H.P. University Syllabus

M.A./MSc. MATHEMATICS

COURSE-M303 — ANALYTIC NUMBER THEORY

SECTION-I

Divisibility Theory in the Integers

The Division Algorithm. The Greatest Common Divisor.

The Euclidean Algorithm, and The Diophantine Equation ax + by = c.

Primes and their Distribution

The Fundamental Theorem of Arithmetic. The Sieve of Eratosthenes and The Goldbash Conjecture.

The Theory of Congruences

Basic Properties of Congruence. Special Divisibility Tests and Linear Congruences.

SECTION-II

Fermat's Theorem

Fermat's Factorization Method. The Little Theorem and Wilson's Theorem.

Number – Theoretic Functions

The Functions τ and σ, The Mobius Inversion Formula, The Greatest Integer Function and An Application to the Calendar.

Euler's Generalization of Fermat's Theorem

Euler's Phi-Function, Euler's Theorem and Some properties of the Phi-Function, An Application to Cryptography.

SECTION-III

Primitive Roots and Indices

The Order of an Integer Modulo *n*, Primitive Roots for Primes, Composite Numbers Having Primitive Roots and The Theory of Indices.

The Quadratic Reciprocity Law

Euler's Criterion, The Legendre Symbol and Its Properties, Quadratic Reciprocity and Quadratic Congruences with Composite Moduli.

Contents

1

CHAPTER

THE DIVISIO

The theore

of number the

Theorem 1. *S*

Statement : G

that $a = bq +$

Given intege

$a = bq + r, 0$

Proof. If $a <$

If $a \geq b,$

b

In the be

But afte

multiple of

Let bq

Now

So let a

$\therefore$

Again,

$\Rightarrow$

$\Rightarrow$

$\Rightarrow$

$\therefore$ we

195-255

256-285

286-324

325-366

1
CHAPTER

DIVISIBILITY THEORY IN THE INTEGERS

THE DIVISION ALGORITHM

The theorem known as division algorithm is of great importance in the development of number theory.

Theorem 1. *State and prove division algorithm theorem.*

Statement : ***Given integers a and b with $b \neq 0$ there exist unique integers q and r such that $a = bq + r$, where $0 \leq r < b$.***

Or

Given integers a and b, with $b > 0$, there exist unique integers q and r such that $a = bq + r$, $0 \leq r < b$.

Proof. If $a < b$, then $a = b.0 + a$ (Here $q = 0, r = a < b$)

If $a \geq b$, the set of multiples of b consists of the numbers

$b, 2b, 3b, 4b, \ldots\ldots$

In the beginning, the multiples of b are less than a.

But after a certain steps, we get a multiple of b such that it is just $\leq a$ and the next multiple of b is $> a$.

Let bq denote the greatest multiple of b such that $a \geq bq$ and $a < (q + 1)\, b$.

Now $a \geq bq \Rightarrow a - bq \geq 0$.

So let $a - bq = r$

$\therefore \quad r \geq 0$.

Again, $a < (q + 1)\, b$

$\Rightarrow \quad a < bq + b$

$\Rightarrow \quad a - bq < b$

$\Rightarrow \quad r < b$

$\therefore$ we have two numbers q and r such that

$$a - bq = r$$

$\Rightarrow$ $a = bq + r$ where $0 \le r < b$ ....(1)

Uniqueness

If possible, let there exist integers q_1 and r_1 such that

$$a = bq_1 + r_1 \text{ where } 0 \le r_1 < b. \quad \text{....(2)}$$

Equating the values of a from (1) and (2), we get

$$bq + r = bq_1 + r_1$$

Or $bq - bq_1 = r_1 - r$

Or $b(q - q_1) = r_1 - r$ ....(3)

$\therefore$ $b \mid (r_1 - r)$ (by definition of divisibility)

But $|r_1 - r| < b$ ($\because$ $0 \le r < b$ and $0 \le r_1 < b$)

$\therefore$ $r_1 - r = 0 \Rightarrow r_1 = r$

[$\because$ if $a|b$ and $b < a$ where a and b are non-negative integers then $b = 0$]

Put $r_1 = r$ in (3), we get

$$b(q - q_1) = 0$$

But $b \neq 0$

$\Rightarrow$ $q - q_1 = 0$

$\Rightarrow$ $q = q_1$

Hence there exists unique integers q and r such that

$$a = bq + r \text{ where } 0 \le r < b.$$

Note

If $a, b \in Z$ and $b \neq 0$, then the relation $a = bq + r$ where $0 \le r < |b|$ establishes uniqueness of division.

Here a is called the **dividend**, b is called the **divisor**, q is the **quotient** and r is called the **remainder**.

Algorithm

An algorithm is a method of obtaining a result by repeated application of an operation.

Corollary. *If a and b are integers, with $b \neq 0$, then there exist unique integers q and r such that $a = qb + r$, $0 \le r < |b|$.*

Proof. If $a = 0$, by taking $q = 0$ and $r = 0$, we have

$0 = b.0 + 0$, $0 \le r < |b|$ and we are done.

Therefore, suppose $a \neq 0$.

Without loss of generality we may suppose $b > 0$, for if $b < 0$, $|b| = -b > 0$.

Then as $|b| > 0$, $\exists$ integers q' and r' such that

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

Or $a = -bq' + r'$

$= b(-q') + r'$ ....(1)

Let $q = -q'$ and $r = r'$ in (1) and we get the conclusion.

Thus we must prove the statement for $a \neq 0$ and $b > 0$.

Let us define $S = \{a - xb : x \text{ is an integer and } a - xb \ge 0\}$.

As $b > 0$, $b \ge 1$.

Therefore, if $a > 0$, $a = a - 0.b \in S$

and if $a < 0 \Rightarrow ab < a \Rightarrow a - ab \in S$.

Thus S is a non-empty subset of non-negative integers and by well ordering principle it has a smallest r $0 \le r$ and $r = a - qb$ for some integer q.

Or $a = bq + r$, $0 \le r$.

We still must show $r < b$.

Suppose $r \ge b$.

Then $r - b = a - qb - b$

$= a - (q + 1) b \ge 0$

$\Rightarrow$ $r - b \in S$

and $r - b < r$,

which is a contradiction.

Hence $r < b$.

We now show that q and r are unique.

If possible, let

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

also $a = bq' + r'$, $0 \le r' < b$

$\Rightarrow$ $bq + r = bq' + r'$ ...(2)

$\Rightarrow$ $bq - bq' = r' - r$

$\Rightarrow$ $b(q - q') = r' - r$

$\Rightarrow$ $|b|\,|q - q'| = |r' - r| < |b|$

$\Rightarrow \quad |b|\,|q - q'| < |b|$

$\Rightarrow \quad |q - q'| < 1$

and this is possible only if $q - q' = 0$ or $q = q'$.

Consequently (2) gives

$r = r'$.

Note

To illustrate the division algorithm when $b < 0$ let us take $b = -7$. Then for the choices of $a = 1, -2, 61$ and -59, we obtain the expressions

$1 = 0\,(-7) + 1$

$-2 = 1\,(-7) + 5$

$61 = (-8)\,(-7) + 5$

$-59 = 9\,(-7) + 4.$

Example 1. *Square of any odd integer is of the form* $8k + 1$, k *an integer.*

Solution. Since any odd integer is of the form $2m + 1$ and

$$(2m+1)^2 = 4m^2 + 1 + 4m \qquad \ldots(1)$$
$$= 4m\,(m+1) + 1.$$

Now $m\,(m + 1)$ is always even, say $2k$.

Hence $4m\,(m + 1) = 4 \times 2k = 8k$

$\therefore$ (1) becomes

$$(2m+1)^2 = 8k + 1.$$

Example 2. *Show that the expression* $\dfrac{a\,(a^2+2)}{3}$ *is an integer for all* $a \geq 1$.

Solution. According to the division algorithm, every a is of the form $3q$, $3q + 1$ or $3q + 2$.

Let us take $a = 3q$, then we have

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

which clearly is an integer.

Similarly, if $a = 3q + 1$, then

$$\frac{a\,(a^2+2)}{3} = \frac{(3q+1)\,[(3q+1)^2+2]}{3}$$

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

which is also an integer.

Finally, for $a = 3q + 2$, we have

$$\frac{a\,(a^2+2)}{3} = \frac{(3q+2)\,[(3q+2)^2+2]}{3}$$
$$= \frac{(3q+2)\,(9q^2+4+12q+2)}{3}$$
$$= \frac{(3q+2)\,(9q^2+12q+6)}{3}$$
$$= \frac{(3q+2)\,3\,(3q^2+4q+2)}{3}$$
$$= (3q+2)\,(3q^2+4q+2)$$

which is also an integer.

Thus we have seen that $\dfrac{a\,(a^2+2)}{3}$ is an integer for all $a \geq 1$.

Example 3. *Prove that* $\dfrac{n\,(n+1)\,(2n+1)}{6}$ *is an integer for* $n \geq 1$.

Solution. On dividing n by 6, by division algorithm, we have

$n = 6q + r$ where $0 \leq r < 6$.

$\Rightarrow \quad n = 6q, 6q + 1, 6q + 2, 6q + 3, 6q + 4, 6q + 5$

If $n = 6q$, then

$$\frac{n\,(n+1)\,(2n+1)}{6} = \frac{6q\,(6q+1)\,(12q+1)}{6}$$
$$= q\,(6q+1)\,(12q+1) \in Z$$

If $n = 6q + 1$, then

$$\frac{n\,(n+1)\,(2n+1)}{6} = \frac{(6q+1)\,(6q+2)\,(12q+2+1)}{6}$$

$$= \frac{(6q+1)(6q+2)(12q+3)}{6}$$

$$= \frac{(6q+1)\cdot 2(3q+1)\cdot 3(4q+1)}{6}$$

$$= \frac{6(6q+1)(3q+1)(4q+1)}{6}$$

$$(6q+1)(3q+1)(4q+1) \in Z$$

If $n = 6q+2$, then

$$\frac{n(n+1)(2n+1)}{6} = \frac{(6q+2)(6q+3)(12q+4+1)}{6}$$

$$= \frac{2(3q+1)\cdot 3(2q+1)(12q+5)}{6}$$

$$= (3q+1)\cdot 3(2q+1)(12q+5) \in Z$$

If $n = 6q+3$, then

$$\frac{n(n+1)(2n+1)}{6} = \frac{(6q+3)(6q+4)(12q+7)}{6}$$

$$= \frac{3(2q+1)\cdot 2(3q+2)(12q+7)}{6}$$

$$= (2q+1)(3q+2)(12q+7) \in Z$$

If $n = 6q+4$, then

$$\frac{n(n+1)(2n+1)}{6} = \frac{(6q+4)(6q+5)(12q+9)}{6}$$

$$= \frac{2(3q+2)(6q+5)3(4q+3)}{6}$$

$$= (3q+2)(6q+5)(4q+3) \in Z$$

If $n = 6q+5$, then

$$\frac{n(n+1)(2n+1)}{6} = \frac{(6q+5)(6q+6)(12q+11)}{6}$$

$$= \frac{6(6q+5)(q+1)(12q+11)}{6}$$

$$= (6q+5)(q+1)(12q+11) \in Z$$

Hence in all cases

$$\frac{n(n+1)(2n+1)}{6} \in Z \ \forall\ n \geq 1.$$

DIVISIBILITY

Definition. *A non zero integer a is said to divide an integer b if there exists another integer c such that $b = ac$.*

In symbols we write it as $a \mid b$.

Note

(i) If no such integer exists, we say that a does not divide b i.e $a \nmid b$.

(ii) a is called a divisor or a factor of b and b is called a multiple of a.

(iii) $a \mid 0$ for each integer $a\ (\neq 0)$,
$1 \mid a$ for each integer a,
$a \mid a$ for each integer $a\ (\neq 0)$.

(iv) For every integer $a \neq 0, \pm 1$ and $\pm a$ are always divisors of a.
These are called ***improper divisors*** of a.
If a has any divisors other than these, then they are called ***proper divisors*** of a.

Theorem 2. ***For integers a, b, c the following hold :***

(i) $a \mid 0, 1 \mid a, a \mid a$.

(ii) $a \mid 1$ *if and only if* $a = \pm 1$.

(iii) *If* $a \mid b$ *and* $c \mid d$, *then* $ac \mid bd$.

(iv) *If* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.

(v) $a \mid b$ *and* $b \mid a$ *then* $a = \pm b$.

(vi) *If* $a \mid b$ *and* $b \neq 0$, *then* $|a| \leq |b|$.

(vii) *If* $a \mid b$ *and* $a \mid c$,

then $a \mid (bx + cy)$ *for arbitrary integers* x *and* y.

Proof. Proof of **(i)** and **(ii)** is obvious.

(iii) Since $a \mid b$,
then by definition of divisibility there exists an integer k_1 such that ...(1)

$$b = ak_1$$

Again since $c \mid d$,
then there exists an integer k_2 such that ...(2)

$$d = ck_2$$

Multiplying (1) and (2), we get

$$bd = ac\, k_1 k_2$$

$\Rightarrow$ $ac \mid bd$ by definition of divisibility.

(iv) Since $a \mid b$,

then by definition of divisibility there exists an integer d such that

$$b = ad \quad \ldots(3)$$

Again since $b \mid c$,
there exists an integer e such that

$$c = be \quad \ldots(4)$$

Now putting the value of b from (3) in (4), we get

$$c = ade$$

$\Rightarrow a \mid c$ by definition of divisibility.

(v) Since $a \mid b$ and $b \mid a$,
therefore neither $a = 0$ nor $b = 0$.
Now $a \mid b$, then by definition of divisibility there exists an integer c such that

$$b = ac$$

Also $b \mid a$

$\Rightarrow$ there exists an integer d such that

$$a = bd.$$

Now $(ab) \cdot 1 = ab = (bd)(ac) = (ab)(cd)$.

Since $ab \neq 0$,
therefore, by cancellation law, we get

$$1 = cd$$

$\Rightarrow$ either $c = 1, d = 1$
Or $c = -1, d = -1$

$\Rightarrow$ either $a = b$ or $a = -b$. ($\because a = bd$)

(vi) Since $a \mid b$
so by definition of divisibility there exists an integer c such that

$$b = ac. \quad \ldots(5)$$

Also $b \neq 0 \Rightarrow c \neq 0$.
Taking modulus on both sides of (5), we get

$$|b| = |ac| = |a|\,|c|.$$

Since $c \neq 0$, it follows that

$$|c| \geq 1.$$

$$\therefore \quad |b| = |a|\,|c| \geq |a|$$

$$\Rightarrow \quad |b| \geq |a|$$

$$\Rightarrow \quad |a| \leq |b|.$$

(vii) Since $a \mid b$,
then by definition of divisibility there exists an integer r such that

$$b = ar.$$

Also $a \mid c$
$\Rightarrow$ there exists an integer s such that

$$c = as.$$

Now $bx + cy = arx + asy$
$= a(rx + sy)$

Since $rx + sy$ is an integer, therefore

$$bx + cy = a(rx + sy)$$

$\Rightarrow a \mid (bx + cy)$ by definition of divisibility.

GREATEST COMMON DIVISOR

Definition. *Let a and b be two integers not both zero i.e at least one of them is not equal to zero. An integer $d > 0$ is called the greatest common divisor (g.c.d.) of a and b if*

(i) $d \mid a$ and $d \mid b$ i.e d is a common divisor of a and b.

(ii) If $c \mid a$, $c \mid b$ then $c \mid d$ i.e every common divisor of a and b is a divisor of d.

In symbols it is written as $(a, b) = d$

e.g $(12, 15) = 3$.

Note

(i) $(a, b) = (b, a)$

(ii) If $d = (a, b)$, then $d \geq 1$ and is unique.

(iii) If $a \mid b$, then $(a, b) = a$

(iv) $(a, a) = a$

(v) $(a, 0) = |a|$

Theorem 3. ***If $a \mid b$, then $(a, b) = a$.***

Proof. We know that $a \mid a$ and a is the greatest common divisor of a.
Also $a \mid b$ (given)
$\therefore$ a is the greatest common divisor of a and b.
i.e $(a, b) = a$.

Greatest common divisor of more than two integers

Definition. *Let $\{a_1, a_2, \ldots, a_n\}$ be a finite set of integers, not all zero. If there exists a positive integer d such that*

(i) d is common divisor of $a_1, a_2, \ldots, a_n$

(ii) each common divisor of $a_1, a_2, \ldots, a_n$ is also a divisor of d, then d is called the g.c.d. of $a_1, a_2, \ldots, a_n$.

In symbols it is written as $d = (a_1, a_2, \ldots, a_n)$

PRIMES

A positive integer p is said to be **prime** if $p > 1$ and p has no divisors except 1 and p.

i.e a number which has exactly two different factors, itself and one, is called a prime number.

Thus 2, 3, 5, 7, 11,..... are primes.

Note

2 is the only even prime number.

Composite

Every number > 1 which is not prime is called a **composite number**.

i.e a number which has more than two different factors is called **composite**.

CO-PRIMES

Two integers a and b are said to be **co-prime** or **relatively prime** if g.c.d. of a and $b = 1$

i.e if $(a, b) = 1$

e.g. $(2, 3) = 1, (4, 5) = 1$.

Mutually Coprime Integers

Integers $a_1, a_2, \ldots, a_n$ are said to be **mutually coprime integers** if $a_1, a_2, \ldots, a_n$ are coprime in pairs.

Note

Mutually coprime integers are always coprime but converse may not be true.

Proof. Let $a_1, a_2, \ldots, a_n$ be mutually coprime integers.

We are to prove that $(a_1, a_2, \ldots, a_n) = 1$

Let $(a_1, a_2, \ldots, a_n) = d$

$\Rightarrow$ $d \mid a_1, d \mid a_2, \ldots, d \mid a_n$

Now $(a_1, a_2) = 1$ ..... ($\because a_1, a_2, \ldots, a_n$ are mutually coprime)

Therefore $d \mid a_1$ and $d \mid a_2$

$\Rightarrow$ $d \mid (a_1, a_2)$ .....

$\Rightarrow$ $d \mid 1$

$\Rightarrow$ $d = 1$

$\therefore$ $(a_1, a_2, \ldots$

Converse may not

Since 3, 5, 6 are co

Twin Primes

A pair of numbers

e.g 3, 5 are twin p

Perfect Number

A number n is said

to $2n$.

e.g 28 is a perfect

Sum of divisors o

Note

1 is neither a prim

It is called **unit**.

Theorem 4. ***Given i***

and y such that g.c.d

If d is the g.c.d. of i

that $d = ax + by$.

If d is the greatest c

$d = bx + cy$.

Proof. By successive

let $r_1, r_2, \ldots, r_n$

Therefore,

$a = bq_1 +$

$b = r_1q_2$

$r_1 = r_2q_3$

$r_{n-2} = r_n$

$\Rightarrow \quad d \mid 1$

$\Rightarrow \quad d = 1$

$\therefore \quad (a_1, a_2, \ldots\ldots, a_n) = 1.$

Converse may not be true.

Since 3, 5, 6 are coprime but 3,5, 6 are not mutually coprime. [since (3, 5, 6) = 1]

Twin Primes

A pair of numbers is said to be **twin primes** if they differ by 2.

e.g. 3, 5 are twin primes.

Perfect Number

A number n is said to be **perfect** if the sum of all divisors of n (including n) is equal to $2n$.

e.g. 28 is a perfect number because divisors of 28 are 1, 2, 4, 7, 14, 28.

Sum of divisors of $n = 28 = 1 + 2 + 4 + 7 + 14 + 28 = 56 = 2n$

Note

1 is neither a prime nor a composite number.

It is called **unit**.

Theorem 4. *Given integers a and b, not both of which are zero, there exist integers x and y such that g.c.d.* $(a, b) = ax + by$

Or

If d is the g.c.d. of integers a and b, $a \neq b$, prove that there exists integers x and y such that $d = ax + by$.

Or

If d is the greatest common divisor of b and c, then there are integers x and y such that $d = bx + cy$.

Proof. By successive application of division algorithm,

let $r_1, r_2, \ldots\ldots, r_n$ be the successive remainders.

Therefore,

$a = bq_1 + r_1, \quad 0 < r_1 < b$ (Dividing a by b)

$b = r_1 q_2 + r_2, \quad 0 < r_2 < r_1$ (Dividing b by remainder r_1)

$r_1 = r_2 q_3 + r_3, \quad 0 < r_3 < r_2$ (Dividing r_1 by remainder r_2)

$\vdots \qquad \vdots$

$\vdots \qquad \vdots$

$r_{n-2} = r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1}$

$$r_{n-1} = r_n q_{n+1} + r_{n+1},\ 0 < r_{n+1} < r_n$$

Since $r_1 > r_2 > \ldots\ldots$ is a set of decreasing integers, this process must terminate after a finite number of steps *i.e* remainder must be zero after some stage.

So let $r_{n+1} = 0$

$\therefore \quad r_{n-1} = r_n q_{n+1} + 0$

Or $\quad r_{n-1} = r_n q_{n+1}$

$\therefore \quad r_n \mid r_{n-1}$, since $(r_{n-1}, r_n) = r_n$ [$\because$ If $a \mid b$, then $(a, b) = a$]

Hence using the theorem, "If $a = bq + r$, then $(a, b) = (b, r)$", we get

$$(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \ldots = (r_{n-1}, r_n) = r_n \ldots(1)$$

i.e g.c.d. of a and b is r_n.

From first of above equations

$$r_1 = a - bq_1$$

$$= ax_1 + by_1 \text{ where } x_1 = 1,\ y_1 = -q_1$$

Putting this value of $r_1 = a - bq_1$ in

$$r_2 = b - r_1 q_2, \text{ we get}$$

$$r_2 = b - (a - bq_1) q_2$$

$$= b - aq_2 + bq_1 q_2$$

$$= -aq_2 + b(1 + q_1 q_2)$$

$$= ax_2 + by_2 \text{ where } x_2 = -q_2,\ y_2 = 1 + q_1 q_2$$

Similarly, $r_3 = ax_3 + by_3$ and so on.

$\therefore \quad r_n = ax_n + by_n$

Or $\quad r_n = ax + by$

where $x_n = x$ and $y_n = y$

i.e g.c.d. of a and $b = r_n$ can be expressed as.

$$(a, b) = d = ax + by.$$

Note

Show that d is the least value of $ax + by$.

Since $(a, b) = d$

$\Rightarrow \quad d \mid a$ and $d \mid b$ ....(1)

$\therefore \quad d \mid (ax + by)$ $\forall$ values of x and y.

$\therefore \quad \exists$ an integer k such that $ax + by = kd$

But least value of k is 1.

$\therefore$ putting $k = 1$ in (1), we get

$ax + by = d$.

Hence d is the least value of $ax + by$.

Theorem 5. ***Let a and b be any integers at least one of them is non zero. Then there exist integers x and y such that***

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

Proof. Let $d = (a, b)$ and S be a set defined as

$$S = \{au + bv : au + bv > 0,\ u, v \text{ integers}\}$$

Since at least one of a or b is non-zero, therefore either $|a|$ or $|b|$ is in S so that S is non empty.

By well ordering principle, S has a least element say

$$d = au_0 + bv_0.$$

By definition $d < |a|, |b|$.

By division algorithm as applied to $|a|$,

$$|a| = dq + r,\ 0 \le r < d$$

$\therefore \quad r = |a| - dq$

$$= \pm a - q(au_0 + bv_0)$$

$$= a(\pm 1 - u_0 q) + (-v_0) b \ge 0$$

and is of the form $au + bv$.

Hence by choice of d, $r = 0$

$\Rightarrow \quad |a| = dq$

$\Rightarrow \quad d \mid |a| \Rightarrow d \mid a.$

Similarly $d \mid b$.

If $c \mid a$ and $c \mid b$, then

$$c \mid au_0 + bv_0$$

$\Rightarrow \quad c \mid d.$

Hence $d = (a, b) = au_0 + bv_0$.

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

Proof. Since $d \mid a$ and $d \mid b$

$\Rightarrow d \mid (ax + by)$ for all integers x, y.

Thus every member of T is a multiple of d.

Conversely, d may be written as

$$d = ax_0 + by_0 \text{ for suitable integers } x_0 \text{ and } y_0,$$

so that any multiple nd 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, lies in T.

Theorem 6. ***Two integers a and b are relatively prime iff there exists integers x and y such that*** $ax + by = 1$.

Or

Let a and b be integers, not both zero. Then a and b are relatively prime if and only if there exist integers x and y such that $1 = ax + by$.

Or

If a and b are relatively prime integers, show that there are integers m and n such that $ma + nb = 1$.

Proof. Let us suppose that a and b are relatively prime.

Then $(a, b) = 1$.

By the theorem, *"If d is of the gcd of integers a and b, a ≠ b, then there exist integers x and y such that* $d = ax + by$*"*, there exist integers x and y such that

$$1 = (a, b) = ax + by.$$

Conversely, suppose that $ax + by = 1$ for some integers x and y.

Let $d = (a, b)$.

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

$\Rightarrow$ $d \mid ax, d \mid by$

$\Rightarrow$ $d \mid (ax + by)$

$\Rightarrow$ $d \mid 1$

Hence $(a, b) = 1$, so a and b are relatively prime.

Corollary 1. *If gcd* $(a, b) = d$, *then gc*

Proof. Since $(a, b) = d$.

Therefore $d \mid a$ and $d \mid b$ (by defi

Then there exist integers a_1 and

$$a = da_1$$

and $b = db_1$

Again since $(a, b) = d$

Therefore there exist integers

$$ax + by = d$$

Putting the values of a and b

$$da_1 x + db_1 y = d$$

Or $a_1 x + b_1 y = 1$

$\therefore$ $(a_1, b_1) = 1$

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

[From (1), $a_1 = \frac{a}{d}$ and fro

Hence the result.

Corollary 2. *If* $a \mid c$ *and* $b \mid c$

If $a \mid x, b \mid x$ *and* $(a, b) = 1$, p

Proof. Since $a \mid c$,

therefore there exists a

$$c = ad$$

Since $b \mid c$,

therefore there exists

$$c = be.$$

Since $(a, b) = 1$.

$\Rightarrow \exists$ integers m and

$$am + bn = 1$$

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

Proof. Since $(a, b) = d$.

Therefore $d \mid a$ and $d \mid b$ (by definition of gcd)

Then there exist integers a_1 and b_1 such that

$$a = da_1 \quad \text{....(1)}$$

and $$b = db_1 \quad \text{....(2)}$$

Again since $(a, b) = d$

Therefore there exist integers x and y such that

$$ax + by = d$$

Putting the values of a and b from (1) and (2) in (3), we get

$$da_1 x + db_1 y = d$$

Or $$a_1 x + b_1 y = 1$$

$\therefore$ $$(a_1, b_1) = 1$$

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

[From (1), $a_1 = \frac{a}{d}$ and from (2) $b_1 = \frac{b}{d}$]

Hence the result.

Corollary 2. If $a \mid c$ *and* $b \mid c$ *with* $gcd\,(a, b) = 1$, *then* $ab \mid c$.

Or

If $a \mid x$, $b \mid x$ *and* $(a, b) = 1$, *prove that* $(ab) \mid x$.

Proof. Since $a \mid c$,

therefore there exists an integer d such that

$$c = ad \quad \text{....(1)}$$

Since $b \mid c$,

therefore there exists an integer e such that

$$c = be. \quad \text{....(2)}$$

Since $(a, b) = 1$.

$\Rightarrow$ $\exists$ integers m and n such that

$$am + bn = 1$$

Multiplying both sides by c, we get

$$acm + bcn = c$$

Putting $c = be$ from (2) in acm and $c = ad$ from (1) in bcn, (3) becomes ....(3)

$$abem + band = c$$

Or $\quad ab\,(em + nd) = c$

$\therefore \quad ab \mid c$

Hence the Proof

Example 4. *Give an example to show that $a \mid c$, $b \mid c$ need not imply that $ab \mid c$.*

Solution. Since $2 \mid 12$ and $4 \mid 12$

but $2 \times 4 = 8$ which is not a divisor of 12.

