Department of Distance Education

Punjabi University, Patiala

Class : B.A. 2 (Mathematics) **Semester : 4**
Paper : 6 (Number Theory) **Unit : I & II**
Medium : English

Lesson No.

Department website : www.pbidde.org

B.A. PART–II (SEM-IV) **MATHEMATICS**

PAPER-VI

NUMBER THEORY

Lesson No. 1.1

DIVISIBILITY THEORY IN THE INTEGERS

Structure :

1.1.1 Division Algorithm :

Given integers a and b, with b > 0, there exist unique integers q and r satisfying

$$a = qb + r, \qquad 0 \leq r < b$$

The integers q and r called respectively the quotient and remainder in the division of a and b.

Proof: We begin by proving that the set

$$S = \{a - xb/x \text{ and integer; } a - xb \geq 0\}$$

is non empty. For this, it is sufficient to prove that if show that $\exists$ a value of x which makes a – xb < 0.

Since $b \geq 1$, we have $|a|\ b \geq |a|$ and so

$$a - (-|a|)\,b = a + |a|\ b \geq a + |a| \geq 0$$

Hence for the choice $x -|a|$, a – xb will lie in S. This paves the way for an application of well known 'Well ordering principle' which states.

Every non-empty S of non-negative integers contains a least element; that is, there is some integer a in S such that for $a \leq b$ for all b belonging to S.

This implies that the set S contains a smallest interger, call it r.

By the definition of S, $\exists$ a integer q

satisfying $r = a - qb, \qquad 0 \leq r$

We argue that r < b. If this were not the case, then $r \geq b$ and

$$a - (q + 1)\, b = (q - qb) - b = r - b \geq 0$$

$\Rightarrow$ a – (q + 1) b has the proper from to belong to the set S. But a – (q + 1) b = r –

$b < r$, leading to a contradiction of the choice of r as the smallest member of S.

Hence $r < b$.

We next prove that q and r are unique. Suppose that a has two representations is

$$a = bq + r \quad \text{and} \quad a = bq' + r'$$

Where $0 \le r = b, \quad 0 \le r' - b$.

Then $r' - r = b(q - q')$ and because of the fact $|\alpha\beta| = |\alpha|\,|\beta|$,

We have $|r' - r| = |b(q - q')| = b|q - q'|$; Note b is +ve.

We also have $-b < -r \le 0$ and

$0 \le r' - r \le b$ we get

$-b \le r' - r \le b$ or

Thus $|r' - r| < b$

$$b|q - q'| < b$$

$$\Rightarrow \quad 0 \le |q - q'| < |$$

Since $|q - q'|$ is a non-negative integer, the only possibility is that

$$q - q' = 0$$

$$\Rightarrow \quad q = q'$$

which gives $r = r'$

Hence uniqueness of r and q is proved, Hence the theorem is proved.

Corollary: If a and b are integers with $b \neq 0$, then there exist unique integers q and r such that

$$a = bq + r, \quad 0 \le r < |b|$$

Proof: We consider the case when b is –ve, because $b > 0$ part has already been proved, Then $|b| > 0$ and the theorem proved above implies the existence of unique integers q' and r for which

$$a = q'|b| + r, \quad 0 \le r < |b|$$

Noting that $|b| = -b$ as $b < 0$

we take $q = -q'$ to get

$$a = qb + r \text{ with } 0 \le r < |b|$$

This proves the corollary.

To illustrate the Division algorithm when $b < 0$, let us take $b = -5$, then for the choices of $a = 1, -3, 57$ and -53, we get

$$1 = 0\,(5) + 1$$
$$-3 = 1\,(-5) + 2$$
$$57 = (-11)\,(-5) + 2$$
$$-53 = (-11)\,(-5) + 2$$

In this context, we want to concentrate on the application of Division Algorithm.

Example 1: Let $a \varepsilon Z$ (the set of integers) show that a^2 leaves the remainder 0 or 1 when it is divided by 4.

OR

Square of any integer is of the form $4q$ or $4q + 1$.

Solution : Divide a by 2 and use Division Algorithm, we get

$$a = 2q + r, \quad 0 \leq r < 2$$
$$0 \leq r < 2 \Rightarrow \quad r = 0 \text{ or } 1$$

Thus, $a = 2q$ or $a = 2q + 1$

$\Rightarrow \quad a^2 = 4q^2$ or $a^2 = 4q^2 + 4q + 1$

$\qquad\qquad\qquad\qquad = 4\,(q^2 + q) + 1$

$\Rightarrow \quad a^2 = 4q^1 \qquad a^2 = 4q'' + 1$

where $q^1 = q^2$ and $q'' = q^2 + q$

$\Rightarrow$ a^2 when divided by 4 leaves remainder 0 or 1.

Similarly, we can prove that if $a \varepsilon Z$, a^3 leaves the remainder 0, 1 or 3 when divided by 4.

Example 2 : Show that $\dfrac{a\left(a^2+2\right)}{3}$ is an integer for all $a \geq 1$.

Solution : When 'a' is divided by 3, then we get by Division Algorithm

$$a = 3q + r, \quad 0 \leq r < 3 \quad \Rightarrow \quad r = 0, 1, 2$$

$\Rightarrow \quad a = 3q$ or $a = 3q + 1$, or $a = 3q + 2$

Now when $a = 3q$

$$a\,(a^2 + 2) = 3q\,(9q^2 + 2)$$

or $\quad \dfrac{a}{3}\left(a^2+2\right) = q\left(9q^2+2\right) \qquad \Rightarrow \dfrac{a\left(a^2+2\right)}{3}$ is an integer.

when $a = 3q + 1$

$$\frac{a\left(a^2+2\right)}{3} = \frac{(3q+1)}{3}\left(9q^2+6q+1+2\right)$$

$= (3q + 2)\ (3q^2 + 2q + 1)$, which is again an integer.

Also when $a = 3q + 2$

$$\frac{a\left(a^2+2\right)}{3} = \frac{(3q+2)}{3}\left(9q^2+12q+4+2\right)$$

$= (3q + 2)\ (3q^2 + 4q + 2)$, which is again an integer.

Hence we have proved that $\frac{a\left(a^2+2\right)}{3}$ is an integer for all $a \geq 1$.

On similar lines, the readers can easily prove that :

(i) Cube of any integer is of the form 9k, 9k + 1 or 9k + 8.

(ii) Square of any integer is of the form 3k or 3k + 1.

Example 3 : Prove that the fourth power of any integer is of the form 5k or 5k + 1.

OR

If $a \in Z$, then a^4 leaves remainder 0 or 1 when divided by 5.

Sol. : By Division Algorithm

$a = 5q + r \qquad 0 \leq r < 5$

$\Rightarrow \quad a = 5q$ or $a = 5q + 1$ or $a = 5q + 2$ or $a = 5q + 3$ or $a = 5q + 4$

Now in 1st case $a^4 = 625q^4 = (625\ q^3)\ q + 0 \Rightarrow$

$= 5\ (125\ q^3) + 0 \Rightarrow a^4 = 5k$, where $k = 125\ q^3$

when $a = 5q + 1 \Rightarrow a^4 = 625\ q^4 + 625\ q^3 + 250\ q^2 + 25q + 1$

$= 5\ [125\ q^3 + 125\ q^2 + 50\ q^2 + 5\ q] + 1$

$= 5\ k + 1$

when $a = 5q + 2 \Rightarrow q^4 = (5q + 2)^4$

$= 625\ q^4 + 1250\ q^3 + 1000\ q^2 + 200\ q + 16$

$= 5\ (125\ q^3 + 250\ q^3 + 200\ q^2 + 40\ q + 3) + 1$

$= 5\ k + 1$

when $a = 5q + 3$

$a^4 = (5q + 3)^4$

$= 625\ q^4 + 1975\ q^3 + 2250\ q^2 + 4025\ q + 81$

$= 5\ (125\ q^4\ 395\ q^3 + 450\ q^2 + 805\ q + 16) + 1$

Similarly we can prove the last part.

In this way, we have proved that a^4 is always of the form 5k or 5k + 1.

1.1.2 The Greatest Common Divisor :

By Division algorithm, we know that

$a = q\ b + r$

i.e. when a is divided by b, q is the quotient and r is the remainder.

In case $r = 0$, we say that b divides a

Now, an integer y is said to be divisible by an integer $x \neq 0$, in symbols x/y, if there exists some integer z such that y = xz. We write x/y to indicate that y is not divisible by x.

For example : – 15 is divisible by 5 i.e. – 15 = 5 (–3)

and 10 is not divisible by 7 as there is no integer k such that 10 = 7k.

The above statement can also be rewritten as x is a divisor of y or x is a factor of y or y is a multiple of x.

If x is a divisor of y, then y is also divisible by –x i.e. $y = x\,z \Rightarrow y = (-x)\,(-z)$, so that divisors of an integer always occur in pairs.

Theorem 2 : For integers x, y, z, the following results hold :

(i) $x/0,\ 1/x,\ x/x$

(ii) $x/1$ iff $x = \pm 1$

(iii) if x/y and z/u then $\frac{xZ}{yu}$

(iv) if x/y and y/z then x/z.

(v) if x/y and y/x if and only if $x = \pm y$

(vi) if x/y and $y \neq 0$, then $|x| \leq |y|$

(vii) if x/y and x/z, then $x/ay + bz$ for arbitrary integers and a and b.

Proof: We understand that the proofs of (i) to (v) are very trivial and students are advised to prove these parts themselves.

We start with the proof of (vi)

If x/y and $y \neq 0$ then $|x| \leq |y|$

If x/y then there exists z such that

$y = xz$ and $y \neq 0$

$\Rightarrow z \neq 0$

On taking absolute values, we have

$$|y| = |x||z| \geq |z| \qquad \text{or} \qquad |x| \leq |y|$$

Proof of (vii) part :

x/y and x/z ensure that

$y = xr$, $z = x\,s$ for suitable integers r and s.

But then, $a\,y + bz = a\,x\,r + b\,x\,s$

$= x\,(a\,r + b\,s)$

Whatever be the choice of a and b.

Since $a\,r + bs$ is an integer, so $a\,y + b\,z$ is divisible by x.

The lost part (vii) can be further extended by induction to the sums of more than two terms. That is,

if x/y_i for $i = 1, 2, \ldots\ldots\ldots\, n$, then

$$x/(y_1a_1 + y_2a_2 + \ldots\ldots + y_na_n)$$

for all integers $a_1, a_2, \ldots\ldots\ldots\ldots, a_n$

Definition: If x and y are arbitrary integers, then an integer d is said to be common divisor of x and y if d/x and d/y. Since 1 is a divisor of every integer, so 1 is a common divisor of x and y; hence the set of positive common divisors is non-empty. Now every integer divides 0, so if $x = y = 0$, then every integer serves as a common divisor of x and y. At this instance, the set of positive common divisors of x and y is infinite. However, when at least one of x or y is different from zero, there are only a finite number of positive common divisors. Among these, there exists a largest one, called the **greatest common divisor** of x and y.

If x and y are given integers, with at least one of them different from zero. The greatest common divisor of x and y denoted by gcd (x, y), is the positive integer d satisfying

(1) d/x , d/y

(2) If z/x , z/y then $z \leq d$.

For Example : The positive divisors of –12 are 1, 2, 3, 4, 6, 12 while those of 30 are 1, 2, 3, 5, 6, 10, 15, 30; hence the positive common divisors of –12 and 30 are 1, 2, 3, 6. As 6 is the largest of these integers, it follow that

g c d (–12, 30) = 6. In the same way, we can show that
g c d (8, –17) = 1, g c d of (–8, –36) = 4
g c d (–5, 5) = 1.

The next theorem is very important as it indicates that g c d of (x, y) can be represented as a linear combination of x and y (by a linear combination of x, y we mean that an expression of the form xr + ys where r and s are integers).

For instance

g c d (–12, 30) = 6 = (–12) 2 + 30 (1)

or

g c d (–8, 36) = 4 = (–8) 4 + 36 (–1)

Theorem 3 : Given integers x and y, not both of which are zero, there exist integers r and s such that

g c d (x, y) = xr + ys

Proof: Consider the set S of all positive combinations of x and y;

$S = \{xu + yv \ / \ xu + yv < 0, u, k \text{ are integers}\}$

Notice first that S is not empty. For example, if $x \neq 0$, then the integer x,

x = xu + y, 0 will be in S

We choose d = 1 or u = –1 according as x is positive or negative. By virtue of the well ordering principle, S must contain a smallest element d. Thus from the definition of S, there exists integers r an s for which

d = rx + yx

We claim that d = g c d (x, y)

Taking stock of the Division Algorithm, one can obtain the integers q and q′ such that $x = qd + q'$ where $0 \leq q' < d$.

Then can be written in the form

$q' = x - qd = x - q\,(ax + by)$

$= x\,(1 - qa) + y\,(-bq)$

When $q' < 0$, this representation implies that q' is a member of S, contradicting the fact that d is the least integer in S (recall that $q' < d$). Therefore $q' = 0$ and so x =

qd or equivalently $\frac{d}{x}$. By similar reasoning $\frac{d}{y}$, the effect of which is to make d a common divisor of both x and y.

Now if z is an arbitrary common divisors of x and y, then past (v) of the theorem on page allows us to conclude that $\frac{z}{xr + ys}$; In other words, $\frac{z}{d}$.

By (6) of the same theorem, z = $|z| \le |d| = d$ so that d is greater than every positive common divisor of x and y. Combining all the facts together, we see that

d = g c d (x, y)

Corollary : of x and y are given integers, nor both zero, then the set

T = {xr + ys /r, s are integers}

is precisely the set of all multiples of d = g c d (x, y)

Proof : Since $\frac{d}{x}$ and $\frac{d}{y}$, we know that d (xr + ys for all integers x and y).

Thus every member of T is a multiple of d. On the other hand d may be written as d = xr = yx, for suitable integers x_0 and y_0 so that any multiple of nd of n is of the form

$nd = n\,(x\,x_0 + y\,y_0)$

$= x\,(n\,x_0) + y\,(n\,y_0)$

Hence nd is a linear combination of x and y and by definition lies in T.

Note : It may happen that 1 and –1 are the only common divisors of x and y so that g c d (x, y) = 1. For example

g c d (2, 5) = g c d (–9, 16) = g c d (–2 $\geq$ 35 = 1)

<u>**We give a defnition below**</u>

Two integers x and y, not both of which are zero, are said to be relatively prime whenever g c d (x, y) = 1.

Note : 1. If g c d (x, y) = d then

$$\text{g c d}\left(\frac{x}{d}, \frac{y}{d}\right) = 1$$

2. If x/y and y/z with g c d (x, y) = 1

then xy/z.

1.1.4 Euclidean Algorithm:

the Euclidean Algorithm may be described as follows: Let x and y be two integers whose greatest common divisor is desired. Since g c d $(|x|, |y|)$ = g c d (x, y), there is no harm in assuming that $x \geq y > 0$. The first step is to apply the Division Algorithm to x and y we get

$$x = q_1 y + r_1 \qquad 0 \leq r_1 < y$$

If it happens that $r_1 = 0$ then y/x and

g c d (x, y) = y. When $r_1 \neq 0$, divided y by r, to produce integers q_2 and r_2 satisfying

$$y = q_2 \ r_1 + r_2 \qquad 0 \leq r_2 < r_1$$

of $r_2 = 0$, then we stop, otherwise we proceed as before to obtain

$$r_1 = q_3 r_2 + r_3 \qquad 0 \leq r_3 < r_2$$

This division process continues until some zero remainder appears, say at the (n + 1)th stage. When r_{n-1} is divided by r_n (a zero remainder occurs sooner or later since the decreasing sequence $y > r_1 > r_2 > \ldots\ldots\ldots \geq 0$ cannot contain more than y integers).

The result is the following system of equations:

$$\begin{aligned}
x &= q_1 y + r_1 && 0 \leq r_1 < y \\
y &= q_2 r_1 + r_2 && 0 \leq r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 && 0 \leq r_3 < r_2 \\
&\ \ . \\
&\ \ . \\
&\ \ . \\
r_{n-1} &= q_{n+1} r_n + 0 && 0 \leq r_n < r_{n-1}
\end{aligned}$$

We argue that r_n, the last non-zero remainder which appears in this manner is equal to g c d (x, y), our proof is based on **lemma:**

Lemma : of x = qy + r then g c d (x, y) = g c d (y, r) whose proof is as follows: of d = g c d (x, y), then the relations

$$\frac{d}{x} \text{and} \frac{d}{y} \qquad \Rightarrow \frac{d}{(x - qy)} \text{ or } \frac{d}{r}.$$

Thus d is a common divisor of both y and r. On the other hand of Z is an arbitrary common divisor of y and r, then $\frac{z}{(yq + r)}$, whence $\frac{z}{x}$. This makes z a common divisor of x and y, s that $z \leq d$. It now follow from the definition of

g c d (y, r) that d = g c d (y, r)

On using the result of this lemma, we simply work down the displayed system of equations obtaining.

$$g\,c\,d\,(x, y) = d = g\,c\,d\,(y, r_1) = \ldots\ldots\ldots\ldots. = g\,c\,d\,(r_n\ 0) = r_n$$

as claimed before.

Example : Find g c d of 12378 and 3054 and express g c d as the linear combination of 12378 and 354.

Solution :

Now

12378 = 4 (3054)	+	162
3054 = 18 (162)	+	138
162 = 1 (138)	+	24
138 = 5 (24)	+	18
24 = 1 (18)	+	6
18 = 3 (6)	+	0

Our previous theorem tell us that, 6 is the greatest divisor of 12378 and 6054.

6 = g c d (12378, 3054)

Now we express 6 as linear combination of

12378 and 3054

Now 6 = 24 – 18

= 24 + (138 – 5.24)

= 6.24 – 138

= 7.0

= 6. (162 – 138) – 138

= 6.162 – 7.138

= 6.162 – 7 (3054 – 18.162)

= 132.162 – 7.3054

= 132.(12378 – 4.3054) – 7.3054

= 132.12378 + (–535). 3054

$\Rightarrow$ 6 = g c d (12378, 3054)

= 12378 r + 3054 s

Here r = 132 and s = –534.

French Mathematician Lama (1795-1870) proved that the number of steps required in the Euclidean Algorithm is at most 5 times the number of digits in the smaller integer.

Theorem : If k > 0, g c d (kx, ky) = k g c d (x, y).

Proof : If each of the equations appearing in the Euclidean algorithm, x and y is multiplied by k, we get

$$x\,k = q_1\,(y\,k) + r_1 \qquad 0 \leq r_1\,k < b\,k$$

$$y\,k = q_2\,(y\,k) + r_2 \qquad 0 \leq r_2\,k < r_1\,k$$

$$r_1\,k = q_3\,(r_2\,k) + r_3$$

.
.
.

