MT302

Institute of Distance and Open Learning
Gauhati University

M.A./M.Sc. in Mathematics
Semester 3

Paper II
Number Theory

Contents:

Contributors :

Prof. Nanda Ram Das	Dept. of Mathematics Gauhati University
Mr. Priyanka Pratim Baruah	Assistant Professor Dept. of Mathematics GIMT, Guwahati

Editorial Team :

Prof. Kuntala Patra	Dept. of Mathematics Gauhati University
Prof. Pranab Jyoti Das	Director, i/c IDOL, Gauhati University
Dipankar Saikia	Editor, (SLM) GU, IDOL

Cover Page Designing:

Mr. Bhaskarjyoti Goswami: IDOL, Gauhati University

Unit - 1

Divisibility and the Primes

Introduction :

An algorithm is a step by step process, complete in a finite number of steps, for solving a given problem. By the division algorithm, we mean that process with which the student became familiar in arithmetic. Divisors, multiples and prime and composite numbers are concepts that have been known and studied at least since the time of Euclid, about 350 BC.

The idea of prime numbers is very simple. Among all the positive integers 1, 2, 3, 4, ..., we can find that some integers have only two positive divisors and the other have more than two positive divisors, except the integer 1, which has just one positive divisor, namely itself. A positive integer which is greater than 1 and has only two positive divisors 1 and itself is called a prime number. An integer which is greater than 1, but is not a prime, is called a composite number.

In this unit, we shall discuss divisibility theory of integers and some properties related to prime number.

Definition 1.1.: An integer b is divisible by an integer $a(\neq 0)$ if there is an integer x such that $b = ax$.

$a \mid b$ means "b is divisible by a". and $a \nmid b$ means "b is not divisible by a". $a \mid 0$ if $a \neq 0$. a is called proper divisor of b if $a \mid b$ and $0 < a < b$.

Theorem 1.2.:

(1) $a \mid b \Rightarrow a \mid bc$ for any integer c.

(2) $a \mid b$ and $a \mid c \Rightarrow a \mid bx + cy$ for any x and y.

(3) $a \mid b$ and $b \mid c \Rightarrow a \mid c$.

(4) $a \mid b$ and $b \mid a \Rightarrow a = \pm b$.

(5) $a \mid b, a > 0, b > 0 \Rightarrow a \leq b$.

(6) if $m \neq 0$, $a \mid b \Leftrightarrow ma \mid mb$.

Proof:

(1) $a \mid b \Rightarrow b = ax$ for some integer x,

$\Rightarrow bc = a(xc) \Rightarrow bc = ay$ $\quad y = xc$ is an integer

$\Rightarrow a \mid bc$.

(2) $a \mid b \Rightarrow b = ax$ for some integer x.

$a \mid c \Rightarrow c = ay$ for some integer y.

Now $bu + cv = ((ax)u + (a)y)v$

$= a(vu + yv)$

$\therefore$ $a \mid bu + cv$.

Proof of the remaining left as exercise.

$a \mid b \Rightarrow b = ax$.

Note 1:

(1) $a \mid b$ and $b \neq 0 \Rightarrow |a| \leq |b|$.

(2) $a \mid b \Rightarrow -a \mid b$, and $a \mid -b$.

(3) $a \mid 0$, $1 \mid a$, and $a \mid a$ $\quad (a \neq 0)$

(4) $a \mid 1 \Rightarrow a = \pm 1$.

(5) $a \mid c$, $b \mid d \Rightarrow ab \mid cd$.

Algorithm:

An algorithm is a mathematical method which is frequently used to obtain a result. e.g.(1) Prime factorisation method.

(2) Principle of induction.

A. 1.3.The Division Algorithm(Euclid):

Give any integer a and b with $a > o$, $\exists$ unique integers q and r s.t. $b = aq + r$, $\quad 0 \leq r < a$.

If $a \nmid b$ then $0 < r < a$ and if $a \mid b$, $r = 0$.

Proof: Consider the A.P.

..... $b - 3a, b - 2a, b - a, b, b + a, b + 2a, b + 3a$,..... extending indefinitely in both direction.

Infact $S = \{b - na \mid n \in Z\}$

Consider the subset $S_1 = \{b - na \mid n \in z, b - na \geq 0\}$

Clearly $S_1 \neq \phi$.

Then by well ordering property (WOP) S_1 has a least member say $r \geq 0$.

$\therefore$ $\quad r = b - qa$ foe some $q \in z$.

$\therefore$ $\quad b = aq + r$.

A. Uniqueness of q and r :

Suppose if possible, $b = aq_1 + r_1$.

We claim $r = r_1$.

Suppose $r < r_1$.

$\therefore$ $\quad 0 \leq r \leq r_1 < a$.

$\Rightarrow 0 \leq r_1 - r < a$.

and $\quad 0 = (q_1 - q)a + (r_1 - r)$

$\Rightarrow (q - q_1)a = r_1 - r$.

$\Rightarrow a \mid r_1 - r.$

$\Rightarrow a \leq r_1 - r$, which is a contradiction.

$\therefore \quad r \nmid r_1.$

Similarly,

$r_1 \nmid r.$

$\therefore \quad r = r_1.$

Then $q = q_1.$

Thus q and r are unique.

B. Division Algorithm in general form :

Given integers a and b with $a \neq 0$, $\exists$ integers q and r such that

$b = qa + r,\ 0 \leq r < |a|.$

Proof: If $a > 0$, by Division Algorithm A $\exists$ integers q and r such that

$b = qa + r,\ 0 \leq r < q \leq |a|.$

If $a < 0$, $-a > 0$.

So $b = q_1(-a) + r$, where $0 \leq r < -a.$

$\therefore \quad b = aq + r \quad 0 \leq r < |a|.$

Thus $b = aq + r \quad 0 \leq r < |a|.$

Exercise 1. :

Find the quotient and reminder when 1, - 2, 61 and - 57 are divided by - 7.

Ans : $1 = (-7)0 + 1$

when 1 is divided by - 7, remainder = 1 and quotinent = 0.

Exercise 2. :

Show that $\frac{a(a^2+2)}{3}$ is an integer for $a \geq 2$.

Solution : We take a and 3. Then by division algorithm $a = 3q, 3q+1, 3q+2.$

If $a = 3q$, then $\quad \frac{a(a^2+2)}{3} = \frac{3q(qq^2+2)}{3} = q(qq^2+2).$

If $a = 3q+1$, then $\quad \frac{a(a^2+2)}{3} = \frac{(3q+1)(qq^2+6q+1+2)}{3}$

$= (3q+1)(3q^2+2q+1).$

If $a = 3q + 2$, then $\dfrac{a(a^2+2)}{3} = \dfrac{(3q+2)(qq^2+12q+4+2)}{3}$

$= (3q+2)(3q^2+4q+2)$.

Thus is all cases, $\dfrac{a(a^2+2)}{3}$ is an integer.

Exercise 3. :

Square of an integer is either $4k$, or $4k+1$.

Try yourself.

Exercise 4. :

Show that no integer in the sequence 11, 111, 1111, 11111, ... is a perfect square.

Solution:

$$\underbrace{111\ldots1}_{n \text{ places}} = 3 + (111\ldots108) = 4k+3$$

($\because$ in 111 ... 108 last two digits are divisible by 4)

A number is perfect square iff it is of the form $4k$ or $4k+1$.

So $\underbrace{111\ldots1}$ which is of the form $4k+3$ is not perfect square.

Exercise 5. :

Square of an odd integer is of the form $8k+1$.

Try yourself.

Exercise 6. :

For $n \geq 2$, $\dfrac{1}{6}n(n+1)(n+2)$ is an integer.

Try yourself.

Exercise 7. :

Prove that in the sequence 99, 999, 9999, 99999,..... no integer is a perfect square.

Try yourself.

Exercise 8. :

If $a - s \mid ab + st$ then $a - s \mid at + bs$.

Try yourself.

Exercise 9. :

$n(n+1)(n+2)$ is a multiple of 3.

Try yourself.

Exercise 10. :

If $k > 1$, then $k^2 + k + 1$ is not a perfect square.

Try yourself.

1.4. Definition : If a and b be given integers with at least one of them different from 0. The greatest common division (gcd) of a and b denoted by gcd(a, b) is the positive integer satisfying,

(i) $d \mid a$ and $d \mid b$.

(ii) if $c \mid a$ and $c \mid b$ then $c \leq d$.

The gcd of integers $a_1, a_2 ..., a_n$ not all zero in the largest integer which is a divisior of each of those integer. It is denoted by gcd $(a_1, a_2 ..., a_n)$.

If gcd $(a_1, a_2 ..., a_n) = ,1$ then $a_1, a_2 ..., a_n$ are called **mutually relatively prime.**

If each pair of integers a_i and a_j from the set is relatively prime then integers $a_1, a_2 ..., a_n$ are called **pairwise relatively prime.**

Clearly pairwise relatively prime implies mutually relatively prime.

The converse is not true.

For e.g. gcd(16, 10, 15) = 1.

$\therefore$ 16, 10, 15 are mutually relatively prime.

But gcd(16, 10) = 2.

$\therefore$ 16, 10, 15 are not pairwise relatively prime.

1.5. Theorem : Given integers a and b not both are zero, then there exists integers x and y such that

gcd(a, b) = ax + by.

Proof: Let $S = \{au + bv \mid au + bv > 0; u, v \text{ are integers}\}$

$S \neq \phi$.

Suppose $a \neq 0$,

If $a > 0$, then $a = a.1 + b.0 > 0$.

If $a < 0$, then $-a = a(-1) + b.0 > 0$.

By virtue of well ordering property (i.e. every non empty set of positive numbers has the least number) the set S has a least number say d.

So $\exists$ integer u and v such that $d = au + bv > 0$.

We can show that d = gcd(a, b).

We have to show (i) $d \mid a, d \mid b$

(ii) $c \mid a, c \mid b \Rightarrow c \leq d$.

(i) By division algorithm $\exists$ integers q and r such that

$a = qd + r, 0 \le r < d.$

If $d \nmid a$ then $r > 0$.

So $r = a - qd = a - q(au + bv) = a(1 - qu) - b(qv) > 0.$

Hence $r \in S$ and $r \ge d$ ($\because$ d is the least member) which contradicts $r < d$.

Thus $d \mid a$.

Similarly, $d \mid b$.

(ii) Suppose $c \mid a$, $c \mid b$ and $c \ge 0$.

To show $c \le d$.

$c \mid a$ and $c \mid b \Rightarrow c \mid au + bv = d \Rightarrow c \le d.$

Hence $\gcd(a, b) = d = au + bv$.

Thus gcd(a, b) can be expressed as ax + by where x and y are two integers.

Illustration :

$\gcd(6, 15) = 3.$

$S = \{6u + 15v \mid 6u + 15v > 0, u, v \text{ are integers}\}$

$= \{6.1 + 15.1.\ 6.0 + 15.1,\ 6(-1) + 15.\ 1,\ 6(-2) + 15.1, \ldots\}$

$= \{21, 15, 9, 3, \ldots\}$

where 3 is the least.

$\gcd(6, 15) = 3 = 6(-2) + 15.1.$

Note : All elements of S are multiple of 3.

1.6. Corollary: If a and b are given integers not both zero, then the set $T = \{ax + by \mid x, y \text{ are integers}\}$ is precisely the set of all multiples of $d = \gcd(a, b)$.

Proof: $d = \gcd(a, b)$

$\Rightarrow d \mid a$ and $d \mid b$

$\Rightarrow d \mid ax + by$ 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 $d = ax + by$ for suitable integer x_0 and y_0, so that any multiple of d is of the form,

$nd = n(ax_0 + by_0)$

$= a(nx_0) + b(ny_0).$

Hence nd is a linear combination of a and b, and by definition it lies in T.

Hence the result.

1.7. Theorem: Given any integers $b_1, b_2, ..., b_n$ not all zero, there exists $x_1, x_2, ..., x_n$ such that

$$\gcd(b_1, b_2, ..., b_n) = \sum_{i=1}^{n} b_i x_i .$$

Proof: Let

$$S = \left\{ \sum_{i=1}^{n} b_i x_i \mid x_i \in Z, \sum_{i=1}^{n} b_i x_i > 0 \right\}.$$

But $S \neq \phi$.

Suppose $b_i \neq 0$ and $b_i > 0$.

Then $b_i = 0b_1 + ... + 0b_{i-1} + 1b_i + 0b_{i+1} + ... + 0b_n$

$\in S \quad (\because b_i > 0)$

If $b_i < 0$, $-b_i = 0b_1 + ... + 0b_{i-1} + (-1)b_i + 0b_{i+1} + ... + 0b_n$

$\in S \quad (\because -b_i > 0)$

So $S \neq \phi$. By well ordering property S has a least member say d. we claim,

$d = \gcd(b_1, b_2, ..., b_n)$

(i) To show $d \mid b_i$, $i = 1, 2, ..., n$.

By definition of S, $d = b_1x_1 + ... + b_nx_n$ $(x_i \in z)$

$> 0 \quad$ (as $d \in S$)

$b_i = qd + r$ where $0 \leq r < d$.

$\Rightarrow r = b_i - qd$

$= b_i - q(b_1x_1 + ... + b_nx_n)$

$= -qx_1b_i\ qx_2b_2 + ... + (1 - qx_i)b_i + ... + (-qx_n)b_n$

If $d \nmid b_i$, $0 < r$ so $r \in S$.

$r < d$, $r \in S$ contradicts that d is the smallest member of S.

$\therefore \quad d \mid b_i \quad (1 \leq i \leq n)$

(ii) Let $c > 0$ and $c \mid b_i$, $i = 1, 2, ..., n$.

To show $c \leq d$.

$c \mid b_i \Rightarrow c \mid \sum_{i=1}^{n} x_i b_i = d$

$\Rightarrow d = nc$ $((c > 0, d > 0)$ where $n \in \angle)$

$\geq c$.

Thus $d = \sum_{i=1}^{n} b_i x_i = \gcd(b_1, b_2, \ldots, b_2)$.

Theorem 1.8.: If a and b are integers, b being non zero, then there are unique integers q and r such that

$$a = qb + r$$

where $-\frac{1}{2}|b| \le r < \frac{1}{2}|b|$ (least absolute remainder)

Proof: by Euclid's Division Algorathim, $\exists$ unique integers q_1 and r_1 such that

$$a = q_1 b + r_1, \text{ where } 0 \le r_1 < |b|.$$

If $0 \le r_1 < \frac{1}{2}|b|$, then put $q = q_1$ and $r = r_1$.

If $\frac{1}{2}|b| \le r_1 < |b|$, then put $q = \begin{cases} q_1 + 1 \text{ if } b > 0 \\ q_1 - 1 \text{ if } b < 0 \end{cases}$

and $r = r_1 - |b|$.

Then $a = qb + r$, where $-\frac{1}{2}|b| \le r < \frac{1}{2}|b|$.

The uniquness of q and r follows from the uniquness of q_1 and r_1.

Theorem 1.9.: Let a and b be integers, not both zero, then a and b are relatively prime (i.e. (a, b) = 1) iff $\exists$ integers a and y such that $1 = ax + by$.

Proof: Suppose a and b are relatively prime.

$\Rightarrow \gcd(a, b) = 1$

$\Rightarrow ax + by = 1$, where x, y are two integers.

Conversely suppose, $1 = ax + by$ for some $x, y \in z$.

then to show that gcd(a, b) = 1.

Suppose gcd(a, b) = d and d is a positive integer.

$\Rightarrow d \mid a$ and $d \mid b$

$\Rightarrow d \mid ax + by = 1$, for some $x, y \in z$.

$\Rightarrow d = 1$.

i.e. gcd(a, b) = 1.

$\therefore$ a and b are relatively prime.

1.10. Corollary: If $\gcd(a, b) = d$ then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Proof: $\gcd(a, b) = d$.

$\Rightarrow d \mid a$, and $d \mid b$.

$\Rightarrow \frac{a}{d}$ and $\frac{b}{d}$ are two integers.

Now $\gcd(a, b) = d$

$\Rightarrow \exists$ integers x and y such that $d = ax + by$.

$\Rightarrow 1 = \frac{a}{d}x + \frac{b}{d}y$

$\Rightarrow \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

1.11. Corollary: If $a \mid c$ and $b \mid c$ with $\gcd(a, b) = 1$ then $ab \mid c$.

Proof: $a \mid c$ and $b \mid c$

$\Rightarrow c = ar$, $c = bs$ for $r, s \in Z$.

$\gcd(a, b) = 1 \Rightarrow ax + by = 1$

$\Rightarrow c = cax + cby$

$\Rightarrow c = absx + abry$

$\Rightarrow c = ab(sx + ry)$

$\Rightarrow ab \mid c$.

1.12. Theorem:

(i) For any +ve integer m, $(ma, mb) = m(a, b)$

(ii) For integers a, b, c, k, $(a + bk, b) = (a, b)$

(iii) If $a \equiv b \pmod m$ then $(a, m) = (b, m)$.

Proof:

(i) let $d = \gcd(a, b)$

To show that $md = \gcd(ma, mb)$

$d = \gcd(a, b)$

$\Rightarrow d \mid a$ and $d \mid b$

$\Rightarrow md \mid ma$ and $md \mid mb$.

Again let $c > 0$ and $c \mid ma$, $c \mid mb$.

To show $c \leq md$.

Now $d = \gcd(a, b)$

$\Rightarrow d = ax + by \qquad (x, y \in Z)$

Again $c \mid ma, c \mid mb.$

$\Rightarrow c \mid max + mby = md$

$\Rightarrow c \leq md.$

$\therefore \quad md = \gcd(ma, mb)$

$\Rightarrow m(a, b) = (ma, mb)$

Proofs of (ii) and (iii) are left as exercise.

1.13. Euclid Lemma: If $a \mid bc$ with $(a, b) = 1$ then $a \mid c$.

Proof: $a \mid bc \Rightarrow bc \Rightarrow ar, r \in z,$

and $(a, b) = 1 \Rightarrow 1 = ax + by$

$\Rightarrow c = cax + cby$

$= cax + ary$

$= a(cx + ry)$

$\therefore \quad a \mid c.$

1.13. Theorem: Let a, b be integers not both zero. For a +ve integer d, $d = (a, b)$ iff

(i) $d \mid a, d \mid b$

(ii) when $c \mid a, c \mid b$ then $c \mid d$.

Proof: Let $d = \gcd(a, b)$.

Then $d \mid a$, and $d \mid b$.

Also $d = ax + by, x, y \in z.$

$c \mid a, c \mid b \Rightarrow c \mid ax + by = d.$

Conversely, suppose (i) and (ii) hold.

By (i), $d \mid a$ and $d \mid b$.

Suppose c is common positive divisor of a and b.

To show $c \leq d$.

By (ii), $c \mid d$

$\Rightarrow d = cp$ where p is a positive integer

$\Rightarrow c \leq p.$

$\therefore \quad d = \gcd(a, b).$

1.14. Theorem: If $d \mid a$ and $d \mid b$ and $d > 0$, then

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}\gcd(a, b).$$

Proof: $d|a, d|b \Rightarrow \frac{a}{d} \in Z, \frac{b}{d} \in Z$

$$d\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \gcd\left(d\frac{a}{d}, d\frac{b}{d}\right) \qquad [\because m(a, b) = (ma, mb)]$$

$$= \gcd(a, b)$$

$$\therefore \quad \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}\gcd(a, b).$$

1.15. Theorem: If $(a, m) = (b, m) = 1$ then $(ab, m) = 1$.

Try yourself.

1.16. Theorem: For any x,

$$(a, b) = (b, a) = (a, -b) = (a, b + ax).$$

Try yourself.

Exercise: show that $((a, b), c) = (a, (b, c))$

Try yourself.

To find gcd of two numbers:

1.16. The Euclidean Algorithm: Given integers b and c and $c > 0$, repeated applications of Division Algorithm we have the following series,

$$b = cq_1 + r_1 \qquad 0 < r_1 < c$$

$$c = r_1q_2 + r_2 \qquad 0 < r_2 < r_1$$

$$r_1 = r_2q_3 + r_3 \qquad 0 < r_3 < r_2$$

.....

$$r_{j-2} = r_{j-1} + q_j + r_j \qquad 0 < r_j < r_{j-1}$$

$$r_{j-1} = r_jq_{j+1} + 0.$$

Thus r_j the last non zero remainder is the gcd of b and c.

Illustration: To find gcd(12378, 3054)

$12378 = 3054 \times 4 + 162$

$3054 = 162 \times 18 + 138$

$162 = 138 \times 1 + 24$

$138 = 24 \times 5 + 18$

$24 = 18 \times 1 + 6$

$18 = 6 \times 3.$

$\therefore$ gcd(12378, 3054) = 6.

$6 = 24 - 18 \times 1$

$= 24 - (138 - 24 \times 5) \times 1$

$= 6 \times 24 - 138$

$= 6(162 - 138 \times 1) - 138$

$= 6 \times 162 - 7 \times 138$

$= 6 \times 162 - 7(3054 - 162 \times 18)$

$= 132 \times 162 - 7 \times 3054$

$= 132 \times (12378 - 4 \times 3054) - 7 \times 3054$

$= 132 \times 12378 + (-535) \times 3054.$

Exercise 1: Prove that $4 \nmid n^2 + 2$ for any integer n.

Exercise 2: The product of n consecutive integers is divisible by n.

Exercise 3: If x - y is even then $4 \mid n^2 - y^2$ where $x, y \in Z$.

Exercise 4: Show that $n \in Z$.

(i) $2 \mid n^2 - n$ (ii) $6 \mid n^3 - n$

(iii) $30 \mid n^5 - n$ (iv) $8 \mid n^2 - 1$ if n is odd.

Exercise 5: If x and y are odd, then $x^2 + y^2$ is even but not divisible by y.

Exercise 6: Prove or disprove,

(i) $a^2 \mid c^3 \Rightarrow a \mid c$

(ii) If $b \mid a^2 - 1$ then $b \mid a^4 - 1$

(iii) If $b \mid a^2 + 1$ then $b \mid a^4 + 1$.

Exercise 7: If $n \geq 2$ and k is an +ve integer,

(i) $(n - 1) \mid n^k - 1$

(ii) $(n - 1)^2 \mid n^k - 1$ iff $n - 1 \mid k$.

Exercise 8: If $(a, b) = (a, c)$ then $(a, b) = (a, b, c)$

Proof: To show $(a, b) = (a, b, c)$ let $d = (a, b) = (a, c)$.

$\therefore$ $d \mid a, d \mid b$ and $d \mid c$.

Suppose $k \mid a, k \mid b$ and $k \mid c$.

$\therefore$ $k \mid a, k \mid b \Rightarrow k \leq d$ as $d = (a, b)$

Therefore $d = (a, b, c)$

Exercise 9: If $(a, b) = 1$ then $(a^2, ab, b^2) = 1$.

Proof: Given $(a, b) = 1$ to show $(a^2, ab, b^2) = 1$.

If $(a, b) = 1 \Leftrightarrow 1 = ax + by$ for some integer x and y.

$\Leftrightarrow 1 = x^2a^2 + b^2y^2 + 2abxy$

$\Rightarrow 1 = (a^2, ab, b^2)$.

Exercise 10: If $2^k - 1$ is a prime number then show that k is also a prime number.

Solution: Let k be a composite number. then $k = ab$ where a, b are integers with $1 < a < k$, and $1 < b < k$. Then the integer $n = 1 + 2^a + \ldots + 2^{(b-1)a}$ is greater than 1. As a sum of geometric series, we get

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

i.e., $2^k - 1 = (2^a - 1)n$.

Since $a > 1$ we get, $2^a - 1 > 1$. hence $2^k - 1$ is a composite number.

We thus get, if $2^k - 1$ is a prime number, then k is also a prime number.

Exercise 11: True or false? For any $n \geq 1, 2^{2^n} + 1$ is a prime.

Ans: False, Euler showed that $1735 = 2^{2^5} + 1$ is not a prime.

Exercise 12: If $(a, b) = 1$ show that $(a + b, a - b)$ is either 1 or 2.

Exercise 13: show that if $ad - bc = 1$, then $(a + b, c + d) = 1$.

Exercise 14: show that if $a + b \neq 0$, $(a, b) = 1$ and p is an odd prime, then

$$\left(a+b, \frac{a^p + b^p}{a+b}\right) = 1 \text{ or } p.$$

Exercise 15: If $(a, b) = 1$, then $(a + b, a^2 - ab + b^2) = 1$ or 3.

Defination 1.17. Least Common Multiple (LCM): The lcm of two integers a and b denoted by [a, b] is the +ve integer m satisfying,

(i) $a \mid m, b \mid m$

(ii) If $a \mid c, b \mid c$ with $c > 0$ then $m \leq c$.

Similarly lcm of $a_1, a_2 \ldots, a_m$ is denoted by $[a_1, a_2 \ldots, a_m]$. e.g. $[-12, 30] = 60$.

Note: $a \mid\mid ab \mid$ and $b \mid\mid ab \mid$ and so $[a, b] \leq \mid ab \mid$.

1.18. Theorem: If $m > 0$ then $[ma, mb] = m[a, b]$ and $[a, -b] = [a, b]$.

Proof: [ma, mb] is multiple of both ma and mb and so it is multiple of m.

Let $[ma, mb] = mh_1$.

Let $[a, b] = h_2$. To show $h_1 = h_2$.

$[a, b] = h_2 \Rightarrow a \mid h_2, b \mid h_2$

$\Rightarrow am \mid mh_2, bm \mid mh_2$

$\Rightarrow mh_1 \leq mh_2$ $\quad (\because [ma, mb] = mh_1)$

$\Rightarrow h_1 \leq h_2$.

$am \mid mh_1$ and $bm \mid mh_1$ as $[ma, mb] = mh_1$

$\Rightarrow a \mid h_1$ and $b \mid h_2$

$\Rightarrow [a, b] \leq h_1$.

$\Rightarrow h_2 \leq h_1$.

$\therefore \quad h_1 = h_2$. $\quad$ Hence $[ma, mb] = m[a, b]$.

2nd part:

Let $[a, -b] = k_1$ and $[a, b] = k_2$.

Now $[a, -b] = k_1 \Rightarrow a \mid k_1, -b \mid k_1$

$\Rightarrow a \mid k_1, b \mid k_1$

$\Rightarrow [a, b] \le k_1$

$\Rightarrow k_2 \le k_1$.

And $[a, b] = k_2$

$\Rightarrow a \mid k_2$ and $b \mid k_2$

$\Rightarrow a \mid k_2$ and $-b \mid k_2$

$\Rightarrow [a, -b] \le k_2$

$\Rightarrow k_1 \le k_2$. Thus $k_1 = k_2$ i.e. $[a, -b] = [a, b]$.

1.19. Theorem: $[a, b]\,(a, b) = |ab|$.

Proof:

Case I : When $a > 0, b > 0$.

Put $d = (a, b)$.

Let $a = dr$ and $b = ds$.

To show $[a,b] = \frac{ab}{d} = m$ $(\because a > 0, b > 0)$.

$$m = \frac{ab}{d} = rb = sa.$$

$\therefore$ $a \mid m$ and $b \mid m$.

Let c be any positive integer such that $a \mid c$ and $b \mid c$.

Let $c = au = bv$.

We know that $d = ax + by$ for some integers x and y.

Then $\frac{c}{m} = \frac{cd}{ab}$ $\left(\because m = \frac{ab}{d}\right)$

$$= \frac{c(ax + by)}{ab}$$

$$= \left(\frac{c}{b}\right)x + \left(\frac{c}{a}\right)y$$

$= ux + vy$, which is an integer.

$\therefore$ $c = m(ux + vy)$.

$\Rightarrow m \mid c$.

$\therefore$ $m = [a, b]$

$$\Rightarrow \frac{ab}{(a,b)} = [a, b]$$

$\Rightarrow (a,b)[a,b] = ab = |ab| \qquad \because a > 0, b > 0.$

Case II : When $a > 0, b < 0$

$$(a, b)[a, b] = (a, -b)[a, -b]$$
$$= a(-b) = |ab|$$

Similarly it is true when $a < 0, b < 0$.

Definition 1.20. Prime Number: An integer $p > 1$ is called a prime number or simply a prime if its only divisors are 1 and p.

An integer greater then 1 which is not a prime is called composite number.

1 is neither prime nor composite.

Theoerm 1.21.: If p is a prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proof: Let p be a prime and $p \mid ab$ and $p \nmid a$.

We have to show $p \mid b$.

$p \nmid a \Rightarrow (p, a) = 1.$

$\Rightarrow 1 = px + ay \qquad (x, y \in z)$

$\Rightarrow b = bpx + bay$

$= bpx + pk_1y \qquad (\because p \mid ab)$

$= p(bx + k_1y)$

$\therefore \quad p \mid b.$

Proved.

Corollary 1: If p is a prime and $p \mid a_1a_2 \ldots a_n$ then $p \mid a_k$, for some k, where $1 \le k \le n$.

Proof: We prove it by the method of induction. This is proved for $n = 2$.

Suppose $p \mid a_1a_2 \ldots a_{k-1} \Rightarrow p \mid a_i$ for some $1 \le i \le k - 1$.

Let $\quad p \mid a_1a_2 \ldots a_k$

$\Rightarrow p \mid (a_1a_2 \ldots a_k)\, a_k$

$\Rightarrow p \mid a_1a_2 \ldots a_k$ or $p \mid a_k$

$\Rightarrow p \mid a_i$ or $p \mid a_k$ for some $1 \le i \le k - 1$.

$\Rightarrow p \mid a_i,\ 1 \le i \le k.$ Hence proved.

Corollary 2: If $p, q_1, q_2, \ldots, q_n$ are all primes and $p \mid q_1q_2 \ldots q_n$, then $p = q_k$ for some k, where $0 \le k$

$\leq n$.

Proof: $p \mid q_1 q_2 \cdots q_n$

$\Rightarrow p \mid q_k$ for some k, $1 \leq k \leq n$

$\Rightarrow p = q_k$, since q_k has only two factors 1 and q_k.

1.22. Fundamental Theorem of Arithmatic: Every positive integer $n > 1$ can be expressed as a product of prime; this representation is unique apart from the order in which the factors occur.

Proof: The integer n is either prime or composite. If n is a prime, there is nothing to prove.

Suppose n is a composite. Then $\exists$ an integer d such that $d \mid n$ and $1 < d < n$.

By well ordering property the set of divisors of n has the smallest member say p_1. then p_1 must be a prime. Otherwise p_1 has a divisior q such that $1 < q < p_1$. Then $q \mid p_1$ and $p_1 \mid n \Rightarrow q \mid n$, which contradicts the choice of p_1 as a smallest positive divisor of n not equal to L.

$\therefore$ We can write $n = p_1 n_1$ where p_1 is a prime, $1 < n_1 < n$.

If n_1 happens to be prime then we have the required representation. If not proceeding as above we have a prime p_2 such that $n_1 = p_2 n_2$.

Thus $n = p_1 p_2 n_2$, $1 < n_2 < n_1$.

If n_2 is prime it is not required to go further. Otherwise, ther is a prime p_3 such that $n_2 = p_3 n_3$.

Hence $n = p_1 p_2 p_3 n_3 \quad 1 < n_3 < n_2$.