EUCLID'S LEMMA

Theorem 7. ***If $a \mid bc$, with gcd $(a, b) = 1$, then $a \mid c$.***

Proof. Since $a \mid bc$.

therefore, there exists an integer d such that

$$bc = ad \quad \text{....(1)}$$

Since $\quad (a, b) = 1,$

$\therefore$ $\exists$ integers x and y such that

$$ax + by = 1 \quad \text{....(2)}$$

Multiplying both sides of (2) by c, we get

$$acx + bcy = c \quad \text{....(3)}$$

Put $bc = ad$ from (1) in (3), we get

$$acx + ady = c$$

Or $\quad a\,(cx + dy) = c$ (by definition of divisibility)

$\therefore \quad a \mid c$

Note

Conclusion of Euclid's lemma is false if $(a, b) \neq 1$.

Solution. Take $a = 12, b = 8, c = 9$

$(a, b) = (12, 8) = 4.$

$12 \mid 8 \cdot 9 = 72$ yet $12 \nmid 8$, $12 \nmid 9$.

Theorem 8. ***If a, b, c are positive integers such that $c \mid ab$ and $(b, c) = 1$, prove that $c \mid a$.***

Or

If c divides ab and gcd $(b, c) = 1$ then prove that c divides a.

Proof. Since $c \mid ab$,

therefore, there exists an integer d such that

$$ab = cd \quad \text{....(1)}$$

Since $\quad (b, c) = 1,$

therefore, there exists integers m and n such that

$$bm + cn = 1 \quad \text{....(2)}$$

Multiplying both sides of (2) by a, we get

$$abm + acn = a \quad \text{....(3)}$$

Putting $ab = cd$ from (1) in (3), we get

$$cdm + acn = a$$

Or $\quad c\,(dm + an) = a$

Or $\quad c \mid (dm + an) = a$ (by definition of divisibility)

$\therefore \quad c \mid a$

Hence the result.

Theorem 9. ***Let a, b be integers, not both zero. For a positive integer d,***

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

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

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

Then by definition of gcd,

$$d \mid a \text{ and } d \mid b$$

$\therefore$ (i) holds.

Again since $d = gcd\,(a, b)$

$\Rightarrow$ $\exists$ integers x and y such that

$$d = ax + by$$

Thus if $c \mid a$ and $c \mid b$, then

$$c \mid ax \text{ and } c \mid by$$

$\Rightarrow \quad c \mid (ax + by)$

But $\quad d = ax + by,$

$\therefore \quad c \mid (ax + by),$

$\Rightarrow \quad c \mid d$

Hence (ii) holds.

Conversely, Let d be any positive integer satisfying the stated conditions.

Given any common divisor c of a and b, we have $c \mid d$ from hypothesis (ii).
The implications is that $d \geq c$, and consequently d is the greatest common divisor of a and b.

Example 5. *If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ $\forall$ $x, y \in Z$.*

Solution. We have $a \mid b$

$\Rightarrow$ $b = am$ for some $m \in Z$

Also $a \mid c$ (by definition of divisibility)

$\Rightarrow$ $c = an$ for some $n \in Z$

Now $bx + cy = (am)\, x + (an)\, y$

$= a\,(mx + ny)$ where $mx + ny \in Z$.

$\therefore$ $a \mid (bx + cy)$ (by definition of divisibility)

Example 6. *If $a \mid x$ and $x \mid a$, then $a = \pm x$.*

Solution. Since $a \mid x$ and $x \mid a$,

therefore, neither $a = 0$ nor $x = 0$.

Now $a \mid x$

$\Rightarrow$ $x = ac$ for some $c \in Z$ (by definition of divisibility)

Also $x \mid a$

$\Rightarrow$ $a = xd$ for some $d \in Z$.

Now $(ax) \cdot 1 = ax = (xd)\,(ac)$

$= (ax)\,(cd)$

Since $ax \neq 0$, therefore, by cancellation law, we get

$1 = cd$

$\Rightarrow$ either $c = 1, d = 1$

Or $c = -1, d = -1$ [$\because a = xd$

$\Rightarrow$ either $a = x$ or $a = -x$

Example 7. *If $a \mid b$ then $a \mid bc$ where $a, b, c \in Z$.*

Solution. Since $a \mid b$,

therefore by definition of divisibility there exists an integer m such that ....(1

$b = am$

Multiplying both sides of (1) by c, we get

$bc = amc$

$\Rightarrow$ $bc = a\,(mc)$

$\Rightarrow$ $a \mid bc$ (by definition of divisibility)

Example 8. *If $a \mid b$ and $a \mid c$ then $a^2 \mid bc$ where $a, b, c \in Z$.*

Solution. Since $a \mid b$

$\Rightarrow$ $b = am$ for some $m \in Z$ (by definition of divisibility) ....(1)

Also $a \mid c$

$\Rightarrow$ $c = an$ for some $n \in Z$ ....(2)

Multiplying (1) and (2), we get

$bc = (am)\,(an)$

$\Rightarrow$ $bc = a^2 mn$

$\Rightarrow$ $bc = a^2\,(mn)$ (by definition of divisibility)

$\Rightarrow$ $a^2 \mid bc$

Example 9. *Given integers a, b, c, verify that $a \mid b$ if and only if $ac \mid bc$, where $c \neq 0$.*

Solution. Let $ac \mid bc$.

Therefore, there exists an integer m such that ....(1)

$bc = acm$

But $c \neq 0$ (given) so dividing both sides of (1) by c, we get

$b = am$ (by definition of divisibility)

$\Rightarrow$ $a \mid b$

Conversely, $a \mid b$ ....(2)

$\Rightarrow$ $\exists$ an integer d such that

$b = ad$

Multiplying both sides of (2) by c, we get

$bc = adc$

$\Rightarrow$ $bc = ac\,(d)$

$\Rightarrow$ $ac \mid bc$.

Hence the result.

Example 10. *If $a \mid b$ and $c \mid d$, then $ac \mid bd$.*

Solution. Since $a \mid b$

$\Rightarrow$ $\exists$ an integer m such that ....(1)

$b = am$

Again $c \mid d$

$\Rightarrow$ $\exists$ an integer n such that

$d = nc$

Multiplying (1) and (2), we get

$bd = (am)(nc)$

$\Rightarrow$ $bd = (ac)(mn)$

$\Rightarrow$ $ac \mid bd$

Example 11. *If* $gcd\ (a, b) = 1$ *and* $gcd\ (a, c) = 1$, *then* $gcd\ (a, bc) = 1$.

Solution. Since $gcd\ (a, b) = 1$, (by definition of divisibi

therefore, there exist integers x_1 , y_1 such that

$ax_1 + by_1 = 1$

Or $by_1 = 1 - ax_1$

Again $(a, c) = 1$

$\Rightarrow$ there exists integers x_2 , y_2 such that

$ax_2 + cy_2 = 1$

Or $cy_2 = 1 - ax_2$

From (1) and (2), we have

$(by_1)(cy_2) = (1 - ax_1)(1 - ax_2)$

Or $(bcy_1\ y_2) = 1 - a(x_1 + x_2) + a^2 x_1 x_2$

Or $a(x_1 + x_2 - ax_1 x_2) + bc(y_1 y_2) = 1$

Or $ax_3 + bcy_3 = 1$,

where $x_3 = x_1 + x_2 - ax_1 x_2$ and $y_3 = y_1 y_2$ are some integers.

Thus, we get

$ax_3 + bcy_3 = 1$

Hence $gcd\ (a, bc) = 1$.

Example 12. *If* $gcd\ (a, b) = 1$ *and* $c \mid a$, *then* $gcd\ (b, c) = 1$.

Solution. Since $gcd\ (a, b) = 1$,

therefore there exist integers x and y such that ....(1

$ax + by = 1$

Since $c \mid a$,

therefore there exists an integer d such that

$a = cd$

Put $a = cd$ in (1), we get

$cdx + by = 1$

Or $c(dx) + b(y) = 1$

Or $b(y) + c(dx) = 1$

$\therefore$ $gcd\ (b, c) = 1$.

Example 13. *If* $gcd\ (a, b) = 1$, *then* $gcd\ (ac, b) = gcd\ (c, b)$.

Solution. Let $gcd\ (ac, b) = d$

and $gcd\ (c, b) = e$

Since $gcd\ (ac, b) = d$

$\Rightarrow$ d is a common multiple of ac and b. ....(1)

$\therefore$ $d \mid e$ [$\because$ $gcd\ (c, b) = e$]

Again, $gcd\ (c, b) = e$ (by definition of gcd)

$\Rightarrow$ $e \mid c$ and $e \mid b$

$\Rightarrow$ $e \mid ac$ and $e \mid b$

i.e e is a common divisor of ac and b. ....(2)

$\therefore$ $e \mid d$ [$\because$ $gcd\ (ac, b) = d$]

From (1) and (2), we get

$d = e$

i.e $gcd\ (ac, b) = gcd\ (c, b)$.

Example 14. *If* $gcd\ (a, b) = 1$, *and* $c \mid a + b$, *then* $gcd\ (a, c) = gcd\ (b, c) = 1$.

Solution. We have $gcd\ (a, b) = 1$,

therefore there exists integers x and y such that ....(1)

$1 = ax + by$

But $c \mid a + b$

$\Rightarrow$ $c \mid a$ or $c \mid b$

$\Rightarrow$ $a = cm$ or $b = cn$.

Put $a = cm$ in (1), we get

$1 = cmx + by$

$\Rightarrow \quad 1 = c(mx) + by$

$\Rightarrow \quad 1 = by + c(mx)$

$\Rightarrow \quad gcd(b, c) = 1$

Again putting $b = cn$ in (1), we get

$1 = ax + cny$

$\Rightarrow \quad 1 = ax + c(ny)$

$\Rightarrow \quad gcd(a, c) = 1$

Thus $gcd(a, b) = 1$ and $c \mid a + b$

$\Rightarrow \quad gcd(a, c) = 1 = gcd(b, c)$.

Example 15. *If $gcd(a, b) = 1$, $d \mid ac$ and $d \mid bc$, then $d \mid c$.*

Solution. Since $gcd(a, b) = 1$,

therefore there exists integers x and y such that

$1 = ax + by$ ...(1)

Since $d \mid ac$,

so by definition of divisibility there exists an integer m such that

$ac = md$

Also $d \mid bc$

$\Rightarrow \quad bc = nd$

Since $ac = md$

$\Rightarrow \quad a = \frac{m}{c} d$

and $bc = nd$

$\Rightarrow \quad b = \frac{n}{c} d$

Putting $a = \left(\frac{m}{c}\right) d$ and $b = \left(\frac{n}{c}\right) d$ in (1), we get

$1 = \left(\frac{m}{c}\right) dx + \left(\frac{n}{c}\right) dy$ ...(2)

Multiplying both sides of (2) by c, we get

$c = mdx + ndy$

$\Rightarrow \quad c = d(mx + ny)$

$\Rightarrow \quad d \mid c$ by definition of divisibility.

Example 16. *If $gcd(a, b) = 1$, prove that $gcd(a^2, b^2) = 1$.*

Solution. Let $gcd(a^2, b^2) = d$.

If $d = 1$, then $gcd(a^2, b^2) = 1$ and the solution is complete.

If $d > 1$, then d has a prime factor say p.

Now $p \mid d$ and $d = (a^2, b^2)$

$\Rightarrow \quad p \mid d$ and $d \mid a^2, d \mid b^2$

$\Rightarrow \quad p \mid a^2$ and $p \mid b^2$

$\Rightarrow \quad p \mid a$ and $p \mid b$, since p is prime

$\Rightarrow \quad p \mid (a, b)$

$\Rightarrow \quad p \mid 1$

which is impossible,

$\because$ p being a prime number ≥ 2.

$\therefore$ we must have $d = 1$ *i.e* $gcd(a^2, b^2) = 1$.

Example 17. *Prove that no integers x, y exist satisfying $x + y = 100$ and $(x, y) = 3$.*

Solution. We have

$x + y = 100$ ....(1)

and $(x, y) = 3$ ....(2)

Since $(x, y) = 3$

$\Rightarrow \quad 3 \mid x$ and $3 \mid y$

$\Rightarrow \quad x = 3a$ and $y = 3b$,

where $a, b \in Z$ and $(a, b) = 1$.

Putting these values of x and y in (1), we get

$3a + 3b = 100$

$\Rightarrow \quad a + b = \frac{100}{3}$, where $a, b \in Z$

But there does not exist $a, b \in Z$ such that $a + b = \frac{100}{3}$

Therefore no integers x, y exist satisfying given equations.

Example 18. *Prove that no integer in the sequence 11, 111, 1111, 11111,..... is a perfect square.*

Solution. By division algorithm, we have

$$11 = 4 \cdot 2 + 3$$
$$111 = 4 \cdot 27 + 3$$
$$1111 = 4 \cdot 277 + 3$$
$$11111 = 4 \cdot 2777 + 3$$
$$\text{- - - - - - - - - - - - - -}$$
$$\text{- - - - - - - - - - - - - -}$$

i.e every integer in the sequence is of the form $4k + 3$

We know that square of an integer is of the form $4k$ or $4k + 1$ which is shown as follows:

On dividing n by 2 by division algorithm, n is of the form $2k$ or $2k + 1$.

When $n = 2k$,

$$n^2 = 4k^2 = 4k' \text{ where } k' = k^2 \in Z$$

and when $n = 2k + 1$,

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$$
$$= 4(k^2 + k) + 1$$
$$= 4k' + 1 \text{ where } k' = k^2 + k \in Z$$

which shows that n^2 is of form $4k$ or $4k + 1$.

Hence no integer in given sequence is a perfect square.

Example 19. *Show that square of any integer is either of the form $3k$ or $3k + 1$.*

Solution. Let n be any integer.

Dividing n by 3, let k be the quotient and r be the least non-negative remainder.

$\therefore \quad n = 3k + r, r = 0, 1, 2$

$\Rightarrow \quad n = 3k$ or $3k + 1$ or $3k + 2$ type.

$\Rightarrow \quad n^2 = 9k^2$ or $9k^2 + 6k + 1$ or $9k^2 + 12k + 4$

$\Rightarrow \quad n^2 = 3(3k^2)$ or $3(3k^2 + 2k) + 1$ or $3(3k^2 + 4k + 1) + 1$

$= 3k$ or $3k + 1$ or $3k + 1$ type

i.e $\quad n^2 = 3k$ or $3k + 1$ type.

Hence n^2 is of the form $3k$ or $3k + 1$.

Example 20. *If $p \geq 5$ is a prime integer, show that $p^2 + 2$ is composite.*

Solution. Divide p by 6, let k the quotient and r, the least non- negative remainder.

$\therefore \quad p = 6k + r, r = 0, 1, 2, 3, 4, 5$

But $\quad r \neq 0, \neq 2, \neq 3, \neq 4,$

because in these cases, p is no longer a prime number.

$\therefore \quad r = 1$ or $r = 5$

$\therefore \quad p = 6k + 1$ or $p = 6k + 5$

i.e $\quad p = 6k \pm 1$ type

Now $\quad p^2 + 2 = (6k \pm 1)^2 + 2$

$= 36k^2 \pm 12k + 1 + 2$

$= 36k^2 \pm 12k + 3$

$= 3(12k^2 \pm 4k + 1)$

$\Rightarrow \quad 3 \mid p^2 + 2$

Hence $p^2 + 2$ is composite number.

Example 21. *Show that any integer of the form $6k + 5$ is also of the form $3j + 2$ but not conversely.*

Solution. Since $6k + 5 = 6k + 3 + 2$

$= 3(2k + 1) + 2$

$= 3j + 2$ where $j = 2k + 1$

Therefore any integer of the form

$6k + 5$ is of the form $3j + 2$.

Now if j is even and

$j = 2m, m \in Z$, then

$3j + 2 = 3(2m) + 2$

$= 6m + 2$

which is not of the form $6k + 5$

Hence the solution.

Example 22. *Find all primes that are one less than a perfect square.*

Or

Find which prime p can be expressed as $p = x^2 - 1$, where x is an integer.

Solution. Since $p = x^2 - 1$

$\Rightarrow \quad p = (x-1)(x+1)$

Since p is prime number,

$\therefore \quad x-1 = \pm 1$ or $x+1 = \pm 1$

Now $x-1 = \pm 1$ iff $x = 2$ or $x = 0$

$x+1 = \pm 1$ iff $x = 0$ or $x = -2$

But $x = 0$ is not possible since in this case p is no longer a prime number.

$\therefore \quad x = 2$ or $x = -2$

Therefore only possible value of p is given by

$p = (\pm 2)^2 - 1 = 3.$

Example 23. *If $p \neq 5$ is an odd prime, prove that either $p^2 - 1$ or $p^2 + 1$ is divisible by 10.*

Or

If p is an odd prime different from 5, prove that either $p^2 + 1$ or $p^2 - 1$ is divisible by 10.

Solution. Let us divide p by 10.

Let k be the quotient and r be the least non-negative remainder.

$\therefore \quad p = 10k + r;\ r = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.$

But $r \neq 0, \neq 2, \neq 4, \neq 5, \neq 6, \neq 8,$

since in these cases, p is no longer a prime number.

$\therefore \quad r = 1$ or 3 or 7 or 9.

Therefore $p = 10k + 1$ or $10k + 3$ or $10k + 7$ or $10k + 9$

i.e $\quad p = 10k \pm 1$ or $p = 10k \pm 3$

If $p = 10k \pm 1$, then

$p^2 = 100k^2 \pm 20k + 1$

$\Rightarrow \quad p^2 - 1 = 10\,(10k^2 \pm 2k)$

$\Rightarrow \quad 10 \mid p^2 - 1$

If $p = 10k \pm 3$, then

$p^2 = 100k^2 \pm 60k + 9$

$\Rightarrow \quad p^2 + 1 = 100k^2 \pm 60k + 10$

$= 10\,[10k^2 \pm 6k + 1]$

$\Rightarrow \quad 10 \mid p^2 + 1$ (by definition of divisibility)

Therefore either $p^2 - 1$ or $p^2 + 1$ is divisible by 10.

Example 24. *Show that square of any integer is of the form $4k$ or $4k + 1$.*

Solution. Let n be any integer.

On dividing n by 2, by division algorithm,

n is of the form $2k$ or $2k + 1$.

When $n = 2k$,

$n^2 = 4k^2 = 4k'$ where $k' = k^2 \in Z$.

When $n = 2k + 1$,

$n^2 = (2k+1)^2$

$= 4k^2 + 4k + 1$

$= 4(k^2 + k) + 1$

$= 4k' + 1$ where $k' = k^2 + k \in Z$.

Hence n^2 is of the form

$4k$ or $4k + 1$.

Example 25. *Show that if a is any positive integer, then $a^2 + a + 1$ is not a square number.*

Solution. Since, we have

$a^2 < a^2 + a + 1$

$< a^2 + 2a + 1 = (a+1)^2$

The next square number greater than a^2 is $(a+1)^2$.

Hence, $a^2 + a + 1$ is not a square number.

Note

If an integer a is a square of some other integer, then a is called a square number.

Example 26. *Prove that $2 \cdot 7^n + 3 \cdot 5^n - 5$ is a multiple of 24.*

Or

Prove that $24 \mid 2 \cdot 7^n + 3 \cdot 5^n - 5$.

Solution. Let $f(n) = 2 \cdot 7^n + 3 \cdot 5^n - 5$

Put $n = 1$,

$f(1) = 2 \cdot 7 + 3 \cdot 5 - 5$

$= 14 + 15 - 5$

$= 24$ which is multiple of 24.

Therefore the result is true for $n = 1$.

Let $f(n)$ be a multiple of 24 for some n.
Therefore, there exists an integer k such that

$$f(n) = 24k$$

$$\Rightarrow \quad 2\cdot7^n + 3\cdot5^n - 5 = 24k$$

$$\Rightarrow \quad 2\cdot7^n = 24k - 3\cdot5^n + 5$$

Changing n to $(n+1)$, we get

$$f(n+1) = 2\cdot7^{n+1} + 3\cdot5^{n+1} - 5$$
$$= 2\cdot7^n\cdot7 + 3\cdot5^n\cdot5 - 5$$
$$= 7\cdot2\cdot7^n + 15\cdot5^n - 5$$

Putting the value of $2\cdot7^n$ from (1) in (2), we get

$$f(n+1) = 7\,[24k - 3\cdot5^n + 5] + 15\cdot5^n - 5$$
$$= 168k - 21\cdot5^n + 35 + 15\cdot5^n - 5$$
$$= 168k - 6\cdot5^n + 30$$
$$= 168k - 6\,[5^n - 5]$$
$$= 168k - 30\,(5^{n-1} - 1)$$
$$= 168k - 30\,(5^{n-1} - 1^{n-1})$$
$$= 168k - 30\,(5-1)\,(5^{n-2} + 5^{n-3} + \ldots\ldots + 1^{n-2})$$
$$= 168k - 120\,(5^{n-2} + 5^{n-3} + \ldots\ldots + 1)$$
$$= 24\,[7k - 5\,(5^{n-2} + 5^{n-3} + \ldots\ldots + 1)]$$

which is a multiple of 24

$\therefore$ $f(n+1)$ is multiple of 24 whenever $f(n)$ is a multiple of 24.

But $f(1)$ is also a multiple of 24.

Therefore, by induction on n, $f(n)$ is a multiple of 24 for all n.

Example 27. *If $a \mid b$ and $b \neq 0$, then $|b| \geq |a|$.*

Solution. We have $a \mid b$

$\Rightarrow$ $b = ac$ for some $c \in Z$.

Since $b \neq 0$, therefore $c \neq 0$ and consequently $|c| \geq 1$.

Now $b = ac$

$\Rightarrow$ $|b| = |ac| = |a|\,|c|$.

Further $|c| \geq 1 \Rightarrow |a| \cdot |c| \geq |a|$

$\Rightarrow$ $|b| \geq |a|$.

Example 28. *If a is an odd integer, then $24 \mid a\,(a^2 - 1)$.*

Solution. Since $a\,(a^2 - 1) = a\,(a-1)\,(a+1)$.

But $(a-1)\,(a+1)$ are two consecutive even numbers;

hence one of them is divisible by 2 and the other by 4.

Again $a-1, a, a+1$ are three consecutive numbers hence one of them is divisible by 3.

Hence $24\ (= 2\cdot4\cdot3) \mid a\,(a^2 - 1)$.

Example 29. *If a is an arbitrary integer show that $360 \mid a^2\,(a^2-1)\,(a^2-4)$.*

Solution. $a^2\,(a^2-1)\,(a^2-4) = a^2\,(a-1)\,(a+1)\,(a-2)\,(a+2)$

$$= (a-2)\,(a-1)\,a\,(q+1)\,(a+2)\,(a+3-3)$$
$$= (a-2)\,(a-1)\,a\,(a+1)\,(a+2)\,(a+3)$$
$$- 3\,(a-2)\,(a-1)\,a\,(a+1)\,(a+2) \quad \ldots.(1)$$

Now $6! \mid (a-2)\,(a-1)\,a\,(a+1)\,(a+2)\,(a+3)$

$\Rightarrow$ $720 \mid (a-2)\,(a-1)\,a\,(a+1)\,(a+2)\,(a+3)$ ....(2)

$\Rightarrow$ $360 \mid (a-2)\,(a-1)\,a\,(a+1)\,(a+2)\,(a+3)$ ....(2)

Again $5! \mid (a-2)\,(a-1)\,a\,(a+1)\,(a+2)$

$\Rightarrow$ $120 \mid (a-2)\,(a-1)\,a\,(a+1)\,(a+2)$ ....(3)

$\Rightarrow$ $360 \mid 3\,(a-2)\,(a-1)\,a\,(a+1)\,(a+2)$

From (1), (2) and (3), we get

$360 \mid a^2\,(a^2-1)\,(a^2-4)$.

Example 30. *Prove that $8 \mid 5^{2n} + 7$ by using induction method.*

Solution. Let $f(n) = 5^{2n} + 7$

Put $n = 1$,

$$f(1) = 5^2 + 7$$
$$= 25 + 7 = 32$$

which is a multiple of 8.

Therefore the result is true for $n = 1$.

Let $f(n)$ be a multiple of 8 for some n,

therefore there exists an integer k such that

$$f(n) = 8k$$
$$\Rightarrow \quad 5^{2n} + 7 = 8k$$
$$\Rightarrow \quad 5^{2n} = 8k - 7.$$

Changing n to $(n+1)$, we get

$$f(n+1) = 5^{2(n+1)} + 7$$
$$= 5^{2n} \cdot 5^2 + 7$$
$$= 5^2 (5^{2n}) + 7$$

Putting the value of $5^{2n} = 8k - 7$ from (1) into (2), we get

$$f(n+1) = 5^2 (8k - 7) + 7$$
$$= 200k - 175 + 7$$
$$= 200k - 168$$
$$= 8 (25k - 21)$$

which is a multiple of 8.

$\therefore$ $f(n+1)$ is also a multiple of 8.

Therefore by induction on n, $f(n)$ is a multiple of 8 for all n.

i.e $\quad 8 \mid 5^{2n} + 7.$

Example 31. *Use mathematical induction to show that*

$$5 \mid 3^{3n+1} + 2^{n+1}$$

Solution. Let $f(n) = 3^{3n+1} + 2^{n+1}$

Put $n = 1$,

$$f(1) = 3^{3+1} + 2^{1+1}$$
$$= 3^4 + 2^2$$
$$= 81 + 4 = 85$$

which is a multiple of 5.

Therefore the result is true for $n = 1$.

Let $f(n)$ be a multiple of 5 for some n.

Therefore there exists an integer k such that

$$f(n) = 5k$$
$$\Rightarrow \quad 3^{3n+1} + 2^{n+1} = 5k$$

$$\Rightarrow \quad 3^{3n+1} = 5k - 2^{n+1} \quad \ldots(1)$$

Changing n to $(n+1)$, we get

$$f(n+1) = 3^{3(n+1)+1} + 2^{(n+1)+1}$$
$$= 3^{(3n+3)+1} + 2^{n+2}$$
$$= 3^{3n} \cdot 3^4 + 2^n \cdot 2^2$$
$$= 3^{3n} \cdot 3 \cdot 3^3 + 2^n \cdot 2^2 \quad \ldots(2)$$
$$= 3^{3n+1} \cdot 3^3 + 2^n \cdot 4$$

Putting the value of $3^{3n+1} = 5k - 2^{n+1}$ from (1) into (2), we have

$$f(n+1) = (5k - 2^{n+1}) \cdot 3^3 + 2^n \cdot 4$$
$$= 5k \cdot 3^3 - 2^{n+1} \cdot 3^3 + 2^n \cdot 4$$
$$= 135k - 2^n \cdot 2 \cdot 27 + 2^n \cdot 4$$
$$= 135k - 54 \cdot 2^n + 4 \cdot 2^n$$
$$= 135k - 50 \cdot 2^n$$
$$= 5 (27k - 10 \cdot 2^n)$$

which is a multiple of 5.

$\therefore$ $f(n+1)$ is a multiple of 5 whenever $f(n)$ is a multiple of 5.

But $f(1)$ is also a multiple of 5.

Therefore, by induction on n,

$f(n)$ is a multiple of 5

i.e $\quad 5 \mid 3^{3n+1} + 2^{2n+1}.$

Example 32. Use induction method to solve $21 \mid 4^{n+1} + 5^{2n-1}$.

Solution. Let $f(n) = 4^{n+1} + 5^{2n-1}$

Put $n = 1$,

$$f(1) = 4^{1+1} + 5^{2-1}$$
$$= 4^2 + 5$$
$$= 16 + 5$$
$$= 21$$

which is a multiple of 21.

Therefore the result is true for $n = 1$.

Let $f(n)$ be a multiple of 21 for some n.

Therefore there exists an integer k such that

$$f(n) = 21k$$

$$\Rightarrow \quad 4^{n+1} + 5^{2n-1} = 21k$$

$$\Rightarrow \quad 4^{n+1} = 21k - 5^{2n-1}$$

Changing n to $(n+1)$, we get

$$f(n+1) = 4^{(n+1)+1} + 5^{2(n+1)-1}$$

$$= 4^{n+1} \cdot 4 + 5^{(2n+2-1)}$$

$$= 4^{n+1} \cdot 4 + 5^{2n+1}$$

$$= 4\,(4^{n+1}) + 5^{2n} \cdot 5$$

Putting the value of 4^{n+1} from (1) in (2), we get

$$f(n+1) = 4\,[21k - 5^{2n-1}] + 5 \cdot 5^{2n}$$

$$= 84k - 4 \cdot 5^{2n-1} + 5 \cdot 5^{2n}$$

$$= 84k - 4 \cdot 5^{2n} \cdot 5^{-1} + 5 \cdot 5^{2n}$$

$$= 84k - 5^{2n}\,(4 \cdot 5^{-1} - 5)$$

$$= 84k - 5^{2n}\left(\frac{4}{5} - 5\right)$$

$$= 84k - 5^{2n}\left(-\frac{21}{5}\right)$$

$$= 84k + 5^{2n-1} \cdot 21$$

$$= 21\,(4k + 5^{2n-1})$$

which is a multiple of 21.