$r_{n-1}\,k = -\,q_{n+1}\,(r_n\,k) + 0 \qquad 0 \le r_n\,k < r_{n-1}\,k$

But this is clearly the Eucildean Algorithm applied to the integers xk and yk, so that their greatest common divisor is the last non-zero remainder r_n k that

$g\,c\,d\,(k\,x, k\,y) = r_n = k\,g\,c\,d\,(x, y)$

Corollary : For any integer k > 0,

$g\,c\,d\,(k\,x, k\,y) = |k|\; g\,c\,d\,(x, y)$

1.1.5 Least Common Multiple

The least common multiple of 1000 non-zero integers a and b denoted by lcm (a,b) is the positive integer m satisfying

(1) $x/_m$ and $y/_m$

(2) If $x/_z$ and $y/_z$ with z > 0, then $m \le Z$.

As an example, the positive common multiples of the integers –12 and 30 are

60, 120, 180, 240, ... Hence

$\lambda\,cm\,(-12, 30) = 80$

$\Rightarrow$ Given non-integers x and y, $\lambda\,cm\,(x, y)$

always exists and $\lambda\,cm\,(x, y) \le |xy|$.

Theorem: For positive integers x and y

$g\,c\,d\,(x, y).\ l cm\,(x, y) \le xy$

Proof : Take d = g c d (x, y) and

$\Rightarrow$ x = dr, y = ds for integer r and s.

of $m = \dfrac{xy}{d}$ then m = x s = r y,

the effective which is to make a (positive) common multiple of x and y. Now let z be any positive integer that is a common multiple of x and y say definiteness z = x u = y v. as are know, there exists p and q satisfying d = xp + qy.

In consequence :

$$\frac{z}{m} = \frac{z}{xy} = \frac{z(ps+qy)}{xy} = \left(\frac{z}{y}\right)p + \left(\frac{z}{x}\right)q$$

$= up + uq$

$\Rightarrow$ The equation states that $\frac{m}{z}$, allowing us to conclude that $m \leq z$.

$$\Rightarrow \lambda\, cm\,(x, y) = \frac{xy}{d} \quad \text{or} \quad xy = md.$$

1.1.6 Fundamental Theorem of Arithmetic:

Every positive integer $n > 1$ can be expressed as a product of primes, this representation is unique, apart from the order in which the factors occur.

We assume that the students are now well aware with the primes, composite numbers.

Some results (without proof):

(i) If p is a prime and $p/_{xy}$ then $p/_{x}$ or $p/_{y}$

(ii) or in general p is a prime and $p/_{x_1 x_2 \ldots\ldots\ldots\ldots x_n}$ then $p/_{x_k}$ for some k, where $1 \leq k < n$

Proof of Fundamental Theorem of Arithmetic :

Case I when n is a prime, then there is nothing to prove, then there is nothing to prove.

Case II of n is composite, then there exists an integer of satisfying $\frac{d}{n}$ and $1<d<n$. Among all these integers d choose p_i to be the smallest (that is possible because of well-ordering principle.). Then p_i must be a prime number. Otherwise it too would have a divisor or q with $1 < q < p_1$, but then $\frac{q}{p_1}$ and $\frac{p_1}{n} = \frac{q}{n}$ which contradicts the choice of p_i as the smallest positive divisor, not equal to 1, of n.

We may therefore write $n = p_i n_1$, where p_i is prime and $1 < n_i < n$. If n_i happens to be a prime, then we have our final representation. In the contrary case, the argument is repeated to produce a second prime number p_2 such that

$n_i = p_2 n_2$, that is

$n = p_1 p_2 n_2 \qquad 1 < n_2 < n_1$

If n_2 is prime, then it is not necessary to go further otherwise

$n_2 = p_3 n_3$ where p_3 is a prime

$n = p_1 p_2 p_3 n_3 \qquad 1 < n_3 < n_2$

The decreasing sequence

$$n > n_1 > n_2 > \dots\dots\dots. > 1$$

Cannot continue indefinitely, so that after a finite number of steps n – is a prime say p_k. This leads to the prime factorisation.

$$n = p_1 p_2 \dots\dots\dots p_k$$

Second part:

Uniqueness of prime factorisation – let us suppose that the integer n can be represented as a product of primes in two ways, say

$$n = p_1 p_2 \dots\dots\dots p_r$$

$$= q_1 q_2 \dots\dots\dots q_s \qquad r \leq s$$

Where p_i and q_i are all primes, written on increasing sequence so that

$$p_i \leq p_2 \leq \dots\dots\dots \leq p_r, \qquad q_i \leq q_2 \leq q_3 \dots\dots\dots \leq p_s$$

Since $\dfrac{p_1}{q_i q_2 \dots\dots p_s}$, the previous theorems tells us that p_1 = q k for some k; but then $p_i \geq q_i$.

Similar reasoning gives $q_i \geq p_i \Rightarrow p_i \geq q_i$ may be cancel this common factor and obtain

$$p_2 \dots\dots\dots p_r = q_2 \dots\dots\dots q_s$$

Now repeat the process to get $p_2 = q_2$ and

$$\Rightarrow p_3 p_4 \dots\dots\dots p_r = q_3 q_4 \dots\dots\dots q_s$$

Continue in this fashion. If the in equality r < s held we should arrive at

$$1 = q_{r+1}\, q_{r+2} \dots\dots\dots q_{r+s}$$

which is meaningless since each $q_i > 1$. Hence r = s and

$$p_1 = q_1,\ p_2 = q_2 \dots\dots\dots,\ p_r = q_r$$

Hence the two representations are identical. This completes the proof.

Corollary : Any positive integer n > 1 can be written uniquely in a canonical form

i.e. $n = p_1^{k_1}, p_2^{k_2} \dots\dots\dots, p_r^{k_r}$

Where for i = 1, 2 ....r, each k_i is a +ve integer and each p_i is a prime, with

$$p_1 < p_2 \dots\dots\dots < p_r$$

To illustrate, Take 4725, Now

$$4725 = 3 \times 1575 = 3 \times 3 \times 525 = 3 \times 3 \times 5 \times 5 \times 7$$

$$= 3^2 .\ 5^2 .\ 7^1$$

EXERCISE

1. Check whether 271 is a prime or not.
2. Lest all primes $\leq$ 100.
3. Prove that the only prime of the form $n^3 - 1$ is 7.

4. State and prime Fundamental theorem of Arithmetic.

Note:

1. In the preparation of this lesson many books listed at the end of syllabus have been consulted.
2 Students are advised to get/purchase at least one book on Number Theory.

Lesson No. 1.2

THE THEORY OF CONGRUENCE

OBJECTIVES:

1.2.1 Definition of Congruence

1.2.2 Some Applications of Congruences

1.2.3 Euler Fermat's Theorem

1.2.4 Wilson's Theorem

1.2.1 Definition:

According to Gauss,

'If a number n divides the difference between two numbers a and b, then a and b are said to be congruent with respect to n; if not, incongruent.

OR

Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n, symbolically

$a \equiv b \pmod{n}$

If n divides the difference of $a - b$; that is

$a - b = kn$, for some integer k

Example : Take n = 7

$3 \equiv 32$ (mode 7)

$-31 \equiv 11$ (mod 7)

$-15 \equiv -64$ (mode 7)

as $(3 - 24) = -21$ is divisible by 7

$(-31 - 11) = -42$ is divisible by 7

but $25 \equiv 12$ (mod 7), since

$25 - 12 = 13$ is not divisible by 7

Hence 25 is not congruent to 12 mod 7, whereas first satisfy the definition of congruence.

It should be noted that any two integers are congruent modulo 1, whereas two integers are congruent modulo 2 when they are both even or both odd.

Given an integer a, let q and r be its quotient and remainder upon division by n, then

$a = qn + r, \; 0 \leq r < n$

Since there are n choices (0, 1, 2..........n–1) for r; and in particular a, 0 (mod n) f and only if n divides a.

The set of integer 0, 1, 2.......... (n –1) is called the set of least positive residues modulo n.

In general a collection of n integers a_1, a_2,......., a_n is said to form a complete set of residues (or a complete system of residues) modulo n of every integer is congruent modulo n to one and one only one of the ak;

For instance

–12, –4, 11, 13, 22, 82, 91

Constitute a complete set of residues modulo 7; because the remainder which we obtain when there numbers are divided by 7 are

2, 3, 4, 6, 1, 5, 0 respectively

This suggests a theorem, which states

Theorem : For arbitrary integers a and b, a $\equiv$ b (mod n) if and ony if a and b leave the same non-negative remainder when divided by it.

Proof : If a $\equiv$ b (mod n) then

a = b + kn for some integer k.

upon division by n, b leaves a certain remainder r then b = qn + r, where 0, r – n.

Therefore a = b + kn = qn + r + kn = n (q + k) + r so leaves the same remainder when divided by n.

Conversely if a and b leave the same remainder when divided by n, say r_1 and r_2 then

$a = q_1 n + r_1$

$b = q_2 n + r_1$

then $a - b = (q_1 - q_2)n$ suggesting that

a $\equiv$ b (mod n)

Note : Some of the elementary properties of equality which carry over to congruence appear in the next theorem.

Theorem 2 : Let n > 0 be fixed and a, b, c, d be arbitrary integers. Then the following properties hold.

(i) a $\equiv$ a (mod n)

(ii) a $\equiv$ b (mod n), then b $\equiv$ a (mod n)

(iii) a $\equiv$ b (mod n), b $\equiv$ c(mod n) then a $\equiv$ c (mod n)

(iv) a $\equiv$ b (mod n) c $\equiv$ d (mod n) then

a + c = b + d (mod n) and ac = bd (mod n)

(v) a $\equiv$ d (mod n), a + n = b + c (mod n) and ac = bc (mod n)

(vi) If a $\equiv$ b (mod n), then $a^k = b^k$ (mod n) for some positive integer k.

Proof: the proof of all these parts are very simple and easy say to prove

(i) a $\equiv$ a (mod n)

obviously (a – a) is divisible by n

(ii) $a - b$ is divisible by n then $(b - a)$ is also divisible by n

(iii) If $a - b$ is divisible by n, $a - b = qn$

and $b - c$ is divisible by n, $b - c = q'n$

on adding $a - c = (q + q')n$

$\therefore a \equiv c \pmod n$

(iv) $a - b = q, n, c - d = q_2 n$

$a + c - b - d = (q_1 + q_2)n$

$(a + c) - (b + d) = (q_1 + q_2)n$

$\therefore a + c \equiv (b + d) \pmod n$

Similarly proof of other parts follow:

The first three parts of theorem suggest that the a b (mod n) is an equivalence relation and hence sets a partition in the set of integers.

1.2.2 Some Applications of Congruences

1. We show that $2^{20} - 1$ is divisible by 41. We begin by noting that

$2^5 \equiv -9 \pmod{41}$ $(2^5 - (-9)$ is divisible by 41)

$\therefore (25)^4 \equiv (-9)^4 \pmod{41}$ (by last part of previous theorem)

or 20

$2 \equiv 81.81 \pmod{41}$

but $81 \equiv (-1)(-1) \pmod{41}$

$\equiv 1 \pmod{41}$

Using these

$2^{20} \equiv 1 \pmod{41}$

$\therefore 2^{20} - 1$ is divisible by 41

Thus 41 divides $2^{20} - 1$

2. Let us find the remainder which we get when

$|\underline{1} + |\underline{2} + |\underline{3} + \ldots\ldots\ldots\ldots + |\underline{100}$ is divided by 12.

Since $|\underline{4} = 24$ and this leaves no remainder when divided by 12, hence

$|\underline{K} = |\underline{4.5.6}\ldots\ldots\ldots\ldots K \equiv 0 \pmod{12}$

$|\underline{1} + |\underline{2} + |\underline{3} + |\underline{4} + |\underline{5} + \ldots\ldots\ldots\ldots + |\underline{K} \equiv |\underline{1} + |\underline{2} + |\underline{3} \pmod{12}$

$+ 0 + 0 \ldots\ldots\ldots$

$\equiv 9 \pmod{12}$

Hence 9 is the remainder we got when

$|\underline{1} + |\underline{2} + |\underline{3} + \ldots\ldots\ldots\ldots + |\underline{100}$ is divided by 12.

Theorem : If $ca \equiv cb \pmod n$ then

$a \equiv b \pmod{n/d}$ where

$d = g\,c\,d\,(c, n)$

Proof: Since ca $\equiv$ cb (mod n)

$\therefore$ ca – cb = kn

c (a – b) = kn, for some integer k.

Since g c d of c & n = d,

so c = dr,

n = ds where r and s are primes

so dr (a – b) = kds

r (a – b) = ks

Hence s divides r (a – b)

and g c d of (r, s) = 1

Hence Theorem gets proved.

Cor. 1. I ca $\equiv$ cb (mod n) and gcd (c, n) = 1, then

a $\equiv$ b (mod n)

Exercise :

Use the thoery of Congruence to show that

89 divides $2^{11} - 1$

and 97 divides $2^{48} - 1$

Consider the congruence 33 $\equiv$ 15 (mod 9)

or

3.11 = 15 (mod 9)

c = 3, a = 11, b = 5 n = 9

Now, 3.1 $\equiv$ 3.5 (mod 9) and gcd (3, 9) = 3

So, by the application of previous theorem

of 11 $\equiv$ 5 mod (3).

Example : Find the remainder when 2^{50} is divided by 7

Now $2^3 = 1$ (mod 7)

$(2^3)^{16} = 1$ (mod 7)

$2^{48} = 1$ (mod 7)

$2^{50} = 4$ (mod 7)

Hence 4 is the remainder when 2^{50} is divided by 7.

Definition : ϕ (n) is the number of positive integers $\equiv$ n and coprime to n. For exmple

ϕ (1) = 1

ϕ (4) = 2 [1, 3 are two +ve integers < 4 and coprine to 4]

ϕ (6) = 2 [1, 5 are two positive integers < 6 and coprime to 6]

ϕ (10) = 4 [1, 3, 7, 9 satisfy the condition]

ϕ (n) : Euler function

1.2.3 Euler-Fermat's theorem : If a is any integer and n is a +ve integer such that (a, n) = 1

then $a^{\phi(n)} \equiv 1 \pmod{n}$

Proof : Lemma : If $a_1, a_2, \ldots\ldots, a_{\phi(n)}$ is reduced residue system modulo (RRS). mod n s.t

$a_1, a_2, \ldots\ldots\ldots a_{\phi(n)} < n$ and

$b_1, b_2, \ldots\ldots\ldots, b_{\phi(n)}$ is another RRS (mod n) then one bj is congruent to exactly one

Proof : Let bj be one number among $b_1, b_2, \ldots\ldots\ldots, b_{\phi(n)}$

Now bj, n are integers such that n > o

By division algorithm, integers q and r are such that

bj = nq + r; o $\uparrow$ r – n

Now (bj, n) = 1 $\uparrow$ r $\uparrow$ 0

$\Leftrightarrow$ r is a +ve integer < n

Also bj $\uparrow$ r (mod n)

(bj, n) = (r, n)

$\uparrow$ 1 = (r, n) $\uparrow$ (r, n) = 1

so r is any one of $a_1, a_2, \ldots\ldots a_{\phi(n)}$

say r = ay

$\uparrow$ bj $\uparrow$ a_i (mod n)

Hence one bj is congruent to some a_i (mod n)

If br and bi are two distinct numbers among

$b_1, b_2, \ldots\ldots\ldots b_{\phi(n)}$ such that

$b_r \uparrow a_i$ (mod n) and b_t = ai (mod n)

then $b_t = b_i$ (mod n)

which is a contradiction

(since $b_1, b_2, \ldots\ldots\ldots b_{\phi(n)}$ is RRS (mod n)

Hence one bj is congruent to exactly one oi (mod n)

Main proof:

Let $a_1, a_2 \ldots\ldots\ldots\ldots, a_{\phi(n)}$ be a RRS (mod n)

since (a, n) = 1

$\uparrow aa_1, aa_2 \ldots\ldots\ldots, a_{\phi(n)}$ is also a RRS (mod n)

By lemmea one number among $aa_1, aa_2, \ldots\ldots\ldots, aa_{\phi(n)}$ is congruent to exactly one of $a_1, a_2 \ldots\ldots\ldots, a_{\phi(n)}$ (mod n)

$\uparrow aa_1, aa_2, \ldots\ldots\ldots, aa_{\phi(n)} = a_1, a_2 \ldots\ldots\ldots\ldots a_{\phi(n)}$ mod (n)

$\uparrow a^{\phi(n)}\ a_1, a_2, \ldots\ldots\ldots\ a_{\phi(n)} = a_1, a_2 \ldots\ldots\ldots\ldots a_{\phi(n)}$ mod (n)

Since $a_1, a_2, \ldots\ldots\ldots, a_{\phi(n)}$ is RRS (mod n)

$\uparrow a_1, a_2, \ldots\ldots\ldots\ldots, a_{\phi(n)}$ are coprime to n

$\Leftrightarrow (a_1, a_2, \ldots\ldots\ldots, a_{\phi(n)}) = 1$

Hence $a^{\phi(n)} = 1$ (mod n)

Cor 1. Fermat's theorem : If p is any prime number s.t p a then $a^{p-1} = 1$ (mod p)

Proof : Now p a $\uparrow$ (a, p) = 1

By Euler-Fermat's theorem

$a^{\phi(n)} = 1$ (mod p)

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

$\uparrow a^p \uparrow a$ (mod p)

Case 2 : If p/a then p/a^p

$\Leftrightarrow p/a^p - a \uparrow a^p \uparrow a$ (mod p)

Hence in each case $a^p \uparrow a$ (mod p)

Applications of Fermet's theorem:

Prove that 42 divides $n^7 - n$ for every integer n.

Now 42 = 6, 7 and $n^7 - n = n(n-1)(n+1)(n^4 + n^2 + 1)$

$= (n-1)n(n+1)(n^4 + n^2 + 1)$

Now n – 1, n, n + 1 three consecutive integers

$\Leftrightarrow \uparrow$ 3 divides $(n-1)n(n+1)$

or 6 divides $(n-1)n(n+1)$

$\Leftrightarrow$ 6 divides $(n-1)n(n+1)(n^4 + n^2 + 1)$

$\Leftrightarrow$ 6 divides $n^7 - n$ by Fermet's the $n^7 \uparrow m$ (mod 7)

$\Leftrightarrow 7/n^2 - n$

Also (6, 7) = 1

Hence $6, 7/n^7 - n$

$\Leftrightarrow$ 42 divides $n^7 - n$ for every integer.

Example : What is the last digit in ordinary decimal representation of 3^{400}, Now $10 = 2 \times 5$

Since $(3, 5) = 1$

By Fermet's theorem

$3^{5-1} \uparrow 1 \pmod 5$

$3^4 \uparrow 1 \pmod 5$

Also $3^4 \uparrow 1 \pmod 2$

Since $(2, 5) = 1$

$\Leftrightarrow 3^4 \uparrow 1 \pmod{2.5}$

$3^4 \uparrow 1 \pmod{10}$

Raise power 100

$(3^4)^{100} = [1 \pmod{10}]^{100}$

$3^{400} = 1 \pmod{10}$

$\uparrow$ 1 is the last digit in decimal representation of 3^{400}

Example : Find the last positive remainder when $(583)^{351}$ is divided by 91.