The decreasing sequence $n > n_1 > n_2 \ldots > 1$ can't continue indefinitely. So, after a finite number of steps n_{k-1} is a prime, say p_k.

This leads to the prime factorization,

$n = p_1 p_2 p_3 \cdots p_k$.

Uniqueness: Let us suppose that the integer n can be represented as product of primes in two ways, says,

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \qquad (r \leq s)$$

where p_i and q_j are primes written is increasing magnitudes so that $p_1 \leq p_2 \leq \ldots \leq p_r$ and $q_1 \leq q_2 \leq \ldots \leq q_s$.

Now $p_1 \mid q_1 q_2 \cdots q_s$

$\Rightarrow p_1 = q_i \geq q_1$

$\therefore \quad p_1 \geq q_1$.

Similarly $q_1 \mid p_1 p_2 \cdots p_r$

$\Rightarrow q_i = p_j \geq p_1$

$\therefore \quad p_1 = q_i$.

Cancelling the common factor we have,

$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$

We repeat the process to get, $p_2 = q_2$ and again cancelling the common factor we get,

$p_3 \cdots p_r = q_3 \cdots q_s$.

and continue the process.

If $r < s$ then we have, $1 = q_{r+1} q_{r+2} \ldots q_s$ which is absurd since $q_i > 1$.

Hence $r = s$.

$\therefore \quad p_1 = q_1, p_2 = q_2 \cdots p_r = q_s = r$.

$\therefore \quad n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_r$ with $p_i = q_i$.

making the two factors identical.

Corollary: Any positive integer $n > 1$ can be written uniquely in a Canonical form $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$.

Where k_i is +ve integer and each p_i is a prime with $p_1 < p_2 < \ldots < p_r$.

Proof: By the fundamental theorem of Arithmatic we have $n = p_1 p_2 .. p_r$ where p_i's are primes.

Several of the primes which appear in factorization may be repeated. By collecting like primes and repalcing them by simple factor we get the Canonical form $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$.

Exercise: Show that every integer has atleast one prime factor.

Proof: Suppose n be any integer, then either n is prime or n is composite.

If n is prime, then there is nothing to prove.

Suppose n is composite. Then $\exists$ integer d such that $d \mid n$. By well ordering property, the set of divisors of n has the smallest number p_1. Then p_1 must be a prime otherwise p_1 has divisors q such that $1 < q < p_1$.

Then $q \mid p_1$ and $p_1 \mid n \Rightarrow q \mid n$, which contradicts the choice of p_1 asa smallest positive divisor of n not equal to 1.

Thus we can write $n = p_1 n_1$, where p_1 is a prime.

Thus every integer has atleast one prime factor.

1.23. Theorem: There is a infinity of primes.

Proof: Suppose there are finite no of primes $p_1, p_2, \ldots, p_r$.

Now we have to construct a new prime.

Consider $k = p_1p_2 \cdots p_n + 1$.

This shows that when k is divided by the primes, $p_1, p_2, \ldots, p_n$ the remainder is 1. So k is not divisible by the primes $p_1, p_2, \ldots, p_n$. We know that every integer must have a prime factor. So there must exists a prime other then these n primes or k itself is a prime. hence the no of primes cannot be finite.

1.24. Theorem: There are arbitrary gaps between primes.

or Given a positive integer k, there are k consecutive integers none of which is a prime.

Proof: Let k be a positive integer.

Consider $\underline{|k+1}+2, \underline{|k+1}+3, \ldots, \underline{|k+1}+k, \underline{|k+1}+k+1$.

Every one of these is a composite because, j divides $\underline{|k+1}+j$ if $2 \le j \le k+1$.

So there are k consecutive composite numbers.

Hence there are arbitrary gaps between primes.

1.25. Theorem: If p_n is the nth prime then $p_n \le 2^{2^{n-1}}$. There are atleast n + 1 primes less than 2^{2^n}.

Proof: Let us first see that $p_{n+1} \le p_1p_2 \cdots p_n + 1 < p_n^n + 1$.

Let $m = p_1p_2 \ldots p_n + 1$, m is not divisible by $p_1, p_2, \ldots, p_n$.

So m is either a prime or divisible by a prime $p_r + 1$ between p_r and m.

i.e. $p_n < p_{n+1} \le m$.

i.e. $p_{n+1} \le p_1p_2 \cdots p_n + 1$

$< p_np_n \cdots p_n + 1$

$= p_n^n + 1$.

Now we prove by induction that $p_n \le 2^{2^{n-1}}$.

For $n = 1, p_1 = 2 = 2^{2^{1-1}} = 2$.

Assume n > 1 and that the result holds for all integers upto n. then

$$p_{n+1} \le p_1p_2 \cdots p_n + 1 < 2\,2^2\,2^{2^2} \ldots 2^{2^{n-1}} + 1$$

$$= 2^{1+2+2^2+\ldots+2^{n-1}} + 1$$

$$= 2^{\frac{2^n-1}{2-1}} + 1$$

$$= 2^{2^n-1} + 1$$
$$< 2^{2^n-1} + 2^{2^n-1}$$
$$= 2.2^{2^n-1}$$
$$= 2^{2^n}$$

So by induction, $p_n \leq 2^{2^n-1}$.

Corollary: There are atleast n + 1 primes less then 2^{2^n}.

Proof: Clearly $p_1 < p_2 < p_3 < \ldots < p_n < p_{n+1} \leq 2^{2^n}$.

Thus there are atleast n + 1 primes less then 2^{2^n}.

1.26. Theorem: there are infinite no primes of the form 4n + 3.

Proof: Suppose there exists on the finite no of primes of the form 4n + 3. Call these $q_1, q_2, \ldots, q_s$.

Consider the positive integer,

$$n_0 = 4q_1q_2\ldots q_s - 1$$
$$= 4(q_1q_2\ldots q_s - 1) + 3$$

Let $n_0 = r_1r_2\ldots r_t$ be its prime factorization.

Since n_0 is an odd integer $r_k \neq 2$ for all k.

So $r_k = 4n + 1, 4n + 3$.

All r_k cann't be of the form 4n + 1, since product of two or more integers of the form 4n + 1 is of the form 4n + 1.

So atleast one r_k say r_i is of the form 4n + 3.

$r_i \mid n_0$ and $r_i \mid 4q_1q_2\ldots q_s$.

$\Rightarrow r_i \mid (4q_1q_2\ldots q_s - r_0) = 1$.

Which is absurd since $r_i > 2$.

So the assumption is wrong. There must be infinite prime of the form 4n + 3.

Exercise 1: If p is a prime and a and b are positive integers such that $p \mid a$ and $p \mid a^2 + b^2$ then $p \mid b$.

Exercise 2: If x and y are integers(odd) then $x^2 + y^2$ cannot be a perfect square.

Exercise 3: Prove that any two integers if both not equal to zero have a unique ged.

Exercise 4: Show that the product of two consecutive integers can never be a square.

Exercise 5: For $n \geq 1$ prove that $\frac{1}{6}n(n+1)(2n+1)$ is an integer.

Exercise 6: If a, b, c are any three integers such that (a, c) = 1 and (b, c) = 1, then show that (ab, c) = 1.

Exercise 7: Prove that 19 is not a divisor of $4n^2 + 4$ for any integer n.

Summary

- Any non-zero integer has only a finite number of divisors.
- Any common divisor of 'a' and 'b' is a divisor of their greatest common divisor (a, b).
- A common multiple of 'a' and 'b' is a multiple of the least common multiple [a, b].
- A necessary and sufficient condition for [a, b] = ab is (a, b) = 1.
- If a, b > 0, then [a, b] (a, b) = ab.
- The infinite set of integers $a_1, a_2, \ldots, a_n, \ldots$ also has the greatest common divisor $(a_1, a_2, \ldots, a_n, \ldots)$.
- The greatest common divisor of two numbers is always unique.
- The least common multiple of two numbers is always unique.
- A positive integer which is greater than 1 and has only two positive divisors 1 and itself is called a prime number.
- A number (> 1) which is not prime, is called composite number.
- For any integer n (> 1), there are n consecutive composite numbers.
- The sequence of primes does not come to an end, i.e. number of primes is infinite.
- If p is prime, and $p \mid ab$ then then $p \mid a$ or $p \mid b$.
- 2 is only even number, which is prime.
- If (a, b) = 1, then there are infinitely many primes of the form aq + b.
- If a and b are two odd integers, then $a^2 + b^2$ cannot be a perfect square.
- Fundamental theorem of arithmetic states that, 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.

Unit - 2
Congruences

Introduction :

The theory of congruences was introduced by carl Friedrich Gauss (1777-1855), one of the greatest mathematician of all times. Gauss contributed to the theory of numbers in many outstanding ways, including the basic idea of this unit. Although Pierre de Fermat (1601-1665) has earlier studied number theory in a somewhat systematic way, Gauss was first to develop the subject as a branch of mathematics, rather than just a scattered collection of interesting problems. In this book "Disquisitioner Arithmatic" written at age 24, Gauss introduced the theory of congruences, which gained ready acceptance as a fundamental tool for the study of number theory.

Definition 2.1. : Let n be a fixed positive integer. Two integers a and b are said to be congruence modulo n symbolised by $a \equiv b \pmod{n}$ if $n \mid a - b$. i.e., $a - b = nk$, for some integer k.

e.g. $3 \equiv 24 \pmod 7$

$-31 \equiv 11 \pmod 7$

$-15 \equiv -64 \pmod 7$

when $n \nmid a - b$ then we say that a is incongruent to b modulo n and in this case we write $a \not\equiv b \pmod n$.

For example, $25 \not\equiv 12 \pmod 7$, since $7 \nmid (25 - 12)$.

Note :

(i) $1 \mid a - b$ so $a \equiv b \pmod 1$ for all integers a and b.

(ii) Two integers are congruent modulo 2 when they are both even or both odd.

(iii) Given an integer a let q and r be its quotient and remainder on division by n. So that

$a = qn + r$

$\Rightarrow n \mid q - r$

$\Rightarrow q \equiv r \pmod a$.

(iv) Every integer is congruent modulo n to exactly one of the values of 0, 1, 2, ..., n - 1.

Let a be any integer. Then

$a = qn + r, \quad 0 \le r \le n.$

$\Rightarrow a \equiv r \pmod n \quad$ for $r = 0, 1, 2, ..., n - 1$

The set {0, 1, 2, ..., n - 1} is called the set of **least positive residues modulo n**.

For example, for n = 5, {0, 1, 2, 3, 4} is the set of residues modulo 5.

$100 \equiv 0 \pmod 5$

$111 \equiv 1 \pmod 5$

Definition 2.2. : A collection of n integers $a_1, a_2, ..., a_n$ is said to form a **complete set of residue modulo n** if every integer is congruent modulo n to one and only one of the a_i's.

Theorem 2.1. : For arbitrary integers a and b, $a \equiv b \pmod n$ iff a and b leave the same non-negative remainder when divided by n.

Proof : Suppose $a \equiv b \pmod n$

$\Rightarrow a = b + kn$ (for some integer k) .....(1)

Let r be the remainder when a is divided by n. i.e.,

$a = qn + r.$

Now (i) $\Rightarrow$ $b = a - kn$

$= qn + r - kn$

$= (q - k)n + r.$

So remainder is r when b is divided by n.

Conversely suppose

$a = q_1 n + r$

$b = q_2 n + r.$

$\therefore$ $a - b = (q_1 - q_2)n$

$\Rightarrow n \mid a - b$

$\Rightarrow a \equiv b \pmod n$ $\therefore$ Proved.

Theorem 2.2. :

(i) $a \equiv a \pmod n$.

(ii) $a \equiv b \pmod n \Rightarrow b \equiv a \pmod n$.

(iii) If $a \equiv b \pmod n$, $b \equiv c \pmod n$ then $a \equiv c \pmod n$.

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

$a + c \equiv b + d \pmod n$

and $ac \equiv bd \pmod n$.

(v) $a \equiv b \pmod n$ then

$ac \equiv bc \pmod n$.

(vi) $a \equiv b \pmod n$ then

$a^k \equiv b^k \pmod n$, $\forall\ k \geq 1$.

Proof:

(i) $a - a = 0$.

$\therefore$ $n \mid a - a$

$\therefore$ $a \equiv a \pmod{n}$.

(ii) $a \equiv b \pmod{n}$.

$\therefore$ $n \mid a - b$

$\Rightarrow n \mid b - a$

$\Rightarrow b \equiv a \pmod{n}$

(iii) $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$

$\therefore$ $n \mid a - b$ and $n \mid b - c$.

$\therefore$ $n \mid (a - b) + (b - c)$

$\therefore$ $n \mid a - c$.

$\therefore$ $a \equiv c \pmod{n}$.

(iv) $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$

$\therefore$ $n \mid a - b$ and $n \mid c - d$.

$\Rightarrow a - b = q_1 n$ and $c - d = q_2 n$ for $q_1, q_2 \in Z$.

Now $(a + c) - (b + d) = (a - b) + (c - d)$

$= q_1 n + q_2 n$

$= (q_1 + q_2)n$.

$\therefore$ $n \mid (a + c) - (b + d)$

$\therefore$ $a + c \equiv b + d \pmod{n}$

and $ac - bd = ac - bc + bc - bd$

$= c(a - b) + b(c - d)$

$= cq_1 n + bq_2 n$

$= n(2q_1 + bq_2)$.

$\therefore$ $n \mid ac - bd$.

$\therefore$ $ac \equiv bd \pmod{n}$.

$a \equiv b \pmod{n}$

$\therefore$ $n \mid a - b$

$\therefore$ $a - b = nq_1$ for $q_1 \in z$.

Now $ac - bc = c(a - b)$

$= cnq_1$

$\therefore$ $n \mid ac - bc$.

$\therefore$ $ac \equiv bc \pmod n$.

(vi) Given $a \equiv b \pmod n$,

$n \mid a - b$.

$a^k \equiv b^k \pmod n$ is clearly true for $k = 1$.

Suppose $a^k \equiv b^k \pmod n$.

Also $a \equiv b \pmod n$.

$\therefore$ By (iv) $a\,a^k = b\,b^k \pmod n$

$\Rightarrow a^{k+1} = b^{k+1} \pmod n$.

Hence by induction, $a^k \equiv b^k \pmod n$ $\forall\, k \geq 1$.

Exercise : Show that $41 \mid 2^{20} - 1$.

Proof : $2^5 \equiv -9 \pmod{41}$

$\Rightarrow (2^5)^4 \equiv 81^2 \pmod{41}$

$\Rightarrow 2^{20} \equiv (81)^2 \pmod{41}$

Also $81^2 \equiv 1 \pmod{41}$

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

$\Rightarrow 41 \mid 2^{20} - 1$.

Exercise : Find the remainder when $\underline{|1} + \underline{|2} + \underline{|3} + \ldots + \underline{|99} + \underline{|100}$ is divided by 12.

Ans : $\underline{|4} = 24 \equiv 0 \pmod{12}$ and

for $k \geq 4$, $\underline{|k} = \underline{|4}(5.6.7.\ldots\ldots k)$

$\equiv 0 \pmod{12}$

$\therefore$ $\underline{|1} + \underline{|2} + \underline{|3} + \ldots + \underline{|100} \equiv 1 + 2 + 6 + 0 + \ldots + 0 \pmod{12}$

$\equiv 9 \pmod{12}$

Thus when $\underline{1} + \underline{2} + \ldots + \underline{100}$ is divided by 12 rremainder is 9.

Theorem 2.3. : If $ca \equiv cb \pmod{n}$ then $a \equiv b \left(\bmod \frac{n}{d} \right)$ where $d = \gcd(c, n)$.

Proof : We can write,

$ca - cb = nk$ for some integer k. .....(1)

Now $d = \gcd(c, n)$

$\Rightarrow d \mid c$ and $d \mid n$

$\Rightarrow c = dr$ and $n = ds$.

Substituting the value of c and n in (i),

$dr\,a - dr\,b = ds\,k$

$\Rightarrow r(a - b) = sk$

$\Rightarrow s \mid r(a - b)$ and $\gcd(r, s) = 1$.

$\Rightarrow s \mid a - b$ (by Euclid's lemma).

$\therefore \quad a \equiv b \pmod{s}$

$\therefore \quad a \equiv b \left(\bmod \frac{n}{d} \right)$.

Corollary :

(i) If $\gcd(c, n) = 1$, then

$ca \equiv cb \pmod{n} \Rightarrow a \equiv b \pmod{n}$.

Corollary :

(ii) If $ca \equiv cb \pmod{p}$ and $p \nmid c$, where p is a prime number, then $a \equiv b \pmod{p}$.

If $p \nmid c \Rightarrow \gcd(p, c) = 1$.

$\therefore \quad ca \equiv cb \pmod{p} \Rightarrow a \equiv b \pmod{p}$.

Linear Diophantine Equation :

Any equation in one or more unknowns which is to be solved in the integers is called Diophantine equation. The simplest form of Diophantine equation is,

$ax + by = c$

where a, b, c are given integers and a, b not zero. (x_0, y_0) is called a solution of this equation if

$ax_0 + by_0 = c$.

Theorem : A linear diophantine equation $ax + by = c$ has a solution iff $d \mid c$ where $d = \gcd(a, b)$.

If (x_0, y_0) is any particular solution of this equation, then all other solutions are given by

$$x = x_0 + \left(\frac{b}{d}\right)t \text{ and } y = y_0 - \left(\frac{a}{d}\right)t, \qquad \text{for varing integer } t.$$

Proof : Suppose $ax + by = c$ has a solution (x_0, y_0)

$d = \gcd(a, b)$

$\therefore$ $a = dr, b = ds.$

Now $ax_0 + by_0 = c$

$\Rightarrow drx_0 + dsy_0 = c$

$\Rightarrow d(rx_0 + sy_0) = c$

$\Rightarrow d \mid c.$

Conversely suppose $d \mid c$, then $c = dt$ for some t.

$d = \gcd(a, b)$

$\Rightarrow \exists$ integers x_0 and y_0 such that $d = ax_0 + by_0$.

$\Rightarrow dt = ax_0t + by_0t.$

$\Rightarrow c = a(x_0t) + b(y_0t).$

$\therefore$ $ax + by = c$ has a solution (x_0t, y_0t)

2 nd part :

Suppose (x_0, y_0) is a solution of $ax + by = c$ then

$ax_0 + by_0 = c.$

Let (x', y') be any other solution of $ax + by = c$ then

$ax' + by' = c.$

Now $a(x_0 - x') = b(y' - y_0).$

$\Rightarrow dr(x_0 - x') = ds(y' - y_0)$

$\Rightarrow r(x_0 - x') = s(y' - y_0)$ .....(1)

$\Rightarrow s \mid r(-x_0 + x')$

$\Rightarrow s \mid (-x_0 + x')$ ($\because \gcd(r, s) = 1$)

$\Rightarrow -x_0 + x' = st$

$\Rightarrow x' = x_0 + \left(\frac{b}{d}\right)t$ .....(*)

Also (i) $\Rightarrow r \mid s(y_0 - y')$ with $\gcd(r, s) = 1$.

$\Rightarrow r \mid y_0 - y'$

$\Rightarrow y_0 - y' = rt$

$\Rightarrow y' = y_0 - rt$

$$= y_0 - \left(\frac{a}{d}\right)t \qquad \text{.....(**)}$$

From (*) and (**) we get the required result.

Example : Solve $172x + 20y = 1000$.

Ans : $172 = 8 \times 20 + 12$

$20 = 1 \times 12 + 8$

$12 = 1 \times 8 + 4$

$8 = 2 \times 4$.

Thus $\gcd(172, 20) = 4$ and $4 \mid 100$.

Thus the equation $172x + 20y = 1000$ has a solution.

Now $4 = 12 - 1 \times 8$

$= 12 - 1(20 - 1 \times 12)$

$= 2 \times 12 - 20$

$= 2 \times (172 - 8 \times 20) - 20$

$= 2 \times 172 + (-17) \times 20$

$\therefore \quad 1000 = 500 \times 172 + (-4250) \times 20$

$\therefore \quad x_0 = 500$ and $y_0 = -4250$ is a solution.

General solutions are,

$$x = x_0 + \left(\frac{b}{d}\right)t \quad \text{and} \quad y = y_0 - \left(\frac{a}{d}\right)t$$

$= 500 + 5t$ $\qquad = -4250 - 43t$.

For positive solution

$500 + 5t > 0$ and $-4250 - 43t > 0$

$t > -100$ $\qquad t < -\frac{4250}{43} = -98\frac{36}{43}$

$\therefore \quad t = -99$

$\therefore$ $x = 500 + 5(-99) = 500 - 495 = 5$

$y = -4250 - 43(-99) = 7.$

$\therefore$ (5, 7) is the only positive solution.

Exercise : Solve $5x + 3y = 52$ in positive integer.

Ans : (8, 4), (5, 9), (2, 14).

Exercise : Solve $12x + 501y = 1$.

Try yourself.

The equation $12x + 501y = 1$ has no solution.

Exercise : Solve $10x - 7y = 17$.

Try yourself.

$\therefore$ There are infinite no of positive solutions.

Theorem 2.4. : Let $p(x) = \sum_{k=0}^{m} c_k x^k$ be a polynomial function of x with integral co-efficient c_k.

If $a \equiv b \pmod n$, then $p(a) \equiv p(b) \pmod n$.

Proof : $a \equiv b \pmod n$

$\Rightarrow a^k \equiv b^k \pmod n$ where $0 \le k \le m$.

$\Rightarrow c_k a^k \equiv c_k b^k \pmod n$

$\Rightarrow \sum_{k=0}^{m} c_k a^k = \sum_{k=0}^{m} c_k b^k \pmod n$

$\Rightarrow p(a) \equiv p(b) \pmod n$.

Definition 2.3. : If $p(x)$ is a polynomial with integral co-efficient then a is a solution of the congruence $p(x) \equiv 0 \pmod n$ if $p(a) \equiv 0 \pmod n$.

Corollary : If a is a solution of $p(x) \equiv 0 \pmod n$ and $a \equiv b \pmod n$ then b is also a solution of $p(x) \equiv 0 \pmod n$.

Proof : By theorem 4.4. $p(a) \equiv p(b) \pmod n$.

So $p(a) \equiv 0 \pmod n$

$\Rightarrow p(b) \equiv 0 \pmod n$

$\therefore$ a is a solution $\Rightarrow$ b is a solution.

Theorem 2.5. : If $N = a_m 10^m + a_{m-1} 10^{m-1} + ... + a_1 10 + a_0$ be decimal expansion of the positive integer N, $0 \le a_k < 10$ and let $S = a_0 + a_1 + a_2 + ... + a_m$.

Then $q \mid N$ iff $q \mid S$.

Try yourself.

Theorem 2.6. : Let $N = a_m 10^m + a_{m-1} 10^{m-1} + ... + a_1 10 + a_0$ be decimal expansion of the positive integer N, $0 \le a_k < 10$ and let, $T = a_0 - a_1 + a_2 + ... + (-1)^m$

Then $11 \mid N$ iff $11 \mid T$.

Try yourself.

Linear Congruence

A congruence of the form $ax \equiv b \pmod n$ is called a linear congruence and by a solution of it we mean an integer x_0 such that $ax_0 \equiv b \pmod n$.

x_0 is a solution of $ax \equiv b \pmod n$

$\Rightarrow ax_0 \equiv b \pmod n$

$\Rightarrow n \mid ax_0 - b$

$\Rightarrow ax_0 - b = nk$

$\Rightarrow b = ax_0 - nk$.

So finding solution of $ax \equiv b \pmod n$ is equivalent to find solution of the equation $ax - nk = b$.

Two solutions of $ax \equiv b \pmod n$ are taken to be equal if they are congruent mod n although they are not equal is usual sense. For example, the solution 3 and - 9 are equal solution of $3x \equiv 9 \pmod{12}$ since $3 \equiv -9 \pmod{12}$ when we refer to the number of solutions of $ax \equiv b \pmod n$, we mean the number of in congruent solutions.

Theorem : The linear congruence $ax \equiv b \pmod n$ has a solution iff $d = \gcd(a, n) \mid b$.

If $d \mid b$ then it has d mutually incongruent solutions of modulo n.

Proof : The equation has a solution iff $d = \gcd(a, x) \mid b$ and if (x_0, y_0) is a solution of it then other solutions are

$$x = x_0 + \left(\frac{n}{d}\right) t$$

and $y = y_0 - \left(\frac{a}{d}\right)t$ for some choice of t.

Among the various integers satisfying the first of these formula consider those that occur when t takes values t = 0, 1, 2, ..., d - 1.

$$x = x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}$$

we claim that these integers are in congruent modulo n, while all other such integers are incongruent to some one of them.

If it happened that,

$$x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 \pmod{n}, 0 \le t_1 \le t_2 \le d-1.$$

Then $\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \pmod{n}$

$$\Rightarrow t_1 \equiv t_2 \left(\mod \frac{n}{\gcd\left(n, \frac{n}{d}\right)} \right)$$

$$\Rightarrow t_1 \equiv t_2 \left(\mod \frac{n}{\frac{n}{d}} \right)$$

$\Rightarrow t_1 \equiv t_2 \pmod{d}$

$\Rightarrow d \mid t_1 - t_2$, which is impossible.

So $x_0, x_0 + \frac{n}{d}, \ldots, x_0 + \frac{n(d-1)}{d}$ are incogruent solutions.

It remains to show that any other solution $x_0 + \left(\frac{n}{d}\right)t$ is congruent modulo n to one of the above d incongruent solutions.

By division algorithm $t = qd + r$, where $0 \le r \le d - 1$.

Hence $x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}(qd + r)$

$$= x_0 + \frac{nr}{d} + nq$$

$$\equiv x_0 + \frac{nr}{d} (\text{mod } n)$$

where $0 \le r \le d-1$.

So any solution $x_0 + \frac{n}{d}t$ is congruent to one of the incongruent solutions.

Corollary : If gcd(a, x) = 1 then $ax \equiv b(\text{mod } n)$ has a unique solution modulo n.

Exercise 1. : Solve $18x \equiv 30(\text{mod } 42)$.

Ans : d = gcd(18, 42) = 6

and 6 | 30.

So $\exists$ 6 incongruent solution of $18x \equiv 30(\text{mod } 42)$.

By inspection $x_0 = 4$ is a solution of $18x \equiv 30(\text{mod } 42)$.

Required incongruent solution are,

$$4, 4+\frac{42}{6}, 4+\frac{42}{6}\times 2, 4+\frac{42}{6}\times 3, 4+\frac{42}{6}\times 4, 4+\frac{42}{6}\times 5$$

$x \equiv 4, 11, 18, 25, 32, 39(\text{mod } 42)$.

Chinese Remainder Theorem:

Theorem : Let $n_1, n_2, ..., n_r$ be positive integers such that

$\gcd(n_i, n_j) = 1$ when $i \ne j$.

Then the system of linear congruences

$x \equiv a_1(\text{mod } n_1)$

$x \equiv a_2(\text{mod } n_2)$

.....

$x \equiv a_r(\text{mod } n_r)$

has a simultaneous solution which is unique modulo the integers $n_1 n_2 ... n_r$.

Proof : We start with $n = n_1 n_2 ... n_r$ and write

$$N_k = \frac{n}{n_k} = n_1 n_2 ... n_{k-1} n_{k+1} ... n_r$$

$\gcd(n_i, n_k) = 1, i = 1, 2, ..., k-1, k+1, ..., r.$

$\gcd(N_k, n_k) = 1.$

Consider the congruence $N_k x \equiv 1(\text{mod } n_k)$.

According to existence theorem of $ax \equiv b(\text{mod } n)$. $N_k x \equiv 1(\text{mod } n_k)$ has a unique solution x_k.

We can prove that,

$$\bar{x} = a_1N_1x_1 + a_2N_2x_2 + \ldots + a_rN_rx_r$$

is a simultaneous solution of the given system.

$$N_i \equiv 0 \pmod{n_k} \text{ if } i \neq k.$$

(Since $N_k = \frac{n}{n_k} = n_1n_2 \ldots n_{k-1}n_{k+1} \ldots n_r$).

$$a_iN_ix_i \equiv 0 \pmod{n_k} \quad i = 1, 2, \ldots, k-1, k+1, \ldots, r$$

and $$a_kN_kx_k \equiv a_kN_kx_k \pmod{n_k}.$$

Adding, $$\bar{x} = a_1N_1x_1 + a_2N_2x_2 + \ldots + a_rN_rx_r$$

$$\equiv a_kN_kx_k \pmod{n_k}$$

$$\equiv a_k \pmod{n_k} \qquad [\because N_kx_k \equiv 1 \pmod{n_k}]$$

$\therefore$ $\bar{x}$ is the simultaneous solution.

Uniqueness:

Suppose x' be any other simultaneous solution. Then

$$\bar{x} \equiv a_k \equiv x' \pmod{n_k}.$$

$\therefore$ $$n_k \mid \bar{x} - x'$$

Because $\gcd(n_i, n_j) = 1$ we have,

$$n = n_1n_2 \ldots n_r \mid (\bar{x} - x')$$

Hence $\bar{x} \equiv x' \pmod{n}$.

So x' is unique modulo $n_1n_2 \ldots n_r$

Hence proved.

Exercise : Solve

$$x \equiv 2 \pmod 3$$

$$x \equiv 3 \pmod 5$$

$$x \equiv 2 \pmod 7$$

Solution : Let $n = 3 \times 5 \times 7$.

$$N_1 = 35, N_2 = 21, n_3 = 15.$$

We consider the linear congruences,

$35x \equiv 1 \pmod 3$ which has solution $x_1 = 2$

$21x \equiv 1 \pmod 5$ which has solution $x_2 = 1$

$15x \equiv 1 \pmod 7$ which has solution $x_3 = 1$

Let $\bar{x} = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3$

$= 70x_1 + 63x_2 + 30x_3$

$= 190 + 63 + 30$

$= 233.$

$\therefore$ 233 modulo$(3 \times 5 \times 7 = 105)$ is the required solution.

i.e., $\bar{x} \equiv 233 \pmod{105}$

$\equiv 23 \pmod{105}$.

Exercise : Solve $17x \equiv 9 \pmod{276}$.

Try yourself.

$\bar{x} \equiv 33 \pmod{276}$ is solution.

Question : Find all the integers which have remainders 1 or 2 when divided by each of 3, 4, 5.

Solution : We have to show,

$x \equiv a_1 \pmod 3$

$x \equiv a_2 \pmod 4$

$x \equiv a_3 \pmod 5$.

We have to consider eight cases,

	a_1	a_2	a_3
A	1	1	1
B	1	2	1
C	1	1	2
D	1	2	2
E	2	1	1
F	2	2	1
G	2	1	2
H	2	2	2

Case A: When $a_1 = a_2 = a_3 = 1$.

The equation are

$$x \equiv 1 (\text{mod } 3)$$

$$x \equiv 1 (\text{mod } 4)$$

$$x \equiv 1 (\text{mod } 5).$$

Let $n = 3 \times 4 \times 5$.

$N_1 = 4 \times 5 = 20$, $N_2 = 3 \times 5 = 15$, $N_3 = 3 \times 4 = 12$.