$\therefore$ $f(n+1)$ is a multiple of 21 whenever $f(n)$ is a multiple of 21.

But $f(1)$ is also a multiple of 21.

Therefore by induction on n, $f(n)$ is a multiple of 21 for all n.

i.e $\quad 21 \mid 4^{n+1} + 5^{2n-1}$.

Example 33. Use induction method to show that $15 \mid 2^{4n} - 1$.

Solution. Let $f(n) = 2^{4n} - 1$

Put $n = 1$.

$$\therefore \quad f(1) = 2^4 - 1$$

$$= 15$$

which is a multiple of 15.

Therefore the result is true for $n = 1$.

Let $f(n)$ be a multiple of 15 for some n.

Therefore there exists an integer k such that

$$f(n) = 15k$$

$$\Rightarrow \quad 2^{4n} - 1 = 15k \qquad \ldots(1)$$

$$\Rightarrow \quad 2^{4n} = 15k + 1$$

Changing n to $(n+1)$, we get

$$f(n+1) = 2^{4(n+1)} - 1$$

$$= 2^{4n+4} - 1 \qquad \ldots(2)$$

$$= 2^{4n} \cdot 2^4 - 1$$

Putting the value of 2^{4n} from (1) into (2), we get

$$f(n+1) = (15k+1) \cdot 2^4 - 1$$

$$= 2^4 \cdot 15k + 2^4 - 1$$

$$= 15k\,(2^4) + 15$$

$$= 15\,[16k + 1]$$

which is a multiple of 15.

$\therefore$ $f(n+1)$ is multiple of 15 whenever $f(n)$ is a multiple of 15.

But $f(1)$ is also a multiple of 15.

Therefore by induction on n, $f(n)$ is a multiple of 15 for all n.

i.e $\quad 15 \mid 2^{4n} - 1$.

Example 34. Prove that the product of three consecutive integers is divisible by 6.

Solution. Let $(n-1)$, n and $(n+1)$ be the three consecutive integers.

Since $(n-1)\,n\,(n+1)$ is the product of three consecutive integers is divisible by $3! = 6$.

$\therefore$ $n\,(n-1)\,(n+1)$ is divisible by 6.

Example 35. *Prove that the product of any four consecutive integers is divisible by 24.*

Solution. Let $(n-1)$, n, $(n+1)$ and $(n+2)$ be the four consecutive integers.

Since $(n-1)\,n\,(n+1)\,(n+2)$ is the product of four consecutive integers is divisible by $4! = 24$.

$\therefore$ $(n-1)\,n\,(n+1)\,(n+2)$ is divisible by 24.

Example 36. *For an arbitrary integer a, verify $2 \mid a\,(a+1)$.*

Solution. Since a is an integer,

$\therefore$ a is even or a is odd.

a is even

So let $a = 2k$

$\therefore$ $a\,(a+1) = 2k\,(2k+1)$

$= 2\,[k\,(2k+1)]$

= an even integer which is divisible by 2.

a is odd

So let $a = 2k+1$

$\therefore$ $a\,(a+1) = (2k+1)\,(2k+1+1)$

$= (2k+1)\,(2k+2)$

$= 2\,(2k+1)\,(k+1)$

= an even integer which is divisible by 2.

Hence $2 \mid a\,(a+1)$ where a is any integer.

Example 37. *If n is an odd number, prove that $n^2 - 1$ is divisible by 8.*

Solution. Let $n = 2k+1$

Now $n^2 - 1 = (2k+1)^2 - 1$

$= 4k^2 + 1 + 4k - 1$

$= 4k^2 + 4k$

$= 4k\,(k+1)$

Since $k\,(k+1)$ being the product of two consecutive numbers is divisible by $2! = 2$

$\therefore$ $4k\,(k+1)$ is divisible by $4 \times 2 = 8$.

Hence $n^2 - 1$ is divisible by 8, if n is an odd number.

Example 38. *Show that 4 does not divide $(n^2 + 2)$ for any integer n.*

Solution. Since n is an integer.

$\therefore$ either n is even or n is odd.

n is even,

So let $n = 2k$

$\therefore$ $n^2 + 2 = (2k)^2 + 2$

$= 4k^2 + 2$

$= 2\,(2k^2 + 1)$

= 2 (an odd integer)

which is not divisible by 4.

n is odd,

So let $n = 2k+1$

$\therefore$ $n^2 + 2 = (2k+1)^2 + 2$

$= 4k^2 + 1 + 4k + 2$

$= (4k^2 + 4k + 2) + 1$

$= 2\,(2k^2 + 2k + 1) + 1$

which being an odd integer is not divisible by 4.

Example 39. *Prove that the product of two odd numbers is always an odd number.*

Solution. Let $a = 2k+1$,

$b = 2k' + 1$.

be two odd numbers.

$\therefore$ $ab = (2k+1)\,(2k'+1)$

$= 4kk' + 2k + 2k' + 1$

$= 2\,(2kk' + k + k') + 1$

$= 2r + 1$,

where $r = 2kk' + k + k'$

$\therefore$ ab is an odd integer.

Example 40. *Show that the sum of an integer and its square is even.*

Solution. Let n be any integer.

We shall prove that $n^2 + n$ is even.

$n^2 + n = n(n+1)$ which is the product of two consecutive integers n and $(n+1)$ and hence it is divisible by $2! = 2$.

Hence $n^2 + n$ is an even number.

Example 41. *If a, b are odd, prove that $a^2 + b^2$ is even but not a multiple of 4.*

Solution. Let $a = 2k + 1$,

$\therefore \quad b = 2k' + 1$

Now $a^2 + b^2 = (2k+1)^2 + (2k'+1)^2$

$= 4k^2 + 1 + 4k + 4k'^2 + 1 + 4k'$

$= 4k^2 + 4k'^2 + 4k + 4k' + 2$

$= 4(k^2 + k'^2) + 4(k + k') + 2$

$= 2[2(k^2 + k'^2) + 2(k + k') + 1]$

which is clearly an even number but it is not divisible by 4.

Therefore, it is not a multiple of 4.

Example 42. *Prove that square of each odd number is of the form $8k + 1$.*

Solution. Let $n = 2m + 1$ be an odd number.

$\therefore \quad n^2 = (2m+1)^2$

$= 4m^2 + 4m + 1$

$= 4m(m+1) + 1$

Now $m(m+1)$ being the product of two consecutive integers is divisible by $2! = 2$

$\therefore \quad m(m+1) = 2k$

Thus $n^2 = 4(2k) + 1$

$= 8k + 1.$

Example 43. *If a and b are odd integers, then prove that 16 divides $a^4 + b^4 - 2$.*

Solution. First we show that square of any integer is of the form

$8k$, $8k + 1$ or $8k + 4$.

By dividing any integer n by 4, n can be one of the forms

$4k$, $4k + 1$, $4k + 2$ or $4k + 3$.

when $n = 4k$,

$n^2 = 16k^2 = 8k'$ where $k' = 2k^2 \in Z$

when $n = 4k + 1$.

$n^2 = 16k^2 + 8k + 1 = 8(2k^2 + k) + 1$

$= 8k' + 1$, where $k' = 2k^2 + k \in Z$

when $n = 4k + 2$,

$n^2 = 16k^2 + 16k + 4$

$= 8(2k^2 + 2k) + 4$

$= 8k' + 4$, where $k' = 2k^2 + 2k \in Z$

when $n = 4k + 3$,

$n^2 = 16k^2 + 24k + 9$

$= 8(2k^2 + 3k + 1) + 1$

$= 8k' + 1$ where $k' = 2k^2 + 3k + 1 \in Z$.

Hence n^2 is of the form $8k$, $8k + 1$ or $8k + 4$.

Since a and b are odd and square of an odd integer is odd.

$\therefore \quad a^2 = 8k + 1, b^2 = 8k' + 1$, for some $k, k' \in Z$.

$\therefore \quad a^4 + b^4 - 2 = (8k+1)^2 + (8k'+1)^2 - 2$

$= 64k^2 + 16k + 1 + 64k'^2 + 16k' + 1 - 2$

$= 16(4k^2 + 4k'^2 + k + k')$

$\Rightarrow \quad 16 \mid a^4 + b^4 - 2$

i.e if a and b are odd integers, then 16 divides $a^4 + b^4 - 2$.

Example 44. *Prove that gcd $(a, a + k)$ divides k for all integers, where a, k are not both zero.*

Solution. Let gcd $(a, a + k) = d$

Then $d \mid a$ and $d \mid (a + k)$

$\Rightarrow \quad d \mid \{(a + k) - a\}$

$\Rightarrow \quad d \mid k$

Hence d divides k.

Example 45. *If gcd $(a, m) = 1$, prove that gcd $(m - a, m) = 1$.*

Solution. Let gcd $(m - a, m) = d$

$\Rightarrow \quad d \mid (m - a)$ and $d \mid m$

$\Rightarrow \quad d \mid \{m - (m - a)\}$

$\Rightarrow \quad d \mid a$

Now $d \mid m$ and $d \mid a$

$\Rightarrow \quad d \mid gcd\,(a, m)$

[$\because$ d is a common divisor of a and m so d divides the gcd of a,

But $gcd\,(a, m) = 1$ (given)

$\therefore \quad d \mid 1$

$\Rightarrow \quad d = 1$ [since only divisor of 1 is

Hence $gcd\,(m - a, m) = 1$

Example 46. *If a and b are odd integers then $8 \mid (a^2 - b^2)$.*

Solution. Let $a = 2k + 1$,

$b = 2k' + 1$

Now $a^2 - b^2 = (2k + 1)^2 - (2k' + 1)^2$

$= 4k^2 + 1 + 4k - 4k'^2 - 1 - 4k'$

$= 4k^2 + 4k - 4k'^2 - 4k'$

$= 4k\,(k + 1) - 4k'\,(k' + 1)$

Since $k\,(k + 1)$ being the product of two consecutive numbers is divisible by $2! = 2$

$\therefore \quad 4k\,(k + 1)$ is divisible by $4 \times 2 = 8$

Similarly $k'\,(k' + 1)$ is the product of two consecutive numbers is divisible by $2! = 2$

$\therefore \quad 4k'\,(k' + 1)$ is divisible by $4 \times 2 = 8$.

Therefore, $4k\,(k + 1) - 4k'\,(k' + 1)$ is divisible by 8.

Hence $8 \mid (a^2 - b^2)$ if a and b are odd integers.

Example 47. *If a and b are integers, not both of which are zero, verify that*

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

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

and $\quad g = gcd\,(a, b + ax)$.

It is clear that $gcd\,(b, a) = gcd\,(a, -b) = d$.

Since we know that if $a \mid b$ and $a \mid c$ imply that $a \mid (bx + cy)$ for any integers x and and $a \mid b$ and $b \mid a$ imply $a = \pm b$, we obtain $d \mid g$ and $g \mid d$

$\Rightarrow \quad d = g$.

Hence the solution.

Example 48. *Prove that the su*

square.

Solution. Let a and b be two o

Let $\quad a = 2k + 1$,

$b = 2k' + 1$

Now $\quad a^2 + b^2 = (2k + 1)^2$

$= 4k^2 + 1$

$= 4k^2 + 4$

$= 4\,(k^2 +$

$= 2\,[2\,(k^2$

which is clearly an even

Example 49. *Prove that, for*

hence $gcd\,(a, a + 1) = 1$.

Solution. Let $gcd\,(a, a + n)$

Then $d \mid a$ and $d \mid (a +$

$\Rightarrow \quad d \mid \{(a + n) - a$

$\Rightarrow \quad d \mid n$

Hence d divides n

i.e. $gcd\,(a, a + n)$ divi

Again let $gcd\,(a, a +$

$\Rightarrow \quad d \mid a$ and $d \mid (a$

$\Rightarrow \quad d \mid \{(a + 1) -$

$\Rightarrow \quad d \mid 1$

$\Rightarrow \quad d = 1$

$\Rightarrow \quad gcd\,(a, a + 1)$

Example 50. *Given inte*

$c = ax + by$ if and only i

Solution. Let $d = gcd\,($

Let us suppose that

Then by definition

Also $\quad d = gcd\,(a,$

$\Rightarrow \exists$ integers u, v

Example 48. Prove that the sum of the squares of two odd integers cannot be a perfect square.

Solution. Let a and b be two odd integers.

Let $a = 2k + 1$,

$b = 2k' + 1$

Now $a^2 + b^2 = (2k + 1)^2 + (2k' + 1)^2$

$= 4k^2 + 1 + 4k + 4k'^2 + 1 + 4k'$

$= 4k^2 + 4k'^2 + 4k + 4k' + 2$

$= 4(k^2 + k'^2) + 4(k + k') + 2$

$= 2[2(k^2 + k'^2) + 2(k + k') + 1]$

which is clearly an even number but it is not perfect square.

Example 49. Prove that, for a positive integer n and any integer a, gcd $(a, a + n)$ divides n, hence gcd $(a, a + 1) = 1$.

Solution. Let gcd $(a, a + n) = d$

Then $d \mid a$ and $d \mid (a + n)$

$\Rightarrow \quad d \mid \{(a + n) - a\}$

$\Rightarrow \quad d \mid n$

Hence d divides n

i.e. gcd $(a, a + n)$ divides n.

Again let gcd $(a, a + 1) = d$

$\Rightarrow \quad d \mid a$ and $d \mid (a + 1)$

$\Rightarrow \quad d \mid \{(a + 1) - a\}$

$\Rightarrow \quad d \mid 1$

$\Rightarrow \quad d = 1$

$\Rightarrow \quad gcd\,(a, a + 1) = 1.$

Example 50. Given integers a and b, prove that there exists integers x and y for which $c = ax + by$ if and only if gcd $(a, b) \mid c$.

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

Let us suppose that $d \mid c$.

Then by definition of divisibility there exists $t \in Z$ such that $c = td$.

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

$\Rightarrow \exists$ integers u, v such that $d = au + bv$

$\therefore \quad td = t(au + bv)$

$= a(tu) + b(tv)$

$\Rightarrow \quad c = a(tu) + b(tv)$

Taking $x = tu$ and $y = tv$, we have

$c = ax + by$

Or $\quad ax + by = c$

Conversely, suppose that $ax + by = c$ has a solution say (x_0, y_0), then

$c = ax_0 + by_0$

Now by corollary, "For any two integers a and b at least one of which is non-zero, set $T = \{ax + by : x, y \in Z\}$ consists of multiples of (a, b)", $ax_0 + by_0$ is a multiple of say

$ax_0 + by_0 = rd.$

$\therefore$ (1) becomes $c = rd$

$\Rightarrow d \mid c$ by definition of divisibility.

Example 51. *Prove that* $2^{4n} - 1$ *is divisible by* 15.

Solution. $2^{4n} - 1 = (2^4)^n - 1$

$= 16^n - 1^n$

$= (16 - 1)[(16)^{n-1} + (16)^{n-2} \cdot 1 + \ldots + 1^{n-1}]$

$[\because x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \ldots + y^{n-1})$ for all $n]$

Or $\quad 2^{4n} - 1 = 15[(16)^{n-1} + (16)^{n-2} + \ldots + 1]$

Therefore, by definition of divisibility $2^{4n} - 1$ is divisible by 15.

Example 52. *Give an odd integer a, establish that*

$a^2 + (a + 2)^2 + (a + 4)^2 + 1$ *is divisible by* 12.

Solution. *Since* a *is an odd integer, so let* $a = 2k + 1$.

Now, $\quad a^2 + (a + 2)^2 + (a + 4)^2 + 1$

$= (2k + 1)^2 + (2k + 1 + 2)^2 + (2k + 1 + 4)^2 + 1$

$= (2k + 1)^2 + (2k + 3)^2 + (2k + 5)^2 + 1$

$= 4k^2 + 1 + 4k + 4k^2 + 9 + 12k + 4k^2 + 25 + 20k + 1$

$= 12k^2 + 36k + 36$

$= 12(k^2 + 3k + 3)$

which is a multiple of 12 so it is divi

Hence, $a^2 + (a + 2)^2 + (a + 4)^2 + 1$ is

Theorem 10. ***If*** $a = bq + r$, ***prove that*** g

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

and $\quad gcd(b, r) = g$

Since $\quad gcd(a, b) = d$

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

$\Rightarrow \quad d \mid a$ and $d \mid bq$

$\Rightarrow \quad d \mid (a - bq)$

$\Rightarrow \quad d \mid r$

$\therefore$ d is a common divisor of b a

$\therefore \quad d \mid g \qquad [\because g$ is th

Again since $gcd(b, r) = g$

$\Rightarrow \quad g \mid b$ and $g \mid r$

$\Rightarrow \quad g \mid bq$ and $g \mid r$

$\Rightarrow \quad g \mid bq + r$

$\Rightarrow \quad g \mid a$

$\Rightarrow g$ is a common divisor of

$\therefore \quad g \mid d \qquad [\because d$ i

From (1) and (2), we have d

i.e $\quad gcd(a, b) = gcd(b,$

Note

The above theorem can als

gcd of a and b is the sam

dividing a by b.

Theorem 11. ***If*** $k > 0$, ***then*** g

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

Then $\quad d \mid a$ and $d \mid b$

$\Rightarrow \quad kd \mid ka, kd \mid kb$

$= 12k^2 + 36k + 36$

$= 12(k^2 + 3k + 3)$

which is a multiple of 12 so it is divisible by 12.

Hence, $a^2 + (a+2)^2 + (a+4)^2 + 1$ is divisible by 12 if a is an odd integer.

Theorem 10. *If $a = bq + r$, prove that $gcd(a, b) = gcd(b, r)$.*

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

and $gcd(b, r) = g$

Since $gcd(a, b) = d$ (by definition of gcd)

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

$\Rightarrow$ $d \mid a$ and $d \mid bq$

$\Rightarrow$ $d \mid (a - bq)$ $(\because a - bq = r)$

$\Rightarrow$ $d \mid r$

$\therefore$ d is a common divisor of b and r. ....(1)

$\therefore$ $d \mid g$ [$\because$ g is the gcd of b and r]

Again since $gcd(b, r) = g$ [by definition of gcd]

$\Rightarrow$ $g \mid b$ and $g \mid r$

$\Rightarrow$ $g \mid bq$ and $g \mid r$

$\Rightarrow$ $g \mid bq + r$ $(\because a = bq + r)$

$\Rightarrow$ $g \mid a$

$\Rightarrow g$ is a common divisor of a and b ....(2)

$\therefore$ $g \mid d$ [$\because$ d is the gcd of a and b]

From (1) and (2), we have $d = g$

i.e $gcd(a, b) = gcd(b, r)$.

Note

The above theorem can also be asked as follows :

gcd of a and b is the same as gcd of b and r, where r is the remainder obtained on dividing a by b.

Theorem 11. *If $k > 0$, then $gcd(ka, kb) = k\, gcd(a, b)$.*

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

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

$\Rightarrow$ $kd \mid ka, kd \mid kb$

Also there exists integers x and y such that

$$d = ax + by$$

$$\Rightarrow \quad kd = kax + kby$$

Let $c \mid ka,\ c \mid kb$

$$\Rightarrow \quad c \mid kax,\ c \mid kby$$

$$\Rightarrow \quad c \mid (kax + kby)$$

$$\Rightarrow \quad c \mid kd$$

$$\Rightarrow \quad gcd\ (ka, kb) = kd$$

$$\Rightarrow \quad gcd\ (ka, kb) = k\ gcd\ (a, b)$$

Hence the result.

Theorem 12. ***If gcd*** $(a, b) = d$ ***then gcd*** $(ka, kb) = |k|\ gcd\ (a, b)$.

For any integer $k \neq 0$, ***gcd*** $(ka, kb) = |k|\ gcd\ (a, b)$.

Or

Proof. Let $gcd\ (ka, kb) = d_1$

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

therefore there exist integers x, y such that

$$d = ax + by$$

$$\Rightarrow \quad kd = (ka)\ x + (kb)\ y \qquad \ldots(1)$$

Now $d_1 = gcd\ (ka, kb)$

$$\Rightarrow \quad d_1 \mid ka \text{ and } d_1 \mid kb$$

$$\Rightarrow \quad d_1 \mid [(ka)\ x + (kb)\ y]$$

$$\Rightarrow \quad d_1 \mid kd \qquad \text{[from (1)]} \qquad \ldots(2)$$

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

$$\Rightarrow \quad d \mid a,\ d \mid b$$

$$\Rightarrow \quad kd \mid ka,\ kd \mid kb$$

$\Rightarrow$ kd is a common divisor of ka and kb.

But d_1 is the gcd of ka and kb.

So by definition of gcd, we have

$$kd \mid d_1 \qquad \ldots(3)$$

From (2) and (3), we have

$$d_1 = \pm kd$$

Since d and d_1 are both positive, therefore

$$d_1 = |k|\ d.$$

LEAST COMMON MULTIPLE

Definition. *Let a and b be two non-zero integers. The* ***least common multiple*** *(LCM) of a and b is the unique positive integer m such that*

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

(ii) $a \mid g$, $b \mid g \Rightarrow m \mid g$.

If m is the L.C.M. of a and b, then in symbols, we write

$$m = [a, b]$$

e.g. $[16, 12] = 48$.

Note

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

(ii) If $(a, b) = d$ and $[a, b] = m$, then $d \mid m$

(iii) If $(a, b) = d$ and $[a, b] = m$, then $dm = |ab|$

Theorem 13. ***For positive integers a and b***

gcd (a, b) ***lcm*** $(a, b) = ab$.

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

$$m = lcm\ (a, b)$$

Since $d = gcd\ (a, b)$ [by definition of gcd]

$$\Rightarrow \quad d \mid a \text{ and } d \mid b$$

Since $d \mid a$

$\Rightarrow \exists$ integer r such that

$$a = dr$$

Also $d \mid b \Rightarrow \exists$ integer s such that

$$b = ds$$

$$\therefore \quad a = dr,$$

$$b = ds \text{ and } gcd\ (r, s) = 1 \qquad \ldots(1)$$

Since $d = gcd\ (a, b)$.

$\Rightarrow \exists$ integers u and v such that

$$d = au + bv$$

Also $m = lcm\ (a, b) = [a, b]$

$\Rightarrow$ $\exists$ integers t and w such that

$m = at$ and $m = bw$

Now $d = au + bv$

$\Rightarrow$ $md = m(au + bv)$

$\Rightarrow$ $md = mau + mbv$

$= bwau + atbv$

$= ab(wu + tv)$ [from

$\Rightarrow$ $ab \mid md$

Also, $\frac{ab}{d} = \frac{drb}{d} = rb$

and $\frac{ab}{d} = \frac{ads}{d} = as$ [by

$\therefore$ $a \mid \frac{ab}{d}, b \mid \frac{ab}{d}$; [by

i.e $\frac{ab}{d}$ is a common multiple of a and b.

$\Rightarrow$ $m \mid \frac{ab}{d}$ or $md \mid ab$ ....

From (3) and (4), we have

$md = ab$

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

$\Rightarrow$ $lcm(a, b)\ gcd(a, b) = ab$

$\Rightarrow$ $gcd(a, b)\ lcm(a, b) = ab$

Hence the pro

Corollary. *For any choice of positive integers a and b,*

$lcm(a, b) = ab$ *if and only if* $gcd(a, b) = 1$.

Proof. From the above theorem, we get

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

But $gcd(a, b) = 1$,

therefore, we have

$lcm(a, b) = ab$

i.e. the least common multiple of a and b is their product.

Example 53. *Find the gcd of 275 and 200 and express it in the form* $275x + 200y$.

Solution. $275 = 200 \cdot 1 + 75$, ...(1)

$200 = 75 \cdot 2 + 50$, ...(2)

$75 = 50 \cdot 1 + 25$, ...(3)

$50 = 25 \cdot 2 + 0$ ....(4)

Hence $gcd(275, 200) = 25$

i.e $d = 25$.

Now substituting the value of 25 from (3), we get

$25 = 75 - 50 \cdot 1$

$= 75 - [200 - 75 \cdot 2] \cdot 1$ [from (2)]

$= 75 - 200 \cdot 1 + 75 \cdot 2$

$= 75 \cdot 3 - 200 \cdot 1$

$= [275 - 200 \cdot 1] \cdot 3 - 200 \cdot 1$ [from (1)]

$= 275 \cdot 3 - 200 \cdot 3 - 200 \cdot 1$

$= 275 \cdot 3 - 200 \cdot 4$

$= 3 \cdot 275 + (-4) \cdot 200$

Hence $gcd(275, 200) = 3 \cdot 275 + (-4) \cdot 200$

so that $x = 3$ and $y = -4$.

Example 54. *Find the gcd of 595 and 252 and express d in the form* $252x + 595y$.

Solution. $595 = 2 \cdot 252 + 91$, ...(1)

$252 = 2 \cdot 91 + 70$, ...(2)

$91 = 1 \cdot 70 + 21$, ...(3)

$70 = 3 \cdot 21 + 7$, ...(4)

$21 = 7 \cdot 3 + 0$ ....(5)

Therefore, *gcd* of 595 and 252 is $d = 7$.

From (4),

$d = 7 = 70 - 3 \cdot 21$ [from (3)

$= 70 - 3(91 - 1 \cdot 70)$

$= 70 - 3 \cdot 91 + 3 \cdot 70$

$= 4 \cdot 70 - 3 \cdot 91$

$= 4(252 - 2 \cdot 91) - 3 \cdot 91$

$= 4 \cdot 252 - 8 \cdot 91 - 3 \cdot 91$

$= 4 \cdot 252 - 11 \cdot 91$ [from

$= 4 \cdot 252 - 11(595 - 2 \cdot 252)$

$= 4 \cdot 252 - 11 \cdot 595 + 22 \cdot 252$

$= 26 \cdot 252 - 11 \cdot 595$ [from

i.e $d = 252x + 595y$

Here $x = 26, y = -11$.

Example 55. *Find the gcd of* 54 *and* 35 *and express it in the form* $54x + 35y$.

Solution. $54 = 35 \cdot 1 + 19,$

$35 = 19 \cdot 1 + 16,$

$19 = 16 \cdot 1 + 3,$

$16 = 3 \cdot 5 + 1,$

$3 = 3 \cdot 1 + 0$

$\therefore$ *gcd* of 54 and 35 is $d = 1$.

From (4), $d = 1 = 16 - 3 \cdot 5$

$= 16 - [19 - 16 \cdot 1] \cdot 5$

$= 16 - 19 \cdot 5 + 16 \cdot 5$ [from (

$= 6 \cdot 16 - 19 \cdot 5$

$= 6 \cdot (35 - 19 \cdot 1) - 19 \cdot 5$ [from (

$= 6 \cdot 35 - 6 \cdot 19 - 19 \cdot 5$

$= 6 \cdot 35 - 11 \cdot 19$

$= 6 \cdot 35 - 11(54 - 35 \cdot 1)$ [from (

$= 6 \cdot 35 - 11 \cdot 54 + 11 \cdot 35$

$= 17 \cdot 35 - 11 \cdot 54$

Hence $gcd(54, 35) = 54(-11) + 35(17)$

$= 54x + 35y,$

where $x = -11,$

$y = 17.$

Example 56. *If* $d > 0, d \mid a$ *and* $d \mid b$ *i.e* d *is the common divisor of* a *and* b, $gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, *show that* $gcd(a, b) = d$.

Solution. Let $gcd(a, b) = d_1$.

