldots, \frac{p-1}{2}$

$\therefore \left[\frac{2j}{p}\right] = 0$; $\forall j$

$$\frac{p^2-1}{8} \equiv -n \pmod 2$$

$$\therefore n = \frac{p^2-1}{8} \quad \text{——} (7)$$

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

Ex: 1. Find $\left(\frac{-98}{31}\right)$

Problem:

Check whether the congruence $x^2 \equiv 2 \pmod{43}$ is solvable and has a soln.

i) $x^2 \equiv 2 \pmod{43}$

$x^2 \equiv 2 \pmod{43}$ has a soln. if $\left(\frac{2}{43}\right) = 1$

$$\left(\frac{2}{43}\right) = (-1)^{\frac{(43)^2-1}{8}} = (-1)^{\text{odd}} = -1$$

$\therefore x^2 \equiv 2 \pmod{43}$ is not solvable.

ii) $x^2 \equiv 5 \pmod{19}$ $\left(\frac{5}{19}\right)$: $a = 5$, $p = 19$ $\frac{p-1}{2} = 9$

Soln: $n = 4$

$\left(\frac{5}{19}\right) = (-1)^4 = 1$

residues: 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256, 289, 324

$x^2 \equiv 5 \pmod{19}$ is solvable.

residues $> \frac{p}{2}$ (9.5)

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

$n = 10, 15, 11, 16$

$n = 4$

W.K.T.

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

$$\left(\frac{5}{19}\right) \equiv 5^9 \pmod{p}$$

$$1 \equiv 5^9 \pmod{19} \Rightarrow 5 \equiv 5^{10} \pmod{19}$$

$$x^2 \equiv 5^{10} \pmod{19}$$

$$x^2 \equiv (5^5)^2 \pmod{19}$$

$$x \equiv \pm 5^5 \pmod{19}$$

i.e., $x \equiv \pm 125 \times 25 \pmod{19}$

$\equiv \pm 11 \times 6 \pmod{19}$

$\equiv \pm 66 \pmod{19}$

$x \equiv \pm 9 \pmod{19}$

19 | 125 (6, 114, 11)

19 | 66 (3, 57, 9)

19 | 25 (1, 19, 6)

3.3 The Jacobi symbol: Let $(P, Q) = 1$, Q be odd +ve so that $Q = q_1 q_2 \ldots q_s$ where q_j are odd primes not necessarily distinct. Then the Jacobi symbol (P/Q) is defined by

$$(P/Q) = \prod_{j=1}^{s} (P/q_j)$$ where (P/q_j) is the legendre symbol.

Pg: 143

m, b

$= q_1 q_2 \ldots q_m$ &

$= q_1' q_2' \ldots q_m'$

$$(P/Q) = \prod_{j=1}^{m} (P/q_j) \prod_{j=1}^{m} \left(\frac{P}{q_j'}\right)$$

$$= \prod_{j=1}^{m} \prod_{j=1}^{n} \left(P/q_i \frac{P}{q_j'}\right)$$

$= (P/Q)$

(3) $\frac{PP'}{Q} = \prod_{j=1}^{m} \left(\frac{PP'}{q_j}\right)$

$= \left(\frac{PP'}{q_1}\right)\left(\frac{PP'}{q_1}\right) \ldots \left(\frac{PP'}{q_m}\right)$

$= \left(\frac{P}{q_1}\right)\left(\frac{P}{q_m}\right)\left(\frac{P'}{q_1}\right) \ldots \left(\frac{P'}{q_m}\right)$

$= (P/Q)(P'/Q)$

(2) $\Rightarrow \frac{QQ}{Q} = \frac{Q}{Q}$

$\gcd(P, Q) = 1$ then $(P/Q) = 1$

$(P^2/Q) = (P/Q)(P/Q) = 1$

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

$\gcd(P, Q^2) = 1, \frac{Q^2}{Q} = P_2 = 1$

(1) $\left(\frac{P^2}{Q}\right) = \left(\frac{PP}{Q}\right) \left(\frac{P}{Q}\right)\left(\frac{P}{Q}\right) = \left(\frac{P}{Q}\right)\left(\frac{P}{Q}\right) = 1$

(4) From (3)

$P'_{Q_1} = P'_{Q_2} = \left(\frac{P'^2}{Q}\right)(1^2 \times 1) = 1$

$\frac{P'P^2}{QQ'} = \left(\frac{P'}{P'Q^2}\right)\left(\frac{P^2}{Q'Q}\right)$

$= \left(\frac{P'}{Q'}\right)\left(\frac{P'}{Q^2}\right)\left(\frac{P'}{Q}\right)$

$= \left(\frac{P'}{Q'}\right) \cdot 1 \cdot 1$

$= (P'/Q')$

ii) Given $P' \equiv P \pmod{Q}$

Let $Q = q_1 q_2 \cdots q_s$

then $P' \equiv P \pmod{q_j}$, $j = 1, 2, \cdots s$

$a \equiv b \pmod{p}$

$\left(\frac{P'}{q_j}\right) = \left(\frac{P}{q_j}\right)$, for each $j \Leftarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

$$\left(\frac{P'}{Q}\right) = \prod_{j=1}^{s} \left(\frac{P'}{q_j}\right) = \prod_{j=1}^{s} \left(\frac{P}{q_j}\right) = \left(\frac{P}{Q}\right)$$