Now $91 = 7.13$

$583 = 2 \pmod 7$

$(583)^{34} = 2^{361} \pmod 7$ ......(i)

Since $(2, 7) = 1$

By Fermet's theorem

$2^{7-1} \uparrow 1 \pmod 7$

$2^6 \uparrow 1 \pmod 7$

$2^{360} = 1^{60} \pmod 7$

$2^{361} = 2 \pmod 7$ ....(ii)

$(583)^{361} = 2 \pmod 7$

$(583)^{361} = 2$ or 0 or 16 or 23 or 30 or 37 or $44 \pmod 7$

Again $583 \uparrow 11 \pmod{13}$

$(583)^{361} = 11^{361} \pmod{13}$

Since $(11, 13) = 1$

By Fermet's theorem, we have

$11^{13-1} \uparrow 1 \pmod{13}$

$11^{12} \uparrow 1 \pmod{13}$

$11^{360} = 1^{30} \pmod{13}$

$= 1 \pmod{13}$

By (4) and (5), we have

$(583)^{361} = 11 \pmod{13}$

$(583)^{361} = 11$ or 24 or $37 \pmod{13}$

by (3) $(583)^{361} = 37 \pmod 7$

$(583)^{361} = 37$ (mod (3) when $(7, 13) = 1$

$(583)^{361} = 37 \pmod{7.13}$

$(583)^{361} = 37 \pmod{91}$

⇔ 37 is the least positive remainder when $(583)^{361}$ is divided by 91.

1.2.4 Theorem : Wilson's theorem. If p is a prime number, then ↑ p – 1 ↑ – (mod p).

Proof : If p = 2, then the given congruence becomes

↑ 2 – 1 ↑ – 1 (mod 2) i.e. 1 ↑ – 1 (mod 2), which is true.

If p = 3, then the given congruent becomes ↑ 3 – 1 = –1 (mod 3) i.e. 2↑ – 1 (mod 3) is which is tru e.

Theorem is verified for p = 2 and p = 3.

For p ↑ 5, consider a set

G = {1, 2, 3, ..., p – 1}

Let at ↑ G be any number then (a, p) = 1

⇔ The congruence ax ↑ 1 (mod p) has exactly one incoguent solution say, 'a' as solution of their congruence.

If a′ = 0, then a.i ↑ 1 (mod p)

i.e. 0↑ 1 (mod p), which is not true

⇔ a′ ↑ G

Thusifa ↑ G, this a′ ↑ G s.t

aa′ ↑ 1 (mod p)

Now a′ = a if a^2 ↑ 2 (mod p)

i.e. if p/a^2 – i.e. p/(a – 1) (a + 1)

i.e. if p/a – 1 or p/a + 1

but p/p

↑ p/a – 1 or p/p – (a + 1)

i.e. p/a – or p/(p – 1) – a

Now (a – 1) is one among 0, 1, 2, ..., (p – 2).

⇔ p/a – 1 ↑ a – 1 = 0 ↑ a = 1

Again (p – 1) – a is one among 0, 1, 2, ..., (p – 2).

⇔ p/(p – 1) – a ↑ (p – 1) – a = 0 ↑ a = p – 1

⇔ a′ = a if a = 1 or (p – 1)

Let G_1 = {2, 3, 4, 5, ..., p – 2}

⇔ ∀ a ↑ G_1, | a′ ↑ in G_1 such that

aa′ ↑ 1 (mod p)

⇔ G_1 can be arranged as

$$\left\{-_1\alpha_1^1, \alpha_2^1, -_2, \ldots\ldots, -_i, \alpha_i^1\right\} \text{ where } i = \frac{p-3}{2}$$

$-_1\alpha_1^1 \uparrow\ 1 \pmod p$

$-_2\alpha_2^1 \uparrow 1 \pmod p$

$-_1\alpha_1^1 \uparrow\ 1 \pmod p$

$\Leftrightarrow$ 2.3.4 .... $(p-2)\uparrow\ -_1\alpha_1^1\ -_2\ \alpha_2^1$..............,$-_1$, α_1^1

$\uparrow$ 1.1..........1 (mod p)

$\uparrow\ \uparrow\ p-2\ \uparrow\ 1 \pmod p$

$(p-1)\uparrow p-2\uparrow (p-1) \pmod p$

$\uparrow p-1\uparrow (p-1) \pmod p$

But $p-1=-1 \pmod p$

$\Leftrightarrow \uparrow p-1\uparrow\ -1 \pmod p$

Hence Wilson's theorem is proved.

Converse of Wilson's theorem.

If $\uparrow n-1\ \uparrow\ -1 \pmod n$, then n is prime number.

Proof : If possible, let n be composite number. say, $n = mk$ where $1 < m,\ k < n$

$\uparrow m/n$

Now $\uparrow n-1\uparrow\ -1 \pmod n$

$n/\uparrow\ n-1 =\ +1$

by (1) and (2), $m/\uparrow\ n-1+1$

but $m < n\uparrow\ m\uparrow\ n-1\uparrow\ m/\uparrow\ n-1$

by the last two results,

$m/\uparrow\ n-1$

i.e. m/1, which is impossible

$\Leftrightarrow$ n is a prime number.

Example : Prove that $\uparrow 18 + 875\uparrow 0 \pmod{437}$

Now $437\uparrow\ 19.23$

Since 19 is a prime number

$\Leftrightarrow$ by Wilson's theorem

$\uparrow\ 19-1\uparrow\ -1 \pmod{19}$

$\uparrow\ \uparrow\ 18+1\uparrow 0 \pmod{19}$

Again 23 is a prime number,

by Wilson's theorem

$\uparrow 23-1\uparrow\ -1 \pmod{23}$

$\uparrow 22\uparrow\ -1 \pmod{23}\uparrow\ (22.21.20)\uparrow\ 18\uparrow\ -1 \pmod{23}$

$(-1)(-2)(-3)(-4)\uparrow\ 18\uparrow\ -1 \pmod{23}$

$24\uparrow\ 18\uparrow\ -1 \pmod{13}\ (24\uparrow\ 1 \pmod{23}$

$\uparrow\ 18\ 1.\uparrow\ 18\uparrow\ -1 \pmod{23}\ \ 1 \pmod{23}$

↑ 18 + 1↑ 0 (mod 23)

Since (19, 23 = 1

by (1) and (2) ↑ 18 + 1↑ 0 (mod 19.23)

i.e.↑ 18 + 1↑ 0 (mod 437)

874↑ 0 (mod 437)

Adding last two results, we set

↑ 18 + 875↑ 0 (mod 437)

Def. Fermat number : A number of the form Fn = $2^{2^n} + 1$, n↑ 0 is called a Fermat number, if Fn is prime then Fn is Fermat prime

$F_0 = 2^{2^0} + 1 = 3$ $F_2 = 2^{2^2} + 1 = 17$

$F_1 = 2^{2^1} + 1 = 5$ $F_3 = 2^{2^3} + 1 = 257$

$F_4 = 2^{2^4} + 1 = 2^{16} + 1$

Note : F_5 is not prime (Check).

Check that F_5 is divisible by 641 and the last last of F_5 is 7.

LESSON NO. 2.1 **Author : Dr. Chanchal**

CRYPTOGRAPHY AND ARITHMETIC FUNCTIONS

Structure :

2.1.0 Objectives

The prime goal of this unit is to enlighten the basic concepts of cryptography, arithmetic functions, primitive roots, indices and quadratic residues with the knowledge of quadratic reciprocity law. During the study in this particular lesson, our main objectives are

* To learn how to convert plain text into Cipher text using Caesar Ciphers and RSA public-key algorithm.
* To discuss about several kinds of arithmetic functions such as d(n), σ(n), μ(n), ϕ (n) and to discuss the important results and definitions based on these arithmetic functions.

2.1.1 Introduction :

Firstly, we give a brief introduction to cryptography and arithmetic functions.

Cryptography is the science of making communications through secret codes. The secret codes are known as ciphers and the message which is to be transmitted is known as plain text. The process of converting the plain text to a secret form (ciphertext) is known as Encryption (or Enciphering) and the reverse process for the conversion of ciphertext to plaintext is called Decryption (or Deciphering).

Julius Caesar introduced a system of cryptography in which each letter of the alphabet is replaced by the letter which occurs three places forward to the alphabet and the last three letters are replaced with the first three letters. Such type of system is known as Caesar cipher.

For example,

Plain Text	:	ZEBRA	MATHEMATICS
Cipher Text	:	CHEUD	PDWKHPDWLFV

Arithmetic Functions :

In brief, on arithmetic function 'f' may be defined as those function whose domain is the set of positive integers and whose range is a subset of the complex numbers. These functions are also called number theoretic functions, or simply numerical functions.

2.1.2 Linear Cipher

If x is a digit of plain text and y is a digit of cipher text, then the congruence $y \equiv ax + b \pmod{26}$, where a, b are integers with (9, 26) = 1 is known as linear cipher.

2.1.3 RSA Public-Key Algerithm

Let p and q be two distinct primes large enough such that n = pq, where n is known as enciphering modulus. Choose enciphering component k such that $(k\ \phi(n))=1$. Then, the pair (n, k) is known as user's encryption key.

The standard procedure of ciphering process starts from the conversion of message into an integer M with the help of digital alphabet in which each letter, number or punctuation mark of the plain text is replaced by a two digit integer, as explained below :

A	B	C	D	E	F	G	H	I	J	K	L	M	
01	02	03	04	05	06	07	08	09	10	11	12	13	
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
14	15	16	17	18	19	20	21	22	23	24	25	26	
,	×	?	0	1	2	3	4	5	6	7	8	9	!
27	28	29	30	31	32	33	34	35	36	37	38	38	40

Also, the two digits 00 indicates the space between words.

2.1.3.1 Working Method for Converting Plain Text into Cipher Text Using RSA System

1. Select two primes p and q such that the enciphering modulus is n=pq.
2. Choose enciphering exponent k among the prime factors of $\phi(n) + 1$.
3. Find the recovery exponent j satisfying $jk \equiv 1 \ (\text{mod.}\phi(n))$.
4. Transform the given message into plain text number M. If m > n, then split M into blocks $M_1, M_2, \ldots\ldots M_t$ such that $M_i < M$ for i = 1, 2,.....t.
5. Let $M_i^K \equiv r_i$ (mod. n) for i = 1, 2, ... t.
   Then, the cipher text is $r_1\, r_2 \ldots\ldots\ldots r_3$.
6. To recover plain text number, compute.
   $r_i^{\,j} \equiv M_i$ (mod n) and we get $M = M_1\, M_2 \ldots\ldots\ldots M_t$.

Example 1 : Encrypt the message RETURN HOME using caesar cipher.

Sol. : Numerically, RETURN HOME is written as

x : 18 05 20 21 18 14; 11 18 16 08

using the congruence $y \equiv x + 3$ (mod. 26)

y = 21 08 23 24 21 17; 11 18 16 08

Cipher text : UHWXUQ K RPH

Note : In caesar cipher, the alphabets are also written digitally as mentioned under the RSA public key algorithm and the space is represented by ';'. Also, if x is a digit of plain text and y is the corresponding digit of cipher text in caesar cipher, then

$y \equiv x + 3$ (mod 26) and $x \equiv y - 3$ (mod. 26)

Example 2 : Encrypt the message NO WAY using the RSA system with key (n, k) = (1537, 47)

Sol. : Here, n = 1537 = 29 × 53

$\therefore$ $\phi(n) = \phi(29)\,\phi(53) = 28\times52 = 1456$

$\Rightarrow$ $\phi(n) + 1 = 1457 = 31\times47$

Here, K = 47 and $jk \equiv 1$ (mod. $\phi(n)$)

$\Rightarrow$ $47j \equiv 1$ (mod 1456)

$\Rightarrow$ The recovery exponent j = 31.

Numerically, NO WAY can be written as M = 141500230125 clearly, M > n. So, split M into blocks of three digit numbers as 141 500 230 125

$$141^{47} \equiv 658 \ (\text{mod } 1537),\ 500^{47} \equiv 1408 \ (\text{mod } 1537)$$

$$230^{47} \equiv 1250 \ (\text{mod } 1537),\ 125^{47} \equiv 1252 \ (\text{mod } 1537)$$

$\therefore$ In RSA system, the given message is written as

0658 1408 1250 1252.

2.1.4 Arithmetic Functions

A real or complex valued function defined on the set of positive integers is known as Arithmetic function or number theoretic or numerical function.

For a positive integer n,

d (n) denote the number of positive divisors of n and

$\sigma(n)$ denote the sum of positive divisors of n.

Mathematically, $d(n) = \sum_{d/n} 1$ and $\sigma(n) = \sum_{d/n} d$.

2.1.4.1 Multiplicative Function

An arithmetic function f which is not identically zero, is said to be multiplicative if f(mn) = f(m) f(n) for (m, n) = 1.

If f(mn) = f(m) f(n) for all m, n then f is said to be totally multiplicative or completely multiplicative.

If f is a multiplicative function, then

f (n) = f(n. 1) = f(n) f(1) $(\because (n,1) = 1)$

But f(n) $\neq$ 0 for any n, so f(1) = 1

2.1.4.2 The Mobius Function $\mu(n)$

It may be defined as :

$$\mu(n) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } p^2 / n \text{ for some prime p} \\ (-1)^k \text{ if } n = p_1 p_2 - p_k \text{ where } p_i\text{'s are different primes} \end{cases}$$

Some Important Numbers

1. An integer is called square free if it is not divisible by the square of any integer > 1.
2. An integer n > 1 is said to be a perfect number if it is the sum of its divisors other than itself. For example : 6 = 1 + 2 + 3

2.1.5 Some Important Results

Theorem 1 : For every positive integer n > 1, prove that

(i) $d(n) = \prod_{p^\alpha \| n} (\alpha + 1)$ (ii) $\sigma(n) = \prod_{p^\alpha \| n} \left(\frac{p^{\alpha+1} - 1}{p - 1} \right)$

Where $p^{\alpha \| n}$ indicates that $p^\alpha | n$ but $p^{\alpha+1} \nmid n$.

Proof : (i) Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_k^{\alpha_k} = \prod_{i=1}^{K_1} p_i^{\alpha_i}$ be the canonical form of n.

$\therefore$ The positive divisors of n are of the form $d = \prod_{i=1}^{K} p_i^{\beta_i}$ where $0 \leq \beta_i \leq \alpha_i$ for all $i = 1, 2, \ldots\ldots, k$.

$\Rightarrow$ There are $\prod_{i=1}^{K}(\alpha_i + 1)$ possible divisers of n because there are $\alpha_i + 1$ possible values for β_i, i = 1, 2, ... k which are 0, 1, 2, ... α_i.

$$\Rightarrow \quad d(n) = \prod_{i=1}^{K}(\alpha_i + 1) = \prod_{p^\alpha \| n}(\alpha + 1)$$

(ii) Since $n = \prod_{i=1}^{K} p_i^{\alpha_i}$ is the canonical form of n.

$\therefore$ Each positive divisor of n appears only single time in the expansion of the product.

$$\left(1 + p_1 + p_1^2 + \ldots\ldots\ldots + p_1^{\alpha_1}\right)\left(1 + p_2 + p_2^2 + \ldots\ldots\ldots + p_2^{\alpha_2}\right) + \left(1 + p_k + p_k^2 + \ldots\ldots\ldots + p_k^{\alpha_k}\right)$$

Also, every divisor of n is of the form $\prod_{i=1}^{k} p_i^{\beta_i}$, $0 \leq \beta_i \leq \alpha_i$. Therefore, we can observe that d is among the terms of above product and all these terms are distinct.

Therefore, $\sigma(n) = \prod_{i=1}^{k}\left(1 + p_i + p_i^2 + \ldots\ldots + p_i^{\alpha_i}\right)$

$$= \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} = \prod_{p^\alpha \| n} \frac{p^{\alpha+1} - 1}{p - 1}$$

Theorem 2 : Show that d(n) and $\sigma(n)$ are multiplicative functions.

Proof : Let (m, n) = 1

For m = n = 1 d(mn) = d(1) = 1 = d(1) d(1) = d(m) d(n)

and $\sigma(mn) = \sigma(1) = 1 = \sigma(1)\,\sigma(1) = \sigma(m)\,\sigma(n)$

For n = 1, m $\neq$ 1 (or m = 1, n $\neq$ 1)

d(mn) = d(m) = d(m) d(1) = d(m) d(n)

and $\sigma(mn) = \sigma(m) = \sigma(m)\,\sigma(1) = \sigma(m)\,\sigma(n)$

For m > 1, n > 1.

Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p_k^{\alpha_k}$ and $n = q_1^{\beta_1} q_2^{\beta_2} \ldots\ldots\ldots q_l^{\beta_l}$

be the canonical forms of m and n.

Because (m, n) = 1, therefore all the p_i's are different from q_j's and canonical form of mn can be expressed as

$$mn = p_1^{\alpha_1} p_2^{\alpha_2} .... p_k^{\alpha_k}\ q_1^{\beta_1} q_2^{\beta_2} .... q_l^{\beta_l}$$

$\Rightarrow$ $d(mn) = (\alpha_1 + 1)(\alpha_2 + 1) .... (\alpha_{k+1})(\beta_1+1)(\beta_2 + 1) .... (\beta_l + 1)$

$= d(m)\, d(n)$

and $$\alpha(mn) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} ..... \frac{p_2^{\alpha_2+1}-1}{p_2-1} ..... \frac{p_k^{\alpha_k+1}-1}{p_k-1} \cdot \frac{q_1^{\beta_1+1}-1}{q_1-1} \cdot \frac{q_2^{\beta_2+1}-1}{q_2-1} ...... \frac{q_l^{\beta_l+1}-1}{q_l-1}$$

$= \sigma(m)\, \sigma(n)$

$\therefore$ d and σ are multiplicative functions.

Self Prove Results :

1. Prove that mobius function μ is multiplicative.
2. Let (m, n) = 1 and d/mn. Then, $d = d_1 d_2$ such that d_1/m, d_2/n and $(d_1, d_2) = 1$.
3. If f is a multiplicative function and n > 1 has canonical form

   $$n = \prod_{i=1}^{k} p_i^{\alpha_i},\ \alpha_i > 0 \text{ then, } f(n) = \prod_{i=1}^{k} f\left(p_i^{\alpha_i}\right).$$

4. If f is a multiplicative function and $f(n) = \sum_{d/n} f(d)$. Then, F is also multiplicative.
5. For each +ve integer n ≥ 1,

   $$\sum_{d/n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

6. For each n ≥ 1, $\phi(n) = \sum_{d/n} \mu(d) \dfrac{n}{d}$.

Theorem 3 (Mobius Inversion Formula) : Let F and f are two arithmetic functions. For every integer n_1 if

$$F(n) = \sum_{d/n} f(d), \text{ then } \qquad f(n) = \sum_{d/n} \mu(d)\, F(n/d)$$

Proof : $\sum_{d/n} \mu(d)\, F(n/d) = \sum_{d/n} \mu(d) \left(\sum_{k/(n/d)} f(k) \right)$

$$= \sum_{d/n} \sum_{k/(n/d)} \mu(d)\, f(k)$$

Since d/n and $k/(n/d) \Rightarrow k/n$ and $d/(n/k)$

$$\Rightarrow \quad \sum_{d/n} \mu(d)\, F(n/d) = \sum_{k/n} \left(\sum_{d/(n/k)} \mu(d)\, f(k) \right)$$

$$= \sum_{k/n} \left(f(k) \sum_{d/(n/k)} \mu(d) \right) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Also, we know that $\sum_{d/(n/k)} \mu(d) = \begin{cases} 1 & \text{if } \frac{n}{k} = 1 \text{ or } n = k \\ 0 & \text{if } \frac{n}{k} > 1 \text{ or } n > k \end{cases}$

Taking k = n in (1), we have

$$\sum_{d/n} \mu(d)\, F(n/d) = \sum_{k=n} f(k) \times 1 = f(n).$$

Example 3 : Verify Mobines Inversion Formula for n = 24.