Since $d \mid a$ and $d \mid b$ (given) ....(1)

Since d_1 is the *gcd* of a and b,

$\therefore \quad d \mid d_1$

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

$\Rightarrow \exists$ integers x and y such that

$1 = x \cdot \frac{a}{d} + y \cdot \frac{b}{d}$ ....(2)

$\Rightarrow \quad d = ax + by$

Now $d_1 = gcd(a, b)$

$\Rightarrow \quad d_1 \mid a$ and $d_1 \mid b$

$\Rightarrow \quad d_1 \mid (ax + by)$ ....(3)

$\Rightarrow \quad d_1 \mid d$ [by (2)]

From (1) and (3), we have

$d_1 = \pm d$

But d_1 and d are both positive,

$\therefore \quad d_1 = d$

Hence $gcd(a, b) = d$.

Example 57. *Find the gcd of* 12378 *and* 3054 *and express it in the form* $12378x + 3054y$.

Solution. $12378 = 4 \cdot 3054 + 162,$ ....(1)

$3054 = 18 \cdot 162 + 138,$ ....(2)

$162 = 1 \cdot 138 + 24,$ ....(3)

$138 = 5 \cdot 24 + 18,$ ....(4)

$24 = 1 \cdot 18 + 6,$ ....(5)

$18 = 3 \cdot 6 + 0$ ....(6)

Therefore, *gcd* of 12378 and 3054 is $d = 6$.

From (5),

$$\begin{aligned} d = 6 &= 24 - 1\cdot 18 \\ &= 24 - (138 - 5\cdot 24) \\ &= 24 - 138 + 5\cdot 24 \qquad [\text{from} \\ &= 6\cdot 24 - 138 \\ &= 6\,(162 - 138) - 138 \\ &= 6\cdot 162 - 6\cdot 138 - 138 \qquad [\text{from} \\ &= 6\cdot 162 - 7\cdot 138 \\ &= 6\cdot 162 - 7\,(3054 - 18\cdot 162) \\ &= 6\cdot 162 - 7\cdot 3054 + 126\cdot 162 \qquad [\text{from} \\ &= 132\cdot 162 - 7\cdot 3054 \\ &= 132\,(12378 - 4\cdot 3054) - 7\cdot 3054 \\ &= 132\cdot 12378 - 528\cdot 3054 - 7\cdot 3054 \qquad [\text{from} \\ &= 132\cdot 12378 - 535\cdot 3054 \\ &= 132\cdot 12378 + (-535)\cdot 3054 \end{aligned}$$

Hence $6 = gcd\,(12378, 3054) = 12378x + 3054y$
where $x = 132$ and $y = -535$.

Example 58. *If* $gcd\,(a, b) = 1$, *show that* $gcd\,(a + b, a - b) = 1$ *or* 2.

Solution. Let $gcd\,(a + b, a - b) = d$.

Then $d \mid (a + b)$ and $d \mid (a - b)$

$\Rightarrow$ $d \mid \{(a + b) + (a - b)\}$

and $d \mid \{(a + b) - (a - b)\}$

$\Rightarrow$ $d \mid 2a$ and $d \mid 2b$

$\Rightarrow$ d is a common divisor of $2a$ and $2b$.

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

$\Rightarrow$ $gcd\,(2a, 2b) = 2$

$\Rightarrow$ 2 is the greatest common divisor of $2a$ and $2b$.

Now d is a common divisor of $2a$, $2b$ and 2 is the greatest common divisor $2a$, $2b$.

Therefore by the definition of *gcd*, we must have $d \mid 2$ which implies that $d = 1$ or 2.

Hence $gcd\,(a + b, a - b) = 1$ or 2.

Example 59. *If* $gcd\,(a, b) = 1$, *show that* $gcd\,(a + b, a^2 - ab + b^2) = 1$ *or* 3.

Solution. Let $gcd\,(a + b, a^2 - ab + b^2) = d$ (by definition of *gcd*)

Then $d \mid (a + b)$, $d \mid (a^2 - ab + b^2)$

$\Rightarrow$ $d \mid (a + b)^2$

$\Rightarrow$ $d \mid (a^2 + b^2 + 2ab)$

Also $d \mid (a^2 - ab + b^2)$

$\Rightarrow$ $d \mid \{(a^2 + b^2 + 2ab) - (a^2 - ab + b^2)\}$

$\Rightarrow$ $d \mid 3ab$

Let $gcd\,(d, a) = e$

$\Rightarrow$ $e \mid d$ and $e \mid a$

But $d \mid (a + b)$

$\Rightarrow$ $e \mid (a + b)$

$\Rightarrow$ $e \mid \{(a + b) - a\}$

$\Rightarrow$ $e \mid b$

so $e \mid gcd\,(a, b)$

$\Rightarrow$ $e \mid 1$

$\Rightarrow$ $e = 1$

$\therefore$ $gcd\,(d, a) = 1$

Similarly $gcd\,(d, b) = 1$

$\therefore$ $d \mid 3 \Rightarrow d = 1$ or 3

Hence $gcd\,(a + b, a^2 - ab + b^2) = 1$ or 3.

Example 60. *Find the gcd of* 143 *and* 227 *or find* $gcd\,(143, 227)$.

Solution.

$$\begin{aligned} 227 &= 143\cdot 1 + 84, \\ 143 &= 84\cdot 1 + 59, \\ 84 &= 59\cdot 1 + 25, \\ 59 &= 25\cdot 2 + 9, \\ 25 &= 9\cdot 2 + 7, \\ 9 &= 7\cdot 1 + 2, \end{aligned}$$

$7 = 2 \cdot 3 + 1,$

$2 = 2 \cdot 1 + 0.$

Hence $gcd\,(143, 227) = 1$

i.e $d = 1.$

Example 61. *Find gcd* (306, 657).

Solution. $657 = 306 \cdot 2 + 45,$

$306 = 45 \cdot 6 + 36,$

$45 = 36 \cdot 1 + 9,$

$36 = 9 \cdot 4 + 0.$

Hence $gcd\,(306, 657) = 9$

i.e $d = 9.$

Example 62. *Find gcd* (272, 1479).

Solution. $1479 = 272 \cdot 5 + 119,$

$272 = 119 \cdot 2 + 34,$

$119 = 34 \cdot 3 + 17,$

$34 = 17 \cdot 2 + 0.$

Hence $gcd\,(272, 1479) = 17$

i.e $d = 17.$

Example 63. *Use the Euclidean Algorithm to obtain integers x and y satisfying*

$gcd\,(56, 72) = 56x + 72y.$

Solution. $72 = 56 \cdot 1 + 16,$

$56 = 16 \cdot 3 + 8,$

$16 = 8 \cdot 2 + 0.$

Hence $gcd\,(56, 72) = 8$

i.e $d = 8.$

From (2),

$8 = 56 - 16 \cdot 3$

$= 56 - (72 - 56 \cdot 1) \cdot 3$ [from (

$= 56 - 72 \cdot 3 + 56 \cdot 3$

$= 56 \cdot 4 - 72 \cdot 3$

$= 56 \cdot 4 + (-3) \cdot 72$

Hence $gcd\,(56, 72) = 56x + 72y.$

where $x = 4, y = -3.$

Example 64. *Use the Euclidean Algorithm to obtain integers x and y satisfying*

$gcd\,(24, 138) = 24x + 138y.$ ....(1)

Solution. $138 = 24 \cdot 5 + 18,$ ....(2)

$24 = 18 \cdot 1 + 6,$ ....(3)

$18 = 6 \cdot 3 + 0$

Hence $gcd\,(24, 138) = 6$

i.e $d = 6$

From (2), [from (1)]

$6 = 24 - 18 \cdot 1$

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

$= 24 - 138 \cdot 1 + 24 \cdot 5$

$= 24 \cdot 6 - 138 \cdot 1$

$= 24 \cdot 6 + (-1) \cdot 138$

Hence $gcd\,(24, 138) = 24x + 138y,$

where $x = 6, y = -1.$

Example 65. *Use the Euclidean Algorithm to obtain integers x and y satisfying*

$gcd\,(119, 272) = 119x + 272y.$ ....(1)

Solution. $272 = 119 \cdot 2 + 34,$ ....(2)

$119 = 34 \cdot 3 + 17,$ ....(3)

$34 = 17 \cdot 2 + 0$

Hence $gcd\,(119, 272) = 17.$

i.e $d = 17$

From (2),

$17 = 119 - 34 \cdot 3$ [from

$= 119 - (272 - 119 \cdot 2) \cdot 3$

$= 119 - 272 \cdot 3 + 119 \cdot 6$

$= 119 \cdot 7 - 272 \cdot 3$

$= 119 \cdot 7 + (-3) \cdot 272$

Hence $gcd\,(119, 272) = 119x + 272y$,
where $x = 7, y = -3$.

Example 66. *Use the Euclidean Algorithm to obtain integers x and y satisfying* $gcd\,(1769, 2378) = 1769x + 2378y$.

Solution. $2378 = 1769 \cdot 1 + 609$,
$1769 = 609 \cdot 2 + 551$,
$609 = 551 \cdot 1 + 58$,
$551 = 58 \cdot 9 + 29$,
$58 = 29 \cdot 2 + 0$

Hence $gcd\,(2378, 1769) = 29$
i.e $d = 29$.
From (4),

$$\begin{aligned}
29 &= 551 - 58 \cdot 9 \\
&= 551 - (609 - 551) \cdot 9 \\
&= 551 - 609 \cdot 9 + 551 \cdot 9 \qquad [\text{from} \\
&= 551 \cdot 10 - 609 \cdot 9 \\
&= (1769 - 609 \cdot 2) \cdot 10 - 609 \cdot 9 \qquad [\text{from} \\
&= 1769 \cdot 10 - 609 \cdot 20 - 609 \cdot 9 \\
&= 1769 \cdot 10 - 609 \cdot 29 \\
&= 1769 \cdot 10 - (2378 - 1769 \cdot 1) \cdot 29 \qquad [\text{from} \\
&= 1769 \cdot 10 - 2378 \cdot 29 + 1769 \cdot 29 \\
&= 1769 \cdot 39 - 2378 \cdot 29 \\
&= 1769 \cdot 39 + (-29) \cdot 2378
\end{aligned}$$

Hence $gcd\,(1769, 2378) = 1769x + 2378y$
where $x = 39, y = -29$.

Example 67. *Use the Euclidean Algorithm to obtain integers x and y satisfying*

$gcd\,(252, 595) = 252x + 595y$.

Solution. $595 = 252 \cdot 2 + 91$,
$252 = 91 \cdot 2 + 70$,

$91 = 70 \cdot 1 + 21$, ...(3)
$70 = 21 \cdot 3 + 7$, ...(4)
$21 = 7 \cdot 3$. ....(5)

Therefore, $gcd\,(252, 595) = 7$
i.e $d = 7$
From (4),

$$\begin{aligned}
7 &= 70 - 21 \cdot 3 \qquad [\text{from (3)}] \\
&= 70 - (91 - 70 \cdot 1) \cdot 3 \\
&= 70 - 91 \cdot 3 + 70 \cdot 3 \qquad [\text{from (2)}] \\
&= 70 \cdot 4 - 91 \cdot 3 \\
&= (252 - 91 \cdot 2) \cdot 4 - 91 \cdot 3 \\
&= 252 \cdot 4 - 91 \cdot 8 - 91 \cdot 3 \qquad [\text{from (1)}] \\
&= 252 \cdot 4 - 91 \cdot 11 \\
&= 252 \cdot 4 - (595 - 252 \cdot 2) \cdot 11 \\
&= 252 \cdot 4 - 595 \cdot 11 + 252 \cdot 22 \\
&= 252 \cdot 26 - 595 \cdot 11 \\
&= 252 \cdot 26 + (-11) \cdot 595
\end{aligned}$$

Hence $gcd\,(252, 595) = 252x + 595y$,
where $x = 26, y = -11$.

Example 68. *Assuming that* $gcd\,(a, b) = 1$, *prove that* $gcd\,(2a + b, a + 2b) = 1$ *or* 3.

Solution. Let $gcd\,(2a + b, a + 2b) = d$

$$\begin{aligned}
&\text{Then} && d \mid (2a + b), \\
& && d \mid (a + 2b). \\
&\Rightarrow && d \mid (2a + b), \\
& && d \mid 2\,(a + 2b) \\
&\Rightarrow && d \mid (2a + b), \\
& && d \mid (2a + 4b) \\
&\Rightarrow && d \mid \{(2a + 4b) - (2a + b)\} \\
&\Rightarrow && d \mid 3b
\end{aligned}$$

Also $d \mid (2a + b)$

$\Rightarrow$ $d \mid 2\,(2a + b)$

$\Rightarrow$ $d \mid (4a + 2b)$

and $d \mid (a + 2b)$

$\Rightarrow$ $a \mid \{(4a + 2b) - (a + 2b)\}$

$\Rightarrow$ $d \mid 3a$

Let $gcd\,(d, a) = e$

$\Rightarrow$ $e \mid d$ and $e \mid a$

But $d \mid (a + 2b)$

$\Rightarrow$ $e \mid (a + 2b)$

$\Rightarrow$ $e \mid \{(a + 2b) - a\}$

$\Rightarrow$ $e \mid 2b$

$\Rightarrow$ $e \mid b$

so $e \mid (a, b)$

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

$\therefore$ $e \mid 1 \Rightarrow e = 1.$

Therefore, $gcd\,(d, a) = 1$

Similarly $gcd\,(d, b) = 1$

$\therefore$ $d \mid 3$

$\Rightarrow$ $d = 1$ or 3.

Example 69. *Assuming that* $gcd\,(a, b) = 1$, *prove that* $gcd\,(a + b, a^2 + b^2) = 1$ *or* 2.

Solution. Let $gcd\,(a + b, a^2 + b^2) = d$

$\Rightarrow$ $d \mid (a + b)$,

$d \mid (a^2 + b^2)$

$\Rightarrow$ $d \mid (a + b)^2$

$\Rightarrow$ $d\,(a^2 + b^2 + 2ab)$

Also $d \mid (a^2 + b^2)$

$\Rightarrow$ $d \mid \{(a^2 + b^2 + 2ab) - (a^2 + b^2)\}$

$\Rightarrow$ $d \mid 2ab$

Let $gcd\,(d, a) = e$

$\Rightarrow$ $e \mid d$ and $e \mid a$

But $d \mid (a + b)$

$\Rightarrow$ $e \mid (a + b)$

$\Rightarrow$ $e \mid \{(a + b) - a\}$

$\Rightarrow$ $e \mid b$

So $e \mid gcd\,(a, b)$

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

$\therefore$ $e \mid gcd\,(a, b) \Rightarrow e \mid 1$

$\Rightarrow$ $e = 1$

$\therefore$ $gcd\,(d, a) = 1$

Similarly $gcd\,(d, b) = 1.$

$\therefore$ $d \mid 2$

$\Rightarrow$ $d = 1$ or 2.

Example 70. *For* $n \geq 1$, *and positive integers* a, b *show that if* $gcd\,(a, b) = 1$, *then* $gcd\,(a^n, b^n) = 1.$

Solution. Let $gcd\,(a^n, b^n) = d$

$\Rightarrow$ $d \mid a^n, d \mid b^n$

$\Rightarrow$ $d \mid (a \cdot a$ ..... up to n times)

and $d \mid (b \cdot b$ ..... up to n times)

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

$\Rightarrow$ $d \mid gcd\,(a, b)$

But gcd of $(a, b) = 1$,

$\therefore$ $d \mid gcd\,(a, b)$

$\Rightarrow$ $d \mid 1.$

Hence $gcd\,(a^n, b^n) = 1.$

Example 71. *For $n \geq 1$ and positive integers a, b show that the relation $a^n \mid b^n$ implies $a \mid b$.*

Solution. Do yourself.

by taking let $gcd\ (a, b) = d$

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

Then by definition of divisibility, there exists integers r and s such that

$a = rd$ and $b = sd$,

where $gcd\ (r, s) = 1$

Since $gcd\ (r, s) = 1$, so we know that $gcd\ (r^n, s^n) = 1$

Then show that $r = 1$ when $a = d$.

Example 72. *Prove that if $gcd\ (a, b) = 1$, then*

$gcd\ (a + b, ab) = 1$.

Or

If $gcd\ (a,b) = 1$, find $gcd\ (a + b, ab)$.

Solution. Let $gcd\ (a + b, ab) = d$

$\Rightarrow$ $d \mid (a + b), d \mid ab$

Let $gcd\ (d, a) = e$

$\Rightarrow$ $e \mid d$ and $e \mid a$

But $d \mid (a + b)$

$\Rightarrow$ $e \mid (a + b)$

$\Rightarrow$ $e \mid \{(a + b) - a\}$

$\Rightarrow$ $e \mid b$

so $e \mid gcd\ (a, b)$

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

$\Rightarrow$ $e \mid 1 \Rightarrow e = 1$

$\therefore$ $gcd\ (d, a) = 1$

Similarly $gcd\ (d, b) = 1$

$\therefore$ $d \mid 1 \Rightarrow d = 1$

Hence $gcd\ (a + b, ab) = 1$

Example 73. *Find lcm (143, 227).*

Solution.

$227 = 143 \cdot 1 + 84,$

$143 = 84 \cdot 1 + 59,$

$84 = 59 \cdot 1 + 25,$

$59 = 25 \cdot 2 + 9,$

$25 = 9 \cdot 2 + 7,$

$9 = 7 \cdot 1 + 2,$

$7 = 2 \cdot 3 + 1,$

$2 = 1 \cdot 2 + 0$

$\therefore$ $gcd\ (143, 227) = 1$

Hence $lcm\ (143, 227) = \dfrac{ab}{gcd\ (a, b)}$

$= \dfrac{143 \cdot 227}{1}$

$= 143 \cdot 227$

$= 32461.$

Example 74. *Find lcm (306, 657).*

Solution. Since we know that

$$lcm\ (a, b) = \frac{ab}{gcd\ (a, b)}$$

Now $657 = 306 \cdot 2 + 45,$

$306 = 45 \cdot 6 + 36,$

$45 = 36 \cdot 1 + 9,$

$36 = 9 \cdot 4 + 0$

$\therefore$ $gcd\ (306, 657) = 9$

$\therefore$ $lcm\ (306, 657) = \dfrac{306 \cdot 657}{9}$

$= 34 \cdot 657$

$= 22338.$

Example 75. *Find lcm (272, 1479).*

Solution. Since we know that

$$lcm\ (a, b) = \frac{ab}{gcd\ (a, b)}$$

Now $1479 = 272 \cdot 5 + 119,$

$272 = 119 \cdot 2 + 34,$

$119 = 34 \cdot 3 + 17,$

$34 = 17 \cdot 2 + 0$

$\therefore\ gcd\ (1479, 272) = 17$

$\therefore\ lcm\ (1479, 272) = \frac{1479 \cdot 272}{17}$

$= 1479 \cdot 16$

$= 23664.$

Example 76. *If a, b are positive integers such that gcd (a,b) = c and lcm (a, b) = d th*
ab = cd.

Solution. Let $c = gcd\ (a, b)$ and
$d = lcm\ (a, b).$

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

$\Rightarrow$ $c \mid a, c \mid b$

Since $c \mid a$

$\Rightarrow$ $a = cr$

and $c \mid b$

$\Rightarrow$ $b = cs$

$\therefore$ $a = cr, b = cs$

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

$\Rightarrow$ $c = au + bv$

$d = lcm\ (a, b) = [a, b]$

$\Rightarrow$ $d = at, d = bw$

$c = au + bv$

$\Rightarrow$ $cd = d\ (au + bv)$

$= abuw + abtv$

$= ab\ (wu + tv)$ [by definition of divisibility]

$\Rightarrow$ $ab \mid cd$

$\frac{ab}{c} = \frac{crb}{c} = rb$

$\frac{ab}{c} = \frac{acs}{c} = as$

$\therefore$ $a \mid \frac{ab}{c}, b \mid \frac{ab}{c}$

$\Rightarrow$ $d \mid \frac{ab}{c}$

$\Rightarrow$ $cd \mid ab$

$\Rightarrow$ $ab = cd.$

Theorem 14. (Mersenne's conjecture)

If $2^n - 1$ is a prime, then n is itself prime.

Proof. Let us assume that n is a composite and that $n = n_1 n_2$, where $1 < n_1 < n$ and $1 < n_2 < n$.

Then $2^{n_1 n_2} - 1$ has the factor $2^{n_1} - 1$ that is neither 1 nor $2^n - 1$.

Hence $2^n - 1$ is a prime

$\Rightarrow$ n is a prime.

But its converse is not always true.

For example, let $p = 11$.

Then $23 \mid 2^{11} - 1$.

Hence $p = 11$ does not imply

$2^{11} - 1$ is a prime.

Thus we conclude that p is a prime and it does not imply $2^p - 1$ is a prime.

Note

The first five Mersenne prime are

$$M_2 = 3, M_3 = 7, M_5 = 31, M_7 = 127, M_{13} = 8191.$$

Example 77. *Prove that if a and b are positive integers, then*

$$a\,!\ b\,!\ \mid (a + b)\,!$$

Solution. If $a = 1, b = 1$, the result is trivially true.

If at least one of a or b is 1,

say, $a = 1$, then

$a\,!\,b\,! = b\,!$ and

$(a+b)\,! = (b+1)\,! = (b+1)\,b\,!$

$\Rightarrow \quad a\,!\,b\,! \mid (a+b)\,!$

Let the result be true for all positive integers a and b for which $a + b = n$ and $n > 1$

Let $a + b = n + 1$ and $a > 1, b > 1$

Then $(a-1) + b = n$ and

$a + (b-1) = n.$

By our assumption, we have

$(a-1)\,!\,b\,! \mid (a+b-1)\,!$ and

$a\,!\,(b-1)\,! \mid (a+b-1)\,!$

i.e $(a+b-1)\,! = k\,(a-1)\,!\,b\,!$ and

$(a+b-1)\,! = k'\,a\,!\,(b-1)\,!$ for

some $k, k' \in Z$.

$\therefore \quad (a+b)\,! = (a+b-1)\,!\,(a+b)$

$= (a+b-1)\,!\,a + (a+b-1)\,!\,b$

$= k\,(a-1)\,!\,b\,!\,a + k'\,a\,!\,(b-1)\,!\,b$

$= ka\,!\,b\,! + k'\,a\,!\,b\,!$

$= (k+k')\,a\,!\,b\,!$

$\Rightarrow \quad a\,!\,b\,! \mid (a+b)\,!$

Thus the result is true for all positive integers whose sum is $n + 1$.

Hence by induction, result is true for all positive integers a and b.

Example 78. *If* $(a, b) = 1$ *and* $c \mid a + b$ *then prove that* $(c, a) = (c, b) = 1$.

Solution. Since $c \mid a + b$

$\Rightarrow \quad a + b = c\,n$ for some $n \in Z$

Let $(c, a) = d$

$\Rightarrow \quad d \mid c$ and $d \mid a$

$\Rightarrow \quad d \mid c$ and $d \mid b$

$\Rightarrow \quad d \mid (a, b)$

$\Rightarrow \quad d \mid 1$

$\Rightarrow \quad d = 1$

$\Rightarrow \quad (c, a) = 1$

$\therefore$ Similarly we can s

Example 79. *If x and y*

Solution. Since x and

therefore x and y

$\Rightarrow x^2$ and y^2 bot

$\Rightarrow \quad x^2 + y^2 =$

$=$

i.e $x^2 + y^2$ is of

If possible let x

$\Rightarrow z^2$ is of the

$3k + 2$.

Hence $x^2 + y^2$

Example 80. *Prov*

unit digits : 0, 1, 4

Solution. Firstly

$5k - 1$.

Let a^2 be giv

Divide a by

Let q be the

$\therefore \quad a = 5$

$\Rightarrow \quad a =$

i.e. $a =$

Or $a =$

$\Rightarrow \quad a^2 =$

i.e a^2

When a^2

then there

$\Rightarrow \quad d = 1$

$\therefore \quad (c, a) = 1$

Similarly we can show that $(c, b) = 1$.

Example 79. *If x and y are co-prime to 3, then show that $x^2 + y^2$ cannot be a perfect square.*

Solution. Since x and y are coprime to 3,

therefore x and y are one of the form $3k + 1$ or $3k + 2$.

$\Rightarrow$ x^2 and y^2 both are of the form $3k + 1$

$$\Rightarrow \quad x^2 + y^2 = (3k_1 + 1) + (3k_2 + 1)$$
$$= 3(k_1 + k_2) + 2$$

i.e $x^2 + y^2$ is of the form $3k + 2$.

If possible let $x^2 + y^2$ be a perfect square and $x^2 + y^2 = z^2$

$\Rightarrow z^2$ is of the form $3k + 2$ which is not true as square of no integer is of the form $3k + 2$.

Hence $x^2 + y^2$ cannot be a perfect square.

Example 80. *Prove that any number which is square must have one of the following for its unit digits : 0, 1, 4, 5, 6, 9.*

Solution. Firstly we shall prove that every square integer is of the form $5k$ or $5k + 1$ or $5k - 1$.

Let a^2 be given square number.

Divide a by 5.

Let q be the quotient and r be the least non-negative remainder.

$\therefore \quad a = 5q + r \; ; r = 0, 1, 2, 3, 4$

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

i.e. $\quad a = 5q$ or $5q + 1$ or $5q + 2$ or $5q - 2$ or $5q - 1$

Or $\quad a = 5q$ or $5q = \pm 1$ or $5q = \pm 2$

$$\Rightarrow \quad a^2 = 25q^2 \text{ or } 25q^2 \pm 10q + 1 \text{ or } 25q^2 \pm 20q + 4$$
$$= 5(5q^2) \text{ or } 5(5q^2 \pm 2q) + 1 \text{ or } 5(5q^2 \pm 4q) + 4$$

i.e $\quad a^2 = 5k$ or $5k + 1$ or $5k + 4$ $(i.e \; 5k - 1)$ type.

When $a^2 = 5k$ type,

then there is 0 or 5 in unit's place.

When $a^2 = 5k + 1$ type, then there is 1 or 6 in unit's place.

When $a^2 = 5k + 4$ type, then there is 4 or 9 in unit's place.

Therefore for any number which is square, we must have one of the number 0, 1, 4, 5, 6, 9 in units place.

Example 81. *If x and y are odd, then 4 does not divide $x^2 + y^2$.*

Solution. Let $x = 2k + 1$ and

$$y = 2k' + 1$$

$$\therefore \quad x^2 + y^2 = (2k + 1)^2 + (2k' + 1)^2$$

$$= (4k^2 + 4k + 1) + (4k'^2 + 4k' + 1)$$

$$= 4(k^2 + k + k'^2 + k') + 2$$

Now $4 \nmid 4(k^2 + k'^2 + k + k') + 2$

$\Rightarrow \quad 4 \nmid x^2 + y^2$.

Example 82. *Show that $4 \nmid n^2 + 2$ for any integer n.*

Solution. Case I

If n is power of 2 only *i.e* if $n = 2^k$ where $k \geq 1$,

then $\quad n^2 = 2^{2k}$

$\Rightarrow \quad n^2 + 2 = 2^{2k} + 2$

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

Since $\quad k \geq 1 \Rightarrow 2k \geq 2 \Rightarrow 2k - 1 \geq 1$

$\Rightarrow \quad 2^{2k-1}$ is even number

$\Rightarrow \quad 2^{2k-1} + 1$ is odd

$\therefore \quad 2 \nmid 2^{2k-1} + 1$

$\Rightarrow \quad 4 \nmid 2(2^{k-1} + 1)$

$\Rightarrow \quad 4 \nmid n^2 + 2$

Case II

If $n = 2^a b$ where $a \geq 0$ and b is odd number.

When $\quad a = 0, n = b$

$\Rightarrow \quad n^2 = b^2$

$\Rightarrow \quad n^2 + 2 = b^2 + 2$

Now $\quad 2 \nmid b^2$

$\Rightarrow \quad 2 \nmid b^2 + 2$

$\Rightarrow \quad 4 \nmid b^2 + 2$

$\Rightarrow \quad 4 \nmid n^2 + 2$

When $a \geq 1$, then

$$n^2 = 2^{2a} b^2$$

$\Rightarrow \quad n^2 + 2 = 2^{2a} b^2 + 2$

$$= 2(2^{2a-1} b^2 + 1)$$

Now 2^{2a-1} is even number

$\Rightarrow \quad 2^{2a-1} b^2$ is even number

$\Rightarrow \quad 2^{2a-1} b^2 + 1$ is odd number

$\Rightarrow \quad 2 \nmid 2^{2a-1} b^2 + 1$

$\Rightarrow \quad 4 \nmid 2[2^{2a-1} b^2 + 1]$

$\Rightarrow \quad 4 \nmid n^2 + 2$

Hence $4 \nmid n^2 + 2$ for any integer n.