Consider

$20x \equiv 1 (\text{mod } 3)$ of which $x_1 = 2$ is solution

$15x \equiv 1 (\text{mod } 5)$ of which $x_2 = 1$ is solution

$12x \equiv 1 (\text{mod } 7)$ of which $x_3 = 1$ is solution

Let $\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3$

$= 40 + 45 + 36$

$= 121.$

Thus, $\bar{x} \equiv 121 (\text{mod } 60)$

$\equiv 1 (\text{mod } 60).$

Ist solution set, $\{\bar{x} = 60k + 1\} = \{1, 61, 121, ...\}$.

Similarly, we can solve for the cases B, C, D, E, F, G, H.

Fermat's Little Theorem : If p is a prime and $p \nmid a$ then $a^{p-1} \equiv 1 (\text{mod } p)$.

Proof : Consider the first (p - 1) positive multiples of a. i.e., the integers a, 2a, 3a, ...(p - 1)a.

None of these numbers is congruent modulo p to any other, nor is any to zero.

Indeed, if it happend that,

$ra \equiv sa (\text{mod } p)$, $1 < s < r < p - 1$

$\Rightarrow r \equiv s (\text{mod } p)$ $\quad (\because \gcd(p, a) = 1)$

$\Rightarrow p \mid r - s.$

which is not possible.

These numbers a,2a,3a, ..., (p - 1)a are congruent modulo p to 1, 2, 3,..., (p -1) taken in same order.

So $a.\ 2a.\ 3a, ...(p - 1)a \equiv 1.2.3....(p - 1) (\text{mod } p)$

$\Rightarrow a^{\underline{|p-1}} \equiv \underline{|p-1} (\text{mod } p)$

$\Rightarrow a^{\underline{|p-1}} \equiv 1 (\text{mod } p)$ $\quad \left(\because \gcd\left(\underline{|p-1}, p\right) = 1\right)$.

Corollary : If p is a prime then $a^p \equiv a(\text{mod } p)$, for any integer a.

Proof : If $p \mid a$, then $p \mid a^p$ and hence

$$p \mid a^p - a$$

$$\Rightarrow a^p \equiv a(\text{mod } p).$$

If $p \nmid a$, then by Fermat's Little Theorem

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

$$\Rightarrow a^p \equiv a(\text{mod } p)(\text{multiplying by a})$$

Thus in all cases, $a^p \equiv a(\text{mod } p)$.

Hence Proved.

Question : Varify that $5^{38} \equiv 4(\text{mod } 11)$.

Ans : By Fermat's Littlr Theorm,

$$5^{10} \equiv 5^{11-1} \equiv 1(\text{mod } 11)$$

$$\Rightarrow 5^{30} \equiv 1(\text{mod } 11)$$

$$\Rightarrow 5^{38} \equiv 5^8(\text{mod } 11) \text{ and } 5^2 \equiv 3(\text{mod } 11)$$

$$\Rightarrow 5^{38} \equiv 3^4(\text{mod } 11) \text{ and } 3^4 \equiv 4(\text{mod } 11)$$

$$\Rightarrow 5^{38} \equiv 4(\text{mod } 11).$$

Note : From the corollary if $a^p \not\equiv a \pmod p$ for same a, then p is a composite.

Question : Show that 117 is not prime.

Solution : It can be shown that,

$$2^{117} \not\equiv 2(\text{mod } 117)$$

$$2^{117} = 2^{7\times 16+5} = (2^7)^{16} \times 2^5.$$

$$2^7 = 128 \equiv 11(\text{mod } 117)$$

$$\Rightarrow (2^7)^{16} \equiv 11^{16}(\text{mod } 117)$$

$$\Rightarrow 2^{117} \equiv 11^{16} \times 2^5(\text{mod } 117)$$

$$\equiv (121)^8 \times 2^5(\text{mod } 117)$$

$$\equiv 4^8 \times 2^5(\text{mod } 117)$$

$$\equiv 2^{21}(\text{mod } 117)$$

$$\equiv (2^7)^3(\text{mod } 117)$$

$\equiv (128)^3 \pmod{117}$

$\equiv 11^3 \pmod{117}$

$\equiv 121 \times 11 \pmod{117}$

$\equiv 4 \times 11 \pmod{117}$

$\not\equiv 2 \pmod{117}$

Thus $2^{117} \not\equiv 2 \pmod{117}$.

This shows that 117 is not a prime.

Lemma : If p and q are distinct prime such that

$a^p \equiv a \pmod{q}$

$a^q \equiv a \pmod{p}$

Then $a^{pq} \equiv a \pmod{pq}$.

Proof : We have $a^p \equiv a \pmod{p}$ for any integer a.

Repalcing a by a^q,

$a^{pq} \equiv a^q \pmod{p}$

$\equiv a \pmod{p}$

$\therefore$ $p \mid a^{pq} - a$..

Similarly, $q \mid a^{pq} - a$

Thus $pq \mid a^{pq} - a$ $\because$ $(p, q) = 1$.

$\therefore$ $a^{pq} \equiv a \pmod{pq}$.

Note : The converse of Fermat's Little theorem is false. By Fermat's Little Theorem,

p is prime $\Rightarrow a^{p-1} \equiv 1 \pmod{p}$ if $p \nmid a$.

We show, $2^{341-1} \equiv 1 \pmod{341}$ but 341 is not a prime.

In fact $341 = 11 \times 31$.

$2^{10} = 1024 = 31 \times 33 + 1$.

$\therefore$ $2^{10} \equiv 1 \pmod{31}$ and $2^{10} \equiv 1 \pmod{11}$

$\Rightarrow 2^{11} \equiv 2 \pmod{31}$ $\Rightarrow 2^{11} \equiv 2 \pmod{11}$

$2^{31} = 2 \times (2^{10})^3$

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

$2^{341} = 2^{11 \times 31} \equiv 2 \pmod{11 \times 31}$

$\Rightarrow 2^{340} \equiv 1 (\text{mod } 341)$

$\Rightarrow 2^{341-1} \equiv 1 (\text{mod } 341)$

and $341 \nmid 2$, but 241 is not prime.

Wilson's Theorem : If p is a prime then $\underline{|p-1} \equiv -1 \pmod{p}$.

Proof : Proof is trivial for $p = 2$ and $p = 3$.

Let us take $p > 3$. Let a be any of the positive integers $1, 2, 3, \ldots, p - 1$.

We consider the congruence

$$ax \equiv 1 (\text{mod } p).$$

Since $\gcd(a, p) = 1$ this congruence has a unique solution modulo p. there is a unique integer a' such that $1 \leq a' \leq p - 1$ satisfying

$$aa' \equiv 1 (\text{mod } p).$$

Since p is prime,

$a \equiv a' (\text{mod } p)$ iff $a \equiv 1 (\text{mod } p)$ or $a \equiv p - 1 (\text{mod } p)$.

Indeed the congruence,

$a^2 \equiv 1 (\text{mod } p)$ is equivalent to,

$(a - 1)(a + 1) \equiv 0 (\text{mod } p)$.

So, either

$a - 1 \equiv 0 (\text{mod } p)$ or $a + 1 \equiv 0 (\text{mod } p)$

$\Rightarrow a \equiv 0 (\text{mod } p)$ $\Rightarrow a \equiv p - 1 (\text{mod } p)$.

If we omite the number 1 and $p - 1$ the effect is to group the remaining integers $2, 3, \ldots, p - 2$ into pairs a and a' where $a \neq a'$ such that

$$aa' \equiv 1 (\text{mod } p).$$

when these $\frac{p-3}{2}$ congruences are multiplied together and the factors rearranged, we get,

$2 . 3 . 4 \ldots (p - 1) \equiv 1 (\text{mod } p)$

$\Rightarrow 1 . 2 \ldots (p - 1) \equiv p - 1 (\text{mod } p) \equiv - 1 (\text{mod } p)$

$\Rightarrow \underline{|p-1} \equiv -1 \pmod{p}$.

Converse of Wilson's Theorem is also true : If $\underline{|n-1} \equiv -1 \pmod{n}$ then n is a prime.

Proof : If n is not a prime, then n has a divisior d, $1 < d < n$.

$$d \le n-1 \Rightarrow d \| \underline{n-1}$$

Given that $n \| \underline{n-1}+1$

and $d|n \Rightarrow d \| \underline{n-1}+1$

$\therefore \quad d|\left(\|\underline{n-1}+1\right)-\left(\|\underline{n-1}\right)$

$\Rightarrow d \mid 1$

$\Rightarrow d = 1$, which contradicts $1 < d$.

Thus n is a prime.

Application :

Theorem : The quadratic congruence $n^2+1 \equiv 0 \pmod p$ where p is an odd prime has a solution iff $p \equiv 1 \pmod 4$.

Proof : Let a be a solution of $n^2+1 \equiv 0 \pmod p$.

$\therefore \quad a^2 \equiv -1 \pmod p$.

By division algorithm $p = 4k+1$ or $4k+3$.

Put $p \neq 4k+3$.

If $p = 4k+3$ we have,

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

By Fermat's Theorem.

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

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

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

$$\equiv -1 \pmod p.$$

$\therefore \quad p \mid 2$

$\Rightarrow p = 2$, contradicts p is an odd prime.

Thus $p = 4k+1$.

$\therefore \quad 4 \mid p-1$

$\therefore \quad p \equiv 1 \pmod 4$.

Now for the opposite direction, consider the product,

$$\underline{|p-1} = 1.2\ldots\frac{p-1}{2}\frac{p+1}{2}\ldots(p-2)(p-1).$$

We have the condruences,

$p - 1 \equiv -1 \pmod p$

$p - 2 \equiv -2 \pmod p$

.....

$$\frac{p+1}{2} \equiv -\frac{p-2}{2} \pmod p.$$

Rearranging the factors produces,

$$\underline{|p-1} \equiv 1.(-1)2(-2)\ldots\frac{p-1}{2}\left(-\frac{p-1}{2}\right) \pmod p$$

$$\equiv (-1)^{\frac{p-1}{2}}\left(1.2\ldots\frac{p-1}{2}\right)^2 \pmod p$$

By Wilson's Theorem, $\underline{|p-1} \equiv -1 \pmod p$.

$$\therefore \quad -1 \equiv (-1)^{\frac{p-1}{2}}\left(\underline{\left|\frac{p-1}{2}\right.}\right)^2 \pmod p.$$

If we assume that p is of the form $4k+1$, then $(-1)^{\frac{p-1}{2}} = 1$ leaving us with the congruence,

$$-1 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod p.$$

Thus the quadratic congruence $n^2 + 1 \equiv 0 \pmod p$ has a solution $\left(\frac{p-1}{2}\right)!$.

Hence proved.

Question : Find the remainder when $2^{73} + 14^3$ is divided by 11.

Ans : We have to find x such that

$$2^{73} + 14^3 \equiv x \pmod{11}$$

Now $14 \equiv 3 \pmod{11}$

$\Rightarrow 14^3 \equiv 3^3 \pmod{11}$

$\Rightarrow 14^3 \equiv 5 \pmod{11}$ .....(1)

And $2^{10} \equiv 1 \pmod{11}$

$\Rightarrow 2^{70} \equiv 1 \pmod{11}$

$\Rightarrow 2^{73} \equiv 8 \pmod{11}$ .....(ii).

From (i) and (ii),

$2^{73} + 14^3 \equiv 13 \pmod{11}$

$\Rightarrow 2^{73} + 14^3 \equiv 2 \pmod{11}$.

$\therefore$ the remainder when $2^{73} + 14^3$ is divided by 11 is 2.

Problem : State true or false :

For any two relatively prime integers a and n, $a^{n-1} \equiv 1 \pmod{n}$.

Ans : This statement is not true as

$3^{4-1} = 3^3 = 27 \equiv 3 \pmod{4}$.

$\therefore$ $3^{4-1} \equiv 3 \pmod{4}$.

Thus $(3, 4) = 1$.

But $3^{4-1} \not\equiv 1 \pmod{4}$.

Problem : State true or false :

If $\lfloor\underline{n} \equiv -1 \pmod{n}$, then n must be a prime.

Ans : The statement is not true.

For $\lfloor\underline{n} \equiv -1 \pmod{n}$

$\Rightarrow n \mid \lfloor\underline{n} + 1$

and $n \mid \lfloor\underline{n}$

$\therefore$ $n \mid \left(\lfloor\underline{n} + 1\right) - \lfloor\underline{n}$

$\therefore$ $n \mid 1$

$\Rightarrow n = 1$, which is not prime.

Exercise :

1. If p is a prime and $a^2 \equiv b^2 \pmod{p}$ then prove that $p \mid a + b$ or $p \mid a - b$.
2. Solve $2x \equiv 3 \pmod{5}$

$4x \equiv 2 \pmod{6}$

$3x \equiv 2 \pmod{7}$.

3. If $a \equiv b(\text{mod } m)$ and $a \equiv b(\text{mod } n)$ and $k = [m, n]$ then prove that $a \equiv b(\text{mod } k)$.

Proof: Given $a \equiv b(\text{mod } m)$

$\therefore$ $m \mid a - b \Rightarrow a - b = mk_1$.

$a \equiv b(\text{mod } n)$

$\therefore$ $n \mid a - b \Rightarrow a - b = nk_2$.

4. Solve $17x \equiv 9(\text{mod } 276)$.

5. Find a number x such that

$x \equiv 3(\text{mod } 11)$

$x \equiv 5(\text{mod } 19)$

$x \equiv 10(\text{mod } 29)$

6. Find the least positive number x satisfying,

$2^{19} \equiv x(\text{mod } 7)$.

7. Solve $111x \equiv 75(\text{mod } 321)$.

8. Find all the integers that give the remainders 1, 2, 3 when divided by 3, 4, 5 respectively.

Summary

- An integer 'a' is said to be congruent to another integer b modulo n, n is any fixed positive integer if $n \mid a - b$. It is written as $a \equiv b$ (modn).
- All usual algebraic law hold for congruence.
- $a \equiv b$ (modn) if and only if 'a' and 'b' have the same remainders with respect to n.
- An expression of the form $ax \equiv b$ (modn), $a \neq 0$ is called a linear congruence modn.
- The linear congruence $ax \equiv b$ (modn) has solution if and only if $d \mid b$ where $d = \text{gcd}(a, m)$.
- A system of linear congruence $x \equiv a_i \text{ (mod } n_i)$ is solvable if and only if (n_i, n_j) divides $(a_i - a_j)$.
- Fermat's little theorem states that "If p is a prime and p X a, then $a^{p-1} \equiv 1$ (mod p).
- If p is prime, then $a^p \equiv a$ (mod p) for any integer a.
- If pand q are distinct primes such that $a^p \equiv a$ (mod q) and $a^q \equiv a$ (mod p), then $a^{pq} \equiv a$ (mod pq).
- Wilson's theorem states that "If p is a prime then $(P - 1)! \equiv -1$ (mod p).

■■■

Unit 3

Quadratic Resides

Introduction :

The subject of primitive roots is more powerful and interesting subject. In this unit, we discuss problems such as the existence of primitive roots, how to find them, the construction of reduced residice systems, the indices and so on. The problem of solving such a congruence as

$$x^2 \equiv a \pmod{p},\ p \nmid a \quad \ldots (1)$$

If (1) has solution, then a is the remainder of some square when divided by p. Therefore we say that a is a quadratic residue of p. Otherwise a is called a quadratic non-residue of p. In this unit we shall discuss the quadratic congruence and quadratic reciprocity law :

Primitive roots

Definition :

Let m be a positive integer and (a, m) = 1. If order of a(mod m) is $\phi(m)$ then a is called a **primitive root** of m.

For example 3 and 5 are primitive roots of 7

3 is primitive root of 4.

Question :

Does every positive integer has a primitive root?

We can show that the integers 2, 4, p^n, $2p^n$ where p is any odd prime and $n \geq 1$, have primitive roots and these are the only integers with primitive roots.

Theorem :

If a is a primitive root of n, then $a, a^2, \ldots, a^{\phi(n)}$ is a reduced set of residues (mod n).

Proof :

Since (a, n) = 1 we get $(a^i, n) = 1$ for all $i \geq 1$. Thus each of the integers in the set

$$a, a^2, \ldots, a^{\phi(n)} \quad \ldots\ldots(1)$$

is relatively prime to n. Next we show that the integers in the set(1) are mutually incongruent (mod n).

Let $1 \leq i < j \leq \phi(n)$.

Then $a^i \equiv a^j \pmod{n}$

$\Rightarrow a^{j-i} \equiv 1 \pmod{n}$

$\Rightarrow$ a is of order $\leq j - 1 \pmod{n}$

$\Rightarrow \phi(n) \leq j - 1$

which is impossible. Thus the set (1) consists of $\phi(n)$ mutually incogruent integers (mod n) each of which is relatively prime to n. Hence (1) is a reduced set of residues (mod n).

Theorem :

If n is a primitive root, then it has exactly $\phi(\phi(n))$ of them.

Proof :

Suppose that a is a primitive root of n. Then $\{a, a^2, ..., a^{\phi(n)}\}$ is a reduced set of residues (mod n). Thus the number of primitive roots of n is the number of integers in $\{a, a^2, ..., a^{\phi(n)}\}$ which are primitive roots of n.

Next we prove the following lemma.

Lemma :

If the integer b has order k modulo n, and $h > 0$, then h has order $\frac{k}{(h,k)}$ modulo n.

Proof of the lemma :

Let $d = (h, k)$. Then we may write $h = h_1 d$, $k = k_1 d$, where $(h_1, k_1) = 1$.

Clearly $(b^h)^{k_1} = b^{h_1 d k_1} = (b^k)^{h_1} = 1 \pmod n$.

Now if b^h has order r modulo n, the $r \mid k_1$. On the other hand, since b has order k modulo n, from the fact that

$$b^{hr} \equiv (b^h)^r \equiv 1 \pmod n$$

We get, $k \mid hr$

Thus $k_1 d \mid h_1 dr$

i.e., $k_1 \mid h_1 r$ or $k_1 \mid r$ $(\because (h_1, k_1) = 1)$

Because k_1, r are positive, we get $r = k_1$.

Hence order of $b^h \pmod n$

$$= k_1 = \frac{k}{d} = \frac{k}{(h,k)}.$$ This proves the lemma.

In view of the lemma we get, for each i, order of $a^i \pmod n = \frac{\varphi(n)}{(i, \varphi(n))}$. Thus a^i is a primiative root of n if and only if $(i, \phi(n)) = 1$. Since there are $\phi(\phi(n))$ values of i in the set $\{1, 2, ..., \phi(n)\}$ such that $(i, \phi(n)) = 1$, we get there are $\phi(\phi(n))$ primitive roots of n in the set $\{a, a^2, ..., a^{\phi(n)}\}$. This completes the proof.

Lemma 1 :

If p is a prime and $d \mid p-1$, then the convergence $x^d - 1 \equiv 0 \pmod p$ has exactly d incongruent roots, and $\phi(d)$ of these roots have order d (mod p).

Proof :

Since $d \mid (p-1)$ we have,

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

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

Now by Formats Theorem, the congruence

$$x^{p-1} - 1 \equiv 0 \pmod p \qquad \ldots\ldots(1)$$

has p - 1 in congruent roots. If a is one of them then

$$(a^d - 1)f(a) \equiv 0 \pmod p.$$

Consequently either $a^d - 1 \equiv 0 \pmod p$ or $f(a) \equiv 0 \pmod p$

Thus each of the p - 1 incorgruent roots of (1) is either a root of

$$x^d - 1 \equiv 0 \pmod p \qquad \ldots\ldots(2)$$

or a root of the congruence

$$f(x) \equiv 0 \pmod p \qquad \ldots\ldots(3)$$

Since f(x) is a polynomial of deg p - 1 - d with leading coefficient 1, (3) has atmost p - 1 - d incongruent roots. This forces us to conclude that (2) has exactly d incongruent roots.

Next let $\Psi(d)$ denote the number of integers k, $1 \le k \le p-1$, that have order d (mod p). Then $\Psi(d)$ is the number of roots of the congruence (2) that have order d (mod p). Since each integer between 1 to p - 1 has order d for some divisor d of p - 1, we get

$$p - 1 = \sum_{d \mid p-1} \Psi(d) \qquad \ldots\ldots(4)$$

On the other hand,

$$p - 1 = \sum_{d \mid p-1} \varphi(d) \qquad \ldots\ldots(5)$$

To prove the theorem we first prove that $\Psi(d) \le \phi(d)$.

Given an arbitrary divisior d of p - 1, there are two possibilities; either we have $\Psi(d) = 0$ on, $\Psi(d) > 0$. If $\Psi(d) = 0$, then we clearly have $\Psi(d) \le \phi(d)$. Suppose now that $\Psi(d) > 0$. Let a be any integer of order d (mod p). Then a is a solution of the congruence

$$x^d - 1 \equiv 0 \pmod p \qquad \ldots\ldots(2).$$

We get $a, a^2, \ldots, a^{d-1}$ are solutions of (2) and are mutually incongruent, since a has order d (mod p).

Thus $a, a^2, ..., a^{d-1}$ are all the incongruent roots of (2). Now since a^i has order $\frac{d}{(i,d)}$, a^i has order d iff $(i, d) = 1$. Since there are $\phi(d)$ many values of i in the set $\{1, 2, ..., d-1\}$ with $(i, d) = 1$ we set there are $\phi(d)$ many integers in the set $\{a, a^2, ..., a^{d-1}\}$ which have order d (mod p).

This shows that $\Psi(d) > 0$, then $\Psi(d) = \phi(d)$. We thus conclude that $\Psi(d) \leq \phi(d)$. Now from (4) and (5) we have,

$$\sum_{d|p-1} \Psi(d) = \sum_{d|p-1} \varphi(d) \qquad \text{.....(6).}$$

Since $\Psi(d) \leq \phi(d)$ for each positive divisor of p - 1 we must get $\Psi(d) = \phi(d)$ for each positive divisor of p - 1 so that the equality (6) is valid. Hence the result follows.

Corollory :

If p is a prime, then there are exactly $\phi(p-1)$ incongruent primitive roots of p.

Proof :

(First we prove the lemms - 1 and then put d = p - 1) we get there are $\phi(p-1)$ roots of

$$x^{p-1} - 1 \equiv 0 \pmod p$$

which have order $p - 1 \equiv \phi(p) \pmod p$. Thus there are $\phi(p-1)$ primitive roots of p.

Question :

For an odd prime p, varify that the sum

$$1^n + 2^n + 3^n + ... + (p-1)^n \equiv \begin{cases} 0 \pmod p & \text{if } p-1 \nmid n \\ -1 \pmod p & \text{if } p-1 \mid n \end{cases}$$

Solution :

If $(p-1) \mid n$ then for $1 \leq r \leq p-1$ we get

$$r^n \equiv 1 \pmod p.$$

Thus $1^n + 2^n + 3^n + ... + (p-1)^n \equiv \overbrace{1+1+...+1}^{(p-1) \text{ times}} \pmod p$

$$\equiv p - 1 \pmod p$$
$$\equiv -1 \pmod p.$$

Let $(p-1) \nmid n$ and a be any primitive root of p.

Then $\{1, a, a^2, ..., a^{p-2}\}$ is a reduced set of residues (mod p). because $\{1, 2, ..., p-1\}$ is a reduced set of residues (mod p), we get $1^n, a^n, a^{2n} ... a^{(p-2)n}$ are congruent (mod p) to the integers $1^n, 2^n, ..., (p-1)^n$

in some order.

Thus $1^n + 2^n + \ldots + (p-1)^n \equiv 1 + a^n + a^{2n} + \ldots + a^{(p-2)n}$

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

Since a is of order p - 1(mod p) and $p - 1 \nmid n$. $a^n \not\equiv 1 \pmod{p}$ i.e. $p \nmid a^n - 1$. However $a^{(p-1)n} \equiv 1 \pmod{p}$ i.e. $p \mid a^{n(p-1)} - 1$. Thus

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

$$\Rightarrow \frac{a^{(p-1)n} - 1}{a^n - 1} \equiv 0 \pmod{p}$$

$$\Rightarrow 1^n + 2^n + \ldots + (p-1)^n \equiv 0 \pmod{p} \text{ if } (p-1) \nmid n.$$

Lemma 1 :

If p is an odd prime, then a primitive root r of p exists such that $r^{p-1} \not\equiv 1 \pmod{p^2}$.

Proof :

Let a be any primitive root of p. If $a^{p-1} \not\equiv 1 \pmod{p^2}$ then we are finished by taking **r = a. On the contrary case, put r = a + p. Since r = a(mod p),** r is also a primitive root of p. Applying Binomial Theorem we have,

$$r^{p-1} = (a + p)^{p-1}$$

$$= a^{p-1} + (p-1)pa^{p-2} + p^2N$$

where N is a positiveinteger. Consequently,

$$r^{p-1} \equiv a^{p-1} + (p-1)pa^{p-2} \pmod{p^2}.$$

But we have assumed that $a^{p-1} \equiv 1 \pmod{p^2}$.

Hence $r^{p-1} \equiv 1 - pa^{p-2} \pmod{p^2}$.

Since a is a primitive root of p, (a, p) = 1 and so $p \nmid a^{p-2}$. Hence $pa^{p-2} \not\equiv 0 \pmod{p^2}$.

Consequently $r^{p-1} \not\equiv 1 \pmod{p^2}$. This proved the result.

Corollory :

If p is an odd prime and if r is a primitive root of p, then either r or r + p is a primitive root of p^2.

Proof :

Let a be any primitive root of p.

Since order of a(mod p) is p - 1, we get,

$$a^k \equiv 1 (\text{mod } p^2) \Rightarrow a^k \equiv 1 (\text{mod } p) \Rightarrow p - 1 \mid k.$$

Thus order of a(mod p^2) is a multiple of p - 1. Since order of a(mod p^2) is a divisor of $\phi(p^2) = p(p - 1)$.

We get order of a (mod p^2) is either p -1 or p(p - 1).

Now let a be the primitive root of p out of r and r + p for which

$$a^{p-1} \not\equiv 1 \pmod{p^2}.$$

Then order of a(mod p^2) is $p(p - 1) = \phi(p^2)$ i.e. a is a primitive root of p^2.

Lemma 2 :

Let p be an odd prime and r be a primitive root of p such that $r^{p-1} \not\equiv 1 \pmod{p^2}$. Then for each positive integer $k \geq 2$.

$$r^{p^{k-2}(p-1)} \not\equiv 1 (\text{mod } p^k).$$

Proof :

We prove the lemma by induction on k.

By hypothesis, the assertion holds for k = 2. Let us assume that it is true for some $k \geq 2$ and show that if it is true for k + 1.

Since $(r, p^{k-1}) = (r, p^k) = 1$.

By Euler's Theorem we get,

$$r^{p^{k-2}(p-1)} = r^{\phi(p^{k-1})} \equiv 1 (\text{mod } p^{k-1})$$

Thus there is an integer a such that

$$r^{p^{k-2}(p-1)} = 1 + ap^{k-1} \qquad \ldots\ldots(1)$$

where $p \nmid a$ by induction hypothesis, taking p^{th} power on both sides of (1) we get,

$$r^{p^{k-2}(p-1)} = \left(1 + ap^{k-1}\right)^p$$

$$\equiv 1 + ap^k \pmod{p^{k+1}}.$$

Since $p \nmid a$ we get,

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^{k+1}}.$$

This shows that the result holds for k + 1 and thus by induction the proof is complete.

Theorem :

If p is an odd prime and $k \geq 1$, there exists a primitive root of p^k.

Proof :

Because p is an odd prime, p has a primitive root r such that $r^{p-1} \not\equiv 1 \pmod{p^2}$.

Then for each positive integer $k \geq 2$,

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k} \qquad \text{.....(1).}$$

We prove that r is a primitive root of p^k, for each $k \geq 1$. Let n be the order of $r \pmod{p^k}$.

Then n must divide,

$$\phi(p^k) = p^{k-1}(p-1).$$

Since r has order $p - 1 \pmod{p}$ and because

$$r^n \equiv 1 \pmod{p^k} \Rightarrow r^n \equiv 1 \pmod{p}.$$

We get, $p - 1 \mid n$. Thus $n = p^m(p-1)$,

where $0 \leq m \leq k - 1$. If $m < k - 1$, then

$$n \mid p^{k-2}(p-1) \text{ and therefore}$$

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

which contradicts (1). Hence $n = p^{k-1}(p-1)$ and r is a primitive root of p^k.

Corollory :

There are primitive roots of $2p^k$, where p is an odd prime and $k \geq 1$.

Proof :

Let r be a primitive root of p^k. We can assume that r is odd, for if not, then $r + p^k$ is odd and is still a primitive root of p^k. Now r being odd

$$(r, 2p^k) = (r, p^k) = 1.$$

Let n be the order of $r \pmod{2p^k}$. then $n \mid \phi(2p^k) = \phi(p^k)$.

Also $r^n \equiv 1 \pmod{2p^k}$

$$\Rightarrow r^n \equiv 1 \pmod{p^k},$$

and therefore $\phi(p^k)$(= order of $a \pmod{p^k}$) divides n. We conclude that $n = \phi(p^k) = \phi(2p^k)$ and thus r is a primitive root of $2p^k$.

Exercise :

3 is a primitive root of all numbers of the form 2.5^k.

We see that 5 has $\phi(4) = 2$ primitive roots namely the integers 2 and 3.

Now since,

$$2^{5-1} \equiv 16 \not\equiv 1 \pmod{25}$$

and $3^{5-1} \equiv 6 \not\equiv 1 \pmod{25}$

2 and 3 are also primitive roots of 25 and therefore of all integers 5^k, $k \geq 1$. Since 3 is an odd primitive root of 5^k, 3 is a primitive root of all integers of the form 2.5^k. $k \geq 1$.

2, 4 have primitive roots (i.e., 1 and 3) we must have the following.

Theorem :

If n is any of the integers 2, 4, p^k, $2p^k$ where p is an odd prime and $k \geq 1$, then n has primitive roots.

Lemma 3 :

If a is an odd integer, then for $k \geq 3$

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

Proof :

If $k = 3$, this congruence because $a^2 \equiv 1 \pmod 8$, which is certainly true (for $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$). assume that the assertion is true for the integer $k \geq 3$, i.e.,

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

Thus $a^{2^{k-2}} = 1 + b2^k$ for same integer b.

Thus, $a^{2^{k-1}} = \left(a^{2^{k-2}}\right)^2$

$$= (1 + b2^k)^2$$
$$= 1 + 2^{k+1}.b + b^2.2^{2k}$$
$$= 1 + 2^{k+1}(b + b^2.2^{k-1})$$
$$\equiv 1 \pmod{2^{k+1}}$$

This shows that the assertion is true for $k + 1$.

By induction, the result follows.

Theorem :

For $k \geq 3$, the integer 2^k has no primitive roots.

Proof :

Let n be any integer with $(a, 2^k) = 1$.

Thus a is odd and therefore we have,

$$a^{2^{k-2}} \equiv 1 \pmod{2^k} \qquad (\text{as } k \geq 3).$$

Since $\phi(2^k) = 2^{k-1}$, the above result shows that order of a (mod 2^k) is less then $\phi(2^k)$.

Hence a is not primitive root of 2^k.