Sol. Let $F(24) = \sum_{d/24} f(d)$ where F and f are two arithmetic functions.

$\therefore \quad \sum_{d/24} \mu(d)\, F(n/d) = \mu(1)\, F(24) + \mu(2)\, F(12) + \mu(3)\, F(8) + \mu(4)\, F(6) + \mu(6)\, F(4) + \mu(8)\, F(3)$

$+ \mu(12)\, F(2) + \mu(24)\, F(1)$

$= F(24) - F(12) - F(8) + 0 + F(4) + 0+0+0$

$= \sum_{d/24} f(d) - \sum_{d/12} f(d) - \sum_{d/8} f(8) + \sum_{d/4} f(d)$

$= f(1) + f(2) + f(3) + f(4) + f(6) + f(8) + f(12) + f(24)$

$- f(1) - f(2) - f(3) - f(4) - f(6) - f(12)$

$- f(1) - f(2) - f(4) - f(8) + f(1) + f(2) + f(4)$

$= f(24)$

So, Mobius Inversion Formula is verified for n = 24.

2.1.6 Euler's ϕ Function

For $n \geq 1$, $\phi(n)$ represents the number of positive integers less than or equal to n which are relatively prime to n.

Also, for any prime number p, $\phi(p) = p - 1$ and ϕ is also multiplicative function (Prove yourself).

2.1.6.1 Gauss Theorem : For any positive integer $n \geq 1, n = \sum_{d/n} \phi(d)$.

Proof : For $n = 1, \sum_{d/n} \phi(d) = \sum_{d/1} \phi(d) = \phi(1) = 1 = n$

$\therefore$ the result is true for n = 1.

For n > 1, Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_k^{\alpha_k}$ be the canonical form of n.

Let $F(n) = \sum_{d/n} \phi(d)$ and F is multiplicative since ϕ is multiplicative function.

$$\therefore \quad F(n) = F\left(p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_k^{\alpha_k}\right) = F\left(p_1^{\alpha_1}\right) F\left(p_2^{\alpha_2}\right) \ldots\ldots F\left(p_k^{\alpha_k}\right)$$

Now, $$F\left(p^{\alpha}\right) = \sum_{d/p^{\alpha}} \phi(d) = \phi(1) + \phi(p) + \phi(p^2) + \ldots\ldots + \phi(p^{\alpha})$$

$$= 1 + (p - 1) + (p^2 - p) + \ldots\ldots\ldots + (p^{\alpha} - p^{\alpha-1}) = p^{\alpha}$$

$$\therefore \quad F(n) = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p_k^{\alpha_k} = n$$

or $$n = \sum_{d/n} \phi(d).$$

2.1.6.2 Some Useful Results :

(1) For any +ve integer n_1

(i) $\sum_{d/n} \phi\left(\frac{d}{n}\right) = n$ (ii) $\phi(n) = \sum_{d/n} \mu(d) \frac{n}{d} = \sum_{d/n} d\mu\left(\frac{n}{d}\right)$

(2) $\phi(n)$ is an even integer for all $n \geq 3$.

Example 4 : Find all possible values of n which satisfies $\phi(n) = 91$.

Sol. We know, for $n \geq 3$, $\phi(n)$ is even and

$\phi(n) = 1$ for $n = 1$ or 2.

$\therefore$ $\phi(n) = 91$ has no solution.

Example 5 : Find the values of d(180) and σ(180).

Sol. Since $180 = 2^3.3^2.5^1$ is the canonical form of 180.

$\therefore$ $d(180) = (2 + 1)(2 + 1)(1 + 1) = .18$

and $$\sigma(180) = \frac{2^3-1}{2-1}.\frac{3^3-1}{3-1}.\frac{5^2-1}{5-1} = 7.13.6 = 546$$

Example 6 : For all $n \geq 1$, show that $\sigma(12n -) \equiv 0 \pmod{12}$.

Sol. Let the positive divisors of 12n–1 in ascending orders are

$$d_1 d_2, \ldots\ldots\ldots, \frac{12n-1}{d_2}, \frac{12n-1}{d_1}$$

$$\therefore \quad \sigma(12n-1) = d_1 + d_2 + \ldots.. + \frac{12n-1}{d_2} + \frac{12n-1}{d_1}$$

$$= \left(d_1 + \frac{12n-1}{d_1}\right) + \left(d_2 + \frac{12n-1}{d_2}\right) + \ldots\ldots\ldots$$

$$= \frac{d_1^2 + 12n - 1}{d_1} + \frac{d_2^2 12n - 1}{d_2} + \ldots\ldots..$$

$$= \sum_{d/12n-1} \frac{d^2 + 12n - 1}{d}$$

Since $d/12n–1 \Rightarrow (d, 12) = 1$ $\left[\begin{array}{l} \because \text{if } (d,12) = g, \text{ then} \\ g/12n-1 \text{ and } g/12n \\ \Rightarrow g/1 \text{ or } \quad g = 1 \end{array}\right]$

Now, By Format's Theorem

$d^2 \equiv 1 \pmod 3$ and $d^2 \equiv 1 \pmod{4} \Rightarrow d^2 \equiv 1 \pmod{12}$

$\Rightarrow$ $d^2 + 12n - 1 \equiv 0 \pmod{12}$

Also, $d^2 + 12n - 1 \equiv 0 \pmod{d}$

Since $d/d^2 + 12n–1$ and $(d, 12) = 1$

$\Rightarrow$ $d^2 + 12n - 1 \equiv 0 \pmod{12d}$

$$\Rightarrow \quad \frac{d^2 + 12n - 1}{d} \equiv 0 \pmod{12}$$

$\Rightarrow \quad \sum_{d/n} \frac{d^2 + 12n - 1}{d} \equiv 0 \ (\text{mod}.12)$

$\Rightarrow \quad \sigma(12n - 1) \equiv 0 \ (\text{mod. } 12).$

Example 7 : Prove that $\mu(n)\ \mu(n + 1)\ \mu(n + 2)\ \mu(n + 3) = 0$ for any +ve integer n.

Sol. Since n is a +ve integer.

$\therefore$ By division algorithm, $n = 4q + r$; $r = 0, 1, 2, 3$ and q is an integer.

$\therefore$ Any +ve integer n is of the form

$4q, 4q + 1, 4q + 2, 4q + 3.$

If $n = 4q$, then $4/n$

If $n = 4q + 1$, then $4/n+3$

If $n = 4q+2$, then $4/n+2$

and if $n = 4q + 3$, then $4/n+1$.

Therefore, for any +ve integer n, $4 = 2^2$ divides either of $n, n+1, n+2, n+3$.

$\Rightarrow \quad \mu(n)\ \mu(n + 1)\ \mu(n + 2)\ \mu(n + 3) = 0$

2.1.7 Some Other Results and Definitions

Result : Let p denote a prime. Then, the largest exponent e such that $p^e | n!$ is

$$e = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$$

Definition : If $2^n - 1$ is a prime, then the numbers of the form $2^{n-1}(2^n - 1)$ is called Euclid Number.

Note : Every even perfect number is Euclid Number.

Definition : For any +ve integer n, $\sigma_k(n)$ denote the sum of k^{th} powers of the divisors of n.

or $\quad \sigma_k(n) = \sum_{d/n} d^k$

For example : $\sigma_2(3) = 1^2 + 3^2 = 1 + 9 = 10$

Example 8 : Find the highest power of 9 dividing 365 !

Sol. Since $9 = 3^2$

$\therefore$ Highest Power of 3 that divides 365 !

$$= \left[\frac{365}{3}\right] + \left[\frac{365}{9}\right] + \left[\frac{365}{27}\right] + \left[\frac{365}{81}\right] + \left[\frac{365}{283}\right] + \left[\frac{365}{729}\right]$$

$= 121 + 40 + 13 + 4 + 1 + 0 = 179$

$\therefore$ Highest Power of $9 = 3^2$ that divides $365! = \left[\frac{179}{2}\right] = 89$

Example 9 : Show that if the integer n has k distinct odd prime factors, then $2^k \mid \phi(n)$.

Sol. Let $n = p_1 p_2 \ldots\ldots\ldots\ldots p_k$ where pi's are distinct primes.

$\therefore$ $\phi(n) = \phi(p_1 p_2 \ldots\ldots\ldots\ldots p_k) = \phi(p_1)\,\phi(p_2) \ldots\ldots\ldots\ \phi(p_k)$

$= (p_1 = 1)(p_2 = 1) \ldots\ldots\ldots\ldots (p_k - 1)$

Since p_i is odd prime for all i = 1, 2, ...k.

$\Rightarrow$ $p_i - 1$ is even number for all i = 1, 2, ... k.

$\Rightarrow$ $2/p_i - 1 \;\forall\; i = 1, 2 \ldots\ldots\ldots k.$

$\Rightarrow$ $2^k \mid (p_1 - 1)(p_2 - 1) \ldots\ldots\ldots (p_k - 1)$

$\Rightarrow$ $2^k \mid \phi(n)$

2.1.8 Summary :

In this lesson, we have studied about the various techniques of cryptography that how we can convert the linear text into cipher text and how to encrypt the message from cipher text. We have also discussed in detail about the arithmetic functions and various useful results concerning these functions. Now, we have the enough knowledge to understand the further concepts of number theory that we will study in the coming part of this unit.

2.1.9 Self Check Exercise

1. Using linear cipher $C \equiv 5P + 11 \pmod{26}$, encrypt the message "NUMBER THEORY IS EASY".
2. Encrypt the message "SOFT TOY" using the RSA algerithm with key (n, k) = (3233, 37).
3. Show that d(n) is an odd integer iff n is a perfect square where n > 1 is an integer.
4. For all +ve integer n, show that $\sum_{d/n} \frac{1}{d} = \frac{\sigma(n)}{n}$
5. If n > 1 is an integer with canonical form $n = p_1^{\alpha 1} p_2^{\alpha 2} \ldots\ldots p_k^{\alpha k}$.

   Then show that $\sum_{a/n} \mu(a)\, d(a) = (-1)^k$.
6. Prove that for any +ve integer n,

   $$\sum_{d=1}^{n} \phi(d) \left[\frac{n}{d}\right] = \frac{n(n+1)}{2}$$

2.1.10 Suggested Readings :

1. Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery, An Introduction to the Theory of Numbers, Wiley-India Edition.
2. T.N. Apostal, An Introduction to Analytic Number Theory, Springer Verlag.

LESSON NO. 2.2 **Author : Dr. Chanchal**

PRIMITIVE ROOTS AND INDICES – I

Structure :

2.2.0 Objectives

The prime objective of this lesson is to discuss the concepts of primitive roots and polynomial congruences alongwith the study of important results and theorems concerning them. Further, to understand the applicability of results, several important examples are also discussed under this lesson.

2.2.1 Introduction

Before discussing the concept of primitive root, it is required to define the following concept :

Def. : Let m denote a positive integer and a be any integer such that (a, m) = 1. Let h be the smallest positive integer such that $a^h \equiv 1 \pmod{m}$. Then, we say that order of a modulo m is h or a belongs to the exponent h modulo m. It is denoted as $\text{ord}_m a$.

For Example : Order of 2 modulo 5 is 4 since $2^1 \equiv 2 \pmod 5$, $2^2 \equiv 4 \pmod 5$, $2^3 \equiv 3 \pmod 5$ and $2^4 \equiv 1 \pmod 5$.

It is **important to notice** that there may exist many such positive integers h such that $a^h \equiv 1 \pmod{m}$ but order of a modulo m is the smallest one. Further, we already know from the Euler's Fermat theorem that $a^{\phi(m)} \equiv 1 \pmod{m}$, so it is clear that order of a modulo m cannot exceed $\phi(m)$. Now, it is appropriate to discuss about the primitive roots.

2.2.2 Primitive Root

Def. : An integer g is called to be **primitive root modulo** m if order of g modulo m is ϕ (m).

For Example : 2 is the primitive root of 11, as discussed below :

Since, $2^1 \equiv 2$ (mod 11), $2^2 \equiv 4$ (mod 11), $2^3 \equiv 8$ (mod 11), $2^4 \equiv 5$(mod 11), $2^5 \equiv 10$ (mod 11), $2^6 \equiv 9$ (mod 11), $2^7 \equiv 7$ (mod 11), $2^8 \equiv 3$ (mod 11), $2^9 \equiv 6$ (mod 11) and $2^{10} \equiv 1$ (mod 11). So, order of 2 modulo 11 is 10 = ϕ (11). Thus, 2 is the primitive root of 11.

Note : (i) As $1^1 \equiv 1$ (mod m) and ϕ (m) ≥ 2 for all m ≥ 3. So, 1 cannot be the primitive root of any integer ≥ 3.

(ii) If g is the primitive root of m, then all integers of the residue class containing g are primitive roots of m.

2.2.3 Polynomial Congruences

Let m > 1 be a positive integer.

1. **Def :** If $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{n} b_i x^i$ are two polynomials with integral coefficients such that $a_i \equiv b_i$ (mod m) $\forall$ i = 0, 1, 2, ..., n, then f (x) $\equiv$ g (x) (mod m)

For example : $7x^3 + 4x^2 + 2x + 9 \equiv 11x^2 - 5x + 2$ (mod 7).

2. **Def :** Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be an integral polynomial such that $a_n \not\equiv 0$ (mod m). Then, we say that degree of f(x) is n (mod m).

3. **Def :** Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be an integral polynomial. An integer x = a is said to be a root of f(x) (mod m) iff f(a) $\equiv$ 0 (mod m).

For example : Readers may easily verify that x = 1, 2, –3 are the roots of $x^2 + 2x - 3$ (mod 5).

4. **Def :** Let f(x) and g(x) be two integral polynomials. Then we say f(x) is divisible by g(x) to modulus m if there exist an integral polynomial h(x) such that f(x) $\equiv$ g(x) h(x) (mod m) and we write g(x) | f(x) (mod m).

2.2.4 Some Important Theorems

Theorem 1 : If a $\equiv$ b (mod m) and $\text{ord}_m a = h$, then $\text{ord}_m b = h$.

Proof : Since $\text{ord}_m a = h$,

so $a^h \equiv 1$ (mod m)

Now a $\equiv$ b (mod m)

$\Rightarrow \quad a^h \equiv b^h \pmod m$

$\Rightarrow \quad 1 \equiv b^h \pmod m$

$\Rightarrow \quad b^h \equiv 1 \pmod m$

Suppose $b^k \equiv 1 \pmod m$ for any positive integer k

Then $a \equiv b \pmod m$

$\Rightarrow \quad a^k \equiv b^k \pmod m$

$\Rightarrow \quad a^k \equiv 1 \pmod m$

Since $\text{Ord}_m\, a = h$

$\therefore \quad h \le k$

Hence $\text{Ord}_m\, b = h$.

Theorem 2 :

If a has order h modulo m and k be a positive integer, then $a^k \equiv 1 \pmod m$ iff h/k.

Proof : Firstly let $h|k \therefore \exists\, h_1 \in Z$ such that $k = hh_1$

Since h is order of a (mod m)

$\equiv \quad a^h \equiv 1 \pmod m$

$$\Rightarrow \quad \left(a^h\right)^{h_1} \equiv 1 \pmod m$$

i.e. $a^{hh_1} \equiv 1 \pmod m$ or $a^k \equiv 1 \pmod m$

Conversely let $a^k \equiv 1 \pmod m$

Since h is order of a

$\therefore \quad h \le k$

By the division algorithm, $\exists$ integer q and r such that

$k = q\,h + r,\ 0 \le r < h$

$\therefore \quad a^{qh+r} \equiv 1 \pmod m$

$\Rightarrow \quad (a^h)^q \cdot a^r \equiv 1 \pmod m$

$\Rightarrow \quad a^r \equiv 1 \pmod m$

Since $0 \le r < h$ and h is the least positive integer such that

$a^h \equiv 1 \pmod m$

$\therefore \quad r = 0$

and hence $k = qh \quad \Rightarrow \quad h/k$.

Theorem 3 : If a has order h modulo m and b has order k modulo m such that (h, k) = 1, then ab has order hk modulo m.

Proof : Let r = order of ab modulo m. Then, $(ab)^r \equiv 1 \pmod m$

To prove r = hk

$(ab)^{hk} = a^{hk}\, b^{hk} = (a^h)^k\, (b^k)^h \equiv 1^k \cdot 1^h \pmod m$

i.e. $(ab)^{hk} \equiv 1 \pmod m$

$\therefore$ $r \mid hk$

Since $Ord_m b = k$, ... (1)

$b^k \equiv 1 \pmod m$

$\Rightarrow$ $b^{rk} \equiv 1 \pmod m$

$\Rightarrow$ $a^{rk} b^{rk} \equiv a^{rk} \pmod m$

$\Rightarrow$ $(ab)^{rk} \equiv a^{rk} \pmod m$

$\Rightarrow$ $a^{rk} \equiv \left((ab)^r\right)^k \pmod m$

$\Rightarrow$ $a^{rk} \equiv 1 \pmod m$

As Ord a = h, $h \mid rk$

Since (h, k) = 1, therefore $h \mid r$

Similarly we have $k \mid r$

Thus, hk/r ... (2)

So, (1) and (2) $\Rightarrow$ $r = hk$.

Theorem 4 : Let (g, m) = 1. Then g is a primitive root modulo m iff the numbers g, $g^2, \ldots, g^{\phi(m)}$ form a reduced residue system modulo m.

Proof : Firstly let g is primitive root mod m.

Since (g, m) = 1, $(g^k, m) = 1 \ \forall\, k \in \{1, 2, \ldots\ldots, \phi(m)\}$

Now $g^i \equiv g^j \pmod m$; $i, j \in [1, 2, \ldots\ldots, \phi(m)]$

$\Rightarrow$ $g^{i-j} \equiv 1 \pmod m$

$\Rightarrow$ $\phi(m) \mid i - j$

$\Rightarrow$ $\phi(n) \mid \mid i - j \mid$ $[\because$ order of g(mod m) is $\phi(m)]$

$\Rightarrow$ $i = j$ $[\because 1 \le i, j \le \phi(m)]$

Thus, (1) $g, g^2, \ldots\ldots\ldots g^{\phi(m)}$ are relatively prime to m

(2) they are $\phi(m)$ in numbers

(3) they are incongruent modulo m

Thus $g, g^2, \ldots\ldots\ldots, g^{\phi(m)}$ form a reduced residue system modulo m.