Example 83. Find gcd of (−18, 24).

Solution. The positive divisors of −18 are 1, 2, 3, 6, 8, 12, 24.

The positive common divisors of −18 and

The greatest common divisors of −18 and

$(-18, 24) = 6$.

Example 84. Find positive integers a and b satisfying $a + b = 100$ simultaneously. Find all solutions.

Solution. Since $(a, b) = 10$

$\Rightarrow \quad 10 \mid a$ and $10 \mid b$

$\Rightarrow \quad a = 10x$ and $b = 10y$

where $x, y \in Z$ and $(x, y) = 1$

$\Rightarrow \quad n^2+2=b^2+2$ [$\because$ b is odd $\Rightarrow$ b^2 is odd $\Rightarrow$ b^2+2 is odd]

Now $2 \nmid b^2$

$\Rightarrow \quad 2 \nmid b^2+2$

$\Rightarrow \quad 4 \nmid b^2+2$

$\Rightarrow \quad 4 \nmid n^2+2$

When $a \geq 1$, then

$n^2=2^{2a} b^2$

$\Rightarrow \quad n^2+2=2^{2a} b^2+2$

$=2\,(2^{2a-1} b^2+1)$

Now 2^{2a-1} is even number [$\because$ $a \geq 1 \Rightarrow 2a \geq 2 \Rightarrow 2a-1 \geq 1$]

$\Rightarrow \quad 2^{2a-1} b^2$ is even number

$\Rightarrow \quad 2^{2a-1} b^2+1$ is odd number

$\Rightarrow \quad 2 \nmid 2^{2a-1} b^2+1$

$\Rightarrow \quad 4 \nmid 2\,[2^{2a-1} b^2+1]$

$\Rightarrow \quad 4 \nmid n^2+2$

Hence $4 \nmid n^2+2$ for any integer n.

Example 83. Find ged of $(-18, 24)$.

Solution. The positive divisors of -18 are 1, 2, 3, 6, 9, 18 and the positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, 24.

The positive common divisors of -18 and 24 are 1, 2, 3, 6.

The greatest common divisors of -18 and 24 is 6.

$\therefore \quad (-18, 24) = 6.$

Example 84. Find positive integers a and b satisfying the equations $(a, b) = 10$ *and* $[a, b] = 100$ *simultaneously. Find all solutions.*

Solution. Since $(a, b) = 10$

$\Rightarrow \quad 10 \mid a$ and $10 \mid b$

$\Rightarrow \quad a = 10x$ and $b = 10y$ ....(1)

where $x, y \in Z$ and $(x, y) = 1$

We know that $ab = (a, b)\,[a, b]$

$\Rightarrow \quad (10x)\,(10y) = 10\text{-}100$

$\Rightarrow \quad xy = 10$ where $(x, y) = 1$

$x = 1, y = 10;\ x = -1, y = -10;$

$x = 2, y = 5;\ x = -2, y = -5;$

$x = 5, y = 2;\ x = -5, y = -2;$

$x = 10, y = 1;\ x = -10, y = -1.$

By (1), $a = 10, b = 100$ is a solution in positive integers.

All solutions are given by

$a = \pm 10, b = \pm 100;$

$a = \pm 20, b = \pm 50,$

$a = \pm 50, b = \pm 20,$

$a = \pm 100, b = \pm 10.$

Example 85. *Prove that a positive integer $a > 1$ is a square if and only if in the canonical form of a, all the exponents of primes are even integers.*

Solution. Firstly, let a be a square, say, $a = m^2$.

Since $a > 1$,

$\therefore \quad m > 1.$

Therefore by fundamental theorem of arithmetic,

$$m = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$$

where p_i's are distinct prime numbers.

$\therefore \quad a = (p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r})^2$

i.e $\quad a = p_1^{2a_1} p_2^{2a_2} \ldots p_r^{2a_r}$

Therefore all the exponents of primes are even in the canonical form of a.

Conversely, Let $a = p_1^{b_1} p_2^{b_2} \ldots p_r^{b_r}$

where p_i's are distinct primes and b_i's are even.

Since $b_1, b_2, \ldots\ldots, b_r$ are integers,

therefore we can take

$$b_1 = 2c_1,\ b_2 = 2c_2,\ \ldots\ldots,\ b_r = 2c_r.$$

$\therefore \quad a = p_1^{2c_1} p_2^{2c_2} \ldots p_r^{2c_r}$

$\ldots p_r^{c_r})^2$

Prove that every integer $n > 1$ can be w

integer and m is odd integer.

fundamental theorem of Arithmetic

$p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$

are distinct odd primes and $a_i \geq 0\ \forall\ i.$

number, then $a = 0$

$p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$

$2^0 \cdot m$ where

$p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$

= odd number

p_i's are odd and product of odd numbers =

If a is even number, then $a \geq 1$

$\therefore \quad t = 2^a p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$

$= 2^a \cdot m$ where $m = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$

= odd number.

Hence every integer $n > 1$ can be written as

$n = 2^a \cdot m$ where a is non-negative integer

THE DIOPHANTINE EQUATION

Diophantine equations are named after the name

who initiated the study of such equations.

It is customary to apply the term Diophantine equ

unknown that is to be solved in the integers. The s

that we shall consider the linear Diophantine equatio

$ax + by = c$

where a, b, c are given integers and a, b are not

A solution of this equation is a pair of integers

equation, satisfy it i.e $ax_0 + by_0 = c$.

i.e $a = (p_1^{c_1} p_2^{c_2} \ldots p_r^{c_r})^2$

$\Rightarrow a$ is a square.

Example 86. *Prove that every integer $n > 1$ can be written as $n = 2^a \cdot m$, where a is non-negative integer and m is odd integer.*

Solution. Since $n > 1$,

therefore by fundamental theorem of Arithmetic, we have

$$n = 2^a p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$$

where p_i's are distinct odd primes and $a_i \geq 0 \ \forall \ i$.

If n is odd number, then $a = 0$

$$\therefore \quad n = 2^0 p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$$

$$= 2^0 m \text{ where}$$

$$m = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$$

= odd number

[Since p_i's are odd and product of odd numbers = odd number]

If n is even number, then $a \geq 1$

$$\therefore \quad n = 2^a p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$$

$$= 2^a \cdot m \text{ where } m = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$$

= odd number.

Hence every integer $n > 1$ can be written as

$n = 2^a \cdot m$ where a is non-negative integer ($i.e\ a \geq 0$) and m is odd number.

THE DIOPHANTINE EQUATION

Diophantine equations are named after the name of the mathematician Diophantus, who initiated the study of such equations.

It is customary to apply the term Diophantine equation to any equation in one or more unknowns that is to be solved in the integers. The simplest type of Diophantine equation that we shall consider the linear Diophantine equation in two unknowns :

$$ax + by = c$$

where a, b, c are given integers and a, b are not both zero.

A solution of this equation is a pair of integers x_0 , y_0 that, when substituted into the equation, satisfy it *i.e* $ax_0 + by_0 = c$.

Linear Diophantine Equations

A linear equation $ax + by = c$ with $a \neq 0, b \neq 0$ and c integers is called a Linear Diophantine equations in two unknowns x and y. A pair of integers x_0, y_0 is called a solution of $ax + by = c$ if $ax_0 + by_0 = c$.

A given Diophantine equation may have more than one solutions.

e.g. $x + 7y = 31$ is satisfied by

$x = 24, y = 1;$

and also by $x = 3, y = 4;$

and also by $x = 17, y = 2.$

On the contrary the Diophantine equation $15x + 51y = 14$ has no solutions.

Now we prove the theorem which tells us when can a given Diophantine have solutions ?

Theorem 15. Show that the linear Diophantine equation $ax + by = c$ has a solution and only if $d \mid c$ where $d = (a, b)$. Further, if x_0, y_0 is any particular solution of the equation then all other solutions are given by

$$x = x_0 + \frac{b}{d}t,$$

$$y = y_0 - \frac{a}{d}t$$

where t is any integer.

Proof. Let the Diophantine equation $ax + by = c$ has a solution $x = x_0, y = y_0$

$\therefore \quad ax_0 + by_0 = c$

Since $d = (a, b)$

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

$\Rightarrow \quad d \mid ax_0$ and $d \mid by_0$

$\Rightarrow \quad d \mid (ax_0 + by_0)$

$\Rightarrow \quad d \mid c$

Conversely, let $d \mid c$

$\Rightarrow \quad c = dq$ for some $q \in Z.$

Also $d = (a, b)$

$\Rightarrow \quad d = au + bv$ for some $u, v \in Z$

$\therefore \quad c = (au + bv)\, q$

...has a solution given by $x = uq$ ...
...if x_0, y_0 is a particular solution of Dio...
...be any other solution of equation, then
$ax' + by' = c$
$ax_0 + by_0 = ax' + by'$
$\therefore \quad a(x' - x_0) = b(y_0 - y')$
$\Rightarrow \quad \frac{a}{d}(x' - x_0) = \frac{b}{d}(y_0 - y')$
Now as a and b are not both zero, we can sup...
from (1), we have
$\frac{b}{d} \mid \frac{a}{d}(x' - x_0)$ and
$\left(\frac{a}{d}, \frac{b}{d}\right) = 1$
$\therefore \quad \frac{b}{d} \mid (x' - x_0)$
$\Rightarrow x' - x_0 = \frac{b}{d}t$ for some $t \in Z.$
Putting the value of $x' - x_0$ in (1), we get
$\frac{a}{d}\cdot\frac{b}{d}t = \frac{b}{d}(y_0 - y')$
$\Rightarrow \quad \frac{a}{d}t = y_0 - y'$
$\Rightarrow \quad y' = y_0 - \frac{a}{d}t$
$\therefore \quad x' = x_0 + \frac{b}{d}t,$
$y' = y_0 - \frac{a}{d}t$
...an infinite...

$= a(uq) + b(vq)$.

Hence $ax + by = c$ has a solution given by $x = uq$ and $y = vq$.

Further if x_0, y_0 is a particular solution of Diophantine equation $ax + by = c$, then

$ax_0 + by_0 = c$.

Let x', y' be any other solution of equation, then

$$ax' + by' = c$$

$$\therefore \quad ax_0 + by_0 = ax' + by'$$

$$\Rightarrow \quad a(x' - x_0) = b(y_0 - y') \qquad \ldots(1)$$

$$\Rightarrow \quad \frac{a}{d}(x' - x_0) = \frac{b}{d}(y_0 - y')$$

Now as a and b are not both zero, we can suppose that $b \neq 0$.

From (1), we have

$$\frac{b}{d} \mid \frac{a}{d}(x' - x_0) \text{ and}$$

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

$$\therefore \quad \frac{b}{d} \mid (x' - x_0)$$

$\Rightarrow x' - x_0 = \frac{b}{d} t$ for some $t \in Z$.

Putting the value of $x' - x_0$ in (1), we get

$$\frac{a}{d} \cdot \frac{b}{d} t = \frac{b}{d}(y_0 - y')$$

$$\Rightarrow \quad \frac{at}{d} = y_0 - y'$$

$$\Rightarrow \quad y' = y_0 - \frac{a}{d} t$$

$$\therefore \quad x' = x_0 + \frac{b}{d} t,$$

$$y' = y_0 - \frac{a}{d} t$$

are an infinite number of solutions of the given equation, one for each value of t.

Corollary. *If $(a, b) = 1$, then the Diophantine equation $ax + by = c$ always have a solu... Further if x_0, y_0 is a particular solution of this equation then all solutions are given b...*

$$x = x_0 + bt,$$

$$y = y_0 - at$$

for integral values of t.

Proof. By above theorem, $ax + by = c$ has a solution if and only if $(a, b) \mid c$.

Since $(a, b) = 1$ and

$$1 \mid c \ \forall\ c \in Z,$$

therefore, $ax + by = c$ always has a solution.

Second part simply follows from the theorem.

Example 87. *Find the general solution of* $10x - 8y = 42$.

Solution. Since $gcd\,(10, 8) = 2$ and $2 \mid 42$

$\therefore$ $10x - 8y = 42$ has a solution.

Now $x = 1, y = -4$ is a particular solution of it.

Hence general solution is

$$x' = 1 - \frac{(-8)}{2}t,$$

$$y' = -4 + \left(\frac{10}{2}\right)t$$

$\Rightarrow$

$$x' = 1 + 4t,$$

$$y' = -4 + 5t.$$

Example 88. *Determine all solutions in positive integers of the Diophantine equation* $172x + 20y = 1000$.

Solution. Given Diophantine equation is

$$172x + 20y = 1000 \qquad \ldots(1)$$

By division algorithm, we have

$$172 = 8 \cdot 20 + 12,$$

$$20 = 1 \cdot 12 + 8,$$

$$12 = 1 \cdot 8 + 4,$$

$$8 = 2 \cdot 4 + 0$$

Since the last non-zero remainder is 4, therefore

$$gcd\,(172, 20) = 4.$$

Since $4 \mid 1000$, the equation (1) has infinitely many solutions.

Now
$$4 = d = 12 - 1 \cdot 8$$
$$= 12 - (20 - 1 \cdot 12)$$
$$= 12 - 20 + 1 \cdot 12$$
$$= 2 \cdot 12 - 20$$
$$= 2\,(172 - 8 \cdot 20) - 20$$
$$= 2 \cdot 172 - 16 \cdot 20 - 20$$
$$= 2 \cdot 172 - 17 \cdot 20$$
$$= 2 \cdot 172 + (-17) \cdot 20$$

$\therefore$
$$1000 = 4 \cdot 250$$
$$= (2 \cdot 172 + (-17) \cdot 20) \cdot 250$$
$$= (2 \cdot 250)\ 172 + 20\ [250 \cdot (-17)]$$
$$= 500 \cdot 172 + 20\,(-4250)$$

$\therefore$
$$x_0 = 500,$$
$$y_0 = -4250$$

is a particular solution of (1).

The general solution of (1) is given by

$$x = 500 + \frac{20}{4}t,$$

$$y = -4250 - \frac{172}{4}t \ \forall\ t \in Z$$

i.e.
$$x = 500 + 5t,$$
$$y = -4250 - 43t \ \forall\ t \in Z.$$

For positive solution,

$$500 + 5t > 0 \text{ and } -4250 - 43t > 0$$

Or
$$5t > -500 \text{ and } -43t > 4250$$

Or
$$t > -100 \text{ and } t < -\frac{4250}{43}$$

Or
$$-100 < t < -98\frac{36}{43} \qquad \ldots(2)$$

Since $t \in Z$,

therefore from (2), the only integral value of t satisfying (2) is given by

$$t = -99$$

Putting the value of $t = -99$ in

$x = 500 + 5t$, $y = -4250 - 43t$, we get

$x = 500 + 5(-99)$,

i.e $y = -4250 - 43(-99)$

$x = 500 - 495$,

$\Rightarrow$ $y = -4250 + 4257$

$x = 5$, $y = 7$.

Thus the given Diophantine equation has unique positive solution

$x = 5$, $y = 7$.

Example 89. *Find all positive solutions, if any, of the equation* $200x + 325y = 100$.

Solution. The given equation is

$$200x + 325y = 100$$

By division algorithm, we have

$325 = 1 \cdot 200 + 125$,

$200 = 1 \cdot 125 + 75$,

$125 = 1 \cdot 75 + 50$,

$75 = 1 \cdot 50 + 25$,

$50 = 2 \cdot 25 + 0$

Since the last non-zero remainder is 25.

$\therefore$ $(325, 200) = 25$

Also $25 \mid 100$,

therefore the given equation is solvable.

Now $25 = d = 75 - 1 \cdot 50$

$= 75 - (1 \cdot 125 - 1 \cdot 75)$

$= 75 - 1 \cdot 125 + 1 \cdot 75$

$= 2 \cdot 75 - 1 \cdot 125$

$= 2(200 - 1 \cdot 125) - 1 \cdot 125$

$= 2 \cdot 200 - 2 \cdot 125 - 1 \cdot 125$

$= 2 \cdot 200 - 3 \cdot 125$

$= 2 \cdot 200 - 3(1 \cdot 325 - 1 \cdot 200)$

$= 2 \cdot 200 - 3 \cdot 325 + 3 \cdot 200$

$= 5 \cdot 200 - 3 \cdot 325$

$= 200(5) + 325(-3)$

$\therefore$ $100 = 25 \times 4$

$= [200(5) + 325(-3)] \times 4$

$= 200(20) + 325(-12)$

$\therefore$ $x_0 = 20$, $y_0 = -12$

is a particular solution of given equation.

The general solution is given by

$$x = 20 + \frac{325}{25}t,$$

$$y = -12 - \frac{200}{25}t \quad \forall\ t \in Z$$

i.e $x = 20 + 13t$,

$y = -12 - 8t \quad \forall\ t \in Z$

Now solution is positive iff

$20 + 13t > 0$ and $-12 - 8t > 0$

i.e iff $13t > -20$ and $-12 > 8t$

i.e iff $t > -\frac{20}{13}$ and $t < -\frac{12}{8}$

i.e iff $-\frac{20}{13} < t < -\frac{3}{2}$

i.e iff $-1 \cdot 53 < t < -1 \cdot 5$

But there is no integer satisfying $-1 \cdot 53 < t < -1 \cdot 5$

Therefore the given equation has no positive integral solution.

Example 90. *Find the general solution of Diophantine equation*

$$1485x + 1745y = 15.$$

Solution. The given Diophantine equation is

$$1485x + 1745y = 15 \quad \ldots(1$$

By division algorithm, we have

$1745 = 1 \cdot 1485 + 260$,

$1485 = 5 \cdot 260 + 185$,

$260 = 1 \cdot 185 + 75$,

$$75 = 2 \cdot 35 + 5,$$

$$35 = 7 \cdot 5 + 0.$$

Since the last non-zero remainder is 5,

$\therefore$ $(1485, 1745) = 5$.

As $5 \mid 15$, therefore the given equation has infinite many solutions.

Now $5 = d = 75 - 2 \cdot 35$

$= 75 - 2(185 - 2 \cdot 75)$

$= 75 - 2 \cdot 185 + 4 \cdot 75$

$= 5 \cdot 75 - 2 \cdot 185$

$= 5(260 - 1 \cdot 185) - 2 \cdot 185$

$= 5 \cdot 260 - 5 \cdot 185 - 2 \cdot 185$

$= 5 \cdot 260 - 7 \cdot 185$

$= 5 \cdot 260 - 7(1485 - 5 \cdot 260)$

$= 5 \cdot 260 - 7 \cdot 1485 + 35 \cdot 260$

$= 40 \cdot 260 - 7 \cdot 1485$

$= 40(1745 - 1485) - 7 \cdot 1485$

$= 40 \cdot 1745 - 40 \cdot 1485 - 7 \cdot 1485$

$= 40 \cdot 1745 - 47 \cdot 1485$

$= (-47) \cdot 1485 + 40 \cdot 1745$

$\therefore$ $15 = 5 \cdot 3$.

$= [(-47) \cdot 1485 + 40 \cdot 1745] \cdot 3$

$= (-141) \cdot 1485 + (120) \cdot 1745$

$\therefore$ $x_0 = -141$, $y_0 = 120$ is a particular solution of the given Diophantine equation.

The general solution is given by

$$x = -141 + \frac{1745}{5} t,$$

$$y = 120 - \frac{1485}{5} t$$

i.e. $\left.\begin{aligned} x &= -141 + 349t, \\ y &= 120 - 297t \end{aligned}\right\}$

when t is any integer.

Example 91. *A customer bought a dozen pieces of fruit, apples and oranges, for $ 1.32. If an apple cost 3 cents more than an orange and more apples than oranges were purchased, how many pieces of each kind were bought ?*

Solution. Let x be the number of apples and y be the number of oranges purchased.

Let z represent the cost (in cents) of an orange.

Then the conditions of the problem lead to

$$(z + 3)x + zy = 132 \quad \ldots.(1)$$

Or equivalently,

$$3x + (x + y)z = 132$$

Since $x + y = 12$, so (1) becomes

$$3x + 12z = 132$$

Or $x + 4z = 44$ $\ldots.(2)$

we are to find integers x and z satisfying the Diophantine equation

$$x + 4z = 44$$

Here $gcd\,(1, 4) = 1$ which is a divisor of 44.

Therefore, the solution exists.

Multiplying the relation

$1 = 1(-3) + 4 \cdot 1$ by 44 to get

$44 = 1(-32) + 4 \cdot 44$

It follows that

$x_0 = -132$, $z_0 = 44$

which serves as one solution.

All other solutions of equations (2) are of the form

$$x = -132 + 4t,$$

$$z = 44 - t$$

where t is an integer.

Not all the choices for t furnish solutions to the original problem.

Only values of t that ensure $12 \geq x > 6$ should be considered.

This requires obtaining those values of t such that

$$12 \geq -132 + 4t > 6$$

Now, $12 \geq -132 + 4t$

implies that $t \leq 36$,

whereas $-132 + 4t > 6$ gives

$$t > 34\frac{1}{2}.$$

The only integral values of t to satisfy both in equalities are

$$t = 35 \text{ and } t = 36.$$

Thus, there are two possible purchases : a dozen apples costing 11 cents a piece (the case where $t = 36$) or 8 apples at 12 cents each and 4 oranges at 9 cents each (the where $t = 35$).

Example 92. *If a cock is worth 5 coins, a hen 3 coins, and three chicks together 1 coin, how many cocks, hens, and chicks, totaling 100, can be bought for 100 coins ?*

Solution. Let the number of cocks $= x$

Let the number of hens $= y$

Let the number of chicks $= z$.

In terms of equations, the above problem is written as

$$5x + 3y + \frac{1}{3}z = 100, \quad \ldots(1)$$

$$x + y + z = 100. \quad \ldots(2)$$

Eliminating one of the unknowns, we are left with a linear Diophantine equation in two other unknowns.

i.e since $z = 100 - x - y$ [from (2)

Putting $z = 100 - x - y$ in (1), we get

$$5x + 3y + \frac{1}{3}(100 - x - y) = 100$$

Or $$5x + 3y + \frac{100}{3} - \frac{x}{3} - \frac{y}{3} = 100$$

Or $$\frac{14}{3}x + \frac{8}{3}y = \frac{200}{3}$$

Or $$14x + 8y = 200$$

Or $$7x + 4y = 100$$

This equation has the general solution $x = 4t$, $y = 25 - 7t$,

so that $z = 75 + 3t$,

where t is an arbitrary integer.

Chang (Chinese Scholar) himself gave several answers :

$x = 4$, $y = 18$, $z = 78$

$x = 8$, $y = 11$, $z = 81$

$x = 12$, $y = 4$, $z = 84$

Thus t must be chosen to satisfy simultaneously the inequalities

$4t > 0$, $25 - 7t > 0$, $75 + 3t > 0$.

The last two of these are equivalent to the requirement $-25 < t < 3\frac{4}{7}$. Because t must have a positive value.

We conclude that $t = 1, 2, 3$, leading to precisely the values *Chang* obtained.

Example 93. *Which of the following Diophantine equations cannot be solved ?*

(a) $6x + 51y = 22$.

(b) $33x + 14y = 115$.

(c) $14x + 35y = 93$.

Solution (a) Applying the Euclidean's Algorithm to evaluate

$gcd\,(6, 51)$

$51 = 6 \cdot 8 + 3,$

$6 = 3 \cdot 2 + 0$

$\therefore \quad gcd\,(6, 51) = 3$

But $3 \nmid 22$,

Therefore solution does not exist.

i.e the given equation cannot be solved.

(b) To the $gcd\,(33, 14)$

$33 = 14 \cdot 2 + 5,$

$14 = 5 \cdot 2 + 4,$

$5 = 4 \cdot 1 + 1,$

$4 = 1 \cdot 4 + 0$

$\therefore$ $gcd\,(33, 14) = 1$ which divides 115.

Thus the solution of the given equation exists so it can be solved.

(c) To get the *gcd* (14, 35).

$$35 = 14 \cdot 2 + 7,$$
$$14 = 7 \cdot 2 + 0.$$

$\therefore$ *gcd* (33, 14) = 7

which does not divide 93.

Hence the given equation cannot be solved.

Example 94. *Determine all solutions in the integers of the Diophantine equation* $56x + 72y = 40$.

Solution. Applying the Euclidean's Algorithm to evaluate the *gcd* of 56 and 72.

$$72 = 56 \cdot 1 + 16,$$
$$56 = 16 \cdot 3 + 8,$$
$$16 = 8 \cdot 2 + 0$$

$\therefore$ *gcd* (56, 72) = 8.

Since 8 divides 40,

therefore, solution of the given equation exists.

Now $8 = 56 - 16 \cdot 3$

$$= 56 - (72 - 56 \cdot 1) \cdot 3$$
$$= 56 - 72 \cdot 3 + 56 \cdot 3$$
$$= 56 \cdot 4 - 72 \cdot 3$$
$$= 56 \cdot 4 + (-3) \cdot 72$$

Multiplying the above relation by 5, we get

$$40 = 5\,[56 \cdot 4 + (-3) \cdot 72]$$
$$= 56 \cdot 20 + (-15) \cdot 72$$

so that $x_0 = 20$ and $y_0 = -15$ provide one solution to the Diophantine equation.

Thus the general solution is given by

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

and $$y = y_0 - \left(\frac{a}{d}\right)t,$$

$\Rightarrow$ $$x = 20 + \left(\frac{72}{8}\right)t,$$

$$y = -15 - \left(\frac{56}{8}\right)t$$

$\Rightarrow$ $x = 20 + 9t,$

$y = -15 - 7t.$

Example 95. *Find the general solution of* $10x - 8y = 42$.

Solution. Since (10, 8) = 2 and 2 | 42

Therefore given equation is solvable.

Now $x_0 = 1, y_0 = -4$ is particular solution of $10x - 8y = 42$.

Therefore its general solution is given by

$$x = 1 + t\left(-\frac{8}{2}\right),$$

$$y = -4 - t\left(\frac{10}{2}\right) \forall\ t \in Z$$

i.e $x = 1 - 4t,$

$y = -4 - 5t \ \forall\ t \in Z$.

Example 96. *Find all positive solutions, if any, of the equation*

$$200x + 325y = 100.$$

Solution. Since (200, 325) = 25 and 25 | 100,

therefore the given equation is solvable.

To find particular solution

Now $325 = 1 \cdot 200 + 125$

$200 = 1 \cdot 125 + 75$

$125 = 1 \cdot 75 + 50$

$75 = 1 \cdot 50 + 25$

$50 = 2 \cdot 25$

Now $25 = 1 \cdot 75 + 1 \cdot 50$

$= 1 \cdot 75 - (1 \cdot 125 - 1 \cdot 75)$

$= 1 \cdot 75 - 1 \cdot 125 + 1 \cdot 75$

$= 2 \cdot 75 - 1 \cdot 125$

$= 2\,(1 \cdot 200 - 1 \cdot 25) - 1 \cdot 125$

$= 2 \cdot 200 - 3 \cdot 125$

$= 2 \cdot 200 - 3\,(1 \cdot 325 - 1 \cdot 200)$

$= 2 \cdot 200 - 3 \cdot 325 + 3 \cdot 200$

$= 5 \cdot 200 - 3 \cdot 325$

i.e $200\,(5) + 325\,(-3) = 25$

$\Rightarrow$ $200\,(20) + 325\,(-12) = 300$

$\therefore$ $x_0 = 20$, $y_0 = 12$ is particular solution of given equation.

All solutions are given by

$$x = 20 + \frac{325}{25}t,$$

$$y = -12 - \frac{200}{25}t \quad \forall\ t \in Z$$

i.e $x = 20 + 13t$

$y = -12 - 8t \quad \forall\ t \in Z$

Now solution is positive iff

$20 + 13t > 0$ and $-12 - 8t > 0$

i.e iff $13t > -20$ and $-12 > 8t$

i.e iff $t > -\frac{20}{13}$ and $t < -\frac{12}{8}$

i.e iff $\frac{20}{13} < t < -\frac{3}{2}$

i.e iff $-1 \cdot 53 < t < -1 \cdot 5$

But there is no integer satisfying $-1 \cdot 53 < t < -1 \cdot 5$

Therefore the given equation has no positive integral solution.