Theorem :

If $(m, n) = 1$ where $m > 2$ and $n > 2$ then the integer mn has no primitive roots.

Proof :

Let a be any integer for which (a, mn) = 1.

Then (a, m) = (a, n) = 1.

Let d = (ϕ(m), ϕ(n)). Since m > 2, n > 2, ϕ(m), ϕ(n) are both open and therefore d ≥ 2. Let $\phi(m) = m_1 d$, $\phi(n) = n_2 d$. Now by Eulers theorem, we have,

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

and therefore

$$a^{m_1 n_1 d} = \left(a^{\phi(m)}\right)^{n_1} \equiv 1 \pmod{m}.$$

Similarly $a^{m_1 n_1 d} = \left(a^{\phi(m)}\right)^{n_1} \equiv 1 \pmod{m}$.

Thus from the fact that (m, n) = 1, we have,

$$a^{m_1 n_1 d} \equiv 1 \pmod{mn} \qquad \text{.....(1)}$$

Since $\phi(mn) = \phi(m)\phi(n) = m_1 n_1 d^2 > m_1 n_1 d$.

From (1) we see that order of a (mod mn) is less then ϕ(mn). Hence a is not a primitive root of mn.

From the above Theorem we have the following :

Theorem :

If n is a positive integer having primitives roots then n must be one of the integers.

2, 4, p^k, $2p^k$ where p is an odd prime and k ≥ 1.

Proof :

If n is a power of 2, then in view of Theorem (3) n is either 2 or k.

If n has more than one odd prime factor, then n can be expressed as n = rs, where r > 2, s > 2, (r, s) = 1 and therefore n has no primitive root.

Now let $n = 2^k p^\ell$ where p is odd prime and $k \geq 0, 1 \geq \ell$. If k > 1 then$(2^k, p^l) = 1$, $2^k > 2$, $p^l > 2$ and so n has no primitive root. Thus k = 0 or 1.

Question :

Show that

(i) if prime p ≡ 1(mod 4) then an integer g is a primitive root of p iff - g is also a primitive root and

(ii) if prime p ≡ 3(mod 4), then an integer g is a primitive root of p iff - g has order

$\frac{1}{2}$(p - 1)(mod p).

Solution :

(i) Let $p = 4k + 1$. Let g be a primitive root of p. Then g has order $4k \pmod p$.

Suppose - g has order $h \pmod p$. If $h < 2k$, then

$$g^{2h} = (-1)^{2h}(-g)^{2h}$$
$$\equiv (-g)^{h.2} \equiv 1 (\mathrm{mod}(p)).$$

and therefore g has order $\leq 2h < 4k \pmod p$ a contradiction. Since order of $-g \pmod p$ divides $p - 1 = 4k$ we conclude that - g has order either $4k$ or $2k \pmod p$. But if - g has order $2k \pmod p$, then

$$g^{2k} = (-g)^{2k} \equiv 1 \pmod p.$$

which cannot be true. Hence - g has order $4k \equiv p - 1 \pmod p$ and so - g is a primitive root of p.

Conversely if - g is a primitive root of p, by the same argument $g = -(-g)$ is a primitive root of p. This proves (i).

(ii) Let $p = 4k + 3$ and g be a primitive root of p. As in the proof of (i) we have - g has order either $p - 1 = 4k + 2$ or $\frac{1}{2}(p - 1) = 2k + 1$.

Now consider the algebraic congruence

$$n^2 - 1 \equiv 0 \pmod p \qquad \ldots\ldots(1).$$

Since p is a prime (i) has exactly two roots, i.e., $x \equiv 1 \pmod p$ and $n \equiv -1 \pmod p$. However, $(g^{2k} + 1)^2 - 1 = g^{p-1} - 1 \equiv 0 \pmod p$, that is , g^{2k+1} is a root of (i). We therefore have,

$$g^{2k+1} \equiv 1 \pmod p, \text{ or, } g^{2k+1} \equiv -1 \pmod p.$$

The first case is not true, because g has order $4k+2 \pmod p$. Thus $g^{2k+1} \equiv -1 \pmod p$.

Consequently,

$$(-g)^{2k+1} = (-1)^{2k+1} g^{2k+1}$$
$$\equiv (-1)(-1) \pmod p$$
$$= 1 \pmod p.$$

This shows that - g has order $2k + 1 = \frac{1}{2}(p - 1) \pmod p$.

Conversely let - g have order $\frac{1}{2}(p - 1) = 2k + 1$.

Suppose g has order $h \pmod p$. Then

$$(-g)^{2h} \equiv h^{2h} \equiv 1 \pmod p.$$

implies $(2k + 1)$ divides $2h$, and so $2k + 1$ being odd $(2k + 1) \mid h$. Since $h \mid \phi(p) = 4k + 2$.

We must have h is either $2k + 1$ or $4k + 2$.

if $h = 2k + 1$, then

$$(-g)^{2k+1} = -(g^{2k+1})$$
$$= (-1)(1)(\text{mod } p)$$
$$= -1(\text{mod } p).$$

which is a contradiction, since - g has order $2k+1$ (mod p). hence g has order $4k+2 \equiv p-1(\text{mod } p)$ and so g is a primitive root of p.

Exercise :

If the integer $m > 2$ has a primitive root, and if $x_1, x_2, \ldots, x_n$ where $n = \phi(m)$, is a reduced set of residues(mod m), show that

$$\prod_{i=1}^{n} x_i \equiv -1(\text{mod } m).$$

Theory of indices :

Definition :

Let 'r' be a primitive root of n. If (a, n) = 1, then the smallest positive integer k such that $a \equiv r^k \pmod{n}$ is called the index of 'a' relative to r. It is denoted by ind_r^a.

Note :

$a \equiv r^{\text{ind}_r^a} \pmod{n}$ [$\because k = \text{ind}_r^a$]

eg : We know 2 is a primitive root of 11.

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

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

$2^3 \equiv 8 \pmod{11}$

$2^4 \equiv 16 \equiv 5 \pmod{11}$

$2^5 \equiv 10 \pmod{11}$

$2^6 \equiv 9 \pmod{11}$

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

$2^8 \equiv 3 \pmod{11}$

$2^9 \equiv 6 \pmod{11}$

$2^{10} \equiv 1 \pmod{11}$

Table of indices :

a	1	2	3	4	5	6	7	8	9	10
ind_2^a	10	1	8	2	4	9	7	3	6	5

Note :

If $a \equiv b \pmod{n}$, then $\text{ind}_r^a \equiv \text{ind}_r^b \pmod{\phi(n)}$

where r is a primitive root of n.

r is a primitive root of n.

$a \equiv r^{\text{ind}_r^a} \pmod{n}$

$b \equiv r^{\text{ind}_r^b} \pmod{n}$

$a \equiv b \pmod{n} \Leftrightarrow r^{\text{ind}_r^a} \equiv r^{\text{ind}_r^b} \pmod{n}$

$\Leftrightarrow \text{ind}_r^a \equiv \text{ind}_r^b \pmod{\phi(n)}$

Theorem :

If r is a primitive root of n, then

(i) $\text{ind}_r(ab)\ \text{ind}_r^a + \text{ind}_r^b \pmod{\phi(n)}$

(ii) $\text{ind}_r^{a^k} \equiv k(\text{ind}_r^a) \pmod{\phi(n)}$

(iii) $\text{ind}_r^1 \equiv 0 \pmod{\phi(n)}$ and

$\text{ind}_r^r \equiv 1 \pmod{\phi(n)}$

Proof :

(i) By definition, $a \equiv r^{\text{ind}_r^a} \pmod{n} \rightarrow (1)$

$b \equiv r^{\text{ind}_r^b} \pmod{n} \rightarrow (2)$

$ab \equiv r^{\text{ind}_r^{(ab)}} \pmod{n} \rightarrow (3)$

From (1) and (2),

$ab \equiv r^{\text{ind}_r^a} . r^{\text{ind}_r^b} \pmod{n}$

$\Rightarrow ab \equiv r^{\text{ind}_r^a + \text{ind}\, r^b} \pmod{n}$

$\Rightarrow r^{\text{ind}_r^{(ab)}} \equiv r^{\text{ind}_r^a + \text{ind}\, r^b} \pmod{n}$

using (3).

$\therefore \text{ind}_r^{(ab)} \equiv r_r^a + \text{ind}\, r^b \pmod{\phi(n)}$

(ii) By definition,

$a \equiv r^{\text{ind}_r^a} \pmod{n}$

$\Rightarrow a^k \equiv \left(r^{\text{ind}_r^a}\right)^k \pmod{n}$

$\Rightarrow a^k \equiv r^{k(\text{ind}_r^a)} \pmod{n} \rightarrow (1)$

Also, by definition,

$a^k \equiv r^{\text{ind}_r^{a^k}} \pmod{n} \rightarrow (2)$

From (1) and (2),

$$r^{ind_r^{a^k}} \equiv r^{k\, ind_r^a} \pmod{n}$$

$$\Rightarrow ind_r^{a^k} \equiv k\, ind_r^a \pmod{\phi(n)}$$

(iii)

$$1 \equiv r^{ind_r^1} \pmod{n}$$

$$\Rightarrow r^0 \equiv r^{ind_r^1} \pmod{n}$$

$$\Rightarrow ind_r^1 \equiv 0 \pmod{\phi(n)}$$

Again,

$$r \equiv r^{ind_r^r} \pmod{n}$$

$$\Rightarrow r^1 \equiv r^{ind_r^r} \pmod{n}$$

$$\Rightarrow ind_r^r \equiv 1 \pmod{\phi(n)}$$

Exercise :

Find the remainders when $3^{25}.5^{15}$ is divided by 11.

Solution :

Let a be the remainder, then

$3^{25}.5^{15} \equiv a \pmod{11}$

$\Rightarrow indr(3^{25}.5^{15}) = ind_r^a \pmod{10}$, where

r is a primitive root of 11.

$\Rightarrow ind_r^{3^{25}} + ind_r^{5^{15}} \equiv ind_r^a \pmod{10}$

$\Rightarrow 25(ind_r^3) + 15(ind_r^5) \equiv ind_r^a \pmod{10} \rightarrow (1)$

We know 2 is a primitive rot of 11.

We construct the table of indices as follows :

a	1	2	3	4	5	6	7	8	9	10
ind_2^a	10	1	8	2	4	9	7	3	6	5

from (1)

$25(ind_2^3) + 15(ind_2^5) \equiv ind_2^a \pmod{10}$

$\Rightarrow 25 \times 8 + 15 \times 4 \equiv ind_2^a \pmod{10}$

$\Rightarrow 260 \equiv ind_2^a \pmod{10}$

$\Rightarrow 0 \equiv ind_2^a \pmod{10}$

$\Rightarrow a = 1$

$\therefore$ required remainder is 1.

Exercise :
Solve the following congruences :
$3x^4 \equiv 5 \pmod{11}$

Solution :
We know 2 is a primitive root of 11. We construct the following table of indices ;

a	1	2	3	4	5	6	7	8	9	10
ind_2^a	10	1	8	2	4	9	7	3	6	5

Given congruence is
$3x^4 \equiv 5 \pmod{11}$

$\Rightarrow \text{ind}_2(3x^4) \equiv \text{ind}_2^5 \pmod{10}$

$\Rightarrow \text{ind}_2^3 + \text{ind}_2^{x^4} \equiv \text{ind}_2^5 \pmod{10}$

$\Rightarrow \text{ind}_2^3 + 4\text{ind}_2^x \equiv \text{ind}_2^5 \pmod{10}$

$\Rightarrow 8 + 4\text{ind}_2^x \equiv 4 \pmod{10}$

$\Rightarrow 4\text{ind}_2^x \equiv -4 \pmod{10}$

$\Rightarrow 4\text{ind}_2^x \equiv 6 \pmod{10}$

$\{[\because (4,10) = 2$, we have 2 incongruent solutions$]\}$

$\Rightarrow \text{ind}_2^x \equiv 4, 9 \pmod{10}$

$\Rightarrow x \equiv 5, 6$ are the required solution.

Theorem : The congruence $x^k \equiv a \pmod{n}$ has a solution iff $d \mid \text{ind}_r^a$ where $d = (k, \phi(n))$ and r is a primitive root of n.

Proof : Given congruence is $x^k \equiv a \pmod{n} \rightarrow (1)$
Given, r is a primitive root of n.
From (1), $x^k \equiv a \pmod{n}$

$\Leftrightarrow \text{ind}_r(x^k) \equiv \text{ind}_r^a \pmod{\phi(n)}$

$\Leftrightarrow k\,\text{ind}_r x \equiv \text{ind}_r^a \pmod{\phi(n)}$

$\Leftrightarrow ky \equiv \text{ind}_r^a \pmod{\phi(n)}$, where $y = \text{ind}_r^x$

We know a linear congruence $ax \equiv b \pmod{n}$ has a solution iff $(a, m) \mid b$.

Thus $ky \equiv \text{ind}_r^a \pmod{\phi(n)}$ has a solution iff $(k, \phi(n)) \mid \text{ind}_r^a$.

Theorem : Let n be an integer having a primitive root 'r' and let $(a, n) = 1$. Then the congruence $x^k \equiv a \pmod{n}$, where $d = (k, \phi(n))$.

If it has a solution then there are exactly d incongruent solutions modn.

Proof :

$$a\frac{\phi(n)}{d} \equiv 1(\text{mod } n)$$

$$\Leftrightarrow \text{ind}_r\left(a\frac{\phi(n)}{d}\right) \equiv \text{ind}_r^1 \ (\text{mod}\,\phi(n))$$

$$\Leftrightarrow \frac{\phi(n)}{d}\,\text{ind}_r^a \equiv 0 \ (\text{mod}\,\phi(n))$$

$$\Leftrightarrow \phi(n) \Big| \frac{\phi(n)}{d}\,\text{ind}_r^a$$

$$\Leftrightarrow d \,|\, \text{ind}_r^a$$

By the previous theorem, $x^k \equiv a(\text{mod}n)$ has a solution iff $d \,|\, \text{ind}_r^a$

Thus $x^k \equiv a(\text{mod}n)$ has a solution iff $a\frac{\phi(n)}{d} \equiv 1 \ (\text{mod}n)$

We assume $x^k \equiv a(\text{mod}n)$ has a solution.
Then we get as the previous theorem,

$k\,\text{ind}_r^x \equiv \text{ind}_r^a \ (\text{mod}\ \phi(n))$

$\Rightarrow ky \equiv \text{ind}_r^a \ (\text{mod}\ \phi(n)),\ y = \text{ind}_r^x$

Since $x^k \equiv a$ (modn) has a solution, so

$ky \equiv \text{ind}_r^a \ (\text{mod}\ \phi(n))$ has a solution.

Since $d = (k, \phi(n))$, so $ky \equiv \text{ind}_r^a \ (\text{mod}\ \phi(n))$ has exactly d incongruent solution, mod $\phi(n)$.

$\Rightarrow x^k \equiv a$ (modn) has d incongruent solutions modn.

Exercise : $x^8 \equiv 10(\text{mod } 11)$. Examine whether the congruence is solvable or not.

Solution : Here $a = 10, k = 8, n = 11$.
And $(a, n) = 1$

$\phi(n) = 10$, $(8, 10) = 2$ and $\frac{\phi(n)}{d} = 5$

Then

$10 \equiv 10 \ (\text{mod } 11) \equiv -1 \ (\text{mod } 11)$

$\Rightarrow 10^5 \equiv -1\,(\text{mod}\,11)$

$$\Rightarrow 10^{\frac{\phi(n)}{d}} \equiv -1\,(\text{mod}\,11)$$

$\Rightarrow$ The congruence has no solution.

Corollary :

$x^k \equiv a \pmod p$ has a solution iff $a^{\frac{p-1}{d}} \equiv 1 \pmod p$, where p is a prime.

Exercise :
If p is an odd prime, then prove that $x^2 \equiv -1 \pmod p$ is solvable iff $p \equiv 1 \pmod 4$

Solution :
Given p is an odd prime.
Now $x^2 \equiv -1 \pmod p$ has a solution iff

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

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

Now,

$$(-1)^{\frac{p-1}{2}} = 1 \text{ if } \frac{p-1}{2} \text{ is even}$$

$$= -1 \text{ if } \frac{p-1}{2} \text{ is odd.}$$

If $(-1)^{\frac{p-1}{2}} = -1$, then $-1 \equiv 1 \pmod p$
$\Rightarrow p \mid 2$, a contradiction as p is an odd prime.

So, $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$ holds

$$\Leftrightarrow \frac{p-1}{2} \text{ is even}$$

$$\Leftrightarrow \frac{p-1}{2} = 2k$$

$$\Leftrightarrow p = 4k+1$$

$$\Leftrightarrow p \equiv 1 \pmod 4$$

Exercise : Show that $x^4 \equiv -1 \pmod p$ is solvable
$\Leftrightarrow p \equiv 1 \pmod 8$

Exercise : Find the index of 5 relative to each of the primitive root of 11.

Solution :
We find the primitive roots of 11.

We know, 2 is a primitive root of 11.

2^k is a primitive root of 11 iff (k, 10) = 1.

iff k = 1, 3, 7, 9.

$2^3 \equiv 8 \pmod{11} \equiv -3 \pmod{11}$

$2^6 \equiv 9 \pmod{11} \equiv -2 \pmod{11}$

$2^7 \equiv -4 \pmod{11} \equiv 7 \pmod{11}$

$2^9 \equiv 6 \pmod{11}$

The primitive roots of 11 are 2, 8, 7, 6, i.e. 2, 6, 7, 8

To find $\text{ind}_2^5, \text{ind}_6^5, \text{ind}_7^5$, and ind_8^5

Let $\text{ind}_2^5 = k$. Then $5 \equiv 2^k \pmod{11}$

$\therefore k = 4$ as $5 \equiv 2^4 \pmod{11}$

$\therefore \text{ind}_2^5 = 4$

Let $\text{ind}_6^5 = k$. Then $5 \equiv 6^k \pmod{11}$

$\Rightarrow k = 6$ as $5 \equiv 6^6 \pmod{11}$

$\therefore \text{ind}_6^5 = 6$

Let $\text{ind}_7^5 = k$. Then $5 \equiv 7^k \pmod{11}$

$\Rightarrow k = 2$ as $5 \equiv 7^2 \pmod{11}$

$\therefore \text{ind}_7^5 = 2$

Let $\text{ind}_8^5 = k$. Then $5 \equiv 8^k \pmod{11}$

$\Rightarrow k = 3$ as $5 \equiv 8^3 \pmod{11}$

$\therefore \text{ind}_8^5 = 3$.

Exercise : Assume is a primitive root of an odd prime p. Then establish the following :

(i) $r^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ holds.

(ii) If r' is any other primitive root of p, then rr' is not a primitive root of p.

(iii) If the integer r' is such that $rr' \equiv 1 \pmod{p}$, then r' is a primitive root of p.

Solution :

(i) r is a primitive root of p.

$\Rightarrow$ Order of is mod p is $\phi(p) = p - 1$.

Now, $r^{p-1} \equiv 1 \pmod{p}$

$\Rightarrow r^{p-1} \equiv \left(r^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod{p}$, as p is odd, $p - 1$ is even.

$\Rightarrow \left(r^{\frac{p-1}{2}}\right)^2 - 1 \equiv 0 \pmod{p}$

$$\Rightarrow \left(r\frac{p-1}{2_{-1}}\right)^2\left(r^{\frac{p-1}{2}}+1\right)\equiv 0 \pmod p$$

$$\Rightarrow p \mid \left(r^{\frac{p-1}{2}}-1\right)\left(r^{\frac{p-1}{2}}+1\right)$$

$\Rightarrow$ Either $p \mid r^{\frac{p-1}{2}}-1$, then $r^{\frac{p-1}{2}} \equiv 1 \pmod p$, which contradicts the fact that r is a primitive root of p.

Thus $\Rightarrow p \mid r^{\frac{p-1}{2}}+1$

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

(ii) r is a primitive root of p.

$$\Rightarrow r^{\frac{p-1}{2}} \equiv -1 \pmod p, \text{ by (i)}$$

Also, r' is another primitive root of p.

so, $\Rightarrow r'^{\frac{p-1}{2}} \equiv -1 \pmod p$, by (i)

Thus, $\Rightarrow r^{\frac{p-1}{2}} r'^{\frac{p-1}{2}} \equiv 1 \pmod p$

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

$\Rightarrow$ order of $rr' \bmod p < p-1$

$\Rightarrow$ rr' is not a primitive root of p.

(iii) Let k be the order of r' mod p.

Then $k \mid \phi(p)$

Given, $rr' \equiv 1 \pmod p$

$\Rightarrow (rr') \equiv 1 \pmod p$

$\Rightarrow r^k \equiv 1 \pmod p \quad [\because r' \equiv 1 \pmod p]$

$\Rightarrow \phi(p) \mid k$.

Thus $k = \phi(p)$

$\Rightarrow$ order of r' mod p is $\phi(p)$

$\Rightarrow r'$ is a primitive root of p.

Exercise : Using the theory of primitive roots prove that Wilson's theorem.

Solution : Wilson's theorem states :

If p is a prime then

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

If $p = 2$, then the result is obvious.

Let p be an odd prime. Then p has a primitive root is :

$\Rightarrow$ The integers r, r^2, ..., r^{p-1} are congruent mod p to 1, 2, ..., p – 1 in some order.

Thus, $r \cdot r^2 \cdot r^3, \ldots, r^{p-1} \; 1, 2, \ldots, (p-1) \pmod{p}$

$r^{1+2+3+\ldots+(p-1)} \; (p-1)! \pmod{p}$

$$\Rightarrow r^{\frac{(p-1)p}{2}} \equiv (p-1)! \pmod{p} \rightarrow (1)$$

Since r is a primitive root of p,

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

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

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

From (1) and (2), we get $(p-1)! \equiv -1 \pmod{p}$

Exercise : If p is a prime then show that product of the $\phi(p-1)$ primitive roots is congruent mod p to $(-1)^{\phi(p-1)}$

Solution : Let r be a primitive root of p.

Now, p has $(p)) = (p-1)$ primitive roots.

Also, rk is a primitive root of p if $(k, (p)) = 1$. i.e. $(k, p-1) = 1$.

Let, ra1, ra2, ra3, ..., ra(p–1) be all the primitive roots of p, s.f $(ai, p-1) = 1$, $i = 1, 2, \ldots (p-1)$

Product of the primitive roots

$$\equiv r^{a_1} r^{a_2} \ldots . r^{a_{\phi(p-1)}} \pmod{p}$$

$$\equiv r^{a_1 + a_2 + \ldots + a_{\phi(p-1)}} \pmod{p}$$

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

$$\left[\because a_1 + a_2 + \ldots + a_{\phi(p-1)} = \frac{1}{2}^{(p-1)\phi(p-1)}\right]$$

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

Euler's Criteria :

We consider a quadratic congruence of the form

$ax^2 + bx + c \equiv 0 \pmod{p}$, p odd prime and p X a. $\rightarrow$ (1)

Since p is odd, (2, p) = 1

$\Rightarrow$ (4, p) = 1.

Also, p X a $\Rightarrow$ (a, p) = 1

So, (4, p) = 1, (a, p) = 1

$\Rightarrow$ (4a, p) = 1.

Then (1) is equivalent to

$4a(ax^2 + bx + c) \equiv 0 \pmod{p}$

$\Leftrightarrow 4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}$

$\Leftrightarrow (2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$

$\Leftrightarrow y^2 \equiv d \pmod{p} \rightarrow (2)$

where $y = 2ax + b$

$d = b2 - 4ac$.

If $x \equiv x_0 \pmod{p}$ is a solution of (1),

then $y \equiv 2ax_0 + b \pmod{p}$ is a solution of (2).

Conversely if $y \equiv y_0$ is a solution of (2), then

$2ax \equiv y_0 - b \pmod{p}$ can be solved to find a solution of (1).

Thus the problem of finding a solution of congruence (1), is equivalent to solving a quadratic congruence $y^2 \equiv d \pmod{p}$ and a linear congruence of the form $2ax \equiv k \pmod{p}$, $k = y_0 - b$.

If, $x = x_0$ is a solution of the congruence

$x^2 \equiv a \pmod{p}$, then $p - x_0$ is another solution of the congruence.

Both x_0 and $p - x_0$ are incongruent mod p. For if $x_0 \equiv p - x_0 \pmod{p}$, then

$2x_0 \equiv p \pmod{p}$

$\Rightarrow 2x_0 \equiv 0 \pmod{p}$

$\Rightarrow x_0 \equiv 0 \pmod{p}$, which is not possible.

Exercise : Solve $x^2 + 7x + 10 \equiv 0 \pmod{11}$.

Solution :

Here $x^2 + 7x + 10 \equiv 0 \pmod{11}$

$\Leftrightarrow 4x^2 + 28x + 40 \equiv 0 \pmod{11}$

$\Leftrightarrow (2x + 7)^2 \equiv 9 \pmod{11}$

$\Leftrightarrow y^2 \equiv 9 \pmod{11}$, where $y = 2x + 7$

$\Leftrightarrow y \equiv \pm 3 \pmod{11}$

$\Leftrightarrow y \equiv 3 \pmod{11}$ or $y \equiv -3 \pmod{11}$

$\therefore y \equiv 8 \pmod{11}$

Now,

$y = 2x + 7 \quad \Rightarrow 2x + 7 \equiv y \pmod{11}$

$y \equiv 3 \pmod{11} \Rightarrow 2x + 7 \equiv 3 \pmod{11}$

$\Rightarrow 2x \equiv -4 \pmod{11}$

$\Rightarrow x \equiv -2 \pmod{11}$

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

$y \equiv 8 \pmod{11} \Rightarrow 2x + 7 \equiv 8 \pmod{11}$

$\Rightarrow 2x \equiv 1 \pmod{11}$

$\Rightarrow 2x \equiv -10 \pmod{11}$

$\Rightarrow x \equiv -5 \pmod{11}$

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

Thus the solutions are

$x \equiv 6, 9 \pmod{11}$

Definition :

Let p be an odd prime and (a, p) = 1. Then a is called a quadratic residue of p, if the congruence $x^2 \equiv a \pmod{p}$ has a solution and a is called a quadratic no-residue of p if $x^2 \equiv a \pmod{p}$ has no solution.

Consider p = 7

We choose a s.f $a \in \{1, 2, 3, 4, 5, 6\}$

$1^2 \equiv 1 \pmod{7} \Rightarrow 1^2 \equiv 6^2 \pmod{7}$

$2^2 \equiv 4 \pmod{7} \Rightarrow 2^2 \equiv 5^2 \pmod{7}$

$3^2 \equiv 2 \pmod{7} \Rightarrow 3^2 \equiv 4^2 \pmod{7}$

$4^2 \equiv 2 \pmod{7}$

$1^2 \equiv 1 \equiv 6^2 \pmod{7}$

$2^2 \equiv 4 \equiv 5^2 \pmod{7}$

$3^2 \equiv 2 \equiv 4^2 \pmod{7}$

$\therefore$ 1, 4,2 are quadratic residues of 7. and 3, 5, 6 are quadratic non-residues of 7.

Exercise : Find all quadratic residues of 11.

Solution : We choose a s.t

$a \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Now,

$1^2 \equiv 1 \equiv 10^2 \pmod{11}$

$2^2 \equiv 4 \equiv 9^2 \pmod{11}$

$3^2 \equiv 9 \equiv 8^2 \pmod{11}$

$4^2 \equiv 5 \equiv 7^2 \pmod{11}$

$5^2 \equiv 3 \equiv 6^2 \pmod{11}$

∴ The quadratic residues of 11 are 1, 4, 9, 5, 3
and quadratic non-residues of 11 are 2, 3, 5, 6, 7, 8, 10

Theorem (Euler's Criteria) :
Let p be an odd prime and (a, p) = 1.
The a is a quadratic residue of p.

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

Proof : Let a be a quadratic residue of p
$\Rightarrow$ The congreuence $x^2 \equiv a \pmod{p}$ has a solution.
Let x_0 be a solution of the congruence.

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

Since, $(a, p) = 1$, $(x_0^2, p) = 1 \Rightarrow (x_0, p) = 1$

Now, $x^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} \pmod{p}$

$\Rightarrow a^{\frac{p-1}{2}} \equiv x_0^{p-1} \pmod{p}$
$\equiv 1 \pmod{p}$, by Fermat's Theorem.

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

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

We show 'a' is a quadratic residue of p.
Since p is a prime, p has a primitive root.
Let p be a primitive root of p.
Then $a \equiv r^k \pmod{p}$, for some k, where $1 \le k \le p-1$.

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

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

$\Rightarrow r_0^{\frac{k(p-1)}{2}} \equiv 1 \pmod{p}$
Since r is a primitive root of p, its order mod p is $\phi(p) = p-1$.

$\Rightarrow p-1 \left| \frac{k(p-1)}{2} \right.$

$\Rightarrow 2 \mid k$

$\Rightarrow k = 2m$ for some integer 'm'.

So,

$a \equiv r^k \pmod p \Rightarrow a \equiv r^{2m} \pmod p$

$\Rightarrow (r^m)^2 a \pmod p$

Thus r^m is a solution of $x^2 \equiv a \pmod p$

$\Rightarrow$ 'a' is a quadratic residue of p.

Corollary : p is an odd prime and (a, b) = 1.

Then 'a' is a quadratic non-pesidue of p iff $a^{\frac{p-1}{2}} \equiv -1 \pmod p$

Proof : Assume, $a^{\frac{p-1}{2}} \equiv -1 \pmod p$

$\Rightarrow a^{\frac{p-1}{2}} \not\equiv 1 \pmod p$

$\Rightarrow$ 'a' is a quadratic none residue of p.

Conversely let, 'a' is a quadratic non-residue of p.

$\Rightarrow a^{\frac{p-1}{2}} \not\equiv 1 \pmod p$

Since, (a, p) = 1, by Fermat's theorem,

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

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

$$\Rightarrow a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p$$

$$\left[pXa^{\frac{p-1}{2}} - 1\right]$$

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

Note :

(i) If 'a' is a quadratic residue of p, then a is not a primitive root of p.

(ii) If 'a' is a quadratic non-residue of p, then a is a primitive root of p.

Exercise : Show that 3 is a quadratic residue of 23 but a non-residue of 31.

Solution : Here, p = 23. $\therefore \frac{p-1}{2} = \frac{23-1}{2} = 11$

$3^3 \equiv 27 \pmod{23} \equiv 4 \pmod{23}$

$3^6 \equiv 16 \pmod{23} \equiv -7 \pmod{23}$

$3^9 \equiv -28 \pmod{23} \equiv -5 \pmod{23}$

$3^{11} \equiv -45 \pmod{23} \equiv -22 \pmod{23}$

$\equiv 1 \pmod{23}$

$\therefore$ 3 is a quadratic residue of 23.

Theorem : There are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues of p.

Proof : Let 'R_0' be the number of quadratic residues of p. and 'No' be the number of quadratic non-residues of p.