Conversely, let $\{g, g^2, \ldots\ldots, g^{\phi(m)}\}$ form a reduced residue system modulo m. Then (g, m) = 1 By

Fermat's theorem $g^{\phi(m)} \equiv 1 \pmod m$

Let $Ord_m g = h$

Then $g^h \equiv 1 \pmod m$

$\Rightarrow$ $g^h \equiv g^{\phi(m)} \pmod m$

Since $1 \le h \le \phi(m)$ and $\{g, g^2, \ldots\ldots, g^{\phi(m)}\}$ is rrs,

so $h = \phi(m)$

and hence g is primitive root mod m.

Cor. 1 : If an integer m has a primitive root, then there are $\phi(\phi(m))$ primitive roots of m.

Proof : Let g be a primitive root of m.

Then $g, g^2, \ldots\ldots, g^{\phi(m)}$ form a reduced residue system mod m.

Let a be any primitive root of m.

$\therefore$ $(a, m) = 1$

Since $g, g^2, \ldots\ldots, g^{\phi(m)}$ is RRS (mod m)

$\therefore$ $a \equiv g^r \pmod{m}$ for $r \in \{1, 2, \ldots\ldots, \phi(m)\}$.

Since a is primitive root of m

$\therefore$ g^r is also primitive root of m

$\Rightarrow$ g^r is of order $\phi(m) \pmod{m}$

Also $\quad \text{ord}(g^r) = \dfrac{\phi, (m)}{(r, \phi(m))}$

so $\quad \text{ord}(g^r) = \phi(m)$

iff $\quad (r, \phi(m)) = 1$

Thus $(r, \phi(m)) = 1$ where $r \in \{1, 2, \ldots\ldots, \phi(m)\}$

$\Rightarrow$ there are $\phi(\phi(m))$ choices of r

$\Rightarrow$ g^r has exactly $\phi(\phi(m))$ choices and hence m has exactly $\phi(\phi(m))$ primtive roots.

Cor. 2 : If a prime p has a primitive root, then it has exactly $\phi(p - 1)$ primitive roots.

Proof : We have seen that if an integer m has a primitive roots then it has exactly $\phi(\phi(m))$ primitive roots.

Take $m = p$ where p is a prime

Then $\phi(m) = \phi(p) = p - 1$

$\therefore$ $\phi(\phi(m)) = \phi(p - 1)$

Thus there are $\phi(p-1)$ primitive roots of prime p.

Theorem 5 (Lagrange's Theorem) : If p is a prime and degree of f(x) (mod p) is n, then $f(x) \equiv 0 \pmod{p}$ cannot have more than n incongruent solutions.

Proof : Let n = 1.

Then $f(x) = ax + b$, where $a \not\equiv 0 \pmod{p}$

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

and hence $f(x) \equiv 0 \pmod{p}$ has exactly one solution. We'll prove the theorem by induction on n.

Assume that the theorem is true for polynomials of degree $\leq n - 1$.

Let f(x) be of degree n (mod p)

Then either $f(x) \equiv 0 \pmod{p}$ has no solution or has solution

In the first case, we have nothing to do

In the second case, let x = a is a solution of $f(x) \equiv 0 \pmod{p}$

Then $f(a) = 0 \pmod{p}$

$\therefore$ $\exists$ an integral polynomial q(x) such that

$f(x) \equiv (x - a)\, q(x) \pmod{p}$

and $q(x)$ is of degree $n - 1 \pmod{p}$

Suppose $x = b$ is a solution of $f(x) \equiv 0 \pmod{p}$ other than a.

Then $f(b) \equiv 0 \pmod{p}$

and $(b - a)\, q(b) \equiv 0 \pmod{p}$

but $b \not\equiv 0 \pmod{p}$

$\therefore$ $q(b) \equiv 0 \pmod{p}$

$\Rightarrow$ b is a solution of $q(x) \equiv 0 \pmod{p}$

Thus any solution of $f(x) \equiv 0 \pmod{p}$

other than $x = a$ is also a solution of $q(x) \equiv 0 \pmod{p}$

Since $q(x)$ is of degree $\leq n - 1$

$\therefore$ $q(x)$ has at most $n - 1$ solutions mod p

Hence by induction, $f(x) \equiv 0 \pmod{p}$ cannot have more than n solutions.

Theorem 6 : If p is a prime and $d/p-1$, then $x^d - 1 \equiv 0 \pmod{p}$ has exactly d solutions.

Proof : Since $d | p-1$, so $\exists\, k \in Z$ such that

$p - 1 = dk$

$x^{p-1} - 1 = x^{dk} - 1 = (x^d)^k - 1$

$= (x^d - 1)\, (x^{d(k-1)} + x^{d(k-2)} + \ldots\ldots. + x^d + 1)$

$= (x^d - 1)\, (x^{p-1-d} + x^{p-1-2d} + \ldots\ldots. + x^d + 1)$

$x^{p-1} - 1 = (x^d - 1)\, h(x)$

where $h(x) = x^{p-1-d} + x^{p-1-2d} + \ldots\ldots. + x^d + 1$

Now, by Femat's Theorem

$x^{p-1} \equiv 1 \pmod{p}$ where $(x, p) = 1$

By Largrange's theorem, $x^{p-1} - 1 \equiv 0 \pmod{p}$ cannot have more than $p - 1$ solutions.

Also since $1, 2, \ldots\ldots\ldots., p-1$ are all incongruent solutions of $x^{p-1} - 1 \equiv 0 \pmod{p}$

therefore, $x^{p-1} - 1 \equiv 0 \pmod{p}$ has exactly $p - 1$ solutions

As $h(x) \equiv 0 \pmod{p}$ has at most $p - 1 - d$ solutions

so $x^d - 1 \equiv 0 \pmod{p}$ has at least d solutions and hence exactly d solutions.

Theorem 7 : Every prime number has a primitive root.

Proof :

Let p be a prime number.

Then $p = 2$ or p is an odd prime

If $p = 2$, then $1^1 \equiv 1 \pmod{2}$

$\therefore$ order of $1 \pmod{2} = 1 = \phi(2)$

$\Rightarrow$ 1 is primitive root of 2.

Now let p be any odd prime

$\therefore$ $p-1$ is an even number.

Let $p-1=p_1^{\alpha_1}p_2^{\alpha_2}..........p_k^{\alpha_k}$ be the prime factorization of p–1, where all p_i's are distinct primes and $\alpha_i \geq \forall\ i$

For each r = 1, 2,........, k, consider

$$x^{p_r^{\alpha_r}}-1\equiv 0 \pmod p \qquad ..... (1)$$

and $$x^{p_r^{\alpha_{r-1}}}-1\equiv 0 \pmod p \qquad ..... (2)$$

Since $x^{p_r^{\alpha_r}} \mid p-1$ and $x^{p_r^{\alpha_r-1}} \mid p-1$

∴ (1) has exactly $p_r^{\alpha_r}$ solutions

and (2) has exactly $p_r^{\alpha_r-1}$ solutions

Let x = a be a solution of (2)

i.e. $p_r^{\alpha_r-1}-1\equiv 0 \pmod p$

i.e. $p_r^{\alpha_r-1}\equiv 0 \pmod p$

⇒ $\left(a^{\alpha_r^{a_{r-1}}}\right)^{p_r}\equiv 1^{p_r} \pmod p$

i.e. $a^{p_r^{\alpha_r}}\equiv 1 \pmod p$

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

⇒ x = a is also a solution of (1)

∴ every solution of (2) is also a solution of (1)

Now since $p_r^{\alpha_r-1}<p_r^{\alpha_r}$

i.e. Number of solution of (2) < number of solutions of (1)

∴ ∃ a solution, say x = b_r, of (1) which is not a solution of (2)

i.e. $b_r^{p_r^{\alpha_r}}-1\equiv 0 \pmod p$

but $b_r^{p_r^{\alpha_{r-1}}}-1\not\equiv 0 \pmod p$

⇒ $b_r^{p_r^{\alpha_r}}-1\equiv 0 \pmod p$

and $b_r^{p_r^{i}}-1\not\equiv \pmod p\ \forall\ 0\leq i\leq \alpha_r-1$

$\Rightarrow$ $p_r^{\alpha_r}$ is the least positive integer such that $b_r^{p_r^{\alpha_r}} \equiv 1 \pmod p$

$\Rightarrow$ order of $b_r \pmod p = p_r^{\alpha_r}$ $\forall$ r = 1, 2, ..., k

Since all p_i's are distinct primes

$\therefore$ order of $b_1 b_2 \ldots\ldots b_k \pmod p = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_k^{\alpha_k}$

$\because$ order of b (mod p) = p – 1,

$= \phi(p)$ where $b = b_1 b_2 \ldots\ldots b_k$

$\Rightarrow$ b is primitive root of p.

Thus every prime must have a primitive root.

Theorem 8 : Let m > 2 has a primitive root g. Then $g^{\frac{\phi(m)}{2}} \equiv -1$ (mod m).

Proof :

Since g is a primitive root of m, therefore

$$g^{\phi(m)} \equiv 1 \pmod m \qquad \ldots\ldots (1)$$

For m > 2, $\phi(m)$ is even. Therefore we can rewrite (1) as

$$\left(g^{\frac{\phi(m)}{2}}\right)^2 - 1 \equiv 0 \pmod m$$

$$\Rightarrow \quad \left(g^{\frac{\phi(m)}{2}} - 1\right)\left(g^{\frac{\phi(m)}{2}} + 1\right) \equiv 0 \pmod m$$

$$\Rightarrow \quad g^{\frac{\phi(m)}{2}} \equiv 1 \pmod m \quad \text{or} \quad g^{\frac{\phi(m)}{2}} \equiv -1 \pmod m$$

As g is a primitive root of m, so $g^{\frac{\phi(m)}{2}} \not\equiv -1 \pmod m$

Hence $g^{\frac{\phi(m)}{2}} \equiv -1 \pmod m$.

2.2.4.1 Some Other Useful Results

1. x = a is a root of f(x) (mod m) iff (x – a)/f(x) (mod m).
2. If p is a prime and f(x) ≡ g (x) h(x) (mod p), then any root of f(x) (mod p) is a root either of g(x) or of h(x).

2.2.5 Some Important Examples

Example 1 : Find order of 2^3 modulo 13. Also find k such that 2^k has the same order as the order of 2 modulo 3.

Sol. Since $2^1 \equiv 2, 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 3,\ 2^5 \equiv 6,\ 2^6 \equiv 12,\ 2^7 \equiv 11,\ 2^8 \equiv 9,\ 2^9 \equiv 5,\ 2^{10} \equiv 10$

$2^{11} \equiv 7,\ 2^{12} \equiv 1$ modulo 13

$\therefore$ order of 2 modulo 13 is 12.

$\Rightarrow$ order of 2^3 modulo $13 = \dfrac{12}{(3,12)} = \dfrac{12}{3} = 4$

Now order of 2^k modulo 13 = 12 = order of 2 modulo 13

iff (k, 12) = 1

i.e. iff k = 1, 5, 7, 11.

Example 2 : If the order of a modulo a prime p is h such that h is even, then show that $a^{\frac{h}{2}} \equiv -1 \pmod p$

Sol. Given that order of a modulo p is h. Therefore

$$a^h \equiv 1 \pmod p \qquad \ldots\ldots (1)$$

Since h is even, there is an integer k such that

$$h = 2k \qquad \ldots\ldots (2)$$

From (1)

$a^{2k} \equiv 1 \pmod p$

$\Rightarrow$ $(a^k)^2 - 1 \equiv 0 \pmod p$

$\Rightarrow$ $(a^k - 1)(a^k + 1) \equiv 0 \pmod p$

$\Rightarrow$ $a^k - 1 \equiv 0 \pmod p$

or $a^k + 1 \equiv 0 \pmod p$

$\Rightarrow$ $a^k \equiv 1 \pmod p$

or $a^k \equiv -1 \pmod p$

Since order of a (mod p) is h and k < h, therefore $a^k \not\equiv 1 \pmod p$

Hence $a^k \equiv -1 \pmod p$

From (2), we have $a^{\frac{h}{2}} \equiv -1 \pmod p$.

Example 3 : Let a be a positive integer and p be a prime. Show that if a is a primitive root of p and $a^{p-1} \not\equiv 1 \pmod{p^2}$, then a is also a primitive root of p^2.

Sol. Let a has order h modulo p^2

Then $a^h \equiv 1 \pmod{p^2} \Rightarrow a^h \equiv 1 \pmod p$

Since a has order $\phi(p) = p - 1$ modulo p

So $p - 1 \mid h$

$\Rightarrow \quad h = k\,(p-1),\ k \in Z$

As a is a primitive root of p

$\therefore \quad (a, p) = 1 \quad \Rightarrow \quad (a, p^2) = 1$

By Euler's Fermat theorem

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

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

$\therefore \quad h \mid p\,(p-1)$

i.e. $\quad k\,(p-1) \mid p\,(p-1)$

$\Rightarrow \quad k \mid p \quad \Rightarrow \quad k = 1$ or p

If $k = 1$, then $h = p - 1$

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

which is not so

Therefore, $\quad k = p$

and $\quad h = p\,(p-1) = \phi(p^2)$

i.e. $\quad$ a has order $\phi(p^2)$ modulo p^2

Hence a is a primitive root modulo p^2.

Example 4 : Show that $f(x) = x^3$ is divisible by $g(x) = x^2 + 2x + 4$ to modulus 4.

Sol. Since $(x^2 + 2x + 4)(x + 2)$

$= x^3 + 4x^2 + 8x + 8$

$\equiv x^3 \pmod 4$

i.e. $\quad x^3 \equiv (x^2 + 2x + 4)(x + 2) \pmod 4$

or $\quad f(x) \equiv g(x)\,h(x) \pmod 4$

where $h(x) = x + 2$ is an integral polynomial

$\therefore \quad x^2 + 2x + 4 \mid x^3 \pmod 4$.

Example 5 : Find all the primitive roots of 17.

Sol. Here $p = 17$

$\therefore \quad p - 1 = 16 = 2^4$

$2^2 \equiv 4,\ 2^4 \equiv -1,\ 2^8 \equiv 1 \pmod{17}$

$\therefore \quad$ 2 is not primitive root of 17

$3^2 \equiv 9,\ 3^4 \equiv 14,\ 3^8 \equiv 16,\ 3^{16} \equiv 1 \pmod{17}$

$\therefore \quad$ 3 is a primitive root of 17.

All primitive roots of 17 are

$3, 3^3, 3^5, 3^7, 3^9, 3^{11}, 3^{13}, 13^{15}$

$\equiv \quad 3, 10, 5, 11, 14, 7, 12, 6 \pmod{17}$

Hence 3, 5, 6, 7, 10, 11, 12, 14 are all primitive roots of 17.

Example 6 : If p is an odd prime and g,g' are primitive roots modulo p, then show that gg' is not a primitive root modulo p.

Sol. Since g and g' are primitive roots of p, so

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

and $$g'^{\frac{p-1}{2}} \equiv -1 \pmod p$$

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

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

Thus gg' cannot be primitive root modulo p.

2.2.6 Self Check Exercise

1. If ab ≡ 1(mod m), then a and b have the same order modulo m.
2. If a has order hk modulo m, then a^h has order k modulo m.
3. If a is primitive root of m and b ≡ a (mod m), then b is also a primitive root of m.
4. Prove Wilson's theorem by using the fact that each prime p has a primitive root.
5. If g is a primitive root of a prime p, then $g^{\frac{p-1}{2}} \equiv -1 \pmod p$.

2.2.7 Suggested Readings

1. Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery, An Introduction to the Theory of Numbers, Wiley-India Edition.
2. T.N. Apostal, An Introduction to Analytic Number Theory, Springer Verlag.

LESSON NO. 2.3 **Author : Dr. Chanchal**

PRIMITIVE ROOTS AND INDICES – II

Structure :

2.3.0 Objectives

The prime objective of this lesson is understand the fundamental theorem of primitive roots. Further, the idea of indices alongwith its various properties and Euler's criterion is also discussed in detail.

2.3.1 Introduction

In continuation with the previous lesson, we are already familiar with the concept of primitive roots. In this lesson, we will introduce about the fundamental theorem of primitive roots and indices, as and when they occur.

2.3.2 Fundamental Theorem of Primitive Roots

The above Theorem states that

Theorem 1 : An integer m > 1 has primitive roots if and only if m is one of the following

$$2, 4, p^k, 2p^k$$

where p is an odd prime and k be any positive integer.

Proof : The proof of this theorem is actually based upon the following theorems and lemmas.

Theorem 2 : If p is an odd prime, then p^k has a primitive root for all $k \geq 1$.

Proof : The proof of this theorem is further based upon the following two Lemmas.

Lemma 1 : If p is an odd prime, there exists a primitive root g (mod p) such that $g^{p-1} \not\equiv 1 \pmod{p^2}$

Proof : Since every prime p has a primitive root, let g be a primitive root of p

As $g + p \equiv g \pmod p$

so $g + p$ is also a primitive root of p

Now either $g^{p-1} \not\equiv 1 \pmod{p^2}$ or $g^{p-1} \equiv 1 \pmod{p^2}$

If $g^{p-1} \not\equiv 1 \pmod{p^2}$, we have done

If $g^{p-1} \not\equiv 1 \pmod{p^2}$, then consider

$$(g+p)^{p-1} = g^{p-1} + (p-1)\,g^{p-2}p + \frac{1}{2}(p-1)\,(p-2)\,g^{p-3}p^2 + \dots + p^{p-1}$$

$$= g^{p-1} - p\,g^{p-2} + p^2\left[g^{p-2} + \frac{1}{2}(p-1)\,(p-2)\,g^{p-3} + \dots + p^{p-3}\right]$$

$\equiv g^{p-1} - p\,g^{p-2} \pmod{p^2}$

$\equiv 1 - p\,g^{p-2} \pmod{p^2}$ $\qquad \left[\mid \because g^{p-1} \equiv 1 \pmod{p^2}\right]$

Since g is primitive root of p

$\therefore$ $(g, p) = 1$

$\Rightarrow$ $(g^{p-2}, p) = 1$

i.e. $p \nmid g^{p-2}$

$\Rightarrow$ $p^2 \nmid pg^{p-2}$

or $pg^{p-2} \not\equiv 0 \pmod{p^2}$

and then $(g + p)^{p-1} \not\equiv 1 \pmod{p^2}$

Thus there is a primitive root $g + p$ such that

$(g + p)^{p-1} \not\equiv 1 \pmod{p^2}$

Lemma 2 : If p be an odd prime and g is a primitive root (mod p) such that

$g^{p-1} \neq 1 \pmod{p^2}$, then

$$g^{p^{k-2}(p-1)} \neq \pmod{p^k} \qquad \forall\, k \geq 2.$$

Proof : Applying induction on k, we prove the lemma

For $k = 2$, $g^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$ becomes $g^{p-1} \not\equiv 1 \pmod{p^2}$

which is true by lemma 1. So, Lemma is true for $k = 2$.