Example 97. *Determine all solutions in the integers of the Diophantine equation* $24x + 138y = 18$.

Or

Find the integral solution of the Diophantine equation $24x + 138y = 18$.

Solution. Applying the Euclidean's Algorithm to evaluate the *gcd* of 24 and 138.

$138 = 24 \cdot 5 + 18,$

$24 = 18 \cdot 1 + 6,$

$18 = 6 \cdot 3 + 0.$

$\therefore$ $gcd\,(138, 24) = 6$

which divides 18.

$\therefore$ The given equation has a solution.

Now $6 = 24 - 18 \cdot 1$

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

$= 24 - 138 \cdot 1 + 24 \cdot 5$

$= 24 \cdot 6 - 138 \cdot 1$

$= 24 \cdot 6 + (-1) \cdot 138$

Multiplying the above relation by 3, by get

$18 = 3\,[24 \cdot 6 + (-1) \cdot 138]$

$\Rightarrow$ $18 = 24 \cdot 18 + (-3) \cdot 138$

$\Rightarrow$ $x_0 = 18,\ y_0 = -3$

provide one solution to the given Diophantine equation.

Thus the general solution is given by

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

$$y = y_0 - \left(\frac{a}{d}\right)t$$

$\Rightarrow$ $$x = 18 + \left(\frac{138}{6}\right)t,$$

$$y = -3 - \left(\frac{24}{6}\right)t$$

$\Rightarrow$ $x = 18 + 23t,$

$y = -3 - 4t.$

Example 98. *Determine all solutions in the integers of the Diophantine equation* $221x + 35y = 11$.

Solution. Let us evaluate the *gcd* of 221 and 35.

$221 = 35 \cdot 6 + 11,$

$35 = 11 \cdot 3 + 2,$

$11 = 2 \cdot 5 + 1,$

$2 = 1 \cdot 2 + 0$

$\therefore$ $gcd\,(221, 35) = 1$ which divides 11.

Hence the given equation has a solution.

Now, $1 = 11 - 2 \cdot 5$

$= 11 - (35 - 11 \cdot 3) \cdot 5$

$= 11 - 35 \cdot 5 + 11 \cdot 15$

$= 11 \cdot 16 - 35 \cdot 5$

$= (221 - 35 \cdot 6) \cdot 16 - 35 \cdot 5$

$= 221 \cdot 16 - 35 \cdot 96 - 35 \cdot 5$

$= 221 \cdot 16 - 35 \cdot 101$

$= 221 \cdot 16 + (-101) \cdot 35$

Multiplying the above relation by 11, we get

$11 = 11\,[221 \cdot 16 + (-101) \cdot 35]$

$\Rightarrow \quad 11 = 221 \cdot 176 + (-1111) \cdot 35$

$\Rightarrow \quad x = 176,\ y = -1111$

which provides one solution to the given Diophantine equation.

Thus the general solution is given by

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

$$y = y_0 - \left(\frac{a}{d}\right)t$$

$$\Rightarrow \quad x = 176 + \left(\frac{35}{1}\right)t,$$

$$y = -1111 - \left(\frac{221}{1}\right)t$$

$$\Rightarrow \quad x = 176 + 35t,$$

$$y = -1111 - 221t.$$

Example 99. *Given one solution in positive integers of the equation $ax + by = c$, find the general solution.*

Solution. If h, k be a solution of $ax + by = c$, then

$$ah + bk = c.$$

Hence $ax + by = ah + bk$ gives

$$a(x - h) = b(k - y).$$

Thus $\frac{x-h}{b} = \frac{k-y}{a} = n,$

where n is an integer.

Therefore, $x = h + bn,$

$y = k - an$ is the general solution.

Example 100. *Find the number of solutions in positive integers of the equation $ax + by = c$.*

Solution. Convert ab into a continued fraction and let $p \mid q$ be the convergent just preceding $a \mid b$; then $aq - bp = \pm 1$.

Case I

Let $aq - bp = +1$.

Then the general solution is

$$x = cq - bn.$$

$$y = an - cp.$$

Positive integral values will be in hand by assigning to n positive integral values not greater than $cq \mid b$ and not less than $cp \mid a$.

(i) Assume that $c \mid a$ and $c \mid b$ are not integers.

Let $\quad cp \mid a = r + f$

$$cq \mid b = s + g.$$

r, s are positive integers and f, g are proper fractions such that $0 \le f < 1$ and $0 < g \le 1$.

Then the least value n can have is $r + \ldots\ldots$, and the greatest value is s, hence N,

The number of solution is

$$N = s - r = cq \mid b - pc \mid b + f - g$$

$$= c \mid ab + f - g.$$

This is now an integer, and may be written $c \mid ab + a$ fraction or $c \mid ab - a$ fraction, according as f is greater than or less than g.

(ii) Assume that $c \mid b$ is an integer.

In this case $g = 0$ and one value of x is gero.

If this is included, $N = c \mid ab + f$, which must be an integer.

Hence the number of solutions is the greatest integer in $c \mid ab$, according as the zero solution is included or excluded.

(iii) Assume that $c \mid a$ is an integer.

In this case $f = 0$ and one value of y is zero.

If this is included, the least value of n is r and the greatest is s, hence

$$N = r - s + 1 \quad \text{Or}$$

$$c \mid (ab) - g - 1.$$

Thus the number of solutions is the greatest integer in $c \mid ab + 1$. Or $c \mid ab$ accordi as the zero solution is included or excluded.

(iv) Assume that $c \mid a$ and $c \mid b$ are both integers.

In this case $f = 0$, $g = 0$ and also $x = 0$, $y = 0$.

Including these, the least value n can have is r and the greatest is s.

Hence the number of solutions is $r - s + 1$ or $c \mid ab + 1$.

In view of exclusion of zero values, the number of solutions is $c \mid ab - 1$.

Case 2

If $aq - bp = -1$, the general solution is $x = bn - cq$, $y = cp - an$ and we have simila results.

Example 101. *Investigate the greatest and the least value of c, in order that the intermediate equation $ax + by = c$ may have exactly N solutions in positive integers (zero solutions, being excluded).*

Solution. Assume that $x = h$, $y = k$ is a particular solution of $ax + by = c$ and that h is the least value that x can have for any particular value of c; so k is the greatest value of y.

The general solution is

$$x = h + bn, \; y = k - an,$$

where n is restricted to the values $0, 1, 2, \ldots\ldots, N - 1$.

In fact, zero solutions are inadmissible, and hence h must lie between 1 and $b - 1$, whereas k must lie between $1 + a(N - 1)$ and $a - 1 + a(N - 1)$.

Now $c = ah + bk$ and the greatest values of h and k are $b - 1$ and $a - 1 + a(N - 1)$ respectively.

Hence the greatest value of

$$c = (N + 1)\, ab - a - b.$$

In view of the least values of h and k being 1 and $1 + a(N - 1)$ respectively, the least value of c is $(N - 1)\, ab + a + b$.

Example 102. *Find a positive integer, which when multiplied by 13 and divided by 17 yields a quotient which exceeds 7 times the remainder by unity. Show that there exist only two such integers.*

Solution. Let us denote the remainder by y and a positive integer to be determined by x.

Then, we have

$$13x = 17(7y + 1) + y$$

$$\Rightarrow \quad 13x = 120y + 17$$

$$\Rightarrow \quad 13x - 120y = 17.$$

Expressing $\frac{120}{13}$, as continued fracti

$$\frac{p_1}{q_1} = 9, \frac{p_2}{q_2} = \frac{37}{4}, \frac{p_3}{q_3} = \frac{120}{13},$$

and $37 \cdot 13 - 120 \cdot 4 = 1$

Then $13x - 120y = 17 = 17(37 \cdot 13 -$

giving $13(x - 629) = 120(y - 68)$

But $gcd(13, 120) = 1$

and hence $(x - 629) \mid 120 = (y - 68)$

where $n = 0, \pm 1, \pm 2, \ldots\ldots$

Thus the general solution of the inter

$$13x - 120y = 17 \text{ is}$$

$$x = 629 + 120n, \; y = 68 + 13n,$$

where $n = 0, \pm 1, \pm 2, \ldots\ldots$

Particularly, if $n = -5$ and $n = -4$,

We have $x = 29$, $y = 3$ and $x = 149$, y

Hence 29, 149 are the only integers v

Example 103. *Prove that if $n > 1$, then* $\sum_{j=}^{n}$

Solution. Before proving the required res

Since $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$,

which is an integer,

$\Rightarrow \quad bd \mid ad + bc$

$\Rightarrow \quad b \mid ad + bc$ and $d \mid ad + bc$

$b \mid ad$ and $d \mid bc$

Then, we have

$13x = 17(7y + 1) + y$

$\Rightarrow \quad 13x = 120y + 17$

$\Rightarrow \quad 13x - 120y = 17.$

Expressing $\frac{120}{13}$, as continued fraction, we have

$$\frac{p_1}{q_1} = 9, \frac{p_2}{q_2} = \frac{37}{4}, \frac{p_3}{q_3} = \frac{120}{13},$$

and $37 \cdot 13 - 120 \cdot 4 = 1$

Then $13x - 120y = 17 = 17(37 \cdot 13 - 120 \cdot 4)$

giving $13(x - 629) = 120(y - 68)$

But $gcd(13, 120) = 1$

and hence $(x - 629) \mid 120 = (y - 68) \mid 13 = x,$

where $n = 0, \pm 1, \pm 2, \ldots\ldots$

Thus the general solution of the intermediate equation

$13x - 120y = 17$ is

$x = 629 + 120n, y = 68 + 13n,$

where $n = 0, \pm 1, \pm 2, \ldots\ldots$

Particularly, if $n = -5$ and $n = -4,$

We have $x = 29, y = 3$ and $x = 149, y = 16.$

Hence 29, 149 are the only integers which were to be determined.

Example 103. Prove that if $n > 1$, *then* $\sum_{j=1}^{n} \frac{1}{j}$ *is an integer.*

Solution. Before proving the required result first we show that if $\frac{a}{b} + \frac{c}{d}$ is an integer then $|b| = |d|$.

Since $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$,

which is an integer.

$\therefore \quad bd \mid ad + bc$

$\Rightarrow \quad b \mid ad + bc$ and $d \mid ad + bc$

$\Rightarrow \quad b \mid ad$ and $d \mid bc$

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

$\Rightarrow$ $b = \pm d$

$\Rightarrow$ $|b| = |d|$ $(\because (a, b) = 1 = |c|$

Now to prove $\sum_{j=1}^{n} \frac{1}{j}$ is an integer.

Let $x = \sum_{j=1}^{n} \frac{1}{j}$ is an integer.

Let $S = \{1, 2, 3, 4, \ldots\ldots, n\}$

Let 2^k be an integer in S which is highest power of 2.

Consider $y = x - \frac{1}{2^k}$

Since x is an integer and $\frac{1}{2^k}$ is perfect fraction,

$\therefore$ y is perfect fraction say, $y = \frac{a}{b}$ where $(a, b) = 1$.

Then from (1), we have

$$x = y + \frac{1}{2^k}$$

i.e $$x = \frac{a}{b} + \frac{1}{2^k}$$

Since x is an integer

$\therefore$ $\frac{a}{b} + \frac{1}{2^k}$ is an integer

$\Rightarrow$ $b = 2^k$

$\therefore$ (1) $\Rightarrow \frac{a}{b} = \sum_{j=1}^{n} \frac{1}{j} - \frac{1}{2^k}$

$$= \left(1 + \frac{1}{2} + \frac{1}{3} + \ldots\ldots + \frac{1}{2^{k-1}} + \frac{1}{2^k} + \frac{1}{2^{k+1}} + \ldots + \frac{1}{n}\right) - \frac{1}{2^k}$$

$\Rightarrow$ $$\frac{a}{b} = \frac{N}{1 \cdot 2 \cdot 3 \ldots\ldots (2^k - 1)(2^k + 1) \ldots n}$$

where N is numerator.

Since L.H.S. is a reduced fraction say, L.H.S. be obtained from R.H.S. by cancelling common factor α from the numerator and denominator.

$\therefore$ $N = \alpha a$ ....(2)

and $1 \cdot 2 \cdot 3 \ldots\ldots (2^k - 1)(2^k + 1) \ldots n = ab$

Now (2) implies

$b \mid 1 \cdot 2 \cdot 3 \ldots\ldots (2^k - 1)(2^k + 1) \ldots n$

$\Rightarrow$ $2^k \mid 1 \cdot 2 \cdot 3 \ldots\ldots (2^k - 1)(2^k + 1) \ldots n$,

which is impossible.

$\therefore$ Our supposition is wrong.

Hence $\sum_{j=1}^{n} \frac{1}{j}$ is not an integer.

Example 104. Show that $\sum_{j=1}^{n} \frac{1}{2j-1}$ *is not an integer for* $n > 1$.

Solution. Before proving the required result first we show that if $\frac{a}{b} + \frac{c}{d}$ is an integer, then $|b| = |d|$.

Suppose $x = \sum_{j=1}^{n} \frac{1}{2j-1}$ is an integer. ....(1)

Let $S = \{1, 3, 5, \ldots\ldots, 2n - 1\}$.

Let 3^k be the integer in S which is highest power of 3.

Consider $y = x - \frac{1}{3^k}$

Since x is an integer and $\frac{1}{3^k}$ is perfect fraction.

$\therefore$ y is perfect fraction, say

$y = \frac{a}{b}$ such that $(a, b) = 1$

Since (1) $\Rightarrow$ $x = y + \frac{1}{3^k}$

$$= \frac{a}{b} + \frac{1}{3^k}$$

Since x is an integer

$$\Rightarrow \quad \frac{a}{b} + \frac{1}{3^k} \text{ is an integer}$$

$$\Rightarrow \quad b = 3^k$$

$$\therefore \text{ (1)} \Rightarrow \frac{a}{b} = \sum_{j=1}^{n} \frac{1}{2j-1} - \frac{1}{3^k}$$

$$= \left(1 + \frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{3^k - 2} + \frac{1}{3^k} + \frac{1}{3^k + 2} + \ldots + \frac{1}{n}\right) - \frac{1}{3^k}$$

$$i.e \quad \frac{a}{b} = \frac{N}{1 \cdot 3 \cdot 5 \ldots (3^k - 2)(3^k + 2) \ldots n},$$

where N is the numerator.

Since L.H.S. is a reduced fraction.

Let L.H.S. be obtained from R.H.S. by cancelling a common factor α from the numerator and denominator.

$$\therefore \quad N = \alpha a$$

and $\quad 1 \cdot 3 \cdot 5 \ldots (3^k - 2)(3^k + 2) \ldots n = \alpha b$

Since (2) implies

$$b \mid 1 \cdot 3 \cdot 5 \ldots (3^k - 2)(3^k + 2) \ldots n$$

$$\Rightarrow \quad 3^k \mid 1 \cdot 3 \cdot 5 \ldots (3^k - 2)(3^k + 2) \ldots n,$$

which is impossible.

$\therefore$ our supposition is wrong.

Hence $\sum_{j=1}^{n} \frac{1}{2j-1}$ is not an integer if $n > 1$.

❑❑❑

2 CHAPTER

PRIMES AND THEIR DISTRIBUTION

PRIMES

A positive integer p is said to be *prime* if $p > 1$ and p has no divisors except 1 and p. *i.e* a number which has exactly two different factors, itself and one, is called a prime number.

Thus 2, 3, 5, 7, 11,..... are primes.

Note

2 is the only even prime number.

COMPOSITE

An integer greater 1 that is not a prime is called *composite*.

Theorem 1. ***If p is a prime and p | ab, then p | a or p | b.***

Or

If a prime number divides the product of two integers, then it must divide one of them.

Proof. Since $p \mid ab$,

Therefore there exists an integer c such that

$$ab = pc \qquad \ldots(1)$$

Since p is prime,

$\therefore$ either $p \mid a$ or $gcd\,(p, a) = 1$.

If $p \mid a$, then obviously the theorem is proved.

If $gcd\,(p, a) = 1$,

then there exists integers x and y such that

$$px + ay = 1$$

Multiplying both sides by b, we get

$$pbx + aby = b$$

Putting $ab = pc$ from (1), we get

$$pbx + pcy = b$$
$$\Rightarrow \quad p(bx + cy) = b$$
$$\Rightarrow \quad p \mid b$$

Hence $p \mid ab \Rightarrow p \mid a$ or $p \mid b$. [by definition of divisibi

Corollary. *If $p \mid a_1 a_2 \ldots\ldots a_n$, then p divides a_i for some i.*

Or

If p is a prime number and $a_1, a_2, \ldots\ldots, a_n$ are integers such that $p \mid a_1 a_2 \ldots\ldots a_n$ then pro that $p \mid a_k$ for some k, $1 \le k \le n$.

Proof. We have

$$p \mid (a_1 a_2 \ldots\ldots a_n)$$

If $p \mid a_1$, then the theorem is proved.

If p is not a divisor of a_1, then p is relatively prime to a_1.

Therefore $p \mid a_1 (a_2 a_3 \ldots\ldots a_n)$

$$\Rightarrow \quad p \mid (a_2 a_3 \ldots\ldots a_n).$$

If $p \mid a_2$, then the theorem is proved.

If p is not a divisor of a_2, then p is relatively prime to a_2.

Therefore,

$$p \mid a_2 (a_3 a_4 \ldots\ldots a_n)$$
$$\Rightarrow \quad p \mid (a_3 a_4 \ldots\ldots a_n)$$

Repeating this process, it follows that, at least, $p \mid a_n$ if p does not divide any of $a_1, a_2, \ldots\ldots, a_{n-1}$.

Corollary. *If $p, q_1, q_2, \ldots\ldots, q_n$ are all primes and $p \mid q_1 q_2 \ldots\ldots q_n$, then $p = q_k$ for some k where $1 \le k \le n$.*

Proof. Using the corollary, "If p is a prime and $p \mid a_1 a_2 \ldots\ldots a_n$ then $p \mid a_k$ for some k where $1 \le k \le n$,",

we know that $p \mid q_k$ for some k, with $1 \le k \le n$.

Being a prime, q_k is not divisible by any positive integer other than one or q_k itself.

Since $p > 1$, so we have $p = q_k$.

Theorem 2. ***State and prove fundamental theorem of arithmetic.***

Statement. Every natural number > 1 can be expressed as a product of primes in one and only one way.

Proof. Let n be a natural number >
Since we know that every natu
Therefore n has a prime factor,
i.e. $p_1 \mid n$
$\therefore$ there exists an integer n_1 su
$n = n_1 p_1$ where $n > n_1$
If $n_1 = 1$,
$n = p_1$ i.e. n is a prime p_1.
If $n_1 > 1$, then n_1 has a prime f
admits of a prime factor so there ex
$n_1 = p_2 n_2$ where $n_1 > n_2$
Putting this value of n_1 in (1), w
$n = p_1 p_2 n_2$ where $n > n_1$
If $n_2 = 1$, then $n = p_1 p_2$
i.e. n is the product of primes p_1
If $n_2 > 1$, we continue this proces
But this process must terminate a
(Since n is finite and $n > n_1 > n_2$
Therefore, there exist primes p_1,
$n = p_1 p_2 \ldots\ldots p_r$
Uniqueness Let if possible, $n = q$
be a second factorization of n as a
From (3) and (4), we have
$p_1 p_2 \ldots\ldots p_r = q_1 q_2 \ldots\ldots q_s$
Now (5) shows that prime p_1 is a f
Therefore p_1 must divide at least o
But q_1 is prime,
$\therefore$ either $p_1 = 1$ or $p_1 = q_1$.
But $p_1 = 1$ is not possible because p

Proof. Let n be a natural number > 1.

Since we know that every natural number other than 1 admits of a prime factor.

Therefore n has a prime factor, say, p_1.

i.e. $p_1 \mid n$

$\therefore$ there exists an integer n_1 such that

$$n = n_1 p_1 \text{ where } n > n_1 \quad \ldots(1)$$

If $n_1 = 1$,

$n = p_1$ i.e. n is a prime p_1.

If $n_1 > 1$, then n_1 has a prime factor p_2 because every natural number other than one admits of a prime factor so there exists a positive integer n_2 such that

$$n_1 = p_2 n_2 \text{ where } n_1 > n_2.$$

Putting this value of n_1 in (1), we get

$$n = p_1 p_2 n_2 \text{ where } n > n_1 > n_2 \quad \ldots(2)$$

If $n_2 = 1$, then $n = p_1 p_2$

i.e. n is the product of primes p_1 and p_2.

If $n_2 > 1$, we continue this process.

But this process must terminate after a finite number of steps.

(Since n is finite and $n > n_1 > n_2 > \ldots\ldots$)

Therefore, there exist primes $p_1, p_2, \ldots\ldots, p_r$ such that

$$n = p_1 p_2 \ldots\ldots p_r \quad \ldots(3)$$

Uniqueness Let if possible, $n = q_1 q_2 \ldots\ldots q_s$ $\ldots(4)$

be a second factorization of n as a product of prime.

From (3) and (4), we have

$$p_1 p_2 \ldots\ldots p_r = q_1 q_2 \ldots\ldots q_s \quad \ldots(5)$$

Now (5) shows that prime p_1 is a factor of the product $q_1 q_2 \ldots\ldots q_s$.

Therefore p_1 must divide at least one of these primes say q_1.

But q_1 is prime,

$\therefore$ either $p_1 = 1$ or $p_1 = q_1$.

But $p_1 = 1$ is not possible because p_1 being prime > 1.

$\therefore \quad p_1 = q_1$.

Therefore (5) becomes

$$p_1 p_2 \ldots\ldots p_r = p_1 q_2 q_3 \ldots\ldots q_s$$

Or $$p_2 p_3 \ldots\ldots p_r = q_2 q_3 \ldots\ldots q_s$$

As before, p_2 must be equal to some one of the primes

$$q_2 , q_3 \ldots\ldots, q_s .$$

Without any loss of generality, we have

$$p_2 = q_2 .$$

Therefore (6) becomes

$$p_2 p_3 \ldots\ldots p_r = p_2 q_3 \ldots\ldots q_s$$

Or $$p_3 p_4 \ldots\ldots p_r = q_3 q_4 \ldots\ldots q_s$$

Similarly, we have

$$p_3 = q_3 , p_4 = q_4 \text{ and so on.}$$

Finally, we prove that $r = s$.

If possible, let $r > s$.

Therefore equation (5) can be written as

$$p_1 p_2 \ldots\ldots p_s p_{s+1} \ldots\ldots p_r = q_1 q_2 \ldots\ldots q_s$$

Putting $q_1 = p_1 , q_2 = p_2 \ldots\ldots q_s = p_s$, we have

$$p_1 p_2 \ldots\ldots p_s p_{s+1} \ldots\ldots p_r = p_1 p_2 \ldots\ldots p_s$$

Dividing both sides by $p_1 p_2 \ldots\ldots p_s$, we get

$$p_{s+1} \ldots\ldots p_r = 1.$$

But this is not possible because each of the factors on L.H.S. being prime > 1.

$\therefore \quad r \not> s.$

Similarly $r \not< s$.

Hence the two factorizations of n namely $p_1 p_2 \ldots\ldots p_r$ and $q_1 q_2 \ldots\ldots q_s$ are identical.

Corollary. *Any positive integer $n > 1$ can be written uniquely in a canonical form* $n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}$ *; where, for $i = 1, 2, \ldots\ldots r$, each k_i is a positive integer and each p_i is a prime, with $p_1 < p_2 < \ldots\ldots < p_r$.*

Proof. By fundamental theorem of arithmetic $n = p_1 p_2 \ldots\ldots p_s p_i$ primes.

First we lump together the repe

$$n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r k_r .$$

Next we arrange them acc

$p_1 , p_2 \ldots\ldots, p_r$ so that

$$n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_i^{k_i} ; p_1 <$$

and k_i are integers each ≥ 1.

At this point we mention why

Suppose we allowed 1 to be pri

$$n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_s^{k_s}$$

$$= 1^r p_1^{k_1} \ldots\ldots p_s^{k_s}$$

$$= 1^t p_1^{k_1} \ldots\ldots p_s^{k_s}$$

with $r \neq t$.

Thus n can have several repres

representations in fundamental the

Uniqueness part in FTA (funda

are number systems in which we

uniqueness is guaranteed.

e.g. Let $E = Ze$, the even integers,

product of 2 or more even integers,

e.g. 6, 10, 14, 18,..... are all prime

Now $60 = 10 \cdot 6 = 2 \cdot 30$

$120 = 10 \cdot 6 \cdot 2 = 2^2 \cdot 30$

Therefore there exists even inte

PYTHAGORAS THEOREM

Theorem 3. *The number $\sqrt{2}$ is irr*

$\sqrt{2}$ is not a rational number.

Proof. Suppose $\sqrt{2}$ is a rational nu

Hence set $\sqrt{2} = \frac{a}{b}$ where a, b a

Since $\sqrt{2} = \frac{a}{b}$

First we lump together the repeated primes, then n can be written as

$$n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r k_r .$$

Next we arrange them according to ascending order and rename them as $p_1, p_2, \ldots\ldots, p_r$ so that

$$n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_i^{k_i} ; p_1 < p_2 < \ldots\ldots < p_r$$

and k_i are integers each ≥ 1.

At this point we mention why we have excluded 1 from being a prime. Suppose we allowed 1 to be prime, then for any n

$$\begin{aligned} n &= p_1^{k_1} p_2^{k_2} \ldots\ldots p_s^{k_s} \\ &= 1^r p_1^{k_1} \ldots\ldots p_s^{k_s} \\ &= 1^t p_1^{k_1} \ldots\ldots p_s^{k_s} \end{aligned}$$

with $r \neq t$.

Thus n can have several representations as product of primes, so that uniqueness of representations in fundamental theorem of arithmetic is lost.

Uniqueness part in FTA (fundamental theorem of arithmetic) is a deep result as there are number systems in which we can factorize integers into product of prime but no uniqueness is guaranteed.

e.g. Let $E = Ze$, the even integers, call an even integers a prime if it cannot be written as product of 2 or more even integers,

e.g. 6, 10, 14, 18,..... are all primes of E.

Now $60 = 10 \cdot 6 = 2 \cdot 30$

$120 = 10 \cdot 6 \cdot 2 = 2^2 \cdot 30$

Therefore there exists even integers with more than one representation.

PYTHAGORAS THEOREM

Theorem 3. ***The number $\sqrt{2}$ is irrational***

Or

$\sqrt{2}$ is not a rational number.

Proof. Suppose $\sqrt{2}$ is a rational number.

Hence set $\sqrt{2} = \frac{a}{b}$ where a, b are integers with $gcd\ (a, b) = 1$.

Since $\sqrt{2} = \frac{a}{b}$

Squaring both sides, we get

$$2 = \frac{a^2}{b^2}$$

$$\Rightarrow \quad a^2 = 2b^2$$

is solvable in integers a, b with $gcd\,(a, b) = 1$.

This implies that a^2 is even, and hence a is even.

Setting $a = 2c$, we have

$$4c^2 = 2b^2$$

i.e $\quad 2c^2 = b^2$.

This shows that b is even, contrary to the hypothesis that

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

Therefore this contradiction proves that $\sqrt{2}$ is an irrational.

Second Proof

From (1) it is clear that $b \mid a^2$.

If $b > 1$, then by fundamental theorem of arithmetic there is at least one prime su

that

$$p \mid b \text{ as } b \mid a^2.$$

$$p \mid a^2 \Rightarrow p \mid a.$$

$$\therefore \quad gcd\,(a, b) \geq p.$$

But $\quad gcd\,(a, b) = 1$

Thus $\quad b = 1$.

Now $\quad b = 1 \Rightarrow a = \sqrt{2}$.

This is clearly not possible since a is a positive integer.

Example 1. *If a positive integer k is not a perfect square then* $\sqrt{k}$ *is irrational.*

Solution. If possible let $\sqrt{k}$ be rational and $\sqrt{k} = \frac{a}{b}$ where a and b are positive integers su

that $(a, b) = 1$.