$\therefore R_0 + N_0 = p - 1 \rightarrow (1)$

Bye Euler's critoria, a is a quadratic residue of p iff $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

iff a satisfies the congruence

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

iff a is a solution of $x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$

Since $x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$ has atmost $\frac{p-1}{2}$

solution, so $R_0 \leq \frac{p-1}{2} \rightarrow (2)$

Similarly, $No \frac{p-1}{2} \rightarrow (3)$

From (1), (2) and (3), we get

$R_0 = \frac{p-1}{2}$

$N_0 = \frac{p-1}{2}$

Legendre's Symbols :

Let p be an odd prime and (a, p) = 1. The legendra symbol $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = 0 \text{ if } p \mid a$$

$= 1$ if a quadratic residue of p

$= -1$ if a is quadratic non residue of p.

Theorem :

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

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

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

Proof :

(i) $\left(\frac{a}{p}\right) = \pm 1$ (by definition) when $(a, p) = 1$

But $a^{\frac{1}{2}(p-1)} \equiv \pm 1 \pmod{p}$ By Eulers criterion.

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

(ii) If a is q.r. and b is q.r., then ab is also q.r. and hence

$$\left(\frac{a}{p}\right) = 1 = \left(\frac{b}{p}\right) \text{ and } \left(\frac{ab}{p}\right) = 1.$$

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

If a is q.r., b is q.n.r. then q.n.r. ab is q.n.r.

$$\therefore \quad \left(\frac{ab}{p}\right) = 1, \left(\frac{b}{p}\right) = -1 \text{ and } \left(\frac{ab}{p}\right) = -1.$$

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

Similarly, we can saw in the other cases.

(iii) $a \equiv b \pmod p$

a is $qr \Rightarrow$ b is q.r.

So, $a \equiv b(\text{mod } p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(iv) $\left(\frac{r^2}{p}\right) = 1$ always for r^2 is always q.r. of p.

(v) $(r, p) = 1 \Rightarrow \left(\frac{ar^2}{p}\right) = \left(\frac{a}{p}\right)$.

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

Exercise : If p is an odd prime, show that $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$.

Solution :

Out of 1, 2, ... (p - 1) half are q.r. and the other half is q.n.r.

$$\therefore \quad \text{for one half } \left(\frac{a}{p}\right) = 1$$

and for other half $\left(\frac{a}{p}\right) = -1$.

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

Theorem :

Let (a, p) = 1. If $p \equiv 1 \pmod 4$ then - a is q.r. mod p iff a is q.r. mod p.

If $p \equiv 3 \pmod 4$ then - a is q.n.r. iff a is q.r.

Proof :

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

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

$$\equiv 1\left(\frac{a}{p}\right) \qquad \because \quad p \equiv 1 \pmod 4$$

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

Thus - a is q.r. iff a is q.r.

If $p \equiv 3 \pmod 4$ then $\frac{1}{2}(p-1) = 2k+1$

$$\therefore \quad \left(\frac{-a}{p}\right) \equiv (-1)^{2k+1}\left(\frac{a}{p}\right) \equiv -\left(\frac{a}{p}\right) \pmod p.$$

$$\Rightarrow \left(-\frac{a}{p}\right) = -\left(\frac{a}{p}\right).$$ Thus - a is q.n.r. iff a is q.r.

Corollary :

If $p \equiv 1 \pmod 4$ then - 1 is q.r.

$p \equiv 3 \pmod 4$ then - 1 is q.n.r.

Gauss Lemma :

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

Let μ denote the number of integers in the sequence $a, 2a, 3a, \ldots, \frac{1}{2}(p-1)a$ ...(1), whose least positive remainders mod p are greater than $\frac{p}{2}$ then $\left(\frac{a}{p}\right) = (-1)^{\mu}$.

Proof :

Let $\alpha_1, \alpha_2, ..., \alpha_\mu$ be those among the least positive remainder of the numbers in (1) which are $> \frac{p}{2}$.

Then if the remaining numbers are $\beta_1, \beta_2, ..., \beta_\lambda$ then

$$\lambda + \mu = \frac{1}{2}(p-1).$$

$$\therefore \quad \alpha_1 . \alpha_2 ..... \alpha_\mu . \beta_1 . \beta_2 ..... \beta_\lambda \equiv a.2a.3a..... \frac{1}{2}(p-1)a \pmod p$$

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

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

$$\alpha_i > \frac{p}{2} \Rightarrow p - \alpha_i \leq \frac{p}{2}.$$

Now the numbers $p - \alpha_1, p - \alpha_2, p - \alpha_\mu, \beta_1, \beta_2, ..., \beta_\lambda$ all occur among $1, 2, ..., \frac{p-1}{2}$.

Moreover, $p - \alpha_i \not\equiv \beta_j \pmod p$.

For $\quad p - \alpha_i \equiv \beta_j \pmod p$.

$$\Rightarrow \alpha_i + \beta_j \equiv 0 \pmod p$$

$$\Rightarrow \alpha_i + pq_1 + \beta_j + pq_2 \equiv 0 \pmod p$$

$$\Rightarrow as + at \equiv 0 \pmod p \qquad \left(1 \leq s, t \leq \frac{p-1}{2}\right)$$

[$\because$ α_i, β_j are remainders when the numbers of the form ka are divided by p]

$$\Rightarrow p \mid a(s+t)$$

$$\Rightarrow p \mid t + s \text{ as } (a, p) = 1$$

which is impossible.

Thus the numbers $p - \alpha_1, ..., p - \alpha_\mu, \beta_1, \beta_2, ..., \beta_\lambda$ are exactly the numbers $1, 2, ..., \frac{1}{2}(p-1)$.

$$\therefore \quad \left\lfloor \frac{p-1}{2} \right\rfloor ! \equiv 1.2 \ldots\ldots \frac{1}{2}(p-1) \pmod p$$

$$\equiv (p-\alpha_1) \ldots (p-\alpha_\mu)\beta_1 \ldots \beta_\lambda \pmod p$$

$$\equiv (-\alpha_1) \ldots (-\alpha_\mu)\,\beta_1 \ldots \beta_\lambda \pmod p$$

$$= (-1)^\mu \alpha_1\alpha_2 \ldots \alpha_\mu\beta_1 \ldots \beta_\lambda \pmod p$$

Putting in (i) and cancelling α_i's and β_j's we get,

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

Since $\left(\frac{a}{p}\right) = \pm 1$ and $(-1)^\mu = \pm 1$ and p is odd it follows that

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

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

Solution :

Consider the numbers,

$$2.1, 2.2, \ldots\ldots, 2.\frac{p-1}{2}$$

i.e. $2, 4, \ldots\ldots, (p-1)$

Clearly μ = the numbers of the type 2x such

$$\frac{p}{2} < 2x < p.$$

i.e. $$\frac{p}{4} < x < \frac{p}{2} \qquad \ldots\ldots(A)$$

Let $p = 8k + \delta, \delta = 1, 3, 5, 7.$

Case I : When $\delta = 1$, then (A) becomes,

$$2k + \frac{1}{4} < x < 4k + \frac{1}{2}$$

i.e. $2k + 1 \le x \le 4k.$

$$\therefore \quad \mu = 4k - (2k+1) + 1 = 2k.$$

$$\therefore \quad \left(\frac{2}{p}\right) = (-1)^{\mu} = (-1)^{2k}$$

$$= 1$$

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

Case II : When $\delta = 3$, then (A) becomes,

$$\frac{8k+3}{4} < x < \frac{8k+3}{2}$$

$$\Rightarrow 2k + \frac{3}{4} < x < 4k + \frac{3}{2}$$

$$\Rightarrow 2k+1 \le x \le 4k+1$$

$$\therefore \quad \mu = (4k+1) - (2k+1) + 1 = 2k+1$$

$$\therefore \quad (-1)^{\mu} = (-1)^{2k+1} = -1$$

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

$$= -1$$

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

Similarly when $\delta = 5, 7$ we have

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

Note : If $p = 8k + r$ then

$$\frac{p^2-1}{8} = 8k^2 + 2kr + \frac{r^2-1}{8} \equiv \frac{r^2-1}{8} \pmod 2$$

and $$\frac{r^2-1}{8} = \begin{cases} 0 & \text{if } r = 1 \\ 1 & \text{if } r = 3 \\ 3 & \text{if } r = 5 \\ 0 & \text{if } r = 7 \end{cases}$$

Hence $(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{r^2-1}{8}} = \begin{cases} 1 & \text{if } r = 1,7 \text{ i.e. } p \equiv 1 (\text{mod } 8) \\ -1 & \text{if } r = 3,5 \text{ i.e. } p \equiv 7 (\text{mod } 8) \end{cases}$

Exercise : Show that if $p \equiv \pm 1 (\text{mod } 8)$ then 2 is q.r.

$p \equiv \pm 3 (\text{mod } 8)$ then 2 is q.n.r.

Exercise : Determine the primes of which the integer 2 is q.r. and those for which it is q.n.r.

Exercise : Determine $\left(\frac{3}{p}\right), \left(\frac{5}{p}\right)$.

Theorem :

$$\text{If } (a, p) = 1, \text{ then } \left(\frac{a}{p}\right) = (-1)^{\sum_{j=1}^{\frac{1}{2}(p-1)} \left[\frac{ja}{p}\right]}$$

Proof :

If we divide ja by p, $j = 1, 2, \ldots, \frac{1}{2}(p-1)$ we obtain $ja = pq + r$ when $0 < r < p$.

$$\therefore \quad \left[\frac{ja}{p}\right] = \left[q + \frac{r}{p}\right] = q.$$

$$\therefore \quad ja = \left[\frac{ja}{p}\right] p + r.$$

$$\text{Thus} \quad \sum_{j=1}^{\frac{1}{2}(p-1)} ja = \sum_{j=1}^{\frac{1}{2}(p-1)} \left[\frac{ja}{p}\right] p + \sum_{i=1}^{\mu} \alpha_i + \sum_{k=1}^{\lambda} \beta_k \qquad \ldots\ldots(1)$$

In the proof of Gauss lemma, we have seen that the numbers $p - \alpha_1, \ldots\ldots, p - \alpha_\mu, \beta_1, \ldots\ldots, \beta_\lambda$ are just numbers $1, 2, \ldots\ldots, \frac{1}{2}(p-1)$ in some orders.

$$\therefore \quad \sum_{j=1}^{\frac{1}{2}(p-1)} j = 1 + 2 + \ldots + \frac{1}{2}(p-1)$$

$$= (p - \alpha_1) + (p - \alpha_2) + \ldots + (p - \alpha_\mu) + \beta_1 + \beta_2 + \ldots + \beta_\lambda$$

$$= p\mu + \sum_{j=1}^{\lambda} \beta_j - \sum_{i=1}^{\mu} \alpha_i \qquad \ldots\ldots(2)$$

(1) - (2) gives

$$(a-1)\sum_{j=1}^{\frac{1}{2}(p-1)} j = p\left\{\sum_{i=1}^{\frac{1}{2}(p-1)} \left[\frac{ja}{p}\right] - \mu\right\} + 2\sum_{i=1}^{\mu} \alpha_i \qquad \ldots\ldots(3)$$

Now $a \equiv 1 \pmod 2$ and $p \equiv 1 \pmod 2$

$\Rightarrow a - 1 \equiv 0 \pmod 2$

So, (3) becomes,

$$0 \equiv 1\left\{\sum_{j=1}^{\frac{1}{2}(p-1)} \left[\frac{ja}{p}\right] - \mu\right\} + 0 \pmod 2$$

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

$$\therefore \quad \sum_{j=1}^{\frac{1}{2}(p-1)} \left[\frac{ja}{p}\right] = \mu + 2\ell, \ell \in Z$$

$$\therefore \quad \left(\frac{a}{p}\right) = (-1)^{\mu} = (-1)^{\mu+2\ell} = (-1)^{\sum_{j=1}^{\frac{1}{2}(p-1)} \left[\frac{ja}{p}\right]}$$

§ Quadratic Reciprocality Law :

If p and q are distinct odd prime numbers then

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

Proof :

Consider the rectangle in the xy coordinate plane whose vertices are $(0, 0), \left(\frac{p}{2}, 0\right), \left(0, \frac{q}{2}\right),$

and $\left(\frac{p}{2},\frac{q}{2}\right)$. Let R denote the region within this rectangle, not including any of the bounding lines.

The general plane of attack is to count the number of lattice points (that is, the points whose coordinates are integers) inside R in two different ways. Since p and q are both odd, the lattice points in R consist of ll points (n, m), where $1 \le n \le \frac{(p-1)}{2}$ and $1 \le m \le \frac{(q-1)}{2}$; the number of such points is clearly $\frac{p-1}{2}\cdot\frac{q-1}{2}$.

Now the diagonal D from (0, 0) to $\left(\frac{p}{2},\frac{q}{2}\right)$ has the equation $y = \left(\frac{q}{p}\right)x$, or equivalently, py = qx. Since gcd(p, q) = 1, none of the lattice points inside R will lie on D. For p must divide the x coordinate of any lattice point on the line py = qx, and q must divide its y coordinate; there are no such points in R. Suppose that T_1 denotes the portion of R which is below the diagonal D, and T_2 the portion above. By what we have just seen, it sufffices to count the lattice points inside each of these traingles.

The number of integers in the interval $0 < y < \frac{kp}{p}$ and $\left[\frac{kq}{p}\right]$. Thus, for $1 \le k \le \frac{(p-1)}{2}$, there are precisely $\left[\frac{kq}{p}\right]$ lallice points in T_1 directly above the point (k, 0) and below D; in other words, lying on the vertical line segment from (k, 0) to $\left(k,\frac{kq}{p}\right)$. it follows that the total number of lattice points contained in T_1 is

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

A similar calculation, with the role of p and q interchanged, shows that the number of lattice points within T_2 is

$$\sum_{j=1}^{\frac{(q-1)}{2}}\left[\frac{jp}{q}\right].$$

This accounts for all of the lattice points R, so that

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

This time has come for Gauss' Lemma to do its duty :

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

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

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

This proof of the Quadratic reciprocity Law is now complete.

An immediate consequence of this is

Corrollary 1 :

If p and q are distinct odd primes, then

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

Exercise : Find $\left(\frac{10}{17}\right)$

Ans : $\left(\frac{10}{17}\right)=\left(\frac{2\times 5}{17}\right)=\left(\frac{2}{17}\right)\left(\frac{5}{17}\right)$

Now $\left(\frac{2}{17}\right)\equiv 2^{\frac{1}{2}(17-1)} \pmod{17}$

$\equiv 256 \pmod{17}$

$\equiv 1 \pmod{17}$

$\left(\frac{5}{17}\right)=(-1)^{\frac{1}{2}(17-1)\frac{1}{2}(5-1)}\left(\frac{17}{5}\right)$ [By Q.R. Law].

$$= \left(\frac{17}{5}\right)$$

$$= \left(\frac{2}{5}\right) \qquad \left[\because \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \text{ if } a \equiv b \pmod{p}\right]$$

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

$$= 4 \pmod 5$$

$$\equiv -1 \pmod 5$$

$$\therefore \quad \left(\frac{10}{17}\right) = 1 \cdot (-1) = -1.$$

Exercise : Find all primes for which (- 3) is a q.r.

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

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

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

$$= \left(\frac{r}{3}\right), p \equiv r(3), r = 1,2.$$

If r = 1, then

$$\left(-\frac{3}{p}\right) = \left(\frac{1}{3}\right) = 1 \qquad \therefore \qquad -3 \text{ is q.r. if } p \equiv 1 \pmod 3$$

If r = 2, then

$$\left(-\frac{3}{p}\right) = \left(\frac{2}{3}\right) \equiv 2^{\frac{1}{2}(3-1)} \pmod 3$$

$$\equiv 2 \pmod 3$$

$$\Rightarrow \left(\frac{-3}{p}\right) = -1$$

$\therefore$ -3 is q.n.r. if $p \equiv 2(3)$.

Ans : $p \equiv 1(3)$.

Exercise : Find all primes for which 5 is a q.r.

$$\left(\frac{5}{p}\right) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(5-1)}\left(\frac{p}{5}\right)$$

$$= (-1)^{\frac{1}{2}(p-1)\cdot 2}\left(\frac{p}{5}\right)$$

$$= \left(\frac{p}{5}\right)$$

$$= \left(\frac{r}{5}\right), p \equiv r(5), r = 1,2,3,4$$

If $r = 2, \left(\frac{5}{p}\right) = \left(\frac{2}{5}\right) \equiv 2^{\frac{1}{2}(5-1)} \pmod 5$

$\equiv 2^2 \pmod 5$

$\equiv -1 \pmod 5$

$\therefore$ 5 is q.n.r. if $p \equiv 2 \pmod 5$.

If $r = 1, \left(\frac{5}{p}\right) = \left(\frac{1}{5}\right) = 1$

$\therefore$ 5 is R if $p \equiv 1 (5)$.

If $r = 3, \left(\frac{5}{p}\right) = \left(\frac{3}{5}\right) = (-1)^{\frac{1}{2}(5-1)\frac{1}{2}(3-1)}\left(\frac{5}{3}\right)$

$$= \frac{5}{3} = \frac{2}{3} \qquad [\because \quad 5 \equiv 2(3)]$$

$$= -1$$

i.e. 5 is q.n.r. if $p \equiv 3 \pmod 5$.

If $r = 4, \left(\frac{5}{p}\right) = \left(\frac{4}{5}\right) = 1$

5 is q.r. if $p \equiv 4 \pmod 5$

$\therefore$ 5 is q.r. if $p \equiv 1, 4 \pmod 5$.

i.e. $p \equiv \pm 1 \pmod 5$.

Q.R. for composite Modulus :

Jacobi's Symbol :

Let (P, Q) = 1 and Q is an odd positive integer with prime decomposition $Q = \prod_{i=1}^{r} p_i^{\alpha_i}$. Then

jacobi's symbol $\left(\frac{P}{Q}\right)$ is defined as,

(i) $\left(\frac{P}{1}\right) = 1 \ \forall P \in Z$.

(ii) $\left(\frac{P}{Q}\right) = \left(\frac{P}{P_1}\right)^{\alpha_1}\left(\frac{P}{P_2}\right)^{\alpha_2} \cdots\cdots \left(\frac{P}{P_r}\right)^{\alpha_r}$.

() is called a Legender's symbol.

Remark :

$\left(\frac{P}{Q}\right) = 0$ if $(P, Q) \neq 1$, from definition of Legendre's symbol.

Proof :

If $(P, Q) \neq 1$, let q be a common factor of P and Q.

$\therefore \quad \left(\frac{P}{q}\right) = 0$ by definition of Legendre's symbol.

But $\left(\frac{p}{q}\right)$ is a factor of $\left(\frac{P}{Q}\right)$. Hence $\left(\frac{P}{Q}\right) = 0$.

Property :

(i) $\left(\frac{P}{Q}\right)$ has nalways the value 1 or - 1 (follows from definition).

(ii) $(P, Q) = 1$ and P is a q.r. of Q then $\left(\frac{P}{Q}\right) = 1$.

Proof :

If $x^2 \equiv P(Q)$ has a root, then for each $i = 1, 2, 3, ..., r$.

The algebric congruence $x^2 \equiv P(p_i)$ has a root.

Consequently $\left(\frac{P}{p_i}\right) = 1$ for $i = 1, 2, 3, ..., r$

$$\therefore \quad \left(\frac{P}{Q}\right) = 1.$$

Remark :

Converse of (ii) is not true.

i.e. if $\left(\frac{P}{Q}\right) = 1$, P need not be a.q.r.

Theorem :

If Q_1, Q_2, P_1, P_2 are odd positive integers then

(i) $\left(\frac{P_1}{Q}\right)\left(\frac{P_2}{Q}\right) = \left(\frac{P_1P_2}{Q}\right)$ (ii) $\left(\frac{P}{Q_1}\right)\left(\frac{P}{Q_2}\right) = \left(\frac{P}{Q_1Q_2}\right)$

(iii) If $P_1 \equiv P_2 \pmod{Q}$, then $\left(\frac{P_1}{Q}\right) = \left(\frac{P_2}{Q}\right)$ (iv) $(P,Q) = 1 \Rightarrow \left(\frac{PP^2}{Q}\right) = \left(\frac{P}{Q}\right)$

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

(vii) If $(P, Q) = 1$ and P is an odd integer,

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

Proof :

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

Thus result is true for $Q = 1$. Let $Q > 1$.

$Q = P_1P_2, \ldots\ldots, P_r$ where P_i are odd are not necessarily distinct.

$$\therefore \quad \left(-\frac{1}{Q}\right)=\left(-\frac{1}{P_1}\right)\left(-\frac{1}{P_2}\right)\ldots\ldots\left(-\frac{1}{P_r}\right)$$

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

$$=\prod_{i=1}^{r}(-1)^{\frac{1}{2}(P_i-1)}$$

$$=(-1)^{\sum_{i=1}^{r}\frac{1}{2}(P_i-1)}.$$

The result will be proved if we can show that,

$$\sum_{i=1}^{r}\frac{1}{2}(P_i-1)=\frac{1}{2}(Q-1)=\frac{1}{2}(P_1P_2,\ldots\ldots,P_r-1)\ (\text{mod } 2) \qquad \ldots\ldots(*)$$

(*) will be proved by induction.

Suppose (*) is true for r - 1.

i.e. $$\sum_{i=1}^{r-1}\frac{1}{2}(P_i-1)=\frac{1}{2}(P_1P_2,\ldots\ldots,P_r-1)\ (\text{mod } 2).$$

$$\therefore \quad \sum_{1}^{r}\frac{1}{2}(P_i-1)=\sum_{i=1}^{r-1}\frac{1}{2}(P_i-1)+\frac{1}{2}(P_r-1)$$

$$=\frac{1}{2}(P_1P_2\ldots\ldots P_{r-1}-1)+\frac{1}{2}(P_r-1) \qquad \ldots\ldots(**)$$

Now P_i are odd primes,

$$\therefore \quad (P_1P_2,\ldots\ldots P_{r-1}-1)(p_r-1)\equiv 0\ (\text{mod } 4)$$

$$\Rightarrow P_1P_2,\ldots\ldots P_r-P_1P_2\ldots\ldots P_{r-1}-P_r+1\equiv 0\ (\text{mod } 4)$$

$$\Rightarrow (P_1P_2\ldots\ldots P_{r-1}-1)-(P_1P_2\ldots\ldots P_r-1)+(P_r-1)\equiv 0\ (\text{mod } 4)$$

$$\Rightarrow \frac{1}{2}(P_1P_2\ldots\ldots P_{r-1}-1)-(P_1P_2\ldots\ldots P_r-1)+(P_r-1)\equiv 0\ (\text{mod } 2)$$

$\therefore$ (**) becomes,

$$\sum_{i=1}^{r}\frac{1}{2}(P_i-1)=\frac{1}{2}(P_1P_2,.....,P_r-1)\pmod 2$$

$$=\frac{1}{2}(Q-1)\pmod 2$$

Hence the result follows by induction.

Proof :

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

$$\left(\frac{2}{Q}\right)=\left(\frac{2}{P_1}\right)\left(\frac{2}{P_2}\right).....\left(\frac{2}{P_r}\right)$$

$$=(-1)^{\frac{P_1^2-1}{8}}(-1)^{\frac{P_2^2-1}{8}}...(-1)^{\frac{P_r^2-1}{8}}$$

$$=(-1)^{\sum_{i=1}^{r}\frac{P_i^2-1}{8}}$$

The Theorem will be proved if we can show that,

$$\sum_{i=1}^{r}\frac{1}{8}(P_i^2-1)=\frac{1}{8}(Q^2-1)=\frac{1}{8}(P_i^2.....P_r^2-1)\pmod 2$$

This will be proved by method of induction.

The result hold for r = 1. Assume it is true for r - 1.

i.e. $$\sum_{i=1}^{r-1}\frac{P_i^2-1}{8}=\frac{1}{8}(P_1^2.....P_r^2-1) \qquad .....(**)$$

$$\sum_{i=1}^{r}\frac{1}{8}(P_i^2-1)=\sum_{i=1}^{r-1}\frac{1}{8}(P_i^2-1)+\frac{1}{8}(P_r^2-1)$$

$$=\frac{1}{8}(P_1^2P_2^2...P_{r-1}^2-1)+\frac{1}{8}(P_r^2-1)\pmod 8$$

.....(A)

If $a \in Z$ is odd, then

$a^2 \equiv 1 \pmod 8 \Rightarrow a^2 - 1 \equiv 0 \pmod 8$.

Consequently

$$(P_1^2p_2^2 \ldots\ldots P_{r-1}^2 - 1)(P_r^2 - 1) \equiv 0 \pmod 4$$

$$\Rightarrow (P_1^2p_2^2 \ldots\ldots P_{r-1}^2 - 1) - (P_1^2P_2^2 \ldots\ldots P_r^2 - 1) + (P_r^2 - 1) \equiv 0 \pmod 4$$

$$\Rightarrow \frac{1}{8}(P_1^2p_2^2 \ldots\ldots P_{r-1}^2 - 1) + \frac{1}{8}(P_r^2 - 1) \equiv \frac{1}{8}(P_1^2P_2^2 \ldots\ldots P_r^2 - 1) \pmod 8$$

Then (A) gives

$$\sum_{i=1}^{r}\frac{1}{8}\left(P_i^2 - 1\right) = \frac{1}{8}\left(P_1^2 \ldots\ldots P_{r-1}^2 - 1\right) \pmod 8.$$

Hence the result follows.

Proof:

(viii) $(P, Q) = 1$ and P is also a positive odd then

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

If each of P and Q is equal to 1, then the result is immediate (L.H.S = R.H.S = 1)

Let $P = q_1q_2 \ldots q_s \qquad Q = P_1P_2 \ldots P_r$

$\because \quad (P, Q) = 1 \Rightarrow p_i \neq q_j \quad \forall\ i, j.$

Consequently $\left(\frac{p_i}{q_j}\right)$ and $\left(\frac{q_j}{p_i}\right)$ are non-zero

$$\therefore \quad \left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \prod_{i=1}^{r}\left(\frac{P}{p_i}\right)\prod_{j=1}^{s}\left(\frac{Q}{q_i}\right).$$

$$= \prod_{i=1}^{r}\left(\prod_{k=1}^{s}\frac{q_k}{p_i}\right)\prod_{j=1}^{s}\left(\prod_{\ell=1}^{n}\frac{p_\ell}{q_j}\right)$$

$$= (-1)^{\Sigma\Sigma\frac{1}{2}(q_j-1)\frac{1}{2}(p_j-1)}$$

$$= (-1)^{\sum_{i=1}^{s}\frac{1}{2}(q_j-1)\sum_{i=1}^{r}\frac{1}{2}(p_j-1)} \qquad \ldots\ldots(*)$$

But

$$\Sigma\frac{1}{2}(P_i - 1) - \frac{1}{2}(P_1, P_2 \ldots\ldots P_r - 1) \pmod 2$$

and the corresponding result for $p = q_1 q_2 \ldots q_s$ yields that the R.H.S. of (*) is equal to $(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}$.

$$\therefore \quad \left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$. Hence Proved.

Exercise : Show that the congruence $x^2 \equiv 15 \pmod{1093}$ has no solution.

Solution :

We have to show that 15 is q.n.r. (mod 1093)

i.e. $\left(\frac{15}{1093}\right) = -1$

$$\left(\frac{15}{1093}\right) = \left(\frac{3}{1093}\right)\left(\frac{5}{1093}\right)$$

$$= \left(\frac{1093}{3}\right)\left(\frac{1093}{5}\right) \qquad \left[\because \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)\right]$$

$$= \left(\frac{1}{3}\right)\left(\frac{3}{5}\right) \qquad \because \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \text{ if } a \equiv b \pmod{p}$$

$$= 1 \cdot \left(\frac{5}{3}\right) \qquad \left[\left(\frac{3}{5}\right) = (-1)^{\frac{3-1}{2}\frac{5-1}{2}}\left(\frac{5}{3}\right)\right]$$

$$\equiv \left(\frac{2}{3}\right) \qquad \left(\because 5 \equiv 2 \pmod{3} \Rightarrow \left(\frac{3}{2}\right) = \left(\frac{2}{3}\right)\right)$$

$$= -1.$$

$\therefore$ 15 is a q.n.r. mod 1093.

$\therefore$ $x^2 \equiv 15 \ (1093)$ has no solution.

Exercise : Show that the congruence $x^2 + 23 = 0 \pmod{59}$ has solution.

Ans : We have to show that - 23 is q.n.r. mod 59.

i.e. $\left(-\frac{23}{59}\right) = 1$.

$$\left(-\frac{23}{59}\right) = \left(-\frac{1}{59}\right)\left(\frac{23}{59}\right)$$

$$= (-1)^{\frac{23-1}{2}\frac{59-1}{2}}\left(\frac{23}{59}\right)$$

$$= \left(\frac{13}{23}\right) \qquad (\because \quad 59 \equiv 13 \pmod{23})$$

$$= (-1)^{\frac{13-1}{2}\frac{23-1}{2}}\left(\frac{23}{13}\right)$$

$$= \frac{10}{13} \quad = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right)$$

$$= (-1)\cdot(-1)^{\frac{5-1}{2}\frac{13-1}{2}}\left(\frac{13}{5}\right)$$

$$= -\left(\frac{3}{5}\right)$$

$$= (-1)\cdot(-1)^{\frac{3-1}{2}\frac{5-1}{2}}\left(\frac{5}{3}\right)$$

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

$\therefore$ -23 is q.r. mod 59.

$\therefore$ $x^2 + 23 \equiv 0 \pmod{59}$ has solution.

Calculate : $\left(\frac{189}{313}\right)$

Ans : $\left(\frac{189}{313}\right) = \left(\frac{3^2 \cdot 21}{313}\right)$

$$= \left(\frac{21}{313}\right) \qquad \because \left(\frac{ar^2}{p}\right) = \left(\frac{a}{p}\right)$$

$$= \left(\frac{3}{313}\right)\left(\frac{7}{313}\right)$$

$$= (-1)^{\frac{3-1}{2}\frac{313-1}{2}}\left(\frac{313}{3}\right)(-1)^{\frac{7-1}{2}\frac{313-1}{2}}\left(\frac{313}{7}\right)$$

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

$$= -1.$$

Summary

- If the integer 'b' has order k modulo n and $h > 0$ then b^h has order $\frac{k}{(h,k)}$ modulo n.
- If n is a primitive root, then it has exactly $\varphi(\varphi(n))$ of them.
- If p is an odd prime and $k \geq 1$, there exists a primitive root of p^k.
- If n is any of the integers 2, 4, p^k, $2p^k$, where p is an odd prime and $k \geq 1$, then n has primitive roots.
- For $k \geq 3$, the integers 2^k has no primitive roots.
- If a is a primitive root of n, then a, a^2, ..., $a^{\varphi(n)}$ is a reduced set of residues mod n.
- If the congruence $x^2 \equiv a \pmod{p}$ is solvable then it has exactly two solutions, where p is an odd prime.
- Let p be an odd prime and (a, p) = 1. Then a is called a quadratic residue of p if the congruence $x^v \equiv a \pmod{p}$ has a solution and a is called quadratic non-residue of p if $x^2 \equiv a \pmod{p}$ has no solution.
- Euler's criteria states that "Let p be an odd prime and (a, p) = 1. Then a is a quadratic residue of p if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
- There are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues of p.
- Let p be an odd prime and (a, p) = 1. The Legendre's symbol $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = 0 \text{ if } p \mid a$$

$= 1$ if a is a quadratic residue of p.
$= -1$ if a is a quadratic non-residue of p.