Assume the lemma is true for $k > 2$

i.e. $g^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$ for $k \geq 2$

Since g is primitive root modulo p.

so $(g, p) = 1$

$\Rightarrow \quad (g, p^{k-1}) = 1$

By Euler's Theorem

$$g^{\phi(p^{k-1})} \equiv 1 \pmod{p^{k-1}}$$

i.e. $\quad g^{p^{k-2}(p-1)} \equiv 1 \pmod{p^{k-1}}$

$$\Rightarrow \quad g^{p^{k-2}(p-1)} = 1 + t\,p^{k-1} \text{ for some } t \in Z \qquad \ldots (2)$$

$$\Rightarrow \quad \left[g^{p^{k-2}(p-1)}\right]^p = \left[1 + t\,p^{k-1}\right]^p$$

$$g^{p^{k-1}(p-1)} = 1 + tp^k + \text{terms containing } p^{k+1}$$

$$\Rightarrow \quad g^{p^{k-1}(p-1)} \equiv 1 + t\,p^k \pmod{p^{k+1}}$$

Claim : $(p, t) = 1$

If $(p, t) \neq 1$, then $p \mid t$

$\Rightarrow \quad p^k \mid t\,p^{k-1}$

i.e. $\quad tp^{k-1} \equiv 0 \pmod{p^k}$

or $\quad 1 + tp^{k-1} \equiv 1 \pmod{p^k}$

From (2) $g^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k}$

which contradict (1)

$\therefore \quad (p, t) = 1$ and then $tp^k \not\equiv 0 \pmod{p^{k+1}}$

$\therefore \quad g^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$

which show that Lemma is true for k + 1.

Now, we can prove the main theorem as :

Proof of Main Theorem 2 : Since p is a prime, $\exists$ a primitive root g (mod p) such that

$$g^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k} \quad \forall\, k \geq 2$$

Claim : g is also a primitive root (mod p^k) for all $k \geq 1$

Obviously theorem is true for k = 1

Let $k \geq 2$ and let order of g (mod p^k) = h

Then $h \mid \phi(p^k)$

i.e. $\quad h \mid p^{k-1}(p-1)$ … (1)

Also $\quad g^h \equiv 1 \pmod{p^k}$

$\Rightarrow \quad g^h \equiv 1 \pmod{p}$

Since g is primitive root of p, so order of g (mod p) = $\phi(p) = p - 1$

$\therefore \quad p - 1 \mid h$ … (2)

From (1) and (2)

$$h = p^r (p-1);\ 0 \le r \le k-1$$

$$\therefore \quad g^{p^r (p-1)} \equiv 1 \pmod{p^k} \qquad \ldots (3)$$

Suppose $0 \le r < k-1$ i.e. $0 \le r \le k-2$

Raising the power p^{k-2-r} both sides of (3), we have

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

which is a contradiction

Thus $r = k-1$ and then

Order of g (mod p^k) = h = $p^{k-1}(p-1) = \phi(p^k)$

and hence g is a primitive root of p^k $\forall$ $k \ge 1$.

Note : If g is a primitive root of an odd prime p such that

$g^{p-1} \ne 1 \pmod{p^2}$,

then g is also a primitive root of p^k, $\forall$ $k \ge 1$

Theorem 3 : If p is odd prime and $k \ge 1$, then $2p^k$ has primitive roots.

Proof : For any odd prime p and $k \ge 1$, p^k has primitive roots.

Let g be a primitive root of p^k

Since $g + p^k \equiv g \pmod{p^k}$

so $g + p^k$ is also a primitive root of p^k

If g is odd, then $g^r \equiv 1 \pmod{2}$ $\forall$ $r \ge 1$

So $\quad g^r \equiv 1 \pmod{2p^k}$

iff $\quad g^r \equiv 1 \pmod{p^k}$

Since order of g (mod p^k) = $\phi(p^k)$,

so order of g (mod $2p^k$) = $\phi(p^k)$

Also $\phi(2p^k) = \phi(2)\,\phi(p^k) = \phi(p^k)$

$\therefore$ $\quad$ Order of g (mod $2p^k$) = $\phi(2p^k)$

$\Rightarrow$ $\quad$ g is primitive root of $2p^k$

If g is even, then $\quad g + p^k$ is odd

and $\quad \therefore$ $g + p^k$ is a primitive root of $2p^k$.

Note : (1) If g is odd primitive root (mod p^k), then g is also primitive root (mod $2p^k$).

(2) If g is even primitive root (mod p^k), then $g + p^k$ is a primitive root (mod $2p^k$).

Lemma 5.1 : Prove that there is no primitive root of 2^k, $k \ge 3$.

Proof : If an integer a is primitive root of 2^k, then $(a, 2^k) = 1$

and Order of a (mod 2^k) = $\phi(2^k) = 2^{k-1}$

$(a, 2^k) = 1 \Rightarrow$ a is odd number

Now, by induction, we'll prove that

$$a^{2^{k-2}} \equiv 1 \pmod{2^k} \text{ for } k \geq 3 \qquad \ldots (1)$$

Let $k = 3$. Some a is odd,

so $a = 2r + 1$ where r is positive integer

$a^2 = 4r^2 + 4r + 1$

$a^2 = 4r(r + 1) + 1$

Since one of r and r + 1 is even

$\therefore$ $a^2 = 8s + 1$ for some integer s

$\Rightarrow$ $a^2 \equiv 1 \pmod 8$

i.e. $a^{2^{3-2}} \equiv 1 \pmod{2^3}$

$\therefore$ (1) is true for $k = 3$

Assume (1) hold for an integer k

i.e. $a^{2^{k-2}} \equiv 1 \pmod{2^k}$

$\Rightarrow$ $a^{2^{k-2}} = 1 + t.2^k$, for some integer t

Now $\left(a^{2^{k-2}}\right)^2 = (1 + t.2^k)^2$

$\Rightarrow$ $a^{2^{k-1}} = 1 + t.2^{k+1} + t^2\, 2^{2k}$

$= 1 + (t + t^2 . 2^{k-1})\, 2^{k+1}$

$= 1 + t' . 2^{k+1}$ for some integer t'

$\Rightarrow$ $a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$

$\therefore$ (1) is true for $k + 1$

Thus for $k \geq 3$, $a^{2^{k-2}} \equiv 1 \pmod{2^k}$

As $2^{k-2} < 2^{k-1} = \phi(2^k)$

So, a cannot be a primitive root of 2^k

Hence there is no primitive root of 2^k, $k \geq 3$.

Cor. : Prove that 2^k has primitive root only for $k = 1, 2$.

Proof : Do yourself.

Lemma 2 : For integers $m > 2$ and $n > 2$ with $(m, n) = 1$, prove that mn has no primitive root.

Proof : Let a be an integer such that $(a, mn) = 1$. Then

$(a, m) = 1$ and $(a, n) = 1$

By Euler's Theorem

$a^{\phi(m)} \equiv 1 \pmod{m}$

and $a^{\phi(n)} \equiv 1 \pmod{n}$

$\Rightarrow$ $a^{[\phi(m),\, \phi(n)]} \equiv 1 \pmod{m}$ and $a^{[\phi(m),\, \phi(n)]} \equiv 1 \pmod{n}$

$\Rightarrow$ $a^{[\phi(m),\, \phi(n)]} \equiv 1 \pmod{m\, n}$

Since both $\phi(m)$ and $\phi(n)$ are even for $m > 2$, and $n > 2$

so $(\phi(m), \phi(n)) \geq 2$

Also we have, $[\phi(m), \phi(n)] = \dfrac{\phi(m)\,\phi(n)}{(\phi(m), \phi(n))} < \phi\,(m)\,\phi(n) = \phi(mn)$

Thus we have an integer $k = [\phi(m), \phi(n)] < \phi(m\, n)$ such that

$a^k \equiv 1 \pmod{mn}$

$\therefore$ a cannot be a primitive root of m n and hence mn has no primitive root.

Proof of Theorem 1 : Combining the results of theorem 5.2, theorem 5.3, lemma 5.1 and lemma 5.2, theorem 5.1 is proved.

Example 1 : Calculate the eight primitive roots of 25.

Sol. We have

$25 = 5^2$

Firstly we find primitive roots of 5

As $\phi(5) = 4$ and $2^2 \equiv 4$, $2^4 \equiv 1 \pmod{5}$

so 2 is a primitive root of 5

Since $2^{5-1} = 16 \not\equiv 1 \pmod{5^2}$

$\therefore$ 2 is also a primitive root of 25

As $\phi(\phi\,(25)) = \phi(20) = 8$

and $(k, 20) = 1 \Rightarrow k = 1, 3, 7, 9, 11, 13, 17, 19$

$\therefore$ the eight distinct primitive roots are given by

$2, 2^3, 2^7, 2^9, 2^{11}, 2^{13}, 2^{17}, 2^{19} \pmod{25}$

Further

$2 \equiv 2$, $2^3 \equiv 8$, $2^7 \equiv 3$, $2^9 \equiv 12$,

$2^{11} \equiv 2^3$, $2^{13} \equiv 17$, $2^{17} \equiv 22$, $2^{19} \equiv 13 \pmod{25}$

Thus the eight distinct primitive roots (mod 25) are

2, 3, 8, 12, 13, 17, 22 and 23.

2.3.3 Indices

If m has a primitive root g, then $g, g^2, g^3, \ldots, g^{\phi(m)}$ form a reduced residue system mod m. Since $g^{\phi(m)} = 1$, equivalently the numbers. $1, g, g^2, \ldots, g^{\phi(m)-1}$ also form a reduced residue system mod m. If a be any integer such that $(a, m) = 1$, then there is a unique integer i, $1 \leq i \leq \phi\,(m)$, for which $a \equiv g^i \pmod{m}$.

Definition : Let g be primitive root modulo m and a be an integer such that $(a, m) = 1$. The smallest positive integer i such that

$g' \equiv a \pmod{m}$

is called the index of a relative to g and is denoted as $i = \text{ind}_g a = \text{ind } a$.

An Important Result : Let g be a primitive root modulo m and (a, m) = 1.

Then $g^k \equiv a \pmod{m}$ if, and only if,

$k \equiv \text{ind } a \pmod{\phi(m)}$.

2.3.4 Properties of the Index

If g be primitive root mod m then, the following properties hold :

Prop. I. : Ind a = Ind b iff $a \equiv b \pmod{m}$

Proof : Let Ind a = i and Ind b = j

$\therefore \quad a \equiv g^i \pmod{m}$ and $b \equiv g^j \pmod{m}$

Now Ind a = Ind b $\Rightarrow \quad i = j$

$\Rightarrow \quad g^i \equiv g^j \pmod{m}$

$\Rightarrow \quad a \equiv b \pmod{m}$

Conversely let $a \equiv b \pmod{m}$

Since $g, g^2, \ldots, g^{\phi(m)}$ is a reduced residue system mod m

$\therefore \quad a \equiv g^i \pmod{m}$

and $\quad b \equiv g^j \pmod{m}$ where $1 \le i, j \le \phi(m)$

$\therefore \quad g^i \equiv g^j \pmod{m} \Rightarrow \text{ind.}ab \equiv i + j \pmod{\phi(m)}$

$\Rightarrow \quad \phi(m) \mid i-j$

$\Rightarrow \quad i = j$

i.e. $\quad$ ind a = ind b

Prop. II. : $\text{ind } a\, b \equiv \text{ind } a + \text{ind } b \pmod{\phi(m)}$

Proof : Let Ind a = i and Ind b = j

$\therefore \quad a \equiv g^i \pmod{m}$

and $\quad b \equiv g^j \pmod{m};\ 1 \le i, j \le \phi(m)$

$\Rightarrow \quad ab \equiv g^{i+j} \pmod{m}$

$\Rightarrow \quad \text{ind } a\, b \equiv \text{ind } a + \text{ind } b \pmod{\phi(m)}$

Prop. III. : $\text{Ind } a^n \equiv n \text{ Ind } a \pmod{\phi(m)}$, n is a positive integer.

Proof : Let Ind a = i and g be a primitive root (mod m)

$\therefore \quad a \equiv g^i \pmod{m}$ where $1 \le i \le \phi(m)$

$\Rightarrow \quad a^n \equiv g^{in} \pmod{m}$

$\Rightarrow \quad \text{ind } a^n \equiv i\, n \pmod{\phi(m)}$

i.e. $\quad \text{ind } a^n \equiv n \text{ ind } a \pmod{\phi(m)}$

Prop. IV. : $\text{ind } 1 \equiv 0 \pmod{\phi(m)}$ and $\text{ind } g \equiv 1 \pmod{\phi(m)}$

Proof : Let g be the primitive root of m

Since $1 \equiv g^{\phi(m)} \pmod{m}$ and $g \equiv g^1 \pmod{m}$

$\therefore \quad \text{ind } 1 \equiv \phi(m) \pmod{\phi(m)} \equiv 0 \pmod{\phi(m)}$

and $\quad \text{ind } g \equiv 1 \pmod{\phi(m)}$

Prop. V. : $\text{ind } (-1) = \dfrac{\phi(m)}{2}$ for all $m > 2$

Proof : The proof is left for the reader.

Remarks :

1. Suppose m has a primitive root and $(a, m) = (b, m) = 1$. Then the linear congruence $ax \equiv b \pmod{m}$ has a unique solution and is given by

$$\text{ind } a + \text{ind } x \equiv \text{ind } b \pmod{\phi(m)}$$

or $\quad \text{ind } x \equiv \text{ind } b - \text{ind } a \pmod{\phi(m)}$

2. Binomial congruence : A congruence of the form

$$x^n \equiv a \pmod{m} \qquad \ldots (1)$$

is called binomial congruence. If $(a, m) = 1$ and m has a primitive root, then (1) is equivalent to $n \text{ ind } x \equiv \text{ind } a \pmod{\phi(m)}$

which is linear congruence with ind x as a variable.

3. Exponential Congruence : A congruence of the form $a^x \equiv b \pmod{m}$ is called exponential congruence. If $(a, m) = (b, m) = 1$ and m has a primitive root, then it is equivalent to the linear congruence $x \text{ ind } a \equiv \text{ind } b \pmod{\phi(m)}$.

Example 2 : Solve $11^x \equiv 28 \pmod{31}$ using 3 as a primitive root (mod 31).

Sol. To construct index table modulo 31 using 3 as a primitive root, we have

$3^1 \equiv 3$	$3^2 \equiv 9$	$3^3 \equiv 9$	$3^4 \equiv 19$	$3^5 \equiv 26$
$3^6 \equiv 16$	$3^7 \equiv 17$	$3^8 \equiv 20$	$3^9 \equiv 29$	$3^{10} \equiv 25$
$3^{11} \equiv 13$	$3^{12} \equiv 8$	$3^{13} \equiv 24$	$3^{14} \equiv 10$	$3^{15} \equiv 30$
$3^{16} \equiv 28$	$31^7 \equiv 22$	$31^8 \equiv 4$	$31^9 \equiv 12$	$3^{20} \equiv 5$
$3^{21} \equiv 15$	$3^{22} \equiv 14$	$3^{23} \equiv 11$	$3^{24} \equiv 2$	$3^{25} \equiv 6$
$32^6 \equiv 18$	$32^7 \equiv 23$	$3^{28} \equiv 7$	$3^{29} \equiv 21$	$3^{30} \equiv 1$

Index Table :

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\text{Ind}_3 a$	30	24	1	18	20	25	28	12	2	14	23	19	11	22	21

a	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Ind_3a	6	7	26	4	8	29	17	27	13	10	5	3	16	9	15

Given congruence

$$11^x \equiv 28 \pmod{31} \qquad \ldots (1)$$

is equivalent to

$$x \text{ ind } 11 \equiv \text{ind } 28 \ (\text{mod } \phi\,(31))$$

Using index table

$$23x \equiv 16 \pmod{30} \qquad \ldots (2)$$

Since (23, 30) = 1, (2) and hence (1) have a unique solution

Now $23\,x \equiv 16 \pmod{30}$

$\Rightarrow \quad 23x \equiv 16 + 30 \pmod{30}$

$\Rightarrow \quad 23x \equiv 46 \pmod{30}$

$\Rightarrow \quad x \equiv 2 \pmod{30}$

which is the required solution of (1).

Example 3 : Construct a table of indices for the prime 17 with respect to the primitive root 5 and solve the congruence $8x^5 \equiv 10 \pmod{17}$

Sol. To construct a table of indices of 17 w.r.t. the primitive root 5, calculate

$$5, 5^2, 5^3, \ldots\ldots, 5^{16} \text{ modulo } 17$$

$\therefore$

$5^1 \equiv 5$	$5^5 \equiv 14$	$5^9 \equiv 12$	$5^{13} \equiv 3$
$5^2 \equiv 8$	$5^6 \equiv 2$	$5^{10} \equiv 9$	$5^{14} \equiv 15$
$5^3 \equiv 6$	$5^7 \equiv 10$	$5^{11} \equiv 11$	$5^{15} \equiv 7$
$5^4 \equiv 13$	$5^8 \equiv 16$	$5^{12} \equiv 4$	$5^{16} \equiv 1$

Index Table :

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ind_5a	16	6	13	12	1	3	15	2	10	7	11	9	4	5	14	8

Given $8x^5 \equiv 10 \pmod{17}$

$\Rightarrow \quad \text{ind } 8 + 5 \text{ ind } x \equiv \text{ind } 10 \pmod{16}$

From above Table, we have

$\text{ind } 8 = 2$ and $\text{ind } 10 = 7$

$\therefore \quad 2 + 5 \text{ ind } x \equiv 7 \pmod{16}$

$\Rightarrow \quad 5 \text{ ind } x \equiv 5 \pmod{16}$

As $\quad (5, 16) = 1,$

$\therefore \quad \text{ind } x \equiv 1 \pmod{16}$

$\Rightarrow$ ind x = 1

Again using the table of indices, we have $x \equiv 5 \pmod{17}$.

Example 4 : Using indices, find the remainder when $3^{24} \times 5^{13}$ is divided by 17.

Sol. Firstly construct index table (mod 17) using any primitive root of 17

Corresponding to the primitive root 3 of 17 we have, modulo 17,

$3^1 \equiv 3,\quad 3^2 \equiv 9,\quad 3^3 \equiv 10,\quad 3^4 \equiv 13,$

$3^5 \equiv 5,\quad 3^6 \equiv 15,\quad 3^7 \equiv 11,\quad 3^8 \equiv 16,$

$3^9 \equiv 14,\quad 3^{10} \equiv 8,\quad 3^{11} \equiv 7,\quad 3^{12} \equiv 4,$

$3^{13} \equiv 12,\quad 3^{14} \equiv 2,\quad 3^{15} \equiv 6,\quad 3^{16} \equiv 1,$

Index Table :

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$ind_5 a$	16	6	13	12	1	3	15	2	10	7	11	9	4	5	14	8

Let r be the remainder when $3^{24} . 5^{13}$ is divided by 17. Then

$$3^{24} . 5^{13} \equiv r \pmod{17}$$

$$\text{ind } (3^{24} . 5^{13}) \equiv \text{ind } r \pmod{16}$$

$$\text{ind } 3^{24} + \text{ind } 5^{13} \equiv \text{ind } r \pmod{16}$$

$$24 \text{ ind } 3 + 13 \text{ ind } 5 \equiv \text{ind } 5 \pmod{16}$$

$$24 \times 1 + 13 \times 5 \equiv \text{ind } r \pmod{16}$$

$$\text{ind } r \equiv 89 \pmod{16}$$

$$\text{ind } r \equiv 9 \pmod{16}$$

$$r \equiv 14 \pmod{17}$$

Thus $r = 14$.