THEOREM - 8.7:

If Q is odd and $Q > 0$, then $\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}$ and ——— (1)

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

Proof:

Let $Q = q_1 q_2 \cdots q_s$

$$\left(\frac{-1}{Q}\right) = \prod_{j=1}^{s} \left(\frac{-1}{q_j}\right) = \prod_{j=1}^{s} (-1)^{\frac{q_j - 1}{2}}$$

$$= (-1)^{\sum_{j=1}^{s} \frac{q_j - 1}{2}} \quad \text{——— (2)}$$

To find $\sum_{j=1}^{s} \frac{q_j - 1}{2}$

Let a and b be odd nos

then $\frac{ab-1}{2} \equiv \left(\frac{a-1}{2} + \frac{b-1}{2}\right) = \frac{ab-1}{2} - \frac{a+b-2}{2}$

$$= \frac{ab - 1 - a - b + 2}{2}$$

$$= \frac{ab - a - b + 1}{2}$$

$$= \frac{a(b-1) - (b-1)}{2}$$

$$= \frac{(b-1)(a-1)}{2}$$

Since a and b are odd $a-1$ [illegible]

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

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod 2$$

$$\frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} \pmod 2$$

Apply this repeatedly for odd no's $q_1 q_2 \cdots q_s$

$$\frac{q_1-1}{2} + \frac{q_2-1}{2} + \cdots + \frac{q_s-1}{2} \equiv \frac{q_1 q_2 \cdots q_s - 1}{2} \pmod 2$$

$$\sum_{j=1}^{s} \frac{q_j-1}{2} \equiv \frac{Q-1}{2} \pmod 2$$

(1) $\Rightarrow$

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

$$\left(\frac{2}{Q}\right) = \prod_{j=1}^{s} \left(\frac{2}{q_j}\right) = \prod_{j=1}^{s} (-1)^{\frac{q_j^2-1}{8}} \quad (-1)^{\text{power}}$$

$$= (-1)^{\sum_{j=1}^{s} \frac{q_j^2-1}{8}} \quad \text{(2)}$$

To find $\sum_{j=1}^{s} \frac{q_j^2-1}{8}$

If a and b are odd, then

$$\frac{a^2b^2-1}{8} - \left(\frac{a^2-1}{8} + \frac{b^2-1}{8}\right) = \frac{a^2b^2-1-a^2-b^2+2}{8}$$

$$= \frac{(a^2-1)(b^2-1)}{8}$$

Since a and b are odd, a^2-1, b^2-1 are even.

$$\frac{a^2b^2-1}{8} - \left(\frac{a^2-1}{8} + \frac{b^2-1}{8}\right) \equiv 0 \pmod 2$$

$$\frac{a^2-1}{8} + \frac{b^2-1}{8} \equiv \frac{a^2b^2-1}{8} \pmod 2$$

Apply this to $q_1, q_2, \cdots q_s$

$$\frac{q_1^2-1}{8} + \frac{q_2^2-1}{8} + \cdots + \frac{q_s^2-1}{8} \equiv \frac{q_1^2 q_2^2 \cdots q_s^2 - 1}{8} \pmod 2$$

$$\sum_{j=1}^{s} \frac{q_j^2-1}{8} \equiv \frac{1}{8}\left(\prod_{j=1}^{s} q_j^2 - 1\right) \pmod 2$$

$$\sum_{j=1}^{s} \frac{q_j^2-1}{8} \equiv \frac{1}{8}(Q^2-1) \pmod 2$$

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

Theorem 3.8:

If P and Q are odd and +ve, and if $(P,Q)=1$,

then $$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$$

Proof:

Let $P = p_1 p_2 \cdots p_r = \prod_{i=1}^{r} p_i$ $\quad\Rightarrow\quad \sum_{i=1}^{r} (-1)^{\left(\frac{p_i-1}{2}\right)}$

$Q = q_1 q_2 \cdots q_s = \prod_{j=1}^{s} q_j$ $\quad\Rightarrow\quad \sum_{i=1}^{r} (-1)^{\left(\frac{q_i-1}{2}\right)}$

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s}\left(\frac{P}{q_j}\right)$$

$$= \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{p_i}{q_j}\right)$$

$$= \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{q_j}{p_i}\right)(-1)^{\left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right)}$$

$$= \left(\frac{Q}{P}\right)(-1)^{\sum_{j=1}^{s}\sum_{i=1}^{r}\left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right)} \longrightarrow (1)$$

but, $$\sum_{j=1}^{s}\sum_{i=1}^{r}\left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right) = \sum_{i=1}^{r}\left(\frac{p_i-1}{2}\right)\sum_{j=1}^{s}\left(\frac{q_j-1}{2}\right)$$

$$\sum_{i=1}^{r}\frac{p_i-1}{2} \equiv \frac{P-1}{2} \pmod 2$$

$$\sum_{j=1}^{s}\frac{q_j-1}{2} \equiv \frac{Q-1}{2} \pmod 2$$

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

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

but, $\frac{Q}{P_i} = \pm 1$

$$\therefore \left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$$