Since $\quad \sqrt{k} = \frac{a}{b}$

$$\Rightarrow \quad k = \frac{a^2}{b^2}$$

By fundamental theorem of arith

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_k^{\alpha_k}$$

and $\quad b = p_1^{\beta_1} p_2^{\beta_2} \ldots\ldots p_k^{\beta_k}$

$$\therefore \quad k = \frac{a^2}{b^2} = \frac{p_1^{2\alpha_1} p_2^{2\alpha_2} \ldots\ldots}{p_1^{2\beta_1} p_2^{2\beta_2} \ldots\ldots}$$

$$= p_1^{2(\alpha_1 - \beta_1)} p_2^{2(\alpha_2 -}$$

$$= (p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2}$$

$\Rightarrow k$ is a perfect square,

which leads to a contradictio

Hence $\sqrt{k}$ is irrational.

Example 2. Show that $n^4 + 4$ *is*

Solution. $n^4 + 4 = (n^2 + 2)^2 - 4$

$$= (n^2 + 2 - 2n$$

$$n > 1 \Rightarrow n \geq 2$$

$$\Rightarrow \quad n - 2 \geq 0$$

$$\Rightarrow \quad n^2 - 2n \geq 0$$

$$\Rightarrow \quad n^2 - 2n + 2 \geq 2$$

Also $\quad n^2 + 2 + 2n > 1$

$\therefore n^4 + 4$ is composite a

$n^2 + 2 - 2n$ and

Example 3. Prove that proc

Solution. Let $a = 4k + 1$,

$$b = 4k' + 1$$

be two numbers of the

$$\therefore \quad ab = (4k + 1)($$

$$= 16kk' + 4$$

$$= 4\,(4kk' +$$

By fundamental theorem of arithmetic a and b can be expressed as

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_k^{\alpha_k}$$

and $$b = p_1^{\beta_1} p_2^{\beta_2} \ldots\ldots p_k^{\beta_k}$$

$$\therefore \quad k = \frac{a^2}{b^2} = \frac{p_1^{2\alpha_1} p_2^{2\alpha_2} \ldots\ldots p_k^{2\alpha_k}}{p_1^{2\beta_1} p_2^{2\beta_2} \ldots\ldots p_k^{2\beta_k}}$$

$$= p_1^{2(\alpha_1 - \beta_1)} p_2^{2(\alpha_2 - \beta_2)} \ldots\ldots p_k^{2(\alpha_k - \beta_k)}$$

$$= (p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \ldots\ldots p_k^{\alpha_k - \beta_k})^2$$

$\Rightarrow$ k is a perfect square,
which leads to a contradiction.
Hence $\sqrt{k}$ is irrational.

Example 2. Show that $n^4 + 4$ is composite if $n > 1$.

Solution. $n^4 + 4 = (n^2 + 2)^2 - 4n^2$

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

$n > 1 \Rightarrow n \geq 2$

$\Rightarrow \quad n - 2 \geq 0$

$\Rightarrow \quad n^2 - 2n \geq 0$

$\Rightarrow \quad n^2 - 2n + 2 \geq 2$

Also $n^2 + 2 + 2n > 1$

$\therefore$ $n^4 + 4$ is composite as both

$n^2 + 2 - 2n$ and $n^2 + 2 + 2n > 1$.

Example 3. Prove that product of two numbers of the form $4n + 1$ is of the form $(4n + 1)$.

Solution. Let $a = 4k + 1$,

$$b = 4k' + 1$$

be two numbers of the forms $(4n + 1)$.

$$\therefore \quad ab = (4k + 1)(4k' + 1)$$

$$= 16kk' + 4k + 4k' + 1$$

$$= 4(4kk' + k + k') + 1$$

$= 4m + 1$, where $m = 4kk' + k + k'$

which is of the form $(4n + 1)$.

Example 4. *Show that every odd prime can be put either in the form* $4k + 1$ *or* $4k + 3$ *(i.e* $4k - 1$*), where* k *is a positive integer.*

Solution. Let n be any odd prime.

If we divide any n by 4, we get

$n = 4k + r$ where $0 \le r < 4$.

i.e $r = 0, 1, 2, 3$

$\therefore$ either $n = 4k$ or

$n = 4k + 1$

Or $n = 4k + 2$

Or $n = 4k + 3$

Clearly, $4n$ is never prime and $4n + 2 = 2(2n + 1)$ cannot be prime unless $n = 0$.

($\because$ 4 and 2 cannot be factors of an odd prime)

Therefore an odd prime n is either of the form $4k + 1$ or $4k + 3$.

But $4k + 3 = 4(k + 1) - 4 + 3$

$= 4k' - 1$ where

$k' = k + 1$.

Therefore an odd prime n is either of the form

$4k + 1$ or $(4k + 3)$ *i.e* $4k - 1$.

Example 5. *Prove that every odd prime* > 3 *can be put in the form* $6n + 1$ *or* $6n + 5$.

Solution. Let n be any odd prime > 3.

If we divide n by 6, we get

$n = 6k + r$ where $0 \le r < 6$.

i.e $r = 0, 1, 2, 3, 4, 5$.

Therefore, $n = 6k$ or $6k + 1$ or

$6k + 2$ or $6k + 3$ or $6k + 4$ or $6k + 5$.

Now each of $n = 6k$, $n = 6k + 2$

$= 2(3k + 1)$,

$6k+3 = 3(2k+1)$,

$6k+4 = 2(3k+2)$

is the product of two factors (both > 1) and hence none of these is prime.

Therefore, an odd prime $n > 3$ is of the form $6n+1$ or $6n+5$.

Note

(i) It should be noted that every number of the form $6k+5$ is of the form $6k-1$ and conversely.

(ii) Every number of the form $6k+5$ or $6k+1$ is not necessarily prime.

For example,

$35 = 6 \cdot 5 + 5$ is of the form $6k+5$, but 35 is not prime;

$49 = 6 \cdot 8 + 1$ is of the form $6k+1$ but is not prime.

(iii) If $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_k^{\alpha_k}$, the number of divisors of $n = (\alpha_1+1)(\alpha_2+1) \ldots\ldots (\alpha_k+1)$.

Example 6. Find the number of divisors of 600.

Solution. $n = 600$

$= 2 \times 2 \times 150$

$= 2 \times 2 \times 2 \times 75$

$= 2^3 \times 3^1 \times 25$

$= 2^3 \times 3^1 \times 5^2$

Hence $\alpha_1 = 3, \alpha_2 = 1, \alpha_3 = 2$.

Therefore, number of divisors of

$n = (\alpha_1+1)(\alpha_2+1)(\alpha_3+1)$

$= (3+1)(1+1)(2+1)$

$= 4 \times 2 \times 3$

$= 24$.

Example 7. Find the number of divisors of 9504.

Solution. Here $n = 9504$

$\therefore \quad n = 9504$

$= 2 \times 2 \times 2 \times 2 \times 2 \times 3 \times 3 \times 3 \times 11$

$= 2^5 \cdot 3^3 \cdot 11^1$

2	9504
2	4752
2	2376
2	1188
2	594
3	297
3	99
3	33
	11

Comparing with

$n = p_1^{\alpha_1} p_1^{\alpha_2} \ldots\ldots$, we have $\alpha_1 = 5, \alpha_2 = 3, \alpha_3 = 1$.

Therefore, number of divisors are

$$n = (\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1)$$
$$= (5 + 1)(3 + 1)(1 + 1)$$
$$= 6 \times 4 \times 2 = 48.$$

Theorem 4. Prove that if $n > 1$ is composite then it must have a prime factor p where $p \le \sqrt{n}$.

Proof. Since n is a composite number,

$\therefore\ n = ab$ for some $1 < a, b < n$

Without any loss of generality, let

$$a \le b$$
$$\Rightarrow \quad a^2 \le ab$$
$$\Rightarrow \quad a^2 \le n$$
$$\Rightarrow \quad a \le \sqrt{n}$$

Since $a > 1$, therefore, a has at least one prime factor, say, p.

$$\Rightarrow \quad p \le a \le \sqrt{n}$$

Also $p \mid a \Rightarrow p \mid ab \Rightarrow p \mid n$

Thus $p \mid n$ and $p \le \sqrt{n}$

Note

In order to check whether a given integer n is a prime or not, it is sufficient to check whether it is divisible by any of the prime $\le \sqrt{n}$.

e.g. Check whether 271 is a prime or not.

Solution. Let $n = 271$

Since $16 < \sqrt{271} < 17$

Therefore if n is composite number then there

$p \le \sqrt{271}$.

But all primes $\le \sqrt{271}$ are 2, 3, 5, 7, 11, 13 and

Hence 271 is a prime number.

THE SIEVE OF ERATOSTHENES

Given a particular integer, how can we determi

The most obvious approach consists of succes

by each of the numbers preceding it; if none of th

the integer must be prime.

Although this method is very simple to descr

practice.

There is a property of composite numbers th

necessary computations – but still the process rem

If an integer $a > 1$ is composite, then it may b

$1 < c < a$.

Let us assume that $b \le c$, we get $b^2 \le bc = a$ a

Since $b > 1$, then fundamental theorem of ar

prime factor p. Then $p \le b \le \sqrt{a}$.

Furthermore, since $p \mid b$ and $b \mid a$, it follows

will always possess a prime divisor p satisfying

In testing the primality of a specific integer a

not exceeding $\sqrt{a}$. This may be clarified by cons

In as much as $22 < \sqrt{509} < 23$, we need only

22 as possible divisors, namely, the primes 2, 3,

Dividing 509 by each of these, in turn, we

The conclusion is that 509 must be a prime num

Another Greek mathematician whose work

Eratosthenes of Cyrene (276–194 B.C).

He was nicknamed 'Beta' because it was sa

Perhaps the most impressive feat of Eratosthe

earth's circumference by a simple application o

We have seen that if an integer $a > 1$ is not

be a prime.

Solution. Let $n = 271$

Since $16 < \sqrt{271} < 17$

Therefore if n is composite number then there exists a prime factor p of n such that $p \leq \sqrt{271}$.

But all primes $\leq \sqrt{271}$ are 2, 3, 5, 7, 11, 13 and none of these divide 271.

Hence 271 is a prime number.

THE SIEVE OF ERATOSTHENES

Given a particular integer, how can we determine whether it is prime or composite ?

The most obvious approach consists of successively dividing the integer in question by each of the numbers preceding it; if none of them (except 1) serves as a divisor, then the integer must be prime.

Although this method is very simple to describe, it cannot be regarded as useful in practice.

There is a property of composite numbers that allows us to reduce materially the necessary computations – but still the process remains cumbersome.

If an integer $a > 1$ is composite, then it may be written as $a = bc$, where $1 < b < a$ and $1 < c < a$.

Let us assume that $b \leq c$, we get $b^2 \leq bc = a$ and so $b \leq \sqrt{a}$.

Since $b > 1$, then fundamental theorem of arithmetic ensures that b has at least one prime factor p. Then $p \leq b \leq \sqrt{a}$.

Furthermore, since $p \mid b$ and $b \mid a$, it follows that $p \mid a$ because a composite number a will always possess a prime divisor p satisfying $p \leq \sqrt{a}$.

In testing the primality of a specific integer $a > 1$, it suffices to divide a by those primes not exceeding $\sqrt{a}$. This may be clarified by considering the integer $a = 509$.

In as much as $22 < \sqrt{509} < 23$, we need only try out the primes that are not larger than 22 as possible divisors, namely, the primes 2, 3, 5, 7, 11, 13, 17, 19.

Dividing 509 by each of these, in turn, we find that none serves as a divisor of 509. The conclusion is that 509 must be a prime number.

Another Greek mathematician whose work in number theory remains significant is Eratosthenes of Cyrene (276–194 B.C).

He was nicknamed 'Beta' because it was said, he stood at least second in every field. Perhaps the most impressive feat of Eratosthenes was the accurate measurement of the earth's circumference by a simple application of Euclidean geometry.

We have seen that if an integer $a > 1$ is not divisible by any prime $p \leq \sqrt{a}$, then a must be a prime.

Eratosthene used this fact as the basis of a clever technique, called the *Sieve of Erathosthenes*, for finding all prime below a given integer n. The scheme calls for writing down the integers from 2 to n in their natural order and then systematically eliminating all the composite numbers by striking out all multiples $2p, 3p, 4p, 5p,....$ of the primes $p \leq \sqrt{n}$. The integers that are leh on the list-those that do not fall through the "sieve" - areprimes.

Now we illustrate how this works,

Suppose we want to find all primes not exceeding 100.

Consider the sequence of consecutive integers 2, 3, 4,....., 100.

Recognizing that 2 is a prime, we begin by crossing out all even integers from our listing, except 2 itself.

The first of the remaining integers is 3, which mist be a prime. We keep 3, but strike out all higher multiples of 3 so that 9, 15, 21,..... are now removed (the even multiples of 3 having been removed in the previous step).

The smallest integer after 3 that has not yet been deleted is 5. It is not divisible by either 2 or 3 – otherwise it would have been crossed out-hence, it is also a prime.

All proper multiples of 5 being composite numbers, we next remove 10, 15, 20,....., while retaining 5 itself.

The first surviving integer 7 is a prime, for it is not divisible by 2, 3, or 5, the only primes that precedes it. After eliminating the proper multiples of 7, the largest prime less than $\sqrt{100} = 10$, all composite integers in the sequence 2, 3, 4,....., 100 have fallen through the sieve.

The positive integers that remain, to wit, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, all are of the primes less than 100.

The following table represents the result of the completed sieve. The multiples of 2 are crossed out by \ ; the multiples of 3 are crossed out by /; the multiples of 5 are crossed out by —; the multiples of 7 are crossed out by ~

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
		~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
~~91~~	~~92~~								

EUCLID

Theorem 5. There is an infinite nu

Prove that the number of primes is

Show that there are infinitely many

Prove that there are an infinite nu

Proof. If possible suppose that numb

Therefore there exists the greate

Let b denote the product of these

i.e $b = 2.3.5 \ldots\ldots\ldots t$

Let $a = b + 1$

Clearly $a \neq 1$.

Therefore, the number a must ha

i.e $p \mid a$ ($\because$ every natural numb

Now p is one of the primes 2, 3

$\therefore p \mid b$

Since $p \mid a$ and $p \mid b$,

therefore $p \mid a - b$

Or $p \mid 1$

Or $p = 1$, which is not possibl

So our assumption is wrong.

Therefore the number of prime

2nd Proof

Suppose there are only finite n

Let us define $P = p_1 p_2 \ldots\ldots p_k$

As $p > 1$ and P cannot be prim

theorem of arithmetic.

Since only primes are $p_1 p_2 \ldots$

$p = p_i$.

p_i then $p_i \mid P$

not possibl

EUCLID

Theorem 5. *There is an infinite number of primes.*

Or

Prove that the number of primes is infinite.

Or

Show that there are infinitely many primes amongst natural numbers.

Or

Prove that there are an infinite number of primes.

Proof. If possible suppose that number of primes is finite.

Therefore there exists the greatest prime say t.

Let b denote the product of these primes 2, 3, 5,....., t

i.e $b = 2 \cdot 3 \cdot 5 \ldots\ldots t$ ....(1)

Let $a = b + 1$ ....(2)

Clearly $a \neq 1$.

Therefore, the number a must have a prime factor say p

i.e $p \mid a$ ($\because$ every natural number other than 1 admits of a prime factor)

Now p is one of the primes 2, 3, 5,....., t

($\because b = 2 \cdot 3 \cdot 5 \ldots\ldots t$)

$\therefore p \mid b$

Since $p \mid a$ and $p \mid b$,

therefore $p \mid a - b$ [From (2), $a - b = 1$]

Or $p \mid 1$

Or $p = 1$, which is not possible. ($\because$ 1 is not a prime number)

So our assumption is wrong.

Therefore the number of primes is infinite.

2nd Proof

Suppose there are only finite number of primes, say $p_1, p_2, \ldots\ldots, p_k$.

Let us define $P = p_1 p_2 \ldots\ldots p_k + 1$.

As $p > 1$ and P cannot be prime, there exists a prime p such that $p \mid P$ by fundamental theorem of arithmetic.

Since only primes are $p_1 p_2 \ldots\ldots p_k$ there exists an i such that

$p = p_i$.

If $p = p_i$ then $p_i \mid P$.

But this is not possible by definition of P; hence a contradiction.

Thus the number of primes cannot be finite.

Note

The above proof is interesting, if we let

$$P_k = p_1 p_2 \ldots\ldots p_k + 1$$

where $p_1, p_2, \ldots\ldots, p_k$ are the first k primes; then

$$P_1 = 2 + 1 = 3$$

$$P_2 = 2 \cdot 3 + 1 = 7$$

$$P_3 = 2 \cdot 3 \cdot 5 + 1 = 31$$

$$P_4 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$$

$$P_5 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$$

are all primes.

Thus $P_k = 2 \cdot 3 \ldots\ldots p_k + 1$,

where p_k is the k^{th} prime shall give all primes.

But then

$$P_6 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 13 + 1$$

$$= 30031 = 59 \cdot 509$$

$$P_7 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1$$

$$= 510511 = 19 \cdot 97 \cdot 277$$

$$P_8 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 + 1$$

$$= 9699691 = 347 \cdot 27953,$$

all are composite.

Theorem 6. Prove that there are arbitrarily large gaps in the sequence of primes.

Or

Given any positive integer n, prove that there exist n consecutive composite num

Proof. Let n be any positive integer.

Consider n consecutive integers

$$(n+1)! + 2, (n+1)! + 3, \ldots\ldots, (n+1)! + (n+1) \quad \ldots (1)$$

Since $k \mid (n+1)! + k \;\forall\; 2 \le k \le n+1$,

therefore each number in sequence (1) is composite.

Thus we can find n consecutive composite integers for any given $n \in N$.

Hence there are arbitrarily large gaps in the sequence of primes.

Theorem 7. *If P_n is the nth prime number, then $p_n \le 2^{2^{n-1}}$.*

Proof. Let us proceed by induction on n.

If $n = 1$, the result is clearly true.

Let us assume that $n > 1$.

Also assume that the result holds for all integers upto n.

Then $p_{n+1} \le p_1 p_2 \ldots\ldots p_n + 1$

$$\le 2 \cdot 2^2 \ldots\ldots 2^{2^{n-1}} + 1 \qquad \ldots\ldots(1)$$

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

Since we know that $1 + 2 + 2^2 + \ldots\ldots + 2^{n-1} = 2^n - 1$, therefore (1) becomes

$$P_{n+1} \le 2^{2^{n-1}} + 1.$$

However, $1 \le 2^{2^{n-1}}$ for al n ;

whereas

$$p_{n+1} \le 2^{2^{n-1}} + 2^{2^{n-1}} = 2 \cdot 2^{2^{n-1}} = 2^{2^n}$$

$$\Rightarrow \quad p_{n+1} \le 2^{2^n}$$

which shows that the result is true for $n > 1$ whenever it is true for all n.

Also it is true for $n = 1$.

Hence by induction hypothesis the result is true.

Corollary. For $n \ge 1$, there is at least $n + 1$ primes less than 2^{2^n}.

Proof. First prove the previous theorem.

From the theorem, we know that $p_1, p_2, \ldots\ldots, p_{n+1}$ are less than 2^{2^n}.

Note

In 1845, Joseph Bertrand conjectured that the prime numbers are well-distributed in the sense that between $n \ge 2$ and $2n$ there is at least one prime. He was unable to establish his conjecture, but verified it for all $n \le 3{,}000{,}000$. (one way of achieving this is to consider a sequence of prime 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 5003, 9973, 39869, 79699, 159389,....., each of which is less than than twice the preceding.) Because it takes some real effort to substantiate this famous conjecture.

Let us content ourselves with saying that the first proof was carried out by the Russian

mathematician P.L. Tchebycheff in 1852.

Granting the result, it is not difficult to show that

$p_n < 2^n$, $n \geq 2$ and as a direct consequence,

$p_{n+1} < 2p_n$ for $n \geq 2$.

In particular,

$11 = p_5 < 2 \cdot p_4 = 14$.

To see that $p_n < 2^n$, we apply the induction on n.

Clearly, $p_2 = 3 < 2^2$, so that the inequality is true here.

Now let us assume that the equality holds for an integer, n, whence $p_n < 2^n$.

Invoking Bertrand's conjecture, there exists a prime number p satisfying $2^n < p < 2^{n+1}$; that is $p_n < p$, which leads to the conclusion that $p_{n+1} \leq p < 2^{n+1}$, which completes the induction.

Hence the proof.

Note

Primes of special form have been of perennial interest. Among these, the repunit primes are of great importance.

Repunit

A repunit is an integer written (in decimal notation) as a string of 1's, such as 11, 111 or 1111. Each such integer must have the form $(10^n - 1) \mid 9$.

These are denoted by the symbol R_n which consists of n consecutive 1's.

Note

A significant feature of these numbers is the apparent scarcity of primes among them. So, far, only R_2, R_{19}, R_{23}, R_{317}, R_{1031}, R_{49081}, and R_{86453} have been identified as primes (the last one in 2001).

It is known that the only possible repunit primes R_n for all $n \leq 45000$ are the seven numbers just indicated.

No conjecture has been made as to the existence of any others.

For a repunit R_n to be prime, the subscript n must be a prime, *i.e* this is not a sufficient condition is shown by

$R_5 = 11111 \quad = 41 \cdot 271$

$R_7 = 1111111 = 239 \cdot 4649$.

GOLDBACH CONJECTURE

According to Goldbach conjecture,
are either primes or 1.

e.g. $2 = 1 + 1$

$4 = 2 + 2 = 1 + 3$

$6 = 3 + 3 = 1 + 5$

$8 = 3 + 5 = 1 + 7$

$10 = 5 + 5 = 3 + 7$

$12 = 1 + 11 = 5 + 7$

$14 = 3 + 11 = 7 + 7 = 1 +$

In fact if we take integers ≥ 4, th
(G_1) every even integer > 4 ca
either a proof or a counter example ha

Lemma

The product of two or more integer

Proof. Let $a = 4k + 1$

and $b = 4k' + 1$

be two numbers of the form $(4n$

$\therefore \quad ab = (4k + 1)(4k' + 1)$

$= 16kk' + 4k + 4k' +$

$= 4(4kk' + k + k') +$

$= 4m + 1$

where $m = 4kk' + k + k'$ which
By induction, if $a_k = 4n_k + 1$;
$4n + 1$.

Theorem 8. *There are an infinite*

Prove that there are infinite num

Proof. If possible, let number of p
These primes are 3, 7, 11 .....
Let $a = 3 \cdot 7 \cdot$ q be the p

GOLDBACH CONJECTURE

According to Goldbach conjecture, every even integer is the sum of two numbers that are either primes or 1.

e.g. $2 = 1 + 1$

$4 = 2 + 2 = 1 + 3$

$6 = 3 + 3 = 1 + 5$

$8 = 3 + 5 = 1 + 7$

$10 = 5 + 5 = 3 + 7$

$12 = 1 + 11 = 5 + 7$

$14 = 3 + 11 = 7 + 7 = 1 + 13$ etc.

In fact if we take integers ≥ 4, the conjecture can be reformulated as :

(G_1) every even integer > 4 can be written as sum of two odd primes. So far either a proof or a counter example has not been found.

Lemma

The product of two or more integers of the form $4n + 1$ is of the same form.

Proof. Let $a = 4k + 1$

and $b = 4k' + 1$

be two numbers of the form $(4n + 1)$.

$$\therefore \quad ab = (4k + 1)(4k' + 1)$$

$$= 16kk' + 4k + 4k' + 1$$

$$= 4(4kk' + k + k') + 1$$

$$= 4m + 1$$

where $m = 4kk' + k + k'$ which is of the form $(4n + 1)$.

By induction, if $a_k = 4_{n_k} + 1$; $k = 1, 2, \ldots\ldots, m$ then $a_1, a_2, \ldots\ldots, a_m$ is also of the form $4n + 1$.

Theorem 8. ***There are an infinite number of primes of the form $4n + 3$.***

Or

Prove that there are infinite number of primes of the form $4k + 3$.

Proof. If possible, let number of primes of the form $(4n + 3)$ be finite.

These primes are $3, 7, 11, \ldots\ldots\ldots, q$ [put $n = 0, 1, 2, \ldots\ldots\ldots$ in $(4n + 3)$]

Let $a = 3 \cdot 7 \cdot 11 \ldots\ldots q$ be the product of all primes of the form $(4n + 3)$.

Let $b = 4a - 1$ ...(1)

$\Rightarrow \quad b > 1$ [$\because a \geq 3$, therefore $b = 4a - 1 \Rightarrow b \geq$

Therefore by fundamental theorem b can be expressed as a product of prime say $p_1, p_2, \ldots\ldots, p_r$

i.e $b = p_1 p_2 \ldots . p_r$ ...(2)

Now $b = 4a - 1$ is odd and hence 2 cannot be a factor of b.

$\therefore$ none of the prime factors in R.H.S. of (2) is 2

i.e every prime factor in R.H.S. of (2) is odd.

$\therefore$ each of $p_1, p_2, \ldots\ldots, p_r$ is of the form $(4n + 1)$ or $(4n + 3)$.

Again, all $p_1, p_2, \ldots\ldots, p_r$ cannot be of the form $(4n + 1)$.

[$\because$ if it were so, then b will also be of the form $(4n + 1)$.

But this is contrary to (1) as $b = 4a - 1$ is of the form $(4n + 3)$].

Therefore, at least one of $p_1, p_2, \ldots\ldots, p_r$ (say p) is of the form $(4n + 3)$

i.e $p \mid b$.

Also $p \mid a$

$\therefore \quad p \mid 4a$

$\Rightarrow \quad p \mid (4a - b)$

$\Rightarrow \quad p \mid 1$ [From (1), $4a - b = 1$]

which is impossible,

$\because$ p being prime > 1.

Therefore, our supposition is wrong.

Hence number of primes of the form $(4n + 3)$ is finite.

DIRICHLET'S THEOREM

Theorem 9. ***If a and b are relatively prime positive integers, then the arithmetic progression $a, a + b, a + 2b, a + 3b, \ldots\ldots$ contains infinitely many primes.***

Proof. Dirichlet's theorem tells us for instance, that there are infinitely many prime numbers ending in 999, such as 1999, 100999, 1000999,..... for these appear in the arithmetic progression determined by $1000n + 999$, where $gcd\ (1000, 999) = 1$.

There is no a rithmetic progression $a, a + b, a + 2b, \ldots\ldots$ that consists solely of prime numbers.

For this suppose that $a + nb = p$, where p is a prime.

If we put $n_k = n + kp$ fo

$a + n_k b = a + (n$

$= (a + n$

$= p + kp$

Since each term on the

In other words, the pro

It is an old, but stil

but finite arithmetic prog

consecutive primes).

The longest progressio

11410337850553 + 46

The prime factoriz

$2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17$

the primes less than 22.

Theorem 10. ***If all the n***

$p, p + d, p + 2d$

are prime numbers, then

Proof. If possible let q be

$q \nmid d$.

Consider the first q te

$p, p + d, p + 2$

We claim that these t

If $p + jd$ and $p + kd$

$\Rightarrow \quad q \mid ((p + jd) -$

$\Rightarrow \quad q \mid (j - k)\, d$

$\Rightarrow \quad q \mid j - k$

which is not possible

Hence the terms in (

Since the q diff

of the remainders

$\Rightarrow \quad q \mid p +$

If we put $n_k = n + kp$ for $k = 1, 2, 3, \ldots\ldots$ then the n_kth term in the progression is

$$a + n_k b = a + (n + kp) b$$
$$= (a + nb) + kpb$$
$$= p + kpb$$

Since each term on the R.H.S. is divisible by p, so is $a + n_k b$.

In other words, the progression must contain infinitely many composite numbers. It is an old, but still unsolved question of whether there exist arbitrarily long finite arithmetic progressions consisting only of prime numbers (not necessarily consecutive primes).

The longest progression found to date is composed of the 22 primes:

$11410337850553 + 4609098694200n$, $0 \le n \le 21$.

The prime factorization of the common difference between the term is $2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 1033$ which is divisible by 9699690, the product of the primes less than 22.

Theorem 10. ***If all the $n > 2$ terms of the arithmetic progression***

$$p, p + d, p + 2d, \ldots\ldots, p + (n - 1) d$$

are prime numbers, then the common difference is divisible by every prime $q < n$.

Proof. If possible let q be a prime less than n such that

$$q \nmid d.$$

Consider the first q terms of the given progression

$$p, p + d, p + 2d, \ldots\ldots, p + (q - 1) d \qquad \ldots.(1)$$

We claim that these terms when divided by q leave different remainders.