■■■

Unit - 4

Arithmetic Functions and some Diphantine Equations

Introduction :

A function, whose domain is the set of natural numbers is called a number theoretic function. These types of functions having special importance in the theory of numbers. In this unit, we shall discuss some important number theoretic function with their important properties. Historically, a problem which has received a good deal of attention has been that of representing numbers as sums of squares. In this unit, we first find necessary and sufficient conditions that a positive integer be representable as the sum of two squares and as the sum of four squares.

Number Theoretic Functions : Any function with domain of definition as the set of positive integers is said to be **Number Theoretic Function.**

Functions τ, σ and ϕ : Given any positive integer n,

$\tau(n)$ = the number of positive divisors of n.

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

1, 2, 3, 4, 6, 12 are positive divisors of n = 12.

$\tau(n) = 6$

$\sigma(n) = 28$.

If p is prime,

$\tau(p) = 2$

$\sigma(p) = 1 + p$.

$\sum_{d|n} f(x)$ = sum of values of f(d) when d runs through positive disors of n.

$\sum_{d|n} f(20) = f(1) + f(2) + f(5) + f(4) + f(10) + f(20)$

$\tau(n) = \sum_{d|n} 1$

$\sigma(n) = \sum_{d|n} d$

Theorem : If $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ is prime factorization of $n > 1$, then the positive divisors of n are precisely those integers of the form $d = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ where,

$0 \le a_1 \le k_1, 0 \le a_2 \le k_2, \ldots, 0 \le a_r \le k_r$.

Note that the divisor $d = 1$ is obtained when $a_1 = a_2 = \ldots = a_r = 0$ and n itself occures when $a_1 = k_1$, $a_2 = k_2, \ldots, a_r = k_r$. Suppose that d is a non trivial divisor of n. Then $n = dd'$, with $d > 1$ and $d' > 1$. Express both d and d' as product of primes, $d = q_1 q_2 \ldots q_s$ and $d' = t_1 t_2, \ldots t_r$ where q_i and t_j are primes. Then

$$n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r} = q_1 q_2 \ldots q_s t_1 t_2 \ldots t_u$$

are two prime factorization of n. By the uniqueness of prime factorization each prime q_i must be one of the p_j. Collecting the equal primes into a single integer power we get,

$$d = q_1 q_2 \ldots q_s = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$$

where the possibility that $a_i = 0$ is allowed.

Conversely every number $d = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ $(o \le a_i \le k_i)$ must be a divisor of n.

$$\begin{aligned} n &= p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r} \\ &= \left(p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}\right)\left(p_1^{k_1 - a_1} p_2^{k_2 - a_2} \ldots p_r^{k_r - a_r}\right) \\ &= dd' \end{aligned}$$

$\therefore \quad d \mid n.$

Theorem : $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ is the prime factorization of $n > 1$, then

(a) $\tau(x) = (k_1 + 1)(k_2 + 1) \ldots (k_r + 1)$

(b) $\sigma(x) = \dfrac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \dfrac{p_2^{k_2+1} - 1}{p_2 - 1} \ldots\ldots \dfrac{p_r^{k_r+1} - 1}{p_r - 1}$

Proof :

(a) The positive divisors of $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ are precisely those integers which can be express as $d = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ where $o \le a_i \le k_i$.

There are $(k_1 + 1)$ choices for the exponent a_1, $(k_2 + 1)$ choices of a_2, and so on ... $(k_n + 1)$ choices for a_n.

Hence there are $(k_1 + 1)(k_2 + 1) \ldots (k_r + 1)$ possible divisors of n.

Hence $\tau(n) = (k_1 + 1)(k_2 + 1) \ldots (k_r + 1)$.

(b) In order to evaluate $\sigma(n)$, we consider the product,

$$\left(1 + p_1 + p_1^2 + \ldots + p_1^{k_1}\right)\left(1 + p_2 + p_2^2 + \ldots + p_2^{k_2}\right) \ldots \left(1 + p_r + p_r^2 + \ldots + p_r^{k_r}\right)$$

each positive divisors of n appears once and only once as a term in the expansion of this product. In other words, this product is equal to sum of the divisors of n.

Hence

$$\sigma(n) = \left(1 + p_1 + p_1^2 + \ldots + p_1^{k_1}\right)\left(1 + p_2 + p_2^2 + \ldots + p_2^{k_2}\right)\ldots\left(1 + p_r + p_r^2 + \ldots + p_r^{k_r}\right)$$

$$= \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots\cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}.$$

Example :

$$\tau(180) = \tau(2^2 \times 3^2 \times 5)$$

$$= (2 + 1)(2 + 1)(1 + 1)$$

$$= 18.$$

$$\sigma(n) = \frac{2^3 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1}$$

$$= 7 \times 13 \times 6$$

$$= 546.$$

Definition : A number theoretic function f is said to be multiplicative if

$$F(m, n) = f(m)f(n)$$

whenever gcd(m, n) = 1.

Note :

(1) If $n_1, n_2, \ldots, n_r$ are relatively prime, for a multiplicative function,

$$f(n_1 n_2 \ldots n_r) = f(n_1)f(n_2)\ldots f(n_r).$$

(2) If $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ then

$$f(n) = f\left(p_1^{k_1}\right) f\left(p_2^{k_2}\right) \ldots f\left(p_r^{k_r}\right).$$

(3) For a multiplicative function $f \not\equiv 0$, $f(1) = 1$.

$f \not\equiv 0$ so $\exists$ x such that

$f(x) \neq 0$.

$f(x) = f(x\,1)$

$= f(x)f(1)$

$\Rightarrow f(1) = 1$ $\qquad (\because f(x) \neq 0).$

Theorem : The functions σ and τ are multiplicative.

Prrof : Let $m, n \in \angle$ such that $\gcd(m, n) = 1$.

(a) To prove $\sigma(mn) = \sigma(m)\,\sigma(n)$ and $\tau(mn) = \tau(m)\,\tau(n)$.

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

$= \sigma(n)\sigma(m)$ ($\because \sigma(m) = \sigma(1) = 1$ by definition)

and if $m = 1$, $\tau(mn) = \tau(n)$

$= \tau(n) \cdot 1$

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

$\therefore$ result also holds when $n = 1$.

Suppose $m > 1, n > 1$

$m = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ and $\gcd(m, n) = 1$

and $n = q_1^{j_1} q_2^{j_2} \ldots q_r^{j_s} \Rightarrow \gcd(p_i, q_j) = 1.$

$\therefore$ $\tau(m) = (k_1 + 1)(k_2 + 1) \ldots (k_r + 1)$

$\tau(n) = (j_1 + 1)(j_2 + 1) \ldots (j_s + 1)$

$mn = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r} q_1^{j_1} q_2^{j_2} \ldots q_r^{j_s}$

$\tau(mn) = (k_1 + 1)(k_2 + 1) \ldots (k_r + 1)(j_1 + 1)(j_2 + 1) \ldots (j_r + 1)$

$= \tau(m)\tau(n).$

$$\sigma(mn) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1} \cdot \frac{q_1^{j_1+1} - 1}{q_1 - 1} \cdots \frac{q_s^{j_s+1} - 1}{q_s - 1}$$

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

Thus σ and τ are multiplicative.

Lemma : If $\gcd(m, n) = 1$, then the set of positive divisors of mn consists of all products $d_1 d_2$, where $d_1 \mid n, d_2 \mid m$ and $\gcd(d_1, d_2) = 1$ and these products are all distinct.

Let $m > 1, n > 1$ and

$m = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$

$n = q_1^{j_1} q_2^{j_2} \ldots q_s^{j_s}$

are respective prime factorization of m and n and p_i and q_j are all distinct primes.

$mn = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r} q_1^{j_1} q_2^{j_2} \ldots q_s^{j_s}$

divisors of mn are,

$$d = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r} q_1^{b_1} \dots q_s^{b_s} \qquad 0 \le a_i \le k_i$$
$$0 \le b_i \le j_i$$

$= d_1 d_2$ wher $d_1 \mid m$ and $d_2 \mid n$.

Also $\gcd(d_1, d_2) = 1$.

Theorem : If f is multiplicative function and F is defined by

$$F(n) = \sum_{d|n} f(d)$$

then F is also multiplication.

Proof : Let m and n be relatively prime.

Thus

$$F(mn) = \sum_{d|mn} f(d)$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2) \quad \text{(By usinng above leamma when } (d_1, d_2) = 1)$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1)(d_2)$$

$$= \left(\sum_{d_1|m} f(d_1) \right) \left(\sum_{d_2|n} f(d_2) \right) = F(m)\, F(n).$$

Thus F is also multiplicative.

Note :

$$\tau(n) = \sum_{d|n} 1$$

But $f(d) = 1$ is multiplicative since,

$$f(d_1 d_2) = 1 = 1.1. = f(d_1) f(d_2).$$

$\therefore$ $\tau(n) = \sum_{d|n} f(d)$ is multiplicative.

$\sigma(n) = \sum_{d|n} d$ and $f(d) = d$ is multiplicative.

$\therefore$ σ is multiplicative.

Inversion Formula

The Mobius Inversion Formula

Definition : For a positive integer n define μ by,

$$\mu(n) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } p^2 \mid n \text{ for some prime } p \\ (-1)^r \text{ if } n = p_1 p_2 \ldots p_r \text{ where } p_i \text{ are distinct primes} \end{cases}$$

Exercise : $\mu(1) = 1$ $\mu(4) = 1$

$\mu(30) = \mu(2.3.5) = (-1)^3 = -1.$

Theorem : Mobius function μ is multiplicative.

Proof : Let m and n be distinct primes. To show

$\mu(mn) = \mu(m)\mu(n).$

If $p^2 \mid m$ or $p^2(n)$ then $p^2 \mid mn.$

Then in this case $\mu(mn) = 0 = \mu(m)\mu(n).$

In this case the theorem is proved.

Let us assume that m and n are square free integers.

Suppose $m = p_1 p_2 \ldots p_r$

and $n = q_1 q_2 \ldots q_s$

where p_i and q_j are distinct primes.

Then

$\mu(mn) = \mu(p_1 p_2 \ldots p_r q_1 q_2 \ldots q_s)$, where p_i and q_j are distinct

as gcd(m, n) = 1

$= (-1)^{r+s}$

$= (-1)^r(-1)^s$

$= \mu(m)\mu(n).$

Hence Mobius function is multiplicative.

Theorem : For each positive integer $n \geq 1$

$$\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } n > 1 \end{cases}$$

where d runs through all divisors of n.

Proof :

Case I : $n = 1,$

$$\sum_{d|n} \mu(d) = \sum_{d|1} \mu(d) = \mu(1) = 1.$$

Case II : Let $n > 1$. Put $F(n) = \sum_{d|n} \mu(d)$.

If $n = p^k$ then $F(n) = \sum_{d|p^k} \mu(d)$

$= \mu(1) + \mu(p) + \mu(p^2) + ... + \mu(p^k)$

$= 1 + (-1)^1 + 0 + ... + 0$

$= 0.$

$\therefore \quad f(p^k) = 0.$

Case III : Suppose $n = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$ any integer and $\gcd\left(p_i^{k_i}, p_j^{k_j}\right) = 1, i \neq j$.

$\therefore \quad \mu(n) = \mu\left(p_1^{k_1} p_2^{k_2} ... p_r^{k_r}\right)$

$= \mu\left(p_1^{k_1}\right)\mu\left(p_2^{k_2}\right)...\mu\left(p_r^{k_r}\right)$

$= 0.0...0$

$= 0.$

$\therefore \quad \sum_{d|n} \mu(d) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } n > 1 \end{cases}$

Theorem (Mobius Inversion Formula) : Let F and f be two Number Theoretic functions related by the function

$$F(n) = \sum_{d|n} f(d)$$

Then

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d).$$

Proof : Two sums $\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$ and $\sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$ are the same, because as d runs over all divisors of n, $\frac{n}{d}$ also runs over all divisors of n.

Now $\quad \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$

$$= \sum_{d|n} \mu(d) \left(\sum_{c|\frac{n}{d}} f(c) \right)$$

$$= \sum_{d|n} \left(\sum_{c|\frac{n}{d}} \mu(d) f(c) \right)$$

It can be verified that $d \mid n$ and $c \mid \frac{n}{d}$ iff $c \mid n$ and $d \mid \frac{n}{c}$.

$$= \sum_{c|n} \left(\sum_{d|\frac{n}{c}} \mu(d) f(c) \right)$$

$$= \sum_{c|n} \left(f(c) \sum_{d|\frac{n}{c}} \mu(d) \right) = \sum_{n=c} f(c) = f(n).$$

$$\therefore \quad f(n) = \sum_{d|n} f(d)$$

$$\Rightarrow f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Illustration :

$$\sum_{d|10} \left(\sum_{c|\frac{10}{d}} \mu(d) f(c) \right)$$

$$= \sum_{c|10} \mu(1) f(c) + \sum_{c|5} \mu(2) f(c) + \sum_{c|2} \mu(5) f(c) + \sum_{c|1} \mu(10) f(c)$$

$$= \mu(1)[f(1) + f(2) + f(5) + f(10)] + \mu(2)[f(1) + f(5)]$$

$$+ \mu(5)[f(1) + f(2)] + f(1).\mu(10)$$

$$= f(1)[\mu(1) + \mu(2) + \mu(5) + \mu(10)] + f(2)[\mu(1) + \mu(5)]$$

$$+ f(5)[\mu(1) + \mu(2)] + f(10)\mu(1)$$

$$= f(1) \sum_{d|10} \mu(d) + f(2) \sum_{d|5} \mu(d) + f(5) \sum_{d|2} \mu(d) + f(10) \sum_{d|1} \mu(d)$$

$$= 0 + 0 + 0 + f(10).1$$

$$= f(10).$$

Application :

(i) $\tau(n) = \sum_{d|n} 1 = \sum_{d|n} f(d), f(d) = 1$

By inversion formula,

$$1 = \sum_{d|n} \mu\left(\frac{n}{d}\right)\tau(d).$$

(ii) $\sigma(n) = \sum_{d|n} d = \sum_{d|n} f(d)$ where $f(d) = d$.

$$f(n) = n = \sum_{d|n} \mu\left(\frac{n}{d}\right)\sigma(d).$$

We have seen that if $F(n) = \sum_{d|n} f(d)$ and f is multiplication then F is also multiplicative.

We prove two converse.

Theorem : If F is multiplicative and $F(n) = \sum_{d|n} f(d)$ then f is also multiplicative.

Proof : Let m and n be relatively primes. Any divisor d of mn can be written as $d = d_1 d_2$ where $d_1 \mid m$, $d_2 \mid n$ and $(d_1, d_2) = 1$.

By the inversion formula,

$$f(mn) = \sum_{d|mn} \mu(d) F\left(\frac{mn}{d}\right)$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1 d_2) F\left(\frac{m}{d_1}\frac{n}{d_2}\right)$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1)\mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right)$$

$$= \sum_{d_1|m} \mu(d_1) F\left(\frac{m}{d_1}\right) \sum_{d_2|n} \mu(d_2) F\left(\frac{n}{d_2}\right)$$

$$= f(m)f(n).$$ Hence Proved.

Euler's Phi-Function ϕ (n) : For $n \geq 1$ let $\phi(n)$ denote the number of positive integers not exceeding n, and relatively prime to n.

For example $\phi(30) = 8$. In fact 1, 7, 11, 13, 17, 19, 23, 29 are relatively prime to 30.

$\phi(1) = 1$ $\phi(2) = 1$

$\phi(3) = 2$

$\phi(p) = p - 1$, where p is a prime.

Theorem : If p is a prime and $k > 0$, then

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

Proof : There are p^{k-1} integers between 1 and p^k divisible by p namely,

$p, 2p, 3p, 4p, ..., p^{k-1}.p.$

These are the integers not relatively prime to p^k.

Numbers of integers not relatively prime to p^k is p^{k-1}. So the number of integers less then p^k and relatively prime to p^k is,

$$\phi(p^k) = p^k - p^{k-1}$$

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

Exercise : $\phi(3^4) = 3^4 - 3^{4-1}$

$= 81 - 27$

$= 54.$

Lemma : Given integers a, b, c

gcd(a, bc) = 1 iff gcd(a, b) = 1 and gcd(a, c) = 1.

Proof : Let gcd(a, bc) = 1

and put d = gcd(a, b).

$\therefore$ $d \mid a, d \mid b \Rightarrow d \mid a, d \mid bc$

$\Rightarrow d \leq \gcd(a, bc) = 1$

$\Rightarrow d = 1.$

$\therefore$ gcd(a, b) = 1.

Similarly gcd(a, c) = 1.

Conversely let gcd(a, b) = 1, gcd(a, c) = 1.

Suppose $\gcd(a, bc) = d_1 > 1$.

Thus d_1 must have a prime factor p.

So $p \mid bc$ ($\because p \mid d_1$ and $d_1 \mid bc$).

So $p \mid b$ or $b \mid c$.

If $p \mid b$ then by virtue of $p \mid a$

$\gcd(a, b) \geq p > 1$, a contradiction to (a, b) = 1.

Similarly, $p \mid c$ leads to a contradiction

$\therefore$ $\quad \gcd(a, bc) = 1.$

Theorem : ϕ is a multiplicative function.

Proof : Let m and n be relatively prime. To show that $\phi(mn) = \phi(m)\phi(n)$.

Lemma : $\quad \gcd(a, bc) = 1$ iff $\gcd(a, b) = 1, \gcd(a, c) = 1.$

This means r is relatively prime to mn iff r is relatively prime to m and n.

Case I : Suppose $m = 1$, then

$\phi(mn) = \phi(n) = 1.\phi(n) = \phi(1)\phi(n) = \phi(m)\phi(n)$ $\quad (\because \phi(1) = 1).$

Similar is the case for $n = 1$.

Case II : $m > 1, n > 1$

We arrange the integers 1, 2, ...mn as follows

1	2	m
m + 1	m + 2	2m
2m + 1	2m + 2	3m
.....		
(n - 1)m + 1	(n - 1)m + 2	mn

We know that $\phi(mn)$ is equal to the number of entries in the above array which are relatively prime to mn and by virtue of the lemma this is the same as the number of integers which are relatively prime to both m and n.

Since $\gcd(qm + r, m) = \gcd(r, m)$

The number in the r^{th} column are relatively prime to m iff r itself is relatively prime to m.

Therefore only $\phi(m)$ colmns contain integers relatively prime to m. We have to show that in such colmn there are $\phi(n)$ elements are relatively prime to n. Then there will be $\phi(m)\phi(n)$ elements in the array which are relatively prime to both m and n, i.e., relatively prime to mn.

Suppose $\gcd(r, m) = 1$. The entries in the r^{th} colmn are,

$\{r, m+r, 2m+r, ...(n-1)m + r\}$.

There are n elements in the column and no two are cogruent modulo n.

Indeed if $km + r \equiv jm + r \pmod n$ where $0 \leq k < j < n$.

Then $km \equiv jm \pmod{n}$

$\Rightarrow k \equiv j \pmod{n}$ as $\gcd(m, n) = 1$.

$\Rightarrow n \mid k - j$.

which is not possible as $0 \le k < j < n$.

Thus the number in the r^{th} column are congruent modulo n to 0, 1, 2, 3, ...(n - 1) in some order.

But if $s \equiv t \pmod{n}$ then $\gcd(s, n) = 1 \Leftrightarrow \gcd(t, n) = 1$.

But there are $\phi(n)$ element in 0, 1, 2,...(n - 1) which are relatively prime to n. So there are $\phi(n)$ elements in the r^{th} column which are relatively prime to n.

So in $\phi(m)$ columns $\phi(m)\phi(n)$ elements are relatively prime to both m and n.

By the lemma $\phi(mn) = \phi(m)\phi(n)$.

Theorem : If $n > 1$ has prime factorization

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \text{ then}$$

$$\phi(n) = \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-2}\right)\dots\left(p_r^{k_r} - p_r^{k_r-2}\right)$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_r}\right)$$

Proof :

$$\phi(n) = \phi\left(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}\right)$$

$$= \phi\left(p_1^{k_1}\right)\phi\left(p_2^{k_2}\right)\dots\phi\left(p_r^{k_r}\right)$$

(as $\gcd\left(p_i^{k_i}, p_j^{k_j}\right) = 1$ and ϕ is multiplicative)

$$= \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)\dots\left(p_r^{k_r} - p_r^{k_r-1}\right)$$

$$= p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_r}\right)$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_r}\right).$$

Exercise : Compute $\phi(360)$.

Ans : $\phi(360) = \phi(2^3.3^2.5)$

$$= 360\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$$= 360\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5} = 96.$$

Exercise : For $n > 2$, $\phi(n)$ is an even integer.

Ans :

Caee I : If $n = 2^k$ then

$$\phi(n) = \phi(2^k)$$

$$= 2^{k-1} - 2^{k-1}$$

$$= 2^{k-1}(2 - 1)$$

$$= 2^{k-1}, \text{ which is even.}$$

In general if 2^k is a factor of n, then

$$\phi(n) = \phi\left(2^k p_1^{k_1} \ldots p_r^{k_r}\right)$$

$$= \phi\left(2^k\right)\phi\left(p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}\right), \text{ which is even.}$$

Case II : If n be any integer such that

$$n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r} \text{ and } p_i \neq 2,$$

Then $$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_r}\right)$$

$$= n\frac{p_1-1}{p_1}\frac{p_2-1}{p_2}\ldots\frac{p_r-1}{p_r}$$

$$= p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}\frac{(p_1-1)(p_2-1)\ldots(p_r-1)}{p_1 p_2 \cdots p_r}$$

$$= p_1^{k_1-1} p_2^{k_1-1} \ldots p_r^{k_r-1}(p_1-1)(p_2-1)\ldots(p_r-1).$$

But $p_i - 1$ is even number if $p_i \neq 2$.

Thus $p_1^{k_1-1} p_2^{k_2-1} \ldots p_r^{k_r-1}(p_1-1)(p_2-1)\ldots(p_r-1)$ is an even integer.

$\therefore$ $\phi(n)$ is an even integer.

Euler's Theorem : If n is a positive integer and $\gcd(a, n) = 1$, then $a^{\phi(x)} \equiv 1 \pmod{n}$.

Lemma : Let $n > 1$ and $\gcd(a, n) = 1$.

If $a_1, a_2, \ldots a_{\phi(x)}$ are positive integers less then n and relatively prime to n then $aa_1, aa_2, \ldots aa_{\phi(x)}$

are congruent modulo to $a_1, a_2, \ldots a_{\phi(x)}$ in some order.

Proof of the Lemma : We can show that no two elements of $aa_1, aa_2, \ldots aa_{\phi(x)}$ are congruent modulo n. For if

$$aa_i \equiv aa_j \pmod n$$

then $a_i \equiv a_j \pmod n \qquad (\because (a, n) = 1)$

which is not possible since a_i and a_j are less then n.

Since $\gcd(a_i, n) = 1$ for all i and $\gcd(a, n) = 1$ we have,

$\gcd(aa_i, n) = 1$.

For each aa_i is relatively prime to n.

For a particular element aa_i. There exists a unoque fixed element b. $0 \le b < n$ for which

$aa_i \equiv b \pmod n$

$\gcd(b, n) \equiv \gcd(aa_i, n) = 1$.

So b must be one of the integers, $a_1, a_2, \ldots a_{\phi(x)}$. Here $aa_1, aa_2, \ldots aa_{\phi(x)}$ are congruent to $a_1, a_2, \ldots a_{\phi(x)} \pmod n$ in some order.

Thus the lemma is proved.

By the lemma,

$aa_1 \equiv a_1^{\,1} \pmod n$

$aa_2 \equiv a_2^{\,1} \pmod n$.

.....

$aa_{\phi(n)} \equiv a_n^{\,1} \pmod n$

where $a_1^{\,1}, a_2^{\,1}, \ldots, a_n^{\,1}$ are nothing but $a_1, a_2, \ldots a_{\phi(n)}$ taken in some order.

On multiplying,

$$a^{\phi(n)}(a_1, a_2, \ldots a_{\phi(n)}) \equiv a_1^{\,1} a_2^{\,1} \ldots a_n^{\,1} \pmod n$$
$$\equiv a_1 a_2 \ldots a_{\phi(n)} \pmod n$$

$\gcd(a_i, n) = 1$ for each i

$\Rightarrow \gcd(a_1 a_2 \ldots a_{\phi(n)}, n) = 1$.

Hence by cancellation law,

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

Corollary : When n = p, a prime $a^{\phi(n)} \equiv a^{p-1} \equiv 1 \pmod p$ which is **Fermat's Little Theorem.**

Exercise : Find the last two digits in decimal representation of 3^{256}.

Ans : We have to find the least number such that

$$3^{256} \equiv r(\text{mod } 100).$$

By Euler's theorem

$$3^{\phi(100)} \equiv 1 \text{ (mod } 100)$$

and $$\phi(100) = \phi(2^2 \times 5^2)$$

$$= 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)$$

$$= 100 \cdot \frac{1}{2} \cdot \frac{4}{5}$$

$$= 40.$$

Thus $3^{40} = 1(\text{mod } 100)$

$\Rightarrow (3^{40})^6 \equiv 1(\text{mod } 100)$

$\Rightarrow 3^{240} \equiv 1(\text{mod } 100).$

$3^{256} = 3^{240}.3^{16} \equiv 3^{16}(\text{mod } 100)$

$\Rightarrow 3^{256} \equiv (81)^4(\text{mod } 100)$

$\equiv (-9)^4(\text{mod } 100)$

$\equiv (361)^2(\text{mod } 100)$

$\equiv (61)^2(\text{mod } 100)$

$\equiv 21(\text{mod } 100)$

So, last two digits are 2 and 1.

Theorem (Gauss) : For each positive integer $n \geq 1$ $n = \sum_{d|n} \phi(d)$ the sum being extended over all positive divisior of n.

Proof : If $n = 1$

$$\sum_{d|n} \phi(d) = \sum_{d|1} \phi(d) = \phi(1) = 1$$

Let $n > 1$. Consider number theoritic function,

$$F(n) = \sum_{d|n} \phi(d)$$

Multiplicity of ϕ implies multiplicity of F.

Let $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$.

$$F(n) = F(p_1^{k_1})\,F(p_2^{k_2}) \dots F(p_r^{k_r}) \qquad \dots\dots(1)$$

$$F(p_r^{k_r}) = \sum_{d \mid p_r^{k_r}} \phi(d)$$

$$= d(1) + \phi(p_r) + \phi(p_r^{2}) + \dots + \phi(p_r^{k_r})$$

$$= 1 + (p_r - 1) + p_r^{2} - p_r + \dots + p_r^{k_r} - p_r^{k_r - 1}$$

$$= p_r^{k_r}.$$

Thus from (1),

$$F(n) = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$$

$$\Rightarrow \sum_{d \mid n} \phi(n) = n.$$

Theorem : For $n > 1$ the sum of the integers less than n and relatively prime to n is $\frac{1}{2} n\phi(n)$.

Proof : To show

$$\sum_{\substack{\gcd(k,n)=1 \\ 1 \le k < n}} k = n\frac{1}{2} n\phi(n).$$

Let $a_1, a_2, \dots a_{\phi(n)}$ be the positive integers relatively prime to n are less than n.

Also $\gcd(k, n) = 1 \Rightarrow \gcd(n - k, n) = 1$.

So $n - a_1, n - a_2, \dots, n - a_{\phi(n)}$ are also relatively prime to n.

Let $S = a_1 + a_2 + \dots + a_{\phi(n)}$

and $S = (n - a_1) + (n - a_2) + \dots + (n - a_{\phi(n)})$

$= n\phi(n) - (a_1 + a_2 + \dots + a_{\phi(n)})$

$= n\phi(n) - S$

$\Rightarrow S = \frac{1}{2} n\phi(n)$.

Thus $\sum_{\substack{\gcd(k,n)=1 \\ 1 \le k < n}} k = \frac{1}{2} n\phi(n)$.

Theorem : For any integer n, $\phi(n) = n \Rightarrow \sum_{d \mid n} \frac{\mu(d)}{d}$.

Proof : We have $F(n) = n\sum_{d|n}\phi(n)$.

By Mobius inversion formula,

$$\phi(n) = \sum_{d|n} F\left(\frac{n}{d}\right)\mu(d)$$

$$= \sum_{d|n} \frac{n}{d}\mu(d)$$

$$= n\sum_{d|n} \frac{\mu(d)}{d}.$$

Deduction : If $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ prove that,

$$\phi(n) = n\prod_{p_i}\left(1 - \frac{1}{p_i}\right).$$

Proof : Consider the product,

$$p = \prod_{p_i|n}\left[\mu(1) + \frac{\mu(p_i)}{p_i} + \ldots + \frac{\mu(p_i^{k_i})}{p_i^{k_i}}\right].$$

Multiplying this out we obtain sum of terms of the form,

$$\frac{\mu(1)\mu(p_1^{\alpha_1})\mu(p_2^{\alpha_2})\ldots\mu(p_r^{\alpha_r})}{p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r}}$$

$$= \frac{\mu(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r})}{p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r}}$$

$$= \frac{\mu(d)}{d}$$

where d is a divisor of n.

$$\therefore \quad \phi(n) = n\sum_{d|n}\frac{\mu(d)}{d}$$

$$= n\prod\left\{\mu(1) + \frac{\mu(p_i)}{p_i} + \frac{\mu(p_i^{\alpha})}{p_i^{\alpha}} + \ldots + \frac{\mu(p_i^{k_i})}{p_i^{k_i}}\right\}$$

$$= n\prod\left(1 - \frac{1}{p_i}\right) \quad \because \quad \mu(p_i^{\alpha_i}) = 0 \text{ when } \alpha_i \geq 2.$$

Fermat's Last Theorem :

The Diophantine equation $x^n + y^n = z^n (n \geq 3)$ has no positive solutions. This problem known as Fermat's Last Theorem, was attracted from every concievable stand point by the best mathematician of the last 350 years. Many interesting results have been established, but the theorem could never be proved till 1993.

E.Kumer (1810 - 1893) made the greatest advances towards a solution. instead of confinding himself to the field of rational numbers he extended his concept of number theory to include the algebraic numbers (these complex numbers which are roots of polynomials with rational co-efficients). In 1843 he submitted what he thought was a proof, but Dirichlet pointed out a flaw in the argument. Kumer had assumed that the factorization into primes is unique in a certain subring of the algebraic numbers where, in fact, this factorization is not unique, because this assumption is essential but proof was not valid.

Kumer returned to the problem and by using the theory of ideals, he was able to solve parts of his proof and to establish very general condition for the insolvability of the Fermat's Theorem. Most of the progress made on the problem in the last century. With the use of high speed electronic computer it was possible to check Kumer's criterian for larger exponents. Till the year 1967 it was found that the Diphantine equation $x^n + y^n = z^n$ has no positive solution if $3 \leq n \leq 25,000$.

However we can fairly safe in assuming that Fermat's never had a valid proof.