2.3.5 Euler's Criterion

Firstly, we will prove an important theorem which states that

Theorem 4 : Let m be an integer which has a primitive root and (a, m) = 1. Then the congruence $x^n \equiv a \pmod{m}$ has a solution iff $a^{\phi(m)/d} \equiv 1 \pmod{m}$, where $d = (n, \phi(m))$

If it has a solution, there are exactly d solutions

Proof :

As $d = (n, \phi(m))$ $\quad\therefore d \backslash \phi(m)$

$\Rightarrow$ $\phi(m) = dd_1$ for some integer d_1

$\Rightarrow$ $\dfrac{\phi(m)}{d} = d_1$

Now $a^{\phi(m)/d} \equiv$ (mod m)

iff $\dfrac{\phi(m)}{d}$ ind a $\equiv$ ind 1 (mod ϕ (m))

i.e. iff d_1 ind a $\equiv$ 0 (mod d d_1)

i.e. iff ind a $\equiv$ 0 (mod d)

i.e. iff d | ind a ... (i)

Also $x^n \equiv a$ (mod m)

iff n ind x $\equiv$ ind a (mod ϕ(m))

$\therefore$ it has solution iff d = (n, ϕ(m)) | ind a

i.e. iff $a^{\phi(m)/d} \equiv$ (1 mod m)

Cor. (Euler's Criterion) : Let p a prime and (a, p) = 1. Then $x^2 \equiv a$ (mod p) has a solution iff $a^{(p-1)/2} \equiv 1$ (mod p)

Proof : We have $x^n \equiv a$ (mod m) has a solution

iff $a^{\phi(m)/d} \equiv 1$ (mod m)

where m hasa primitive root and (a, m) = 1, d = (n, ϕ(m))

Therefore the congruence $x^2 \equiv a$ (mod p) has a solution

iff $a^{\phi(p)/d} \equiv 1$ (mod p) where ϕ (p) = p – 1 and d =(2, p–1) = 2

Thus $x^2 \equiv a$ (mod p) has a solution iff $a^{(p-1)/2} \equiv 1$ (mod p).

Example 5 : If p is an odd prime, then show that $x^2 \equiv -1$ (mod p) is solvable iff $p \equiv 1$ (mod 4)

Sol. We have, if p is a prime and (a, p) = 1, then $x^2 \equiv a$ (mod p) has a solution iff $a^{(p-1)/2} \equiv 1$ (mod p)

Given

$x^2 \equiv -1$ (mod p) ... (1)

$\therefore$ a = –1 and (–1, p) = 1

(1) is solvable iff $(-1)^{(p-1)/2} \equiv 1$ (mod p)

Now $\dfrac{p-1}{2}$ is either odd or even.

If $\dfrac{p-1}{2}$ is odd, then $(-1)^{\frac{p-1}{2}} = -1$

$\therefore$ $-1 \equiv 1$ (mod p) $\Rightarrow$ $-2 \equiv 0$ (mod p)

or $2 \equiv 0$ (mod p)

which is not possible as p is an odd prime

$\therefore$ $\dfrac{p-1}{2}$ must be even

Thus $x^2 \equiv -1 \pmod p$ is solvable iff $\frac{p-1}{2}$ is even

i.e. iff $\frac{p-1}{2} = 2k$, for some integer k

i.e. iff $p = 1 + 4k$

i.e. iff $p \equiv 1 \pmod 4$.

2.3.6 Self Check Exercise

1. Solve $5^x \equiv 4 \pmod{19}$
2. Solve $13x^8 \equiv 3 \pmod{25}$
3. If p is an odd prime, then show that $x^4 \equiv -1 \pmod p$ is solvable iff $p \equiv 1 \pmod 8$.

2.3.7 Suggested Readings

1. Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery, An Introduction to the Theory of Numbers, Wiley-India Edition.
2. T.N. Apostal, An Introduction to Analytic Number Theory, Springer Verlag.

LESSON NO. 2.4 **Author : Dr. Chanchal**

QUADRATIC RESIDUES AND QUADRATIC RECIPROCITY LAW

Structure :

2.4.0 Objectives

The prime objective of this lesson is to understand the concept of residues specially quadratic residues modulo m. During the study, we will discuss the following important topics.

* Quadratic residues and Euler's criterion based on them.
* Legendre's Symbol with Euler's Criterion.
* Gauss Lemma.
* Jacobi's Symbol.
* Quadratic Reciprocity and Jacobi's Reciprocity Law.

2.4.1 Introduction

In order to understand the concept of quadratic residues, it is required to be familiar with the knowledge of n^{th} power residue modulo m, which may be defined as:

An integer a is said to be an **nth power residue modulo m or nth power residue of m** if the congruence $x^n \equiv a \pmod{m}$ has atleast one solution modulo m.

In particular for n = 2, 3, 4 we call a as a quadratic, cubic, biquadratic residue modulo m respectively.

In this lesson, we deals with the Quadratic Congruences of the form

$$x^2 \equiv a \pmod{m} \text{ where } (a, m) = 1.$$

2.4.2 Quadratic Residue Modulo m

Def : Let a be any integer and m be a positive integer such that (a, m) = 1.

Then, a is called quadratic residue modulo m if the congruence

$$x^2 \equiv a \pmod{m} \text{ has a solution.}$$

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

For Example : 2 is a quadratic residue modulo 7 but 3 is not a quadratic residue modulo 7. (since $x^2 \equiv 2$ (mod. 7) but $x^2 \neq 3$ (mod. 7))

Remarks :

1. Since $x^2 \equiv 1 \pmod{m}$ has solution for all $m \geq 1$, so 1 is a quadratic residue for all m.
2. Since $x^2 \equiv a \pmod{m} \Rightarrow x^2 \equiv a + m \pmod{m}$, $\therefore$ a + m is a quadratic residue or non-residue modulo m according as a is or is not a quadratic residue.

3. If $a \equiv b \pmod{m}$, then a is quadratic residue or non-residue of m if and only if b is quadratic residue or non-residue of m.
4. Any integer a with $(a, m) = 1$ is either a quadratic residue or quadratic non-residue of m.
5. Since $x^2 \equiv a^2 \pmod{m}$ has solution for all integers a, so a^2 is quadratic residue of m iff $(a, m) = 1$.

Theorem 1 : Let a be an integer and $m > 2$ such that $(a, m) = 1$.
Prove that a is quadratic residue of m iff ind a is even.

Proof : We have a is quadratic residue of m
iff $x^2 \equiv a \pmod{m}$ has a solution
i.e. iff $2 \text{ ind } x \equiv \text{ind } a \pmod{\phi(m)}$ has a solution
i.e. iff $(2, \phi(m)) \mid \text{ind } a$ [$\because$ for $m > 2$, $\phi(m)$ is even]
i.e. iff $2 \mid \text{ind } a$
i.e. iff ind a is an even number.

Note : The readers can easily prove the corollary based on above theorem, which states that "a is quadratic non-residue of m iff ind a is odd."

Theorem 2 (Euler's Criterion) : Let p be an odd prime and $(a, p) = 1$. Then a is quadratic residue of p iff

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

First Proof : Firstly let a be quadratic residue of p

$\therefore$ $x^2 \equiv a \pmod{p}$ has a solution say $x = \xi$

i.e. $\xi^2 \equiv a \pmod{p}$

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

Since $(a, p) = 1$, $\therefore$ $(\xi, p) = 1$
By using Fermat's theorem, we have

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

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

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

Let g be a primitive root of p
Then $\{g, g^2, \ldots\ldots, g^{p-1}\}$ form a reduced residue system mod p.
For any a such that $(a, p) = 1$,

$$a \equiv g^r \pmod{p}, \text{ where } 1 \le r \le p - 1 \qquad \ldots (1)$$

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

$\Rightarrow$ order of $g \mid \frac{r(p-1)}{2}$ $\Rightarrow$ $p - 1 \mid \frac{r(p-1)}{2}$

$\Rightarrow$ $2 \mid r$ $\Rightarrow$ r is even number.
$\Rightarrow$ $r = 2k$; k is an integer
(1) $\Rightarrow$ $g^{2k} \equiv a \pmod{p}$
or $(g^k)^2 \equiv a \pmod{p}$
$\Rightarrow$ $x = g^k$ is a solution of $x^2 \equiv a \pmod{p}$

Thus a is quadratic residue of p.

Cor. : Let p be on odd prime such that (a,p) = 1, then a is quadratic non-residue iff

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

Proof : The proof is left as an exercise for the reader.

Theorem 3 : For any odd prime p, prove that there are $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residue.

OR

Let g be a primitive root of an odd prime p. Prove that the quadratic residue of p are congruent to $g^2, g^4, \ldots\ldots, g^{p-1}$ and that the non-residues are congruent to $g, g^3, \ldots.., g^{p-2}$.

Proof : Let g be a primitive root of p.

Then $\{g, g^2, g^3, \ldots\ldots\ldots, g^{p-1}\}$ form a reduced residue system modulo p.

Let a be an integer such that (a, p) = 1

Then $a \equiv g^r \pmod p$ for some $1 \le r \le p - 1$

$\Rightarrow$ ind a = r, $1 \le r \le p - 1$

Since a is quadratic residue or non-residue according as ind a = r is even or odd,

$\therefore$ $g^2, g^4, \ldots\ldots., g^{p-1}$ are quadratic residue of p.

and $g, g^3, \ldots\ldots.., g^{p-2}$ are quadratic non-residue of p.

Thus there are $\frac{p-1}{2}$ quadratic residue as well as non-residue of p.

Example 1 : Let r be quadratic residue modulo prime p. Is r primitive root mod p ? Justify.

Sol. No.

Let r be a quadratic residue modulo p.

Then, $x^2 \equiv r \pmod p$ has a solution ... (1)

Let it be $x = x_0$.

Therefor e$x_0^2 \equiv r \pmod p$

Since (r, p) = 1, therefore $(x_0^2, p) = 1$

$\Rightarrow$ $(x_0, p) = 1$

By Fermat's Theorem,

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

From (1),we have

$$(x_0^2)^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}} \pmod p$$

$$\Rightarrow \quad x_0^{p-1} \equiv r^{\frac{p-1}{2}} \pmod p \quad \ldots (3)$$

From (2)and (3), we get

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

Therefore order of r (mod p) $\le \frac{p-1}{2}$.

Hence r cannot be a primitive root of p.

Example 2 : Find all the quadratic residues of 13.

Sol. Here p = 13

Number of quadratic residue of $13 = \frac{13-1}{2} = 6$

We have

$1^2 \equiv 1 \pmod{13}$, $2^2 \equiv 4 \pmod{13}$, $3^2 \equiv 9 \pmod{13}$

$4^2 \equiv 3 \pmod{13}$, $5^2 \equiv 12 \pmod{13}$, $6^2 \equiv 10 \pmod{13}$

Therefore, all the quadratic residue of 13 are 1, 3, 4, 9, 10 and 12.

Example 3 : Show that 3 is a quadratic residue of 13 but a quadratic non-residue of 7.

Sol. We have $3^{\frac{13-1}{2}} = 3^6 \equiv 1 \pmod{13}$

and $3^{\frac{7-1}{2}} = 3^3 \equiv -1 \pmod{7}$

By Euler's Criterion 3 is a quadratic residue of 13 and a quadratic non-residue of 7.

2.4.3 Legendre's Symbol

Def : If p is an odd prime and (a, p) = 1, then the Legendre symbol $\left(\frac{a}{p}\right)$ is defined as follows :

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

Theorem 2.4.4 (Euler's Criterion) : Let p be an odd prime and a an integer such that (a, p) = 1, then

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

Proof : Let p be an odd prime and (a, p) = 1, By Fermat's theorem

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

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

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

so $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$

We know that

(i) a is quadratic residue of p iff $a^{(p-1)/2} \equiv 1 \pmod{p}$

(ii) a is quadratic non residue of p iff $a^{(p-1)/2} \equiv -1 \pmod{p}$

Consequently, we have

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

Theorem 2.4.5 : Let p be an odd prime. Then

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

(2) If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

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

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

(5) If (r, p) = 1, then $\left(\frac{ar^2}{p}\right) = \left(\frac{a}{p}\right)$

Proof : (1) Since $x^2 \equiv a^2 \pmod{p}$ has solutions namely $x = \pm a$

$\therefore$ a^2 is a quadratic residue of p

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

(2) If $a \equiv b \pmod{p}$, then
either both a and b are quadratic residues or non-residue of p.
In each case, we have

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

(3) If both a and b are quadratic residues of p then, a b is also quadratic residue of p

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

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

If both a and b are quadratic non-residue of p then, a b is quadratic residue of p.

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

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

If one of a and b is quadratic residue and other is non-residue of p, then a b is quadratic non-residue of p.

Let a be quadratic residue of p and b be non-residue of p.

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

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

The proof of (4) and (5) is left as an exercise for the reader.

Cor. : If p is an odd prime, then

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

Proof : Given p be an odd prime

$\therefore$ $(-1, p) = 1$

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

Every odd prime is either of the form 4k + 1 or 4k + 3.

If p = 4 k + 1, then $\frac{p-1}{2} = 2k$

i.e. $\frac{p-1}{2}$ is even number

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

If p = 4 k + 3, then p –1 = 4 k + 2 $\frac{p-1}{2} = 2k+1$

i.e. $\frac{p-1}{2}$ is odd number

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

Theorem 2.4.6 (Gauss Lemma) : Let p be an odd prime and a be any integer such that (a, p) = 1. Consider the least positive residues mod p of the integers $a, 2a, 3a, \ldots\ldots, \frac{p-1}{2}a$

If n denotes the number of these residues which exceed $\frac{p}{2}$, then

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

Proof : The integers a, 2a, 3a, ..., $\frac{p-1}{2}$a are incongruent mod p

$\because$ if $r\,a \equiv s\,a \pmod p, 1 \le r, s \le \frac{p-1}{2}$

then $r \equiv s \pmod p$ $[\because (a, p) = 1]$

$\Rightarrow$ $r = s$ $[\because 0 \le |r - s| < p]$

Divide a, 2a + 3a, ..., $\frac{p-1}{2}$a by p

Let A = $\{\alpha_1\ \alpha_2, \ldots\ldots, \alpha_m\}$ be the set of all least positive residues < $\frac{p}{2}$ and B = $\{\beta_1\ \beta_2, \ldots\ldots, \beta_n\}$ be the set of all least positive residue > $\frac{p}{2}$. Then all α_i and β_i are distinct and non-zero.

Also $\quad m + n = \frac{p-1}{2}$

Consider the set

$$C = \{p - \beta_1, p-\beta_2, \ldots\ldots, p - \beta_n\}$$

As $\quad \frac{p}{2} < \beta_i < p \therefore -p < -\beta_i < -\frac{p}{2} \Rightarrow 0 < p - \beta_i < \frac{p}{2}$

The members of A and C lies between 0 and $\frac{p}{2}$ and are distinct.

$\because$ if $\alpha_i = p - \beta_j$

then $\alpha_i \equiv \alpha\, a \pmod p$ and $\beta_j \equiv \beta\, a \pmod p$ for $1 \le \alpha, \beta \le \frac{p-1}{2}$

$\Rightarrow \quad (\alpha + \beta)\, a \equiv \alpha_i + \beta_i \equiv p \equiv 0 \pmod p$

$\Rightarrow \quad \alpha + \beta \equiv 0 \pmod p$

This is impossible $\because$ $1 < \alpha + \beta \le p - 1$.

Thus the set $A \cup C = \{\alpha_1, \alpha_2, \ldots\ldots\ldots, \alpha_m, p - \beta_1, p - \beta_2, \ldots\ldots\ldots, p - \beta_n\}$ consists of m + n = $\frac{p-1}{2}$ integers in the interval $\left[1, \frac{p-1}{2}\right]$ and hence

$$\{\alpha_1, \alpha_2, \ldots\ldots\ldots, \alpha_m, p - \beta_1, p - \beta_2, \ldots\ldots\ldots, p - \beta_n\} = \left\{1, 2, 3\ldots\ldots\ldots, \frac{p-1}{2}\right\}$$

$$\Rightarrow \quad \alpha_1\alpha_2\ldots\ldots\ldots\alpha_m (p - \beta_1)(p - \beta_2)\ldots\ldots\ldots(p-\beta_n) = 1.2.3\ldots.. \left(\frac{p-1}{2}\right) = \left(\frac{p-1}{2}\right)!$$

$$\Rightarrow \quad \left(\frac{p-1}{2}\right)! \equiv (-1)^n \alpha_1\alpha_2\ldots\ldots\alpha_m\ \beta_1\beta_2\ldots\ldots\ldots\beta_n \pmod p$$

$$\equiv (-1)^n\ a.2\,a.3\,a\ldots.\left(\frac{p-1}{2}a\right) \pmod p$$

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

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

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

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

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

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

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

Now, the readers can easily prove the below stated theorem and corollary.

Theorem 2.4.7 : If p is an odd prime and a is an odd integer such that (a, p) = 1, then,

$$\left(\frac{a}{p}\right) = (-1)^t \text{ where } t = \sum_{j=1}^{(p-1)/2} \left[\frac{ja}{p}\right]$$

Cor. : If p is an odd prime, then

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

Theorem 2.4.8 : If pis an odd prime, then

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

Proof : We know that

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

Any odd prime p is one of the form

8 k + 1, 8k + 3, 8k + 5 or 8k + 7

If $\quad p = 8k+1, \frac{p^2-1}{8} = \frac{1}{8}(64k^2 + 16k + 1 - 1) = 8k^2 + 2k$

$\therefore \quad \frac{p^2-1}{8}$ is even.

If $p = 8k + 3$, $\frac{p^2-1}{8} = \frac{1}{8}(64k^2 + 48k + 9 - 1) = 8k^2 + 6k + 1$

$\therefore \quad \frac{p^2-1}{8}$ is odd.

If $p = 8k + 5$, $\frac{p^2-1}{8} = \frac{1}{8}(64k^2 + 80k + 25 - 1) = 8k^2 + 10k + 1$

$\therefore \quad \frac{p^2-1}{8}$ is odd.

If $p = 8k + 7$, $\frac{p^2-1}{8} = \frac{1}{8}(64k^2 + 112k + 49 - 1) = 8k^2 + 4k + 6$

$\therefore \quad \dfrac{p^2-1}{8}$ is even.