If $p + jd$ and $p + kd$; $0 \le k < j \le q - 1$ leave same remainder when divided by q, then

$$q \mid ((p + jd) - (p + kd))$$
$$\Rightarrow \quad q \mid (j - k) d$$
$$\Rightarrow \quad q \mid j - k \qquad (\because q \nmid d)$$

which is not possible as $0 < j - k < q$.

Hence the terms in (1) leave different remainder when divided by q.

Since the q different remainders produced from (1) are 0, 1,....., $q - 1$, therefore, one of the remainders must be zero.

$$\Rightarrow \quad q \mid p + td \text{ for some } 0 \le t \le q - 1.$$

Two cases arise :

Case I $p < n$

In this case $p + pd$ occurs in the given $A.P.$ and

$p + pd = p(1 + d)$ is composite, a contradiction.

Case II $p \geq n$

Since $q < n \Rightarrow p \leq p + td$ and $q \mid p + td$

$\therefore$ $p + dt$ is composite number for $0 \leq t \leq q - 1 < n - 1$ which is again a contradiction.

Hence $q \mid d$.

Hence the Proof.

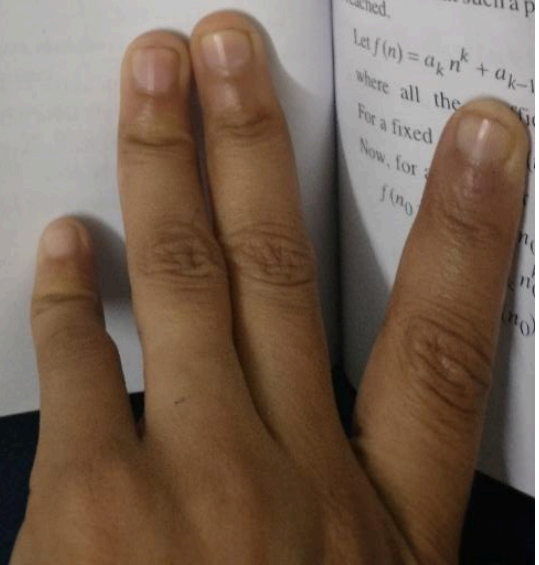
Note

1. There exist arithmetic progressions of finite (but otherwise arbitrary) length, composed of consecutive prime numbers. Examples of such progressions consisting of three and four primes, respectively, are 47, 53, 59 and 251, 257, 263, 269.
2. It was widely believed years ago that the quadratic polynomial $f(n) = n^2 + n + 41$ assumed only prime values. This was shown to be false by Euler, in 1772.

From the following table we see that the claim is a correct one for

$n = 0, 1, 2, \ldots\ldots, 39$.

n	$f_{(n)}$	n	$f_{(n)}$	n	$f_{(n)}$
0	41	16	313	32	1097
1	43	17	347	33	1163
2	47	18	383	34	1231
3	53	19	421	35	1301
4	61	20	461	36	1373
5	71	21	503	37	1447
6	83	22	547	38	1523
7	97	23	593	39	1601
8	113	24	641		
9	131	25	691		
10	151	26	743		
11	173	27	797		
12	197	28	853		
13	223	29	911		
14	251	30	971		
15	281	31	1033		



But this conjecture is shattered in the cases $n = 40$ and $n = 41$, where there is a factor of 41 :

$$f(40) = 40 \cdot 41 + 41 = 41^2 \text{ and } f(41) = 41 \cdot 42 + 41 = 41 \cdot 43$$

The next value of $f(42) = 1847$ which is a prime once again. In fact, for the first 100 integer values of n, the so-called Euler polynomial represents 86 primes.

Although it starts off very well in the production of primes, there are another quadratics such as

$$g(n) = n^2 + n + 27941$$

that begin to best $f(n)$ as the values of n become larger.

For example, $g(n)$ is prime for 286129 values of $0 \le n \le 10^6$, where as its famous rival yields 261081 primes in this range.

It has been shown that no polynomial of the form $n^2 + n + q$, with q a prime, can do better than the Euler polynomial in giving primes for successive value of n. Thus no other quadratic polynomial of any kind was known to produce more than 40 successive prime values.

The Polynomial

$h(n) = 103n^2 - 3945n + 34381$ found in 1998, produces 43 distinct prime values for $n = 0, 1, 2, \ldots\ldots, 42$

The current record holder in this regard $k(n) = 36n^2 - 810n + 2753$ does slightly better by giving a string of 45 prime values.

The failure of the previous functions to be prime-producing is no accident, since it is easy to prove that there is no non constant polynomial $f(n)$ with integral coefficients that takes on just prime values for integral n.

We assume that such a polynomial $f(n)$ actually does exist and argue until a contradiction is reached.

Let $f(n) = a_k n^k + a_{k-1} n^{k-1} + \ldots\ldots + a_2 n^2 + a_1 n + a_0$

where all the coefficients $a_0, a_1, \ldots, a_k$ are integers, and $a_k \neq 0$.

For a fixed value of (n_0), $p = f(n_0)$ is a prime number.

Now, for any integer t, we consider the following expression :

$$\begin{aligned} f(n_0 + tp) &= a_k (n_0 + tp)^k + \ldots\ldots + a_1 (n_0 + tp) + a_0 \\ &= (a_k n_0^k + \ldots\ldots + a_1 n_0 + a_0) + pQ(t) \\ &= f(n_0) + pQ(t) \end{aligned}$$

$$= p + pQ(t)$$
$$= p(1 + Q(t))$$

where $Q(t)$ is a polynomial in t having integral coefficients.

Thus we have

$$f(n_0 + tp) = p(1 + Q(t))$$
$$\Rightarrow \quad p \mid f(n_0 + tp),$$

hence from our own assumption that $f(n)$ takes on only prime values, $f(n_0 + tp) = p$ for any integer t.

Since a polynomial of degree k cannot assume the same value more than k times, so we get the required contradiction.

Example 8. *Show that if* $5 \nmid (n-1)$, $5 \nmid n$ *and* $5 \nmid (n+1)$, *then* $5 \mid (n^2+1)$.

Solution. Since we know that a positive integer is divisible by 5, if the digit of the unit place of the given number is either 0 or 5.

Also, the digit of unit place of a number not divisible by 5 must be

1, 2, 3, 4, 6, 7, 8, 9.

Since it is given that $5 \nmid (n-1)$, $5 \nmid n$ and $5 \nmid (n+1)$.

Therefore, unit digit of n can be 4 or 9 otherwise $(n+1)$ will be divisible by 5.

Also, if the unit digit of n is 2 or 8, then the unit digit of n^2+1 will be $4+1=5$ *i.e* $5 \mid (n^2+1)$.

Similarly, if the unit digit of n is 3 or 7, then 0 will be unit digit of n^2+1, which is again divisible by 5.

Hence, if $5 \nmid (n-1)$, $5 \nmid n$ and $5 \nmid (n+1)$, then $5 \mid (n^2+1)$.

Example 9. *Show that every odd number greater than or equal to 9 is the sum of three odd primes.*

Solution. We know that, the smallest number, which is the sum of three odd primes is $3+3+3=9$.

Let n be the given odd integer greater than or equal to 9.

Also, let p_1 be an odd prime such that $p_1 < n-9$.

Then $n - p_1$ is even and greater than 4.

Thus, by Goldbach's conjecture, it can be expressed as the sum of two odd primes p_2 and p_3 *i.e*

$$n - p_1 = p_2 + p_3$$
$$\Rightarrow \quad n = p_1 + p_2 + p_3.$$

Hence, the given odd intege

Example 10. *If p and q are twi*

Solution. Since p and q are twi

$$q = p + 2$$

Then, $p + q = p + p + 2$
$$= 2p + 2$$
$$= 2(p+1)$$
$$= 2(3k+2+$$
$$= 2(3k+3)$$
$$= 6(k+1)$$
$$= 6 \cdot 2m$$
$$= 12m$$
$$\Rightarrow \quad 12 \mid (p+q).$$

Example 11. *Prove that if n*

Solution. Let $d \in N$ be such

Then $1 \le d \le n-1$ and

$$d \mid (n-1)!$$

Now $n \mid (n-1)! + 1$

$\therefore \quad d \mid (n-1)! + 1$

From (1) and (2), we

$$d \mid (n-1)! +$$
$$\Rightarrow \quad d \mid 1$$
$$\Rightarrow \quad d = 1.$$

Hence n is prime.

$$n - p_1 = p_2 + p_3$$

$$\Rightarrow \quad n = p_1 + p_2 + p_3.$$

Hence, the given odd integer n can be expressed as the sum of three odd primes.

Example 10. If p and q are twin primes, then show that $12 \mid (p+q)$, when $p > 3$.

Solution. Since p and q are twin primes, therefore

$$q = p + 2$$

Then, $p + q = p + p + 2$

$$= 2p + 2$$

$$= 2(p+1) \qquad \text{(Taking } p = 3k+2\text{)}$$

$$= 2(3k + 2 + 1)$$

$$= 2(3k + 3)$$

$$= 6(k+1) \qquad (\because k \text{ cannot be even})$$

$$= 6 \cdot 2m$$

$$= 12m$$

$$\Rightarrow \quad 12 \mid (p+q).$$

Example 11. Prove that if $n > 1$ and $n \mid (n-1)! + 1$ then n is prime.

Solution. Let $d \in N$ be such that $d \mid n$ and $d < n$. ....(1)

Then $1 \le d \le n - 1$ and hence

$$d \mid (n-1)! \qquad \text{....(2)}$$

Now $n \mid (n-1)! + 1$ and $d \mid n$,

$$\therefore \quad d \mid (n-1)! + 1$$

From (1) and (2), we get

$$d \mid (n-1)! + 1 - (n-1)!$$

$$\Rightarrow \quad d \mid 1$$

$$\Rightarrow \quad d = 1.$$

Hence n is prime.

❑❑❑

CHAPTER 3

THE THEORY OF CONGRUENCES

Definition. *Let n be a fixed positive integer. Two integers a and b are said to be* **congruent modulo n**, *written as $a \equiv b \pmod{n}$ if n divides the difference $a - b$ i.e. if $n \mid (a - b)$. The integer n is called modulus.*

Note

If n is not a divisor of $a - b$, then we say that a is not congruent to b modulo n and we write $a \not\equiv b \pmod{n}$.

Theorem 1. ***For arbitrary integers a and b, $a \equiv b \pmod{n}$ if and only if a and b leave the same non negative remainder when divided by n.***

Proof. Let $a \equiv b \pmod{n}$

$\Rightarrow \quad n \mid (a - b)$

$\Rightarrow \quad a - b = kn$ for some integer k

$\Rightarrow \quad a = b + kn$

Upon division by n, b leaves a certain remainder r, than is, $b = qn + r$, where $0 \le r < n$.

Therefore $a = b + kn$ becomes

$$a = (qn + r) + kn$$
$$= (q + k)\, n + r$$

which shows that a has the same remainder as b.

Conversely, suppose we can write

$$a = q_1 n + r \text{ and}$$

$$b = q_2 n + r,$$

with the same remainder r $(0 \le r < n)$. Then

$$a - b = (q_1 n + r) - (q_2 n + r)$$

$$= (q_1 - q_2)\, n$$

$$\Rightarrow \quad n \mid (a - b)$$

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

Note

1. Since the integers -56 and -11 can be expressed in the form

$$-56 = (-7)\,9 + 7$$

$$-11 = (-2)\,9 + 7$$

with the same remainder 7.

Above theorem tells us that

$$-56 \equiv -11 \pmod{7}$$

Going in the other direction, the congruence

$$-31 \equiv 11 \pmod{7}$$

implies that -31 and 11 have the same remainder when divided by 7; that is clear from the relations

$$-31 = (-5)\,7 + 4$$

$$11 = 1 \cdot 7 + 4.$$

2. Congruence may be viewed as a generalized form of equality in the sense that its behaviour with respect to addition and multiplication is reminiscent of ordinary equality.

Theorem 2. Two integers are congruent modulo n iff their difference is divisible by $n \neq 0$.

Proof. Let a and b be two integers.

By Euclidean algorithm, a and b can be expressed by the following equations :

$$a = q_1 n + r_1,\ 0 \le r_1 < |n| \qquad \ldots(1)$$

and $$b = q_2 n + r_2,\ 0 \le r_2 < |n| \qquad \ldots(2)$$

Let us first assume that

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

Then the remainder in the above equations are identical.

Then we have

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

(by definition of divisibility)

which implies $n \mid (a - b)$

Conversely, let us assume that

$$n \mid (a - b)$$

$\Rightarrow$ $a - b = kn$ where k is an integer.

Since $a = q_1 n + r_1$,

$b = q_2 n + r_2$,

where $0 \le r_1, r_2 < |n|$.

Then $a - b = n(q_1 - q_2) + (r_1 - r_2)$

Since $n \mid (a - b)$

$\Rightarrow$ $n \mid \{n(q_1 - q_2) + (r_1 - r_2)\}$

$\Rightarrow$ $n \mid (r_1 - r_2)$

But $r_1 - r_2 < n$

$\Rightarrow r_1 - r_2 = 0$ as we know that if $a \mid b$ and $b < a$ where a and b are non-negative integers, then $b = 0$.

Therefore $r_1 = r_2$ and hence

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

Theorem 3. *Let $n > 1$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold :*

(i) $a \equiv a \pmod{n}$

(ii) If $a \equiv b \pmod{n}$, *then* $b \equiv a \pmod{n}$

(iii) If $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$

(iv) If $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$, *then*
$a + c \equiv b + d \pmod{n}$ *and* $ac \equiv bd \pmod{n}$

(v) If $a \equiv b \pmod{n}$, *then* $a + c \equiv b + c \pmod{n}$ *and*
$ac \equiv bc \pmod{n}$

(vi) If $a \equiv b \pmod{n}$, *then* $a^k \equiv b^k \pmod{n}$
for any positive integer k.

Proof. (i) We know that $n \mid 0$ $(n \ne 0)$

$\therefore$ $n \mid (a - a)$

Or $a \equiv a \bmod n$ (by definition of congruence)

i.e every integer is congruent to itself.

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

$\Rightarrow$ $n \mid (a - b)$

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

$\Rightarrow$ $n \mid (b - a)$

$\Rightarrow$ $b \equiv a \bmod n$.

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

and $b \equiv c \pmod{n}$

$\therefore$ $n \mid (a - b)$ and $n \mid$

$\Rightarrow$ $n \mid \{(a - b) + (b -$

$\Rightarrow$ $n \mid (a - c)$

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

Note

Results of (i), (ii) and
properties of congruences.

(iv) Since $a \equiv b \pmod{}$

and $c \equiv d \pmod{n}$

$\therefore$ $n \mid (a - b)$ and

$\Rightarrow$ $n \mid [(a - b) +$

$\Rightarrow$ $n \mid [(a + c) -$

$\Rightarrow$ $a + c \equiv a + d$

Now we prove that

$ac \equiv bd \pmod{}$

Since $n \mid (a - b)$ a

Therefore there ex

$a - b = nx$

and $c - d = ny$

$\therefore$ $a = b + nx$

$c = d + ny$

Multiplying the

$ac = (b +$

$= bd$

Or $ac - bd$

Or $ac - bd$

Theref

$\Rightarrow$

$\Rightarrow \quad n \mid (b-a)$

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

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

and $\quad b \equiv c \pmod{n}$

$\therefore \quad n \mid (a-b)$ and $n \mid (b-c)$

$\Rightarrow \quad n \mid \{(a-b)+(b-c)\}$

$\Rightarrow \quad n \mid (a-c)$

$\Rightarrow \quad a \equiv c \pmod{n}$.

Note

Results of (i), (ii) and (iii) are respectively called reflexive, symmetric and transitive properties of congruences.

(iv) Since $a \equiv b \pmod{n}$

and $\quad c \equiv d \pmod{n}$

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

$\Rightarrow \quad n \mid [(a-b)+(c-d)]$

$\Rightarrow \quad n \mid [(a+c)-(b+d)]$

$\Rightarrow \quad a+c \equiv a+d \pmod{n}$

Now we prove that

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

Since $n \mid (a-b)$ and $n \mid (c-d)$

Therefore there exist integers x and y such that

$$a-b = nx$$

and $\quad c-d = ny$

$\therefore \quad a = b+nx$ and

$$c = d+ny$$

Multiplying the two equations, we get

$$ac = (b+nx)(d+ny)$$

$$= bd + bny + ndx + n^2 xy$$

Or $\quad ac - bd = bny + ndx + n^2 xy$

Or $\quad ac - bd = n(by + dx + nxy)$

Therefore by definition of divisibility $n \mid (ac-bd)$

$\Rightarrow \quad ac \equiv bd \pmod{n}$.

(v) Since $a \equiv b \pmod{n}$

$\Rightarrow \quad n \mid (a-b)$

$\Rightarrow \quad n \mid (a+c-b-c)$

$\Rightarrow \quad n \mid [(a+c)-(b+c)]$

$\Rightarrow \quad a+c \equiv b+c \pmod{n}$

Again $n \mid (a-b)$

$\Rightarrow \quad n \mid c\,(a-b)$

$\Rightarrow \quad n \mid (ac-bc)$

$\Rightarrow \quad ac \equiv bc \pmod{n}$.

(vi) We know that

$$a^k - b^k = (a-b)\,(a^{k-1} + a^{k-2}\,b + a^{k-3}\,b^2 + \ldots + b^{k-1})$$

But $\quad a \equiv b \pmod{n}$

$\Rightarrow \quad n \mid (a-b)$

Therefore there exist integers t such that $a - b = nt$

Putting this value of $(a-b)$ from (2) in (1), we get

$$a^k - b^k = nt\,(a^{k-1} + a^{k-2}\,b + \ldots\ldots + b^{k-1})$$

$\therefore \quad n \mid (a^k - b^k)$

$\Rightarrow \quad a^k \equiv b^k \pmod{n}$.

Example 1. *Show that* 41 *divides* $2^{20} - 1$.

Solution. Since $2^5 \equiv -9 \pmod{41}$,

$\Rightarrow \quad (2^5)^4 \equiv (-9)^4 \pmod{41}$

$\Rightarrow \quad 2^{20} \equiv 81 \cdot 81 \pmod{41}$

But $\quad 81 \equiv -1 \pmod{41}$

and so $81 \cdot 81 \equiv 1 \pmod{41}$.

Since we know that

if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$ and

$a + c \equiv b + c \pmod{n}$, $ac \equiv bc \pmod{n}$

We have

$$2^{20} - 1 \equiv 81 \cdot 81 - 1 \equiv 1 - 1 \equiv 0 \pmod{41}$$

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

Theorem 4. *The relation "congruence modulo n" is an equivalence relation in the set of integers.*

Proof. Let Z be the set of integers.

If n is any fixed positive integer, then we say that

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

$n \mid (a - b)$.

We shall show that this defines an equivalence relation on the set Z.

Reflexivity

Let a be any integer.

Then $a - a = 0$ and $n \mid 0$.

Thus $a \equiv a \pmod{n}$ $\forall$ $a \in Z$.

Therefore the relation is reflexive.

Symmetry

Let $a, b \in Z$ be such that $a \equiv b \pmod{n}$.

Then we have $n \mid (a - b)$

$\Rightarrow$ $a - b = kn$ for some $k \in Z$.

$\Rightarrow$ $b - a = (-k)\, n$ where $-k \in Z$.

$\Rightarrow$ $n \mid (b - a)$

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

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

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

and therefore the relation is symmetric.

Transitivity

Let $a, b, c \in Z$ be such that $a \equiv b \pmod{n}$.

$b \equiv c \pmod{n}$.

Then we have

$n \mid (a - b)$ and $n \mid (b - c)$

$\Rightarrow$ $n \mid \{(a - b) + (b - c)\}$

$\Rightarrow$ $n \mid (a - c)$

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

Thus $a \equiv b \pmod{n}$ and

$b \equiv c \pmod{n}$

$\Rightarrow \quad a \equiv c \pmod{n}$.

Therefore the relation is transitive.

Hence congruence modulo n is an equivalence relation on Z.

Theorem 5. *If* $ca \equiv cb \pmod{n}$, *then* $a \equiv b \left(\text{mod } \frac{n}{d}\right)$, *where* $d = gcd\ (c, n)$.

Proof. Since $gcd\ (c, n) = d$

i.e d is the greatest common divisor of c and n.

Therefore, there exist integers r and s such that

$c = dr$, $n = ds$ where $gcd\ (r, s) = 1$.

Now $ca \equiv cb \pmod{n}$ (given)

$\Rightarrow \quad n \mid (ca - cb)$

$\Rightarrow \quad n \mid c\ (a - b)$

Putting the value of n and c, we have

$ds \mid dr\ (a - b)$ or $s \mid r\ (a - b)$

But $gcd\ (r, s) = 1$

Therefore by Gauss theorem,

$s \mid (a - b)$

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

But $n = ds$

$\Rightarrow \quad s = \frac{n}{d}$

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

$\Rightarrow \quad a \equiv b \left(\text{mod } \frac{n}{d}\right)$

Note

The converse of the above theorem is as follows :

Let $a \equiv b \left(\text{mod } \frac{n}{d}\right)$

$\Rightarrow \quad a \equiv b \pmod{s}$ $\quad (\because n = ds)$

$\Rightarrow \quad s \mid (a - b)$

$\Rightarrow \quad ds \mid d\ (a - b)$

$\Rightarrow \quad n \mid d\ (a - b)$

Or $\quad n \mid d\ (a - b)$

$[\because$ If $a \mid b$, then $a \mid bc \ \forall\ c]$

Therefore $n \mid dr\,(a-b)$ $(\because dr = c)$

Or $n \mid c\,(a-b)$

Or $n \mid (ac-cb)$

Or $ac \equiv bc\ (mod\ n)$.

Corollary. If $ca \equiv cb\ (mod\ n)$ *and* $gcd\ (c, n) = 1$, *then*

$a \equiv b\ (mod\ n)$.

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

$\Rightarrow$ $n \mid (ca-cb)$

$\Rightarrow$ $n \mid c\,(a-b)$

But $gcd\ (c, n) = 1$

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

$\Rightarrow$ $a \equiv b\ (mod\ n)$.

Corollary. If $ca \equiv cb\ (mod\ p)$ *and* $p \nmid c$, *where p is a prime number; then* $a \equiv b\ (mod\ p)$.

Proof. Since $ca \equiv cb\ (mod\ p)$

$\Rightarrow$ $p \mid (ca-cb)$

$\Rightarrow$ $p \mid c\,(a-b)$ ....(1)

But $p \nmid c$ and p is a prime number

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

$\therefore$ (1) gives

$p \mid (a-b)$

$\Rightarrow$ $a \equiv b\ (mod\ p)$.

Note

In the theorem if $ca \equiv cb\ (mod\ n)$, then $a \equiv b\left(mod\ \frac{n}{d}\right)$, where $d = gcd\ (c, n)$, it is unnecessary to stipulate that $c \not\equiv 0\ (mod\ n)$. In fact if $c \equiv 0\ (mod\ n)$, then $gcd\ (c, n) = n$ and the conclusion of the theorem would state that $a \equiv b\ (mod\ 1)$, this holds trivially for all integers a and b.

Example 2. *If* $a \equiv b\ (mod\ n)$ *and* $m \mid n$, *then* $a \equiv b\ (mod\ m)$.

Solution. Since $a \equiv b\ (mod\ n)$,

then $n \mid (a-b)$.

But $m \mid n$ and hence

$m \mid (a-b)$,

$\Rightarrow a \equiv b \pmod m$

Example 3. *If* $a \equiv b \pmod n$ *and* $c > 0$, *then* $ca \equiv cb \pmod{cn}$.

Solution. Let $a \equiv b \pmod n$

$\therefore \quad n \mid (a-b)$

$\therefore \quad cn \mid c(a-b)$ $\quad (\because c > 0$ given$)$

$\Rightarrow \quad cn \mid (ca-cb)$

$\Rightarrow \quad ca \equiv cb \pmod{cn}$

Example 4. *If* $a \equiv b \pmod n$ *prove that* $gcd\,(a, n) = gcd\,(b, n)$.

Solution. $a \equiv b \pmod n$

$\Rightarrow \quad b - a = nz$ for some integer z.

Since $gcd\,(a, n) \mid a$ and

$gcd\,(a, n) \mid n$,

we have $gcd\,(a, n) \mid b$ and

hence $gcd\,(a, n) \mid gcd\,(b, n)$

Similarly $gcd\,(b, n) \mid gcd\,(a, n)$

Thus we have $gcd\,(a, n) = gcd\,(b, n)$, as we know that if $p \mid q$ and $q \mid p$ then $p = q$.

Note

Converse may not be true

i.e $\quad (a, n) = (b, n)$ may not imply

$a \equiv b \pmod n$.

e.g. let $a = 6, b = 2, n = 8$

$\therefore \quad (a, n) = (6, 8) = 2$ and

$(b, n) = (2, 8) = 2$

$\therefore \quad (a, n) = (b, n)$

But $\quad 6 \not\equiv 2 \pmod n$

i.e $\quad a \not\equiv b \pmod n$.

Example 5. *Find the remainder when the following sum is divided by 12*

$1! + 2! + 3! + 4! + \ldots\ldots + 99! + 100!$

Solution. Since $4! \equiv 24 \equiv 0 \pmod{12}$,

thus for $k \geq 4$,

$k! \equiv 4! \cdot 5 \cdot 6 \ldots\ldots k \equiv 0 \cdot 5 \cdot 6 \ldots\ldots k \equiv 0 \pmod{12}$

In this way, we get

$1! + 2! + 3! + 4! + \ldots\ldots\ldots + 100!$

Thus the given sum leaves a remainder of 9 when divided by 12.

Example 6. Find the remainder when the sum

$S = 1! + 2! + 3! + \ldots\ldots\ldots + 1000!$

is divisible by 8.

Solution. We know that $k!$ is divisible by 8 for all $k \geq 4$, we have

$$\begin{aligned} S &= 1! + 2! + 3! + \ldots\ldots + 1000! \\ &= 1 \cdot 2! + 3! \pmod 8 \\ &= 1 + 2 + 6 \\ &= 9 \\ &= 1 \pmod 8 \end{aligned}$$

Hence the required remainder is 1.

Example 7. Find the remainder when the sum $S = 1! + 2! + 3! + \ldots\ldots + 100!$ *is divisible by* 12.

Solution. We know that $k!$ is divisible by 12 for all $k \geq 4$, we have

$$\begin{aligned} S &= 1! + 2! + 3! + \ldots\ldots + 1000! \\ &\equiv 1! + 2! + 3! \pmod{12} \qquad [\because 4! \equiv 24 \equiv 0 \pmod{12}] \\ &\equiv 1 + 2 + 6 \pmod{12} \\ &\equiv 9 \pmod{12}. \end{aligned}$$

Hence the required remainder is 9.

Example 8. What is the remainder when the following sum is divisible by 15 ?

$\underline{11} + \underline{12} + \underline{13} + \ldots\ldots + \underline{1100}$.

Solution. We know that $k!$ is divisible by 15 for all $k \geq 5$, we have

$$\begin{aligned} S &= \underline{11} + \underline{12} + \underline{13} + \underline{14} + \ldots\ldots + \underline{1100}. \\ &\equiv \underline{11} + \underline{12} + \underline{13} + \underline{14} + 0 + \ldots\ldots + 0 \pmod{15} \qquad [\because \underline{15} \equiv 120 = 0 \pmod{15}] \\ &\equiv 1 + 2 + 6 + 24 \pmod{15} \\ &\equiv 33 \pmod{15} \\ &\equiv 3 \pmod{15} \end{aligned}$$

Hence the required remainder is 3.

Example 9. *Find the remainder when* 2^{50} *divided by* 7.

Solution. We know that

$$2^1 \equiv 2 \pmod 7$$
$$2^2 \equiv 4 \pmod 7 \quad \ldots(1)$$
$$2^3 \equiv 8 \pmod 7$$

Or $2^3 \equiv 1 \pmod 7$

Raising to power 16, we get

$$(2^3)^{16} \equiv 1 \pmod 7$$

$\Rightarrow$ $2^{48} \equiv 1 \pmod 7 \quad \ldots(2)$

Multiplying (1