The Theorem was written in 1637, where Pierre de fermat was studying an ancient greek test on number theory called Arithmetica by Diofantus. At that time he came across the famus Pythagorian equation $x^2 + y^2 = z^2$. When Fermat saw this he noted that for any exponent greater than 2, the equation could not have solutions in whole numbers. He also wrote in lattice that he had discovered his own wonderful proof, but that the margin was too small to contain it. No such proof has even been found. fermat made many such marginal questions and over the centuries they were all answered except this one, the Fermat's last theorem.

The solution of Fermat's last theorem was established by Andrew Wile of Princetone University in 1993. He first came across Fermat's problem at the age of 10 years in a library in cambridge, England, where he grew up. He vowed that he would solve the problem one day. Even after he had presented a result, a small but crucial error was found and this led further investigation. Again there seem to be no solution. But there was one— "Wiles called this last insight, the most important moment of my working life. It was so indescribably beautiful, it was so simple for all and elegent and I just donot believe"

Did fermat really complete his own proof in 17th century, undoubtly the same will continue for look his evidence he did, but it is highly unlikely. Wiles made use of newly developed mathematics of

19th and 20th century that did not exist in Fermat's time.

The Diophantive equation $x^2 + y^2 = z^2$ .....(*)

has infinite solutions.

For if (a, b, c) is a solution then (ka, kb, kc) is also a solution for each $k \in \mathbb{Z}$

Theorem :

If (a, b, c) is a solution of (*) and (a, b) = d then (b, c) = (c, a) = d.

Proof :

$a^2 + b^2 = c^2$ and (a, b) = d.

$\therefore$ $d \mid a, d \mid b \Rightarrow d^2 \mid a^2, d^2 \mid b^2$

$\Rightarrow d^2 \mid a^2 + b^2$

$\Rightarrow d^2 \mid c^2$

$\Rightarrow d \mid c.$

$\therefore$ $d \mid a, d \mid c.$

$\therefore$ $d \leq (a, c).$

Suppose $(a, c) = d_1$.

$\therefore$ $d_1 \mid a, d_1 \mid c.$

$\therefore$ $d_1^2 \mid a^2, d_1^2 \mid c^2 \Rightarrow d_1^2 \mid c^2 - a^2 = b^2$

$\Rightarrow d_1 \mid b.$

$\therefore$ $d_1 \mid a, d_1 \mid b \Rightarrow d_1 \mid d.$

$= (a, c) \mid d.$

$\therefore$ $d = (a, c)$

Similarly $d = (b, c).$

$\therefore$ (b, c) = (c, a) = d. Hence proved.

Definition :

If (a, b, c) is a solution of $x^2 + y^2 = z^2$ such that (a, b, c) = 1, then (a, b, c) is called **primitive Solution.**

We are interested in primitive solutions of

$x^2 + y^2 = z^2$ .....(*)

i.e. these integers x, y and z such that (x, y) = (y, z) = (z, x) = 1.

How many solutions of (*) are there so that these are relatively prime.

Lemma 1 :

If (x, y, z) is a primitive solution of (*) then one of x and y is even and the other is odd.

Proof :

Since (x, y) = 1, both x and y cannot be even.

If both of them are odd then x^2 and y^2 are also odd and so $x^2 + y^2 = z^2$ is even. This implies z is even.

Now x is odd $\Rightarrow x \equiv 1$ or $3 \pmod 4$

$\Rightarrow x^2 \equiv 1 \pmod 4$

Similarly y is odd $\Rightarrow y^2 \equiv 1 \pmod 4$

$\therefore \quad x^2 + y^2 \equiv 2 \pmod 4$

$\Rightarrow z^2 \equiv 2 \pmod 4$.

But z being even say $z = 2m$.

$(2m)^2 \equiv 2 \pmod 4$

$\Rightarrow 4m^2 \equiv 2 \pmod 4$ and $4m^2 \equiv 0 \pmod 4$

$\Rightarrow 2 \equiv 0 \pmod 4$, which is not true.

So x and y both cannot be odd.

Therefore one of x and y is even and other is odd.

Note : In our discussion from now onwards we shall assume x is odd and y is even.

Lemma 2 :

If (x, y, z) is a primitive solution of (*) then $\left(\frac{z-x}{2}, \frac{z+x}{2}\right) = 1$.

Proof :

Suppose $\left(\frac{z-x}{2}, \frac{z+x}{2}\right) = g$:

Then $g \left| \frac{z-x}{2} \right.$ and $g \left| \frac{z+x}{2} \right.$.

$\therefore \quad g \left| \frac{z-x}{2} + \frac{z+x}{2} \Rightarrow g \right| z.$

and $\quad g \left| \frac{z+x}{2} - \frac{z-x}{2} \Rightarrow g \right| x.$

$\therefore \quad g \mid z, g \mid x \qquad \therefore \quad g \leq 1 \quad (\because \quad (z, x) = 1)$

$\therefore \quad g = 1$

$\therefore \quad \left(\frac{z-x}{2}, \frac{z+x}{2}\right) = 1.$

Lemma 3 :

If $(x, y) = 1$ and $xy = d^2$, then each of x and y is also a square.

Proof :

Suppose $x = p_1 p_2 \ldots\ldots p_\alpha$

$y = q_1 q_2 \ldots\ldots q_\beta$

where not necessarily p_i's and q_j's are distinct.

$\therefore$ $p_1 p_2 \ldots\ldots p_\alpha q_1 q_2 \ldots\ldots q_\beta = d^2$ and $(p_i, q_j) = 1$ since $(x, y) = 1$.

So each of $p_1 p_2 \ldots\ldots p_\alpha$ and $q_1 q_2 \ldots\ldots q_\beta$ must be a square. Hence x and y are also squares.

Question :

$$x^2 + y^2 = z^2 \qquad \ldots\ldots(*)$$

If (x, y, z) is a primitive solution of (*), x is even, then $y = 2st$, $x = s^2 - t^2$, $z = s^2 + t^2$, where s and t are positive integers satisfying the following three conditions.

(i) $(s, t) = 1$

(ii) $s > t$

(iii) one of s and t is even and the other is odd. (i.e. s and t are of opposite parity).

Proof :

Let (x, y, z) be primitive solution of (*).

$\therefore$ $x^2 + y^2 = z^2$

$\Rightarrow y^2 = z^2 - x^2 = (z + x)(z - x)$

$$\Rightarrow \left(\frac{y}{2}\right)^2 = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right).$$

By lemma 2 $\left(\frac{z+x}{2}, \frac{z-x}{2}\right) = 1$.

So, by lemma 3, $\frac{z+x}{2} = s^2$ and $\frac{z-x}{2} = t^2$. Clearly $s > t$.

Solving we get, $z + x = 2s^2$ $\quad z - x = 2t^2$.

$\therefore$ $z = s^2 + t^2$ and $x = s^2 - t^2$.

So $y^2 = 4s^2t^2$ and $y = 2st$.

If s and t both are odd or both are even then so z and x both are even.

But $(z, x) = 1$.

$\therefore$ s and t are of opposite parity.

$\therefore$ $(s, t) = 1$.

If $(s, t) = d > 1$, then $d \mid z$ and $d \mid x$, a contradiction.

Conversely, suppose $\exists$ s, t such that

$(s, t) = 1$, $s > t$ and s and t are opposite parity.

To prove $z = s^2 + t^2$, $y = 2st$, $x = s^2 - t^2$ is a primitive solution of (*).

If $(x, y) = d$ then $(y, z) = (z, x) = d$, since (x, y, z) is a solution of (*).

Let $(2st, s^2 - t^2) = d$ then $(2st, s^2 + t^2) = (s^2 + t^2, s^2 - t^2) = d$.

But $s > t$, $(s, t) = 1$ and

s, t are of opposite parity implies $d = 1$.

Since an infinite of such choice of s and t are possible so it follows that $x^2 + y^2 = z^2$ has infinite number of primitive solutions.

Theorem :

The diophantine equation $x^4 + y^4 = z^2$ .....(*)

has no positive solution.

Proof :

Suppose (*) has a positive solution (x_0, y_0, z_0).

Then $x_0^4 + y_0^4 = z_0^2$

$\Rightarrow (x_0^2)^2 + (y_0^2)^2 = z_0^2$

$\therefore$ (x_0^2, y_0^2, z_0) is a solution of $x^2 + y^2 = z^2$.

By the preceding result $\exists$ s, t such that $s > t$ and

$x_0^2 = s^2 - t^2$, $y_0^2 = 2st$, $z_0 = s^2 + t^2$.

So we get, $x_0^2 + t^2 = s^2$.

Again by the preceding result, $\exists$ a, b $\in$ N such that $a > b$ such that

$x_0 = a^2 - b^2$, $t = 2ab$ and $s = a^2 + b^2$

On substituting,

$y_0^2 = 2st$

$= 2(a^2 + b^2)2ab$.

$$\Rightarrow \left(\frac{y}{2}\right)^2 = (a^2 + b^2)ab .$$

Since, $(a, b) = 1$, we have

$(a^2 + b^2, a) = 1 = (a^2 + b^2, b)$.

So each of a, b and $a^2 + b^2$ is a perfect square.

So $a = a_0^2, b = b_0^2$

$s = a^2 + b^2 = s_0^2$

Then $s_0^2 = a^2 + b^2 = a_0^4 + b_0^4$.

$\therefore$ (a_0, b_0, s_0) is again a solution of (*).

where $s_0 \leq s < s^2 + t^2 = z_0$.

$\therefore$ (x_0, y_0, z_0) is a solution $\Rightarrow (a_0, b_0, s_0)$ is a solution such that $s_0 < z_0$.

We see that if a positive solution (x_0, y_0, z_0) exist there must exist another positive solution (a_0, b_0, s_0), where $s_0 < z_0$. It follows from the method of descent that no positive solution of (*) can exist.

Therefore $x^4 + y^4 = z^2$ has no positive solution.

Corollory :

$x^4 + y^4 = z^4$ has no positive solution.

Note : Method of descent :

Let $\exists$ a positive integer n with a certain property such that $\exists$ a smaller positive integer that has the same property. Such n cannot exist because if it does, we obtain an infinite decreasing sequence positive integers having the same specific property which is clearly impossible.

Two squares problem :

To find those positive integers which can be expressed as sum of two squares.

Lemma A :

If a and b can be written as sum of two squares then the product ab can also be written as a sum of two squares.

Proof :

Let $a = p^2 + q^2$

$b = r^2 + s^2$.

$ab = p^2r^2 + p^2s^2 + q^2r^2 + q^2s^2$

$= (pr)^2 + (qs)^2 + 2pr.qs + (ps)^2 + (qr)^2 - 2ps.\ qr$

$= (pr + qs)^2 + (ps - qr)^2$.

Lemma B :

$(a, p) = 1 \Rightarrow x \equiv ay \pmod p$ has a solution (x_0, y_0) such that

$$0 < |x_0| < \sqrt{p} \text{ and } 0 < |y_0| < \sqrt{p}$$

Proof :

Let $m = [\sqrt{p}]$.

Consider the set of numbers,

$1 + a, 1 + 2a, \ldots\ldots 1 + (m + 1)a$

$2 + a, 2 + 2a, \ldots\ldots 2 + (m + 1)a$

$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$

$(m + 1) + a, (m + 1) + 2a, \ldots\ldots (m + 1) + (m + 1)a.$

This set contains $(m + 1)^2$ numbers (not necessarily distinct).

Since $(m + 1)^2 > p$ $\quad (\because \quad m + 1 > \sqrt{p})$

i.e. at least two of the numbers (say) $x_1 + y_1a$ and $x_2 + y_2a$ must lie inthe same residue class (modulo p) where $x_1 \neq x_2$ or $y_1 \neq y_2$.

$\therefore \quad (x_1 + y_1a) - (x_2 + y_2a) \equiv 0 \pmod{p}$

$\Rightarrow (x_1 - x_2) + (y_1 - y_2)a \equiv 0 \pmod{p}$

$\Rightarrow x_1 - x_2 \equiv (y_2 - y_1)a \pmod{p}$ $\qquad \ldots\ldots(1)$

Since one of $x_1 - x_2$ and $y_1 - y_2$ is not zero therefore neither of them is zero.

$\therefore \quad 0 < x_1, x_2, y_1, y_2 \leq m + 1$

$0 < |x_1 - x_2| \leq m < \sqrt{p}.$

Similarly $\quad 0 < |y_1 - y_2| \leq m < \sqrt{p}.$

and $\quad p \mid |x_1 - x_2|$

$\therefore \quad p \leq |x_1 - x_2| \leq m.$

$\therefore \quad p \leq m$ amd $m \leq \sqrt{p}$ i.e. $m^2 \leq p.$

$\therefore \quad m^2 < p \leq m.$ $\qquad$ which is a contradiction.

If we let $\quad x_0 = x_1 - x_2$

$y_0 = y_1 - y_2$

Then we get, from (1)

$x_0 \equiv y_0a \pmod{p}.$

with $0 < |x_0| < \sqrt{p}, 0 < |y_0| < \sqrt{p}.$

Definition :

If the congruence $x^2 \equiv a \pmod{m}$ has a solution then a is said to be a **quadratic residue**(R) mod m. If there is no solution then a is said to be a **quadratic non residue (N) mod (m).**

Recall :

- 1 is q.r. mod p iff $p \equiv 1 \pmod{4}$
- 1 is q.n.r. mod p iff $p \equiv 3 \pmod{4}$.

Theorem :

The odd prime number p can be written as a sum of two squares iff $p \equiv 1 \pmod 4$ (i.e. p is of the form $4n + 1$).

Proof :

Let $p = a^2 + b^2$ (To prove $p \equiv 1 \pmod 4$).

$\because$ p is prime $p \neq 0$.

Again $p \nmid b$ for if $p \mid b$, $p \mid a$ also.

$\therefore$ $p \mid b \Rightarrow p^2 \mid b^2$

$p \mid a \Rightarrow p^2 \mid a^2$

$\therefore$ $p^2 \mid a^2 + b^2 = p$.

$\Rightarrow p^2 \mid p$, impossible.

$\therefore$ $p \nmid b$.

$\therefore$ $(p, b) = 1$.

$\therefore$ $\exists\, x_0, y_0 \in Z$ such that $px_0 + by_0 = 1$.

$\Rightarrow by_0 = 1 - px_0 \equiv 1 \pmod p$.

$\Rightarrow (by_0)^2 \equiv 1 \pmod p$.

Thus $y_0^2 p = y_0^2(a^2 + b^2)$

$= (y_0 a)^2 + (y_0 b)^2 \equiv (y_0 a)^2 + 1 \pmod p$.

$\Rightarrow (y_0 a)^2 + 1 \equiv 0 \pmod p$.

$\Rightarrow (y_0 a)^2 \equiv -1 \pmod p$.

$\therefore$ -1 is a q.r. $(\mathrm{mod}\ p)$.

$\therefore$ $p \equiv 1 \pmod 4$.

Conversely let $p \equiv 1 \pmod 4$

i.e. $p = 4n + 1$, $n \in \mathbf{N}$

To prove $p = a^2 + b^2$.

$\because$ $p \equiv 1 \pmod 4$, -1 is a q.r. $(\mathrm{mod}\ p)$.

$\therefore$ $\exists\, a \in z$ such that $a^2 \equiv -1 \pmod p$

$\Rightarrow a^2 + 1 \equiv 0 \pmod p$ .....(*)

Now obviously $(a, p) = 1$ ($\because$ $p \nmid 1$)

and by one preceding lemma, $\exists\, x_0, y_0 \in z$ such that

$$0 < |x_0| < \sqrt{p}\,,\ 0 < |y_0| < \sqrt{p}$$

where $x_0 \equiv ay_0 \pmod p$

Multiplying (*) by y_0^2.

$y_0^2(a^2+1) = y_0^2a^2 + y_0^2 \equiv 0 \pmod p$.

$\Rightarrow x_0^2 + y_0^2 \equiv 0 \pmod p$.

$\Rightarrow x_0^2 + y_0^2 = kp$ (some $k \in \mathbb{N}$).

$\therefore$ $0 < |x_0| < \sqrt{p}$ and $0 < |y_0| < \sqrt{p}$.

$\therefore$ $x_0^2 < p$ and $y_0^2 < p$.

$\therefore$ $kp = x_0^2 + y_0^2 < 2p$.

$\Rightarrow k < 2$ and $k \in z^+$

$\Rightarrow k = 1$.

$\therefore$ $x_0^2 + y_0^2 = p$.

Theorem :

Let N be a positive integer of the form m^2k (k is square free). Then N can be written as a sum of two squares iff k has no prime factor of the form $4n+3$.

Proof :

If k has no prime factor of the form $4n+3$, then it has prime factor of the form $4n=1$. So by the preceding result, k can be written as a sum of two squares (say) $k = a^2+b^2$.

$N = m^2k = m^2(a^2+b^2) = (ma)^2 + (mb)^2$.

Conversely suppose $m^2k = N = a^2+b^2$, to prove k doesnot contain a factor of the form $4n+3$.

Let $(a, b) = d$

Then $d \mid a$ and $d \mid b$.

$\Rightarrow d^2 \mid a^2$ and $d^2 \mid b^2$.

$\Rightarrow d^2 \mid a^2 + b^2 = m^2k$.

$\Rightarrow d^2 \mid m^2$ ($\because$ k is square free)

$\Rightarrow \frac{m^2}{d^2} = \lambda \in \mathbb{N}$ say.

$\Rightarrow \frac{m^2k}{d^2} = \frac{N}{d^2} = \lambda k$

$\because$ $d \mid a, d \mid b$.

$\Rightarrow a = da', b = db'$ $(a', b') = 1$.

and $\frac{N}{d^2} = \frac{a^2+b^2}{d^2} = \left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2 = a'^2 + b'^2$.

Also from $\frac{N}{d^2} = \lambda k$ we get, $k \mid \frac{N}{d^2} = a'^2 + b'^2$

$a'^2 + b'^2 \equiv 0 \pmod{k}$ .....(*).

Let p be an odd prime factor of k.

$\therefore$ $a'^2 + b'^2 \equiv 0 \pmod{p}$ .....(**)

$\because$ $(a', b') = 1$, one of a' and b' (say a') is relatively prime to p.

Let $(a', p) = 1$.

So $\exists\ c, c' \in Z$ such that

$ca' + c'p = 1$

$\Rightarrow ca' \equiv 1 \pmod{p}$

$\Rightarrow (ca')^2 \equiv 1 \pmod{p}$.

From (**)

$(ca')^2 + (cb')^2 \equiv 0 \pmod{p}$

$\Rightarrow (cb')^2 \equiv -1 \pmod{p}$

$\therefore$ $x^2 \equiv -1 \pmod{p}$ has a solution.

$\therefore$ -1 is a q.r.(mod p).

$\Rightarrow p \equiv 1 \pmod{4}$.

So, a factor of k is of the form $4n + 1$.

Four square problem

Lemma :

If a and b can be written as a sum of four squares so can the product.

Proof :

Suppose a and b can be written as a sum of four squares,

Let $a = x_1^2 + x_2^2 + x_3^2 + x_4^2$

$b = y_1^2 + y_2^2 + y_3^2 + y_4^2$

$$ab = (x_1^2 + x_2^2)(y_1^2 + y_2^2) + (x_1^2 + x_2^2)(y_3^2 + y_4^2) + (x_3^2 + x_4^2)(y_1^2 + y_2^2) + (x_3^2 + x_4^2)(y_3^2 + y_4^2)$$

$$= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_1)^2 + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2$$

Notation :

We call

$(a, b) \equiv (c, d) \pmod{m}$

if $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$.

Lemma :

A set of ordered pairs of integers, containing more than m^2 elements must have two elements that are congruent mod m.

Proof :

Each ordered pair of integers is congruent (mod m) to one of the following m^2 ordered pairs

(1, 2), (1, 2) ..... (1, m)

(2, 1), (2, 2) ..... (2, m)

.....

(m, 1), (m, 2) ..... (m, m)

If a set contains more then m^2 ordered pairs at least two them must be congruent mod m to one of the ordered pairs in the above list. Obviously these two ordered pairs are congruent mod m.

Lemma :

Let a, b, c, d be given integers and p be a prime. Then the system of congruences

$ax + by - z \equiv 0 \pmod p$

$cx + dy - u \equiv 0 \pmod p$.

has non trivial solution x_0, y_0, z_0, u_0 such that each number in the solution is less then $\sqrt{p}$ in absolute value (i.e. $|x_0| < \sqrt{p}, |y_0| < \sqrt{p}, |z_0| < \sqrt{p}, |u_0| < \sqrt{p}$).

Proof :

Define $\alpha = \alpha(x, y, z, u) = ax + by - z$

$\beta = \beta(x, y, z, u) = cx + dy - u$

where x, y, z, u are independent variables.

As x, y, z, u vary over the domain,

$$\{0, 1, 2, ..., m - 1, m = \left[\sqrt{p}\right]\}$$

we obtain $(m + 1)^4$ values of α and $(m + 1)^4$ values of β (not necessarily distinct).

Thus we have $(m + 1)^4$ values of ordered pairs (α, β) with (α, β) corresponding to the same value of x, y, z, u.

Since $\left[\sqrt{p}\right] = m$, $(m + 1)^4 > p^2$ and hence it follows from one previous lemma that atleast two ordered pairs (α_1, β_1) and (α_2, β_2) have corresponding component that are congruent modp^2 and therefore congruent mod p.

$\alpha_1 \equiv ax_1 + by_1 - z_1 \equiv \alpha_2 \equiv ax_2 + by_2 - z_2 (p)$

$$\beta_1 \equiv cx_1 + dy_1 - u_1 \equiv \beta_2 \equiv cx_2 + dy_2 - u_2 (p)$$

And this implies that

$$a(x_1 - x_2) + b(y_1 - y_2) - (z_1 - z_2) \equiv 0 \pmod p$$
$$c(x_1 - x_2) + d(y_1 - y_2) - (u_1 - u_2) \equiv 0 \pmod p$$

$\therefore$ (α_1, β_1) and (α_2, β_2) correspond to different values of x, y, z, u at least one of the numbers $x_1 - x_2, y_1 - y_2, z_1 - z_2$ and $u_1 - u_2$ is not zero.

If we recall range of values for x, y, z, u we see that $x_1 - x_2, y_1 - y_2, z_1 - z_2$ and $u_1 - u_2$ less than $\sqrt{p}$ in absolute values.

$$|x_1 - x_2|, |y_1 - y_2|, |z_1 - z_2|, |u_1 - u_2| \le m < \sqrt{p}.$$

If we now let $x_0 = x_1 - x_2, y_0 = y_1 - y_2, z_0 = z_1 - z_2, u_0 = u_1 - u_2$

We get, $ax_0 + by_0 - z_0 \equiv 0 \pmod p$

where $|x_0| < \sqrt{p}, |y_0| < \sqrt{p}, |z_0| < \sqrt{p}, |u_0| < \sqrt{p}$.

$$cx_0 + dy_0 - u_0 \equiv 0 \pmod p$$

Lemma :

If p is an odd prime, then there exists integers a, b, such that $a^2 + b^2 \equiv -1 \pmod p$.

Proof :

Consider the following two sets

$$A = \left\{ 0^2, 1^2, 2^2, \ldots\ldots, \left(\frac{p-1}{2}\right)^2 \right\}$$

$$B = \left\{ -0^2 - 1^1, -1^2 - 1^2, -2^2 - 1^2, \ldots, -\left(\frac{p-1}{2}\right)^2 - 1^2 \right\}$$

obiviously the elements of A are incongruent mod p.

Also the elements of B are incongruent mod p.

Since the union of A and B contains more then p-elements at least two numbers in the union are congruent mod one of these numbers, say a^2 must be in A and the other say $-b^2 - 1$ must be in B and they are congruent mod p

i.e. $a^2 \equiv -b^2 - 1 \pmod p$

$\Rightarrow a^2 + b^2 \equiv -1 \pmod p$ Hence Proved.

Theorem :

For any $p(>2)$ $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$ is solvable with x_1, x_2, x_3, x_4 which are not all divisible by p and $1 \le m < p$.

Proof :

Consider the sets of $\frac{1}{2}(p+1)$ numbers.

$$S_1 = \left\{0^2, 1^2, 2^2, \ldots\ldots, \left(\frac{p-1}{2}\right)^2\right\} \text{ and the set of } \frac{1}{2}(p+1) \text{ numbers.}$$

$$S_2 = \left\{-0^2 - 1, -1^2 - 1, -2^2 - 1, \ldots, -\left(\frac{p-1}{2}\right)^2 - 1\right\}$$

$\therefore \quad x^2 \equiv y^2 \pmod p \Rightarrow p \mid (x - y)(x + y).$

We see that no two numbers of S_1 are congruent madulo p and also no two numbers of S_2 are congruent modulo p i.e. they are incongruent to each other (mod p) in pairs. Now there are $(p + 1)$ numbers in the two sets together but since, there are only p distinct residue classes (mod p) we conclude that some number x^2 of S_1 is congruent modulo p to some number $- y^2 - 1$ of S_2.

Hence there are an x and a y each numerically less than $\frac{p}{2}$ such that

$$x^2 \equiv -y^2 - 1 \pmod p$$
$$\Rightarrow x^2 + y^2 + 1 \equiv 0 \pmod o$$
$$\Rightarrow x^2 + y^2 + 1^2 + 0^2 = mp$$

$$\left(0 \le x \le \frac{p-1}{2}, 0 \le y \le \frac{p-1}{2}\right)$$

Now the condition

$$1 \le m \Rightarrow 1 \le \frac{1}{p}\left(x^2 + y^2 + 1\right)$$

$$\le \frac{1}{p}\left[2\left(\frac{p-1}{2}\right)^2 + 1\right]$$

as $x \le \frac{p-1}{2}, y \le \frac{p-1}{2}$

$$\le \frac{1}{p}\left[\frac{1}{2}p^2 - p + \frac{3}{2}\right]$$

$$< \frac{1}{p}\left[\frac{1}{2}p^2 + 1\right]$$

$$< \frac{1}{p}p^2 \qquad (\because \quad p > 2)$$

$$< p.$$

Thus with the condition $1 \le m < p$ we have obtained integers to satisfy $x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp$.

Theorem :

For every prime p, $p = x_1^2 + x_2^2 + x_3^2 + x_4^2$ is solvable.

Proof :

For $p = 2$, this is obvious as $2 = 1^2 + 1^2 + 0^2 + 0^2$.

Therefore let $p > 2$. But by the preceding theorem we know that there is multiple of p such that $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$ is solvable with x_1, x_2, x_3, x_4 not all divisible by p.

Now we shall prove that the least such multiple of p is p itself.

Let Mp be the least such multiple of p.

Case (a) : M be even.

Then $Mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$ is also even.

Here either (i) x_1, x_2, x_3, x_4 are all even.

(ii) all odd.

(iii) two are even and two are odd.

If exactly two of the x's are even, we can take them in such a way that x_1, x_2 are even and x_3, x_4 are odd.

Then $x_1 + x_2, x_1 - x_2, x_3 + x_4, x_3 - x_4$ are all even and so

$$\left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 = \frac{1}{2}Mp$$

when the four terms on the LHS are integers.

These squares are not all divisible by p, since x_1, x_2, x_3, x_4 are not all divisible by p.

This result contradict our assumption that M is the least. Hence M must be odd.

Case (b) : M is odd.

Since M is odd, we must have $3 \le M < p$.

For $1 \le i \le 4$, let us now choose numbers b_1, b_2, b_3, b_4 such that $y_1 = x_1 - b_1M$, $y_2 = x_2 - b_2M$, $y_3 = x_3 - b_3M$, $y_4 = x_4 - b_4M$.

which gives $y_i \equiv x_i \pmod{M}$.

with condition $-\frac{M-1}{2} \le y_i \le \frac{M-1}{2}$.

$$\therefore \quad y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \pmod{M}$$
$$\equiv 0 \pmod{M} \qquad [x_1^2 + x_2^2 + x_3^2 + x_4^2 = Mp]$$

and therefore we can write

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = Mn \qquad \text{.....(A)}$$

with condition,

$$0 \le Mn = y_1^2 + y_2^2 + y_3^2 + y_4^2$$
$$\le 4\left(\frac{M-1}{2}\right)^2 < M^2$$

i.e. $0 \le Mn < M^2$

$\Rightarrow 0 \le n < M$.

For $n = 0$, we have $y_1 = y_2 = y_3 = y_4 = 0$ (from (A))

and $x_1 \equiv x_2 \equiv x_3 \equiv x_4 \equiv 0 \ (M)$ ($\because$ $y_i \equiv x_i \pmod{M}$)

$\therefore$ $Mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \ (M^2)$

i.e. $p \equiv 0 \ (M)$ which is not possible since $3 \le M < p$.

Therefore $n > 0$ and $0 < n < M$.

Now $M^2 np = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)$

$= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2$

$+ (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2$

$= z_1^2 + z_2^2 + z_3^2 + z_4^2$ (say) .....(B)

Now $z_1 = \Sigma x_i y_i \equiv \Sigma x_i^2 \equiv 0 \pmod{M}$

[$\because$ $y_i \equiv x_i \pmod{M}$]

Similarly $z_2 \equiv z_3 \equiv z_4 \equiv 0 \pmod{M}$.

Also $x_iy_j - x_jy_i \equiv x_ix_j - x_jx_i \equiv 0 \pmod{M}$.

$\therefore$ we can take

$z_1 = Mt_1, z_2 = Mt_2, z_3 = Mt_3, z_4 = Mt_4$.

$M^2np = M^2t_1^2 + M^2t_2^2 + M^2t_3^2 + M^2t_4^2$

$\Rightarrow np = t_1^2 + t_2^2 + t_3^2 + t_4^2$ with $0 < n < M$.

This shows that M is not least if $M > 1$.

Hence $M = 1$ and the theorem is established.

Lagranges theorem :

Every positive integer is a sum of four squares (i.e. the diophantine equation

$n = x_1^2 + x_2^2 + x_3^2 + x_4^2$ is solvable for every $n \geq 0$).

Proof :

By Euler's identity it follows that the statement is true for n_1n_2 whenever it is true for n_1 and n_2.

By the last theorem it is true when n is prime.

Now let $n = p_1p_2 \ldots\ldots p_t$ not all distinct primes.

So by the preceding remark, the theorem is established.

Summary

- A function whose domain is the set of positive integers is called a number theoretic function.
- $\tau(n)$ is the number of positive divisors of n including 1 and n.
- $\sigma(n)$ is the sum of positive divisors of n.
- A number theoretic function 'f' is said to be multiplicative if $f(mn) = f(m)\,f(n)$, whenever gcd $(m,n) = 1$.
- τ and σ both are multiplicative functions.
- The Mobius function $\mu(n)$ is multiplicative.
- If F(n) is multiplicative function, and $F(n) = \sum_{d|n} f(d)$, then f is also multiplicative.
- Euler's function $\varphi(n)$ is defined as the number of positive integers relatively prime to 'n' not exceeding 'n'.
- $\varphi(n) = n - 1$ if and only if n is prime.
- φ is a multiplicative function.
- For any integer n, $\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$.
- If (a, b, c) is a solution of $x^2 + y^2 = z^2$ such that gcd (a, b, c) = 1, then (a, b, c) is called

primitive solution.