Thus $\dfrac{p^2-1}{8}$ is even if p = 8 k + 1 or 8k + 7

and $\dfrac{p^2-1}{8}$ is odd if p = 8 k + 3 or 8k + 5

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

In other words

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

$$= \begin{cases} 1 & \text{if } p \equiv \pm 1 \text{ (mod 8)} \\ -1 & \text{if } p \equiv \pm 3 \text{ (mod 8)} \end{cases}$$

Example 2.4.4 :

Find $\left(-\dfrac{38}{13}\right)$

Sol. $\left(-\dfrac{38}{13}\right) = \left(\dfrac{-1}{13}\right)\left(\dfrac{38}{13}\right)$

$= 1 \,.\left(\dfrac{38}{13}\right)$ [$\because$ 13 ≡ 1 (mod 4)]

$= \left(\dfrac{12}{13}\right)$ [$\because$ 38 ≡ 12 (mod 13)]

$$= \left(\frac{2^2.3}{13}\right) = \left(\frac{3}{13}\right) \equiv 3^{\frac{13-1}{2}} \equiv 3^6 \equiv (27)^2 \equiv 1 \,(\text{mod}.13) \; = \left(\frac{3}{13}\right) \Rightarrow \left(\frac{-38}{13}\right) = 1\,.$$

Example 2.4.5 : Show that there are infinitely many primes of the form 4k + 1.

Sol. Suppose there are finitely many primes of the form 4k + 1.

Let they are 5, 13, 17, ……., q

where q is the largest prime of the form 4k + 1.

Consider N = $(2.5.13.17\ldots\ldots\ldots q)^2 + 1$

Then N is an odd and therefore there exists an odd prime p such that

$p \mid N$ … (1)

$\Rightarrow$ N ≡ 0 (mod p)

$\Rightarrow$ $(2.5.13.17\ldots\ldots. q)^2 \equiv -1$ (mod p)

$\Rightarrow$ $x^2 \equiv -1$ (mod p) has a solution

Thus –1 is a quadratic residue of p and $\left(\dfrac{-1}{p}\right) = 1$

But $\left(\dfrac{-1}{p}\right) = 1$ if p is of the form 4k + 1

$\Rightarrow$ p is one of 5, 13, 17,……., q

$\Rightarrow$ $p \mid (2.5.13.17 \ldots\ldots\ldots q)^2$

i.e. $p \mid N-1$ … (2)

(1) and (2) $\Rightarrow p \mid N-(N-1)$ i.e. $p \mid 1$

which is a contradiction

Hence there must exist infinitely many prime of the form 4k + 1.

Example 2.4.6 : Using Gauss Lemma, show that 2 is quadratic non residue and 3 is a quadratic residue modulo 13.

Sol. Here $p = 13$

Firstly take $a = 2$

Consider the integers

2, 2.2, 3.2, 4.2, 5.2, 6.2

$2 \equiv 2$ (mod. 13), $2.2 \equiv 4$ (mod 13), $3.2 \equiv 6$ (mod. 13), $4.2 \equiv 8$ (mod. 13),
$5.2 \equiv 10$ (mod. 13), $6.2 \equiv 12$ (mod 13)

Here, n = number of residues which exceed $\frac{13}{2}$ = 3

so, $\left(\frac{2}{13}\right) = (-1)^3 = -1$

$\Rightarrow$ 2 is a quadratic non residue of 13

Now take $a = 3$

Consider the integers

3, 2.3, 3.3, 4.3, 5.3, 6.3

$3 \equiv 3$ (mod 13), $2.3 \equiv 6$ (mod 13), $3.3 \equiv 9$ (mod 13)

$4.3 \equiv 12$ (mod 13), $5.3 \equiv 2$ (mod 13), $6.3 \equiv 5$ (mod 13)

Here, n = number of residues which exceed $\frac{13}{2}$ = 2

so $\left(\frac{3}{13}\right) = (-1)^2 = 1$

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

Example 2.4.7 : Verify that 3 is a quadratic residue of 23.

Sol. Since 23 is a prime number and $23 \equiv -1$ (mod 12)

Therefore, $\left(\frac{3}{23}\right) = 1$

Hence 3 is a quadratic residue of 23.

Example 2.4.8 : Find the value of $\left(\frac{150}{1009}\right)$

Sol. $\left(\frac{150}{1009}\right) = \left(\frac{2.3.5^2}{1009}\right) = \left(\frac{2}{1009}\right)\left(\frac{3}{1009}\right)\left(\frac{5^2}{1009}\right)$

$= \left(\frac{2}{1009}\right)\left(\frac{3}{1009}\right)$

$= \left(\frac{3}{1009}\right)$ $\quad 1009 \equiv 1 \pmod 8$

$= \left(\frac{1009}{3}\right)$ $1009 \equiv 1 \pmod 4$

$= \left(\frac{1}{3}\right)$ $1009 \equiv 1 \pmod 3$

$= 1.$

Example 2.4.9 : Show that the congruence $x^2 \equiv 105 \pmod{199}$ has no solution.

Sol. The given congruence is $x^2 \equiv 105 \pmod{199}$

We have

$$\left(\frac{105}{199}\right) = \left(\frac{3\times5\times7}{199}\right) = \left(\frac{3}{199}\right)\left(\frac{5}{199}\right)\left(\frac{7}{199}\right)$$

Now, $\left(\frac{3}{199}\right) = -\left(\frac{199}{3}\right)$ $3 \equiv 3 \pmod 4$ and $199 \equiv 3 \pmod 4$

$= -\left(\frac{1}{3}\right)$ $199 \equiv 1 \pmod 3$

$= -1$

$\left(\frac{5}{199}\right) = \left(\frac{199}{5}\right)$ $5 \equiv 1 \pmod 4$

$= \left(\frac{4}{5}\right)$ $199 \equiv 4 \pmod 5$

$= 1$ $4 = 2^2$

$\left(\frac{7}{199}\right) = \left(\frac{199}{7}\right)$ $7 \equiv 3 \pmod 4$ and $199 \equiv 3 \pmod 4$

$= -\left(\frac{3}{7}\right)$ $199 \equiv 3 \pmod 7$

$= \left(\frac{7}{3}\right)$ $3 \equiv 3 \pmod 4$ and $7 \equiv 3 \pmod 4$

$= \left(\frac{1}{3}\right)$ $7 \equiv 1 \pmod 3$

$= 1$

Therefore

$$\left(\frac{105}{199}\right) = (-1)\times1\times1 = -1.$$

Thus the given congruence (1) has no solution.

Example 2.4.10 : List all the quadratic residues of prime number 7.

Sol. An integer a is a quadratic residue of an odd prime p iff $\left(\frac{a}{p}\right) = 1$

We have $\left(\frac{1}{7}\right)=1$ and $\left(\frac{2}{7}\right)=1$

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

$$\left(\frac{4}{7}\right)=\left(\frac{2^2}{7}\right)=1$$

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

$$\left(\frac{6}{7}\right)=\left(\frac{2}{7}\right)\left(\frac{3}{7}\right)=-1$$

Thus all the integers a such that

$a \equiv 1, 2$ or 4

(mod 7) are quadratic residues of 7.

2.4.4 Quadratic Reciprocity Law

Theorem 2.4.9 : If p and q are distinct odd primes, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

Proof : Since p and q are distinct odd primes, $\therefore$ (p, q) = 1

$\therefore$ (p, q) = 1 and By Gauss' Lemma

$$\left(\frac{p}{q}\right)=(-1)^{\sum_{j=1}^{\frac{(q-1)}{2}}\left(\frac{jp}{q}\right)} \text{ and } \left(\frac{q}{p}\right)=(-1)^{\sum_{j=1}^{\frac{(p-1)}{2}}\left(\frac{jq}{p}\right)}$$

$$\Rightarrow \quad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\sum_{j=1}^{\frac{(q-1)}{2}}\left[\frac{jp}{q}\right]+\sum_{j=1}^{\frac{(p-1)}{2}}\left[\frac{jq}{p}\right]}$$

We have to prove

$$\sum_{j=1}^{\frac{(q-1)}{2}}\left[\frac{jp}{q}\right]+\sum_{j=1}^{\frac{(p-1)}{2}}\left[\frac{jq}{p}\right]=\frac{p-1}{2}\cdot\frac{q-1}{2}$$

For this consider the set

$$S=\left\{(x,y)\,;\,1\le x\le\frac{p-1}{2},\,1\le y\le\frac{q-1}{2} \text{ where x, y are integers}\right\}$$

Then S has $\frac{p-1}{2}\cdot\frac{q-1}{2}$ members.

Note that there is no pairs of integers in S such that qx = py

$\because$ if qx = py then $x = \frac{p}{q}y \Rightarrow \frac{p}{q}y$ is integer but it is not possible

$\because$ p and q are distinct primes and $1 \le y \le \frac{q-1}{2}$

Take $S_1 = \{(x, y);\ qx > py\}$ and $S_2 = \{(x, y);\ qx < py\}$

i.e. $S_1 = \left\{(x, y); 1 \le x \le \frac{p-1}{2} \text{ and } 1 \le y < \frac{q}{p}x\right\}$

and $S_2 = \left\{(x, y); 1 \le x \le \frac{p}{q}y \text{ and } 1 \le y < \frac{q-1}{2}\right\}$

$\Rightarrow$ S_1 has $\sum_{x=1}^{\frac{(p-1)}{2}}\left[\frac{qx}{p}\right]$ members and S_2 has $\sum_{y=1}^{\frac{(p-1)}{2}}\left[\frac{py}{q}\right]$ members

Also, $S_1 \cup S_2 = S$ and $S_1 \cap S_2 = \phi$

$\Rightarrow$ $O(S_1) + O(S_2) = O(S)$

$$\Rightarrow \sum_{j=1}^{\frac{(p-1)}{2}}\left[\frac{jq}{p}\right] + \sum_{j=1}^{\frac{(q-1)}{2}}\left[\frac{jp}{q}\right] = \frac{p-1}{2}\cdot\frac{q-1}{2}$$

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

Now, the readers can easily prove the below stated cordlaries and theorem.

Cor. 1 : Prove that $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$

Cor. 2 : If atleast one of the primes p and q is of the form 4k+1, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

Cor. 3 : If both primes p and q are of the form 4k + 3, then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Theorem 2.4.10 : If $p \ne 3$ is an odd prime, show that

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12} \end{cases}$$

Example 2.4.11 : If p and q are odd primes such that p is a qudratic residue of q and $p \equiv 1 \pmod 4$ then show that q is a quadratic residue of p.

Sol. Since p is a quadratic residue of q, so, $\left(\frac{p}{q}\right) = 1$

Now as, $p \equiv 1 \pmod 4$

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

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

so q is a quadratic residue of p.

2.4.5 Jacobi's Symbol

Def. : Let Q be an odd positive integer and P be any integer such that (P, Q) = 1

If $Q = q_1 q_2 \ldots\ldots q_k$, where $q_1, q_2, \ldots, q_k$ are odd primes not necessarily distinct, then Jacobi's symbol $\left(\frac{P}{Q}\right)$ is defined by $\left(\frac{P}{Q}\right)=\left(\frac{P}{q_1}\right)\left(\frac{P}{q_2}\right)\ldots\ldots\left(\frac{P}{q_k}\right)$ where $\left(\frac{P}{q_1}\right)$ is Legendre symbol.

Theorem 2.4.11 : Let Q and Q' be two odd positive integers and Pand P' are integers such that (PP', QQ') = 1. Then

1. $\left(\frac{P}{QQ'}\right)=\left(\frac{P}{Q}\right)\left(\frac{P}{Q'}\right)$ 2. $\left(\frac{PP'}{Q}\right)=\left(\frac{P}{Q}\right)\left(\frac{P'}{Q}\right)$

3. $\left(\frac{P^2}{Q}\right)=\left(\frac{P}{Q^2}\right)=1$ 4. $\left(\frac{P'P^2}{Q'Q^2}\right)=\left(\frac{P'}{Q'}\right)$

5. $P \equiv P' \pmod{Q} \Rightarrow \left(\frac{P}{Q}\right)=\left(\frac{P'}{Q}\right)$

Proof : Let $Q = q_1 q_2 \ldots\ldots q_r$ and $Q' = q_1' q_2' \ldots\ldots q_r'$ where q_i and q_1' are odd primes not necessarily distincts.

1. $$\left(\frac{P}{QQ'}\right)=\left(\frac{P}{q_1 q_i \ldots\ldots q_r q_1' q_2' \ldots\ldots q_s'}\right)$$

$$=\left(\frac{P}{q_1}\right)\left(\frac{P}{q_2}\right)\ldots\left(\frac{P}{q_r}\right)\left(\frac{P}{q_1'}\right)\left(\frac{P}{q_2'}\right)\ldots\ldots\left(\frac{P}{q_s'}\right)$$

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

2. $$\left(\frac{PP'}{Q}\right)=\left(\frac{PP'}{q_1}\right)\left(\frac{PP'}{q_2}\right)\ldots\ldots\left(\frac{PP'}{q_r}\right)$$

$$=\left(\frac{P}{q_1}\right)\left(\frac{P'}{q_1}\right)\left(\frac{P}{q_2}\right)\left(\frac{P'}{q_2}\right)\ldots\left(\frac{P}{q_r}\right)\left(\frac{P'}{q_r}\right)$$

$$=\left(\frac{P}{q_1}\right)\left(\frac{P}{q_2}\right)\ldots\left(\frac{P}{q_r}\right)\left(\frac{P'}{q_1}\right)\left(\frac{P'}{q_2}\right)\ldots\left(\frac{P'}{q_r}\right)$$

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

The proof of (3) to (5) parts is left as an exercise for the reader.

Theorem 2.4.12 : If Q is an odd integer and Q > 0, then

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

Proof : Do yourself.

Theorem 2.4.13 : (Jacobi's Reciprocity Law) : If P and Q are positive odd integers with (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 $P = p_1p_2 \ldots\ldots\ldots p_r$ and $Q = q_1q_2 \ldots\ldots\ldots q_s$ where p_i's and q_j's are odd primes and $(p_i, q_j) = 1$

Now $\left(\frac{P}{Q}\right) = \left(\frac{P}{q_1q_2\ldots\ldots q_s}\right)$

$$= \left(\frac{P}{q_1}\right)\left(\frac{P}{q_2}\right)\ldots\ldots\ldots\left(\frac{P}{q_s}\right) \qquad \ldots.\ (1)$$

For any prime q_k, we have

$$\left(\frac{P}{q_k}\right) = \left(\frac{p_1p_2\ldots\ldots p_r}{q_k}\right) = \left(\frac{p_1}{q_k}\right)\left(\frac{p_2}{q_k}\right)\ldots\ldots\left(\frac{p_r}{q_k}\right)$$

$$= (-1)^{\frac{q_k-1}{2}\cdot\frac{p_1-1}{2}}\left(\frac{q_k}{p_1}\right)(-1)^{\frac{q_k-1}{2}\cdot\frac{p_2-1}{2}}\left(\frac{q_k}{p_2}\right)\ldots.(-1)^{\frac{q_k-1}{2}\cdot\frac{p_r-1}{2}}\left(\frac{q_k}{p_r}\right)$$

Using Legendre's Reciprocity Law

$$= (-1)^{\frac{q_k-1}{2}\left(\frac{p_1-1}{2}+\frac{p_2-1}{2}+\ldots\ldots+\frac{p_r-1}{2}\right)}\cdot\left(\frac{q_k}{p_1p_2\ldots\ldots p_r}\right)$$

$$= (-1)^{\frac{q_k-1}{2}\cdot\frac{p-1}{2}}\left(\frac{q_k}{P}\right) \quad \left[\because \frac{p_1-1}{2}+\frac{p_2-1}{2}+\ldots\ldots+\frac{p_r-1}{2} \equiv \frac{P-1}{2} \pmod 2\right]$$

$$(1) \Rightarrow \left(\frac{P}{Q}\right) = \left(\frac{P}{q_1}\right)\left(\frac{P}{q_2}\right)\ldots\ldots\left(\frac{P}{q_s}\right)$$

$$= (-1)^{\frac{q_1-1}{2}\cdot\frac{P-1}{2}}\left(\frac{q_1}{P}\right)(-1)^{\frac{q_2-1}{2}\cdot\frac{P-1}{2}}\left(\frac{q_2}{P}\right)\ldots\ldots\ldots(-1)^{\frac{q_s-1}{2}\cdot\frac{P-1}{2}}\left(\frac{q_s}{P}\right)$$

$$= (-1)^{\frac{P-1}{2}\left(\frac{q_1-1}{2}+\frac{q_2-1}{2}+\ldots\ldots+\frac{q_s-1}{2}\right)}\left(\frac{q_1q_2\ldots\ldots\ldots q_s}{P}\right)$$

$$= (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{Q}{P}\right) \quad \left[\because \frac{q_1-1}{2}+\frac{q_2-1}{2}+\ldots\ldots+\frac{q_s-1}{2} \equiv \frac{Q-1}{2} \pmod 2\right]$$

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

Cor : The Reciprocity Law can also be stated as follows :

$$\left(\frac{P}{Q}\right)=\begin{cases}\left(\frac{Q}{P}\right) & \text{if atleast one of P and Q is of the form } 4n+1\\ -\left(\frac{Q}{P}\right) & \text{if both P and Q are of the form } 4n+3\end{cases}$$

Proof : Do yourself.

Example 2.4.12 : Apply both Jacobi and Legendre symbol to determine whether the congruence $x^2 \equiv 21$ (mod. 253) has a solution.

Sol. Given congruence $x^2 \equiv 21$ (mod 253) where 253 is not a prime.

Using Jacobi symbol, we have

$$\left(\frac{21}{253}\right)=\left(\frac{253}{21}\right)=\left(\frac{1}{21}\right)=1$$

However, we also have

$$\left(\frac{21}{253}\right)=\left(\frac{21}{11.23}\right)=\left(\frac{21}{11}\right)\left(\frac{21}{23}\right)$$

Using Legendre symbol, we have

$$\left(\frac{21}{11}\right)=\left(\frac{-1}{11}\right)=-1$$

So, there is no solution of $x^2 \equiv 21$ (mod 11)

Also as $\left(\frac{21}{23}\right)=\left(\frac{3.7}{23}\right)=\left(\frac{3}{23}\right)\left(\frac{7}{23}\right)=\left(\frac{23}{3}\right)\left(\frac{23}{7}\right)=\left(\frac{2}{3}\right)\left(\frac{2}{7}\right)=-1$

So there is no solution of $x^2 \equiv 21$ (mod 23)

Hence there is no solution of $x^2 \equiv 21$ (mod 253).

2.4.6 Self Check Exercise

1. If a is a quadratic residue of m > 2, then $a^{\frac{\phi(n)}{2}} \equiv 1$ (mod m).
2. Define legendre symbol and find $\left(\frac{5}{13}\right)$.
3. List all quadratic residues of mod 11.
4. Prove that there are infinitely many primes of the form 4k + 1.
5. Solve $\left(\frac{2}{61}\right)$ and $\left(\frac{10}{89}\right)$.

2.4.7 Suggested Readings

1. Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery, An Introduction to the Theory of Numbers, Wiley-India Edition.
2. T.N. Apostal, An Introduction to Analytic Number Theory, Springer Verlag.