- If (x, y, z) is a primitive solution of $x^2 + y^2 = z^2$, x is even, then $y = 2st$, $x = s^2 - t^2$, $z = s^2 + t^2$, where s and t are positive integers satisfying the following conditions.

  (i) $(s, t) = 1$

  (ii) $x > t$.

  (iii) one of s and t is even and the other is odd.

- The diophantine equation $x^4 + y^4 = z^2$ has no positive solution.
- The odd prime number 'p' can be written as a sum of two squares iff $p \equiv 1 \pmod 4$ (i.e. p is of the form $4n + 1$).
- Let N be a positive integer of the form m^2k (k is square free). Then N can be written as a sum of two squares iff k has no prime factor of the form $4n + 3$.
- For any $p(> 2)$, $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$ is solvable with x_1, x_2, x_3, x_4 which are not all divisible by p and $1 \leq m < p$.
- For every prime p, $p = x_1^2 + x_2^2 + x_3^2 + x_4^2$ is solvable.
- Lagranges Theorem states that "Every positive integer is a sum of four squares."

On arithmetic Function

Q(1992) : State true or false :

For a positive integer k, there are at most $\phi(k)$ primes among the integers $k + 1, k + 2, ..., 2k$.

Ans : Suppose there are $\phi(k) + 1$ primes among the integers $k + 1, k + 2, ..., 2k$. But each of $k + 1, k + 2, ..., 2k$ is congruent to some of $1, 2, ...k$ modulo k. And thus there are $\phi(k) + 1$ numbers are relatively prime to k among $1, 2, ..., k$, which is not possible.

Therefore for a positive integer k, there are at most $\phi(k)$ primes among the integers $k + 1, k + 2, ..., 2k$.

Q(1992) : What can you consider about the multiplicationess of $\frac{\phi(n)}{n}$?

Ans : Let $F(n) = \frac{\phi(n)}{n}$

and $(m, n) = 1$

Now $F(mn) = \frac{\phi(mn)}{mn}$

$$= \frac{\phi(m)\phi(n)}{mn}$$

$$= \frac{\phi(m)}{m}\,\frac{\phi(n)}{n}$$

$$= F(m)F(n)$$

Therefore $F(n) = \frac{\phi(n)}{n}$ is a multiplicative function.

Q(1992) : Evaluate $\sum_{n=1}^{\infty}\mu\left(\frac{|}{}n\right)$

Ans: $\sum_{n=1}^{\infty}\mu\left(\frac{|}{}n\right)$

$$= \mu\left(\frac{|}{}1\right)+\mu\left(\frac{|}{}2\right)+\mu\left(\frac{|}{}3\right)+\mu\left(\frac{|}{}4\right)+\ldots\ldots$$

$$= \mu(1) + \mu(1.2) + \mu(2.3) + \mu(2.3.4) + \ldots\ldots$$

$$= \mu(1) + \mu(2) + \mu(2.3) + \mu(2^2.6) + \ldots\ldots$$

$$= 1 + (-1)^1 + (-2)^2 + 0 \qquad \because \quad \mu(n) = 0, \text{ if } p^2 \mid n$$

$$= 1 - 1 + 1$$

$$= 1.$$

Q (1993) : State true of false :

For $n \geq 2$, $\phi(n)$ is always even.

Ans : False when $n = 2$, $\phi(n) = \phi(2) = 1$, which is not even.

Q (1994) : Give example of a positive integer n such that $\phi(n) = 32$.

Ans : When $n = 64 = 2^6$, $\phi(2^6) = 2^6\left(1-\frac{1}{2}\right) = 2^5 = 32$.

$\therefore \quad \phi(64) = 32.$

Q : If k denotes the number of distinct prime factors of a positive integer n, then show that $\sum_{d|n}|\mu(d)| = 2^k$.

Here μ denotes the Mobius fuction.

Ans : Given k is the no of distinct prime factors of a positive integer n,

$\therefore \quad n = p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}$.

Now $\sum_{d|n}|\mu(d)| = \prod_{i=1}^{k}\left\{|\mu(1)|+|\mu(p_i)|+|\mu(p_i^2)|+\ldots+|\mu(p_i^{k_i})|\right\}$

$$= \prod_{i=1}^{k}\left(|\mu(1)|+|\mu(p_i)|\right)$$

$$= \prod_{i=1}^{k}(1+1)$$

$$= 2^k.$$

Q : Find $\tau(180)$ and $\sigma(180)$.

Ans : we have

$$180 = 2^2 . 3^2 . 5$$

we know if $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, p_i are distinct primes and $k_i \geq 1$ then

$$\tau(n) = (k_1 + 1)(k_2 + 1) \ldots (k_r + 1)$$

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}$$

Now $\tau(180) = (2 + 1)(2 + 1)(1 + 1)$

$$= 18$$

$$\sigma(180) = \frac{2^3 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^3 - 1}{5 - 1}$$

$$= 7 . 13 . 6$$

$$= 596.$$

Q(1996) : Varify that

$$\tau(n) = \tau(n + 1) \text{ and } \tau(n) \leq 2\sqrt{n} \text{ for } n = 3655.$$

Ans: $n = 3655 = 5 \times 17 \times 43$

$\tau(n) = (1 + 1)(1 + 1)(1 + 1)$

$= 8.$

$n + 1 = 3656 = 2^3 . (457)$

$\therefore$ $\tau(n + 1) = (3 + 1)(1 + 1)$

$= 8.$

$\therefore$ $\tau(n) = \tau(n + 1)$ when $n = 3655$.

Again $2\sqrt{n} = 2\sqrt{3655}$

$= 2 \times 60.45$

$= 120.91$

$\therefore \quad \tau(n) < 2\sqrt{n}$ for $n = 3655$.

Q(1996) : Find $\mu(30)$ and $\mu(72)$.

Ans: $30 = 2 \cdot 3 \cdot 5$

$\mu(30) = (-1)^3 = -1$

$72 = 2^3 \cdot 3^2$

$\therefore \quad \mu(72) = 0$ as $3^2 \mid 72$.

Q (1997) : Find $\tau(59319)$ and $\sigma(59319)$.

Ans: $59319 = 3^3 \cdot 13^3$

$\therefore \quad \tau(59319) = (3+1)(3+1)$

$= 16.$

$$\sigma(59319) = \frac{3^4 - 1}{3-1} \cdot \frac{13^4 - 1}{13-1}$$

$= 40 \times 2380$

$= 95200.$

Q (1997) : Find the number of positive integers less then 3600 and relatively prime to 3600.

Ans : We have to find $\phi(3600)$.

$3600 = 2^4 \cdot 3^2 \cdot 5^2$

$$\phi(3600) = 3600\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$= 960.$

Q(1997) : Let n be an integer > 1. Then the following held.

(i) $\tau(n)$ is odd $\Leftrightarrow$ n is a perfect square.

(ii) $\sigma(n)$ is odd $\Leftrightarrow$ n is a perfect square or twice a perfect square.

(ii) $\prod_{d \mid n} d = n^{\frac{\tau(n)}{2}}$.

Proof :

Let $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, p_i being distinct primes and integers $k_i \geq 1$.

(1) we know that,

$$\tau(n) = (k_1 + 1)(k_2 + 1) \dots (k_r + 1)$$

$\tau(n)$ is odd $\Leftrightarrow (k_1 + 1)(k_2 + 1) \dots (k_r + 1)$ is odd

$\Leftrightarrow k_i + 1$ is odd $\forall\ i = 1, 2, \dots, r.$

$\Leftrightarrow k_i$ is even $\forall\ i = 1, 2, \dots, r.$

Suppose $k_i = 2m_i\ i = 1, 2, \dots, r.$ Then

$$n = p_1^{2m_1} p_2^{2m_2} \dots p_r^{2m_r}$$

$$= \left(p_1^{m_1}\right)^2 \left(p_2^{m_2}\right)^2 \dots \left(p_r^{m_r}\right)^2 \text{ which is a perfect square.}$$

(ii) Also

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \dots \frac{p_r^{k_r+1} - 1}{p_r - 1}$$

$$= \left(1 + p_1 + \dots + P_1^{k_1}\right)\left(1 + p_2 + \dots + P_2^{k_2}\right) \dots \left(1 + p_r + \dots + P_r^{k_r}\right)$$

$\therefore$ $\sigma(n)$ is odd $\Leftrightarrow \left(1 + p_1 + \dots + P_1^{k_1}\right)\left(1 + p_2 + \dots + P_2^{k_2}\right) \dots \left(1 + p_r + \dots + P_r^{k_r}\right)$ is odd

$\Leftrightarrow 1 + p_1 + \dots + P_1^{k_1}$ is odd $\forall\ i = 1, 2, \dots, r$

$\Leftrightarrow k_i$ is even $\forall$ i, if all p_i are odd and if one p_i say $p_1 = 2$ then k_i is even $\forall\ i = 2, 3, \dots, r$

$\Leftrightarrow k_i = 2m_i$ for some integer $m_i\ \forall\ i = 1, 2, \dots, r$

$k_i = 2m_i^1$ for some integer $m_i^1\ \forall\ i = 2, 3, \dots, r$ and k_i is any integer ≥ 1.

$$\Leftrightarrow n = \left(p_1^{m_1} \dots p_r^{m_r}\right)^2$$

$$2 = 2^{k_1}\left(p_2^{m_2'} \dots p_r^{m_r'}\right)^2$$

Now if k_1 is even, then

$$n = \left(2^{\frac{k_1}{2}} p_2^{m_2'} \dots p_r^{m_r'}\right)^2 ; \text{ and}$$

if k_1 is odd say $_1 = 2m_1^1 + 1$, then

$$n = 2\left(2^{m_1'} p_2^{m_2'} \dots p_r^{m_r'}\right)^2.$$

Hence $\sigma(n)$ is odd $\Leftrightarrow$ n is a perfect square or twice a perfect sqare.

(iii) we know if d is an integer such that $d \mid n$, then $\exists$ an integer d' such that $n = dd'$.

$$\Rightarrow d' \mid n \text{ and } d' = \frac{n}{d}.$$

Thus divisors d of n are in pairs $\left(d, \frac{n}{d}\right)$.

$$\Rightarrow \text{Product of all divisors of } n = \left(\prod_{d|n} d\right)^2 = n^{\tau(n)}.$$

or $\prod_{d|n} d = n^{\tau(n)}$ where $\tau(n)$ is the number of divisors of n.

Now if $\tau(n)$ is even, $\frac{\tau(n)}{2}$ is an integer so that $n^{\frac{\tau(n)}{2}}$ is an integer and if $\tau(n)$ is odd, n is a perfect square, so that,

$$n^{\frac{\tau(n)}{2}} = \left(n^{\frac{1}{2}}\right)^{\tau(n)} \text{ is again an integer. Thus}$$

$$\prod_{d|n} d = n^{\frac{\tau(n)}{2}}.$$

Exercise

Prove that

Q.1.(93) For integers a, b and c if $\gcd(a^2, b^2) = c^2$, then $\gcd(a, b) = c$.

Q. 2.(94) If a prime integer $p > 3$ then prove that $2p + 1$ and $4p + 1$ cannot be prime simultaneously.

Q.3.(93) State the Chinese Remainder Theorem. Use it to prove that for any positive integer k, we can find k consecutive positive integers each of which is not divisible by a square.

Q.4.(99) if p is a prime and $a \equiv b \pmod{p^n}$ then prove that for all integral values of n and s,

$$a^{p^s} \equiv b^{p^s} \pmod{p^{n+s}}.$$

Q.5.(93) If k denotes the numbers of distinct prime factors of a positive integer n, then show that

$$\sum_{d|n} \mu(d)\tau(d) = (-1)^k.$$

Q.6.(94) Given an odd prime p and an integer a such that $p \nmid a$ then $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$.

Q.7.(95) For any integer $n \geq 1$, prove that

$$\tau(n) \leq 2\sqrt{n}.$$

Q.8.(95) Prove that for a an even integer n,

$$\sum_{d|n} \mu(d)\phi(d) = 0$$

Q.9.(96) If S integers $r_1, r_2, ..., r_s$ form a reduced residue system modulo m, then prove that $S = \phi(m)$.

On Congruence

Theorem :

If $n_1, n_2, ..., n_m$ is a complete set of residues (mod m) and if (a, m) = 1, and b is any integer then $ax_1 + b, ax_2 + b, ..., ax_m + b$ is a complete set of residues (mod m).

Proof :

We have $ax_i + b \equiv ax_j + b \pmod{m}$

$\Rightarrow ax_i \equiv ax_j \pmod{m}$

$\Rightarrow x_i \equiv x_j \pmod{m}$ $\quad (\because \quad (a, m) = 1)$

$\Rightarrow i = j$ since $\{x_1, x_2, ..., x_m\}$ are mutually incongruent

Hence $ax_i = b$, i = 1, 2, ..., m are m mutually in congruent integers (mod m) and so the result follows.

Theorem :

If (m, n) = 1 and if $x_1, x_2, ..., x_n$ is a complete set of residues (mod m) and $y_1, y_2, ..., y_n$ is a complete set of residues (mod n) then the mn integers $(nx_i + my_j)$ where i = 1, 2, ..., m, j = 1, 2, ..., n form a complete set of residues (mod mn).

Proof :

We have,

$nx_i + my_j \equiv nx_k + my_l \pmod{mn}$

$\Rightarrow nx_i + my_j \equiv nx_k + my_l \pmod{m}$

$nx_i + my_j \equiv nx_k + my_l \pmod{n}$

$\Rightarrow nx_i \equiv nx_k \pmod{m} my_j \equiv my_l \pmod{n}$

$\Rightarrow x_i \equiv n_k \pmod{m}$ $y_j \equiv y_l \pmod{m}$ since (m, n) = 1.

$\Rightarrow i = k, j = l$

Hence $\{nx_i + my_j\}$ i, j is mutually incongruent. Since there are mn elements in the set, the result follows:

Definition :

A **reduced residue system** or a **reduced set of residues** modolu m is a set of integers $r_1, r_2, ..., r_{\phi(m)}$, such that every integer which is relatively prime to m is congruent to exactly one of the integers r_i. In otherwords, á reduced set of residues modulo m is the subset of a complete set of residues consisting of the integers which are relatively prime to m. $\phi(m)$ stands for number of integers relatively prime to m.

Ex. 1. : If p is a prime then $\{1, 2, 3, ..., p - 1\}$ forms a reduced set of residues modolu p.

Ex. 2. : $\{1, 2\}$, $\{1, 5\}$ and $\{1, 3, 7, 9\}$ are reduced set of residues modulo respectively 3, 6 and 10.

Note : If $x_1, x_2, ..., x_{\phi(m)}$ are $\phi(m)$ integers each is relatively prine to m then they form a reduced set of residues (mod m).

Theorem :

If $x_1, x_2, ..., x_{\phi(m)}$ is a reduced set of residues (mod m) and if a is an integer such that (a, m) = 1, then $ax_1, ax_2, ..., ax_{\phi(m)}$ is á reduced set of residues (mod m).

Proof :

For each i, we have $(x_i, m) = 1$.

Since (a, m) = 1, we have $(ax_i, m) = 1$. Also

$$ax_i \equiv ax_j \pmod m$$

$$\Rightarrow x_i \equiv x_j \pmod m \qquad (\because \quad (a, m) = 1)$$

$$\Rightarrow i = j.$$

Thus $ax_1, ax_2, ..., ax_{\phi(m)}$ are $\phi(m)$ integers, each one of which is relatively prime to m and no two of which are congruent modulo m.

Hence they form a reduced set of residus (mod m).

Problem :

What is the last two digits in the ordinary decimal representation of 3^{400}?

Solution :

We have, (3, 5) = 1. Thus

$$3^4 \equiv 1 \pmod 5$$

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

$$\Rightarrow 3^4 \equiv 1 \pmod{10} \qquad \because \quad (5, 2) = 1$$

$$\Rightarrow 3^{4x} \equiv 1 \pmod{10}$$

which shows that the last digit of 3^{900} is 1.

Problem :

If p is any prime other then 2 or 5, prove that p divides infinitly many of the integers 9, 99, 999, 9999, ... Also p divides infinitly many of the integers 1, 11, 111, ...

Solution :

We have the set,

$$S = \{9, 99, 999, ...\} = \{10^n - 1, : n = 1, 2, 3, ...\}.$$

Now let p be any prime other then 2 and 5.

Then $p \nmid 10$ i.e. $(p, 10) = 1$.

Thus $10^{p-1} \equiv 1 \pmod p$

$\Rightarrow 10^{m(p-1)} \equiv 1 \pmod p$

$\Rightarrow p \mid 10^{m(p-1)} - 1$ for $m = 1, 2, ...$

Thus p divides $10^{m(p-1)} - 1$, $m = 1, 2, ...$

which is an infinity elements in S.

Again $S_1 = \{1,11,111,...\} = \left\{\frac{x}{9}, x \in S\right\}$.

If $p = 3$, then p divides all numbers of S_1, whose sums of the digits are divisible by 3. As there are infinitly many integers of this kind in S_1, (i.e. 111, 111111, and so on) p divides infinitely many members of S_1. If $p \neq 3$ then $(p, q) = 1$. Thus whenever $p \mid x$, $x \in S$, we get $p \left| \frac{x}{9} \right.$. Hence p divides infinitely many integers in S_1.

Problem :

State true or false :

For any two relatively prime integers a and n, $a^{n-1} \equiv 1 \pmod n$?

Ans :

False $(5, 6) = 1$, but $5^5 \equiv 5 \pmod 6$.

Solution of Congruence

The number of solutions of $f(x) \equiv 0 \pmod m$ is the number of integers in a complete set of residues which are solutions of $f(x) \equiv 0 \pmod m$.

Example :

$x^2 + 1 \equiv 0 \pmod 7$ has no solutions.

$x^2 + 1 \equiv 0 \pmod 5$ has two solutions.

$x^2 - 1 \equiv 0 \pmod 8$ has four solutions.

Theorem :

Let $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$. If $a_0 \not\equiv 0$.

The degree of the congruence $f(x) \equiv 0 \pmod m$ is n. If $a_0 \equiv 0 \pmod m$, then the degree of the congruence is x - j, where j is the least positive integer such that $a_j \not\equiv 0 \pmod m$.

Theorem :

The system of congruences

$$x \equiv a \pmod m$$

$$x \equiv b \pmod n \qquad \ldots\ldots(1)$$

has a solution if and only if $(m, n) \mid b - a$.

If this is the case and if x_0 is a solution then the general solution is

$$x \equiv x_0 \pmod{[m, n]}.$$

Proof :

Let $d = (m, n)$ and suppose $m = dm_1$, $n = dn_1$.

Let (1) have a solution x_0. Then $m \mid a - x_0$ and $n \mid b - x_0$. Thus $d \mid a - x_0$, $d \mid b - x_0$ and therefore $d \mid a - b$.

Now let $d \mid a - b$. We have $x = a + tm$, where t is any integer is a solution of $x \equiv a \pmod m$. For a common solution we must find t such that

$$a + tm \equiv b \pmod n$$

i.e. $mt \equiv b - a \pmod n$ .....(2).

Since $d = (m, n) \mid b - a$, (2) has a solution. Hence the system (1) has a common solution.

Let $M = [m, n]$ and x_0 be any common solution of (1).

Then $x \equiv x_0 \pmod m$

$x \equiv x_0 \pmod n$

which gives $dm_1 = m \mid x - x_0$, $dn_1 = n \mid x - x_0$ and therefore

$$[m, n] = dm_1n_1 \mid x - x_0.$$

i.e. $x \equiv x_0 \pmod M$

Also if $x \equiv x_0 \pmod M$

Then $x \equiv x_0 \equiv a \pmod m$

$x \equiv x_0 \equiv b \pmod n$

Hence $x \equiv x_0 \pmod M$ is the general common solution of (1).

Congruence of Highere Degree

The following theorem, known as Lagrange's theorem, gives an upper bound to the number of distinct roots of an algebric congruence of prime modulus.

Theorem :

If p is a prime and if $a_n \equiv 0 \pmod p$ then the algebraic congruence

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \equiv 0 \pmod p \qquad \ldots\ldots(1)$$

has not more than n roots incongruent (mod p).

Proof :

We use induction on n. The result is true for algebric congruence of degree 1. Since the linear congruence $a_1 x + a_0 \equiv 0 \pmod p$ has exactly one solution if $a_1 \not\equiv 0 \pmod p$. Now assume that the result holds for all congruences of degree n - 1, and consider the congruence (1) of degree n.

Suppose that the algebraic congruence (1) has atleast n + 1 incongruent roots, namely $b_1, b_2, \ldots, b_{n+1}$. Then $f(b_1) \equiv 0 \pmod p$ and consequently,

$$f(x) \equiv f(x) - f(b_1) \pmod p$$

$$= \sum_{x=0}^{n} a_r \left(x^r - b_1^r \right)$$

$$= (x - b_1) f_1(x)$$

where, $f_1(x) = a_n x^{n-1} + (a_n b_1 + a_{n-1}) x^{n-2} + \ldots + (a_n b_1^{n-1} + \ldots + a_1)$.

Thus $f(x) \equiv (x - b_1) f_1(x) \pmod p$.

Since $f(b_i) \equiv 0 \pmod p$ $i = 2, 3, \ldots, n + 1$

It follows that,

$$(b_i - b_1) f_1(b_i) \equiv 0 \pmod p \qquad (i = 2, 3, \ldots, n + 1)$$

But $b_i \not\equiv b_1 \pmod p$ which gives,

$$f_1(b_i) \equiv 0 \pmod p \qquad (i = 2, 3, \ldots, n + 1)$$

This shows that $f_1(x) \equiv 0 \pmod p$ is a congruence of degree n - 1 having n incongruent roots. This contradicts the induction hypothesis. Hence the congruence (1) cannot have more then n incongruent roots. The theorem thus follows by induction.

Note : The result is not true for an algebric congruence with a composite modulus. For example, $x^2 - x \equiv 0 \pmod 6$ is a **quadratic** congruence with four roots $x = 0, 1, 3, 4 \pmod 6$.

Theorem :

If the algebric congruence

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \equiv 0 \pmod{p}$$

of degree n has r incongruent roots $b_1, b_2, \ldots, b_r$ then

$$f(x) \equiv (x - b_1)(x - b_2) \ldots (x - b_r) f_r(x) \pmod{p}$$

where $f_r(x)$ is a polynomial of degree n - r with integral co-efficient and highest co-efficient a_n.

Proof :

As in the previous theorem we show that

$f(x) = (x - b_1) f_1(x) \pmod{p}$ where,

$f_1(x) =$ is a polynimial of degree n - 1 and $f_1(b_i) = 0 \pmod{p}$ for $i \geq 2$. By the same argument we see that,

$f_1(x) \equiv (x - b_2) f_2(x) \pmod{p}$, where $f_2(x)$ is a polynomial of degree n - 2 with integral co-efficient and highest co-efficient a_n, and $f_2(b_i) \equiv 0 \pmod{p}$ for $i \geq 3$.

The result follows in r steps.

The linear polynomial $(x - b_i)(i = 1, 2, \ldots, r)$ are called the linear factors (mod p) of f(x). From the theorem we see that,

An integral polynomial f(x) has a factor (x - b) (mod p) iff $f(b) \equiv 0 \pmod{p}$.

Problem :

Factorize the polynomial $x^3 + 3x + 1 \pmod{5}$.

Solution :

If the complete set of residues $0, \pm 1, \pm 2 \pmod{5}$, we have 1 and 2 as the roots of the congruence $x^3 + 3x + 1 \equiv 0 \pmod{5}$.

Thus x - 1 and x - 2 are factors of $x^3 + 3x + 1 \pmod{5}$.

We have $x^3 + 3x + 1 = (x - 1)(x^2 + x + 4) + 5$

$x^2 + x + 4 = (x - 2)(x + 3) + 10$

Thus $x^3 + 3x + 1 \equiv (x - 1)(x^2 + x + 4) \pmod{5}$

$\equiv (x - 1)(x - 2)(x + 3) \pmod{5}$

$\equiv (x - 1)(x - 2)(x - 2) \pmod{5}$

$\equiv (x - 1)(x - 2)^2 \pmod{5}$

Problem :

Show that the polynomial $x^3 + 2x + 1$ is irreducible (mod 3).

Solution :

If the complete set of residues $0, \pm 1$, none is a root of the congruence

$x^3 + 2x + 1 \equiv 0 \pmod 3$.

Hence $x^3 + 2x + 1$ has no linear factor (mod 3). But in any factorization of $x^3 + 2x + 1$ (mod 3) there must be at least one linear factor.

Hence we conclude that $n^3 + 2x + 1$ has no factorization (mod 3).

Theorem :

If the positive integer $m > 1$ has the prime decomposition $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$ and if $f(x)$ is any polynomial in x with integral co-efficient, then

(i) the algebriac congruence $f(x) \equiv 0 \pmod m$ .....(1)

is soluble if and only if each of the algabraic congruence $f(x) \equiv 0 \left(\text{mod } p_i^{\alpha_i} \right)$

$i = 1, 2, \ldots, r$ .....(2)

is soluble and

(ii) If N(n) represent the number of solutions of the congruence $f(x) \equiv 0 \pmod n$,

then $N(m) = N\left(p_1^{\alpha_1}\right) N\left(p_2^{\alpha_2}\right) \ldots\ldots N\left(p_r^{\alpha_r}\right)$.

Proof :

(i) If $f(b) \equiv 0 \pmod m$ then clearly

$f(b) \equiv 0 \left(\text{mod } p_i^{\alpha_i} \right)$ $(i = 1, 2, \ldots, r)$

Hence if the congruence (1) is soluble then each of the congruences (2) is soluble. Suppose now that each of the congruences (2) is soluble. Let $b_i (i = 1, 2, \ldots, r)$ be integers such that

$f(b_i) \equiv 0 \left(\text{mod } p_i^{\alpha_i} \right)$ $(i = 1, 2, \ldots, r)$.

Then by the Chinese Remainder theorem, we can find an integer a such that

$a \equiv b_i \left(\text{mod } p_i^{\alpha_i} \right)$ $(i = 1, 2, \ldots, r)$.

Then $f(a) \equiv f(b_i) \equiv 0 \left(\text{mod } p_i^{\alpha_i} \right)$ $(i = 1, 2, \ldots, r)$

which implies $f(a) \equiv 0 \left(\text{mod } m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r} \right)$.

This shows that the congruence (1) has a solution.

(ii) By Chinese Remaider Theorem, the integer a obtained in the proof part (1) is unique (mod

m). It follows that a different root of the congruence (1) must arise from a different set $b_1, b_2, ..., b_r$ of roots of the congruence (2). Henec all the roots of (1) will be obtained by allowing $b_1 \ldots b_r$ ro take all possible values. Since for each i, b_i can take $N\left(p_i^{\alpha_i}\right)$ distinct values, the result follows.

Theorem :

If b is a root of the algebraic congruence

$$f(x) \equiv 0 \pmod{p^{\alpha-1}} \quad (\alpha \geq 2)$$

Satisfying $0 \leq b \leq p^{\alpha-1} - 1$, and if $f'(x)$ is the formal derivative of $f(x)$, then

(i) If $f'(b) \not\equiv 0 \pmod{p}$, there is a unique root of $f(x) \equiv 0 \pmod{p^\alpha}$ corresponding to b;

(ii) If $f'(b) \equiv 0 \pmod{p}$, there are p roots of $f(x) \equiv 0 \pmod{p^\alpha}$ corresponding to b when $f(b) \equiv 0 \pmod{p^\alpha}$ and no such root when $f(b) \not\equiv 0 \pmod{p^\alpha}$.

Proof :

If $a = p^{\alpha-1}t + b$, then

$$f(a) = f\left(b + p^{\alpha-1}t\right) = f(b) + p^{\alpha-1}t\,f'(b) + \left(p^{\alpha-1}t\right)^2 \frac{f''(b)}{\lfloor 2} + \ldots\ldots + \left(p^{\alpha-1}t\right)^n \frac{f^n(b)}{\lfloor n}$$

where n is the degree of the polynomial f. Now for some integer k, we have

$$f(b) = kp^{\alpha-1}.$$

Thus $f(a) = \{tf'(b) + k\}p^{\alpha-1} + Np^{2\alpha-2}$

where N is an integer. Since $2\alpha - 2 = \alpha + (\alpha - 2) \geq \alpha$. We decide that

$$f(a) = (tf'(b) + k)p^{\alpha-1} \pmod{p^\alpha}$$

Consequently $f(a) \equiv 0 \pmod{p^\alpha}$ iff

$$tf'(b) + k \equiv 0 \pmod{p} \qquad \ldots\ldots(1)$$

(i) If $f'(b) \not\equiv 0 \pmod{p}$, then the linear congruence

(i) in t has a unique solution say t_0. Thus t_0 is the unique integer such that $a = t_0p^{\alpha-1} + b$ is a solution of $f(x) \equiv 0 \pmod{p^\alpha}$. Hence the result follows.

(ii) Now let $f'(b) \equiv 0 \pmod{p}$. Then (i) is satisfied if and only if $k \equiv 0 \pmod{p}$. but

$$k \equiv 0 \pmod{p} \Leftrightarrow f(b) \equiv 0 \pmod{p}.$$

Thus if b is not a root of $f(x) \equiv 0 \pmod{p^\alpha}$, then for no t, $a = p^{\alpha-1}t + b$ is a root of $f(x) \equiv 0 \pmod{p^\alpha}$. If b is a root of $f(x) \equiv 0 \pmod{p^\alpha}$. Then $k \equiv 0 \pmod{p}$ and so for each value of t, (i) is satisfied. Thus putting $t = 0, 1, 2, ..., p - 1$, we get p incongruent roots $a = p^{\alpha-1}t + b$ of the congruence $f(x) \equiv 0 \pmod{p^\alpha}$ corresponding to the root b of $f(x) \equiv 0 \pmod{p^{\alpha-1}}$. This proves (ii).

Exercise : Solve $x^3 + 2x + 2 \equiv 0 \pmod{5^2}$ .....(1)

Solution :

First we consider the congurence,

$$x^3 + 2x + 2 \equiv 0 \pmod{5^2} \quad \text{.....(2)}$$

By inspection we find the solutions of (2) to be $x \equiv 1, 3 \pmod 5$. We have $f'(x) \not\equiv 3x^2 + 2$. Roots of (1) corresponding to root $x = 1$ of (2) we have, $f(1) = 5 = 5 \cdot 1$ i.e. $k = 1$ [$(f(1) \neq 0 \pmod 5)$]

$f'(1) = 5$.

Since $f'(1) \equiv 0 \pmod 5$ and 1 is not a root of (1) there is no root of (1) corresponding to the root 1 of (2).

Roots of (i) corresponding to the root 3 of (2).

Here $f(3) = 35 = 7.5$ $(k = 7)$

$f'(3) = 29 \equiv -1 \pmod 5$

$\equiv 0 \pmod 5$..

We see that there is a unique root $a = t5 + 3$ of (i) corresponding to the root 3 of (2), where t is the solution of,

$$-1 \cdot t + 7 \equiv 0 \pmod 5$$

which is $t \equiv x \pmod 5$. hence the only root of (1) is $x \equiv 13 \pmod{25}$.

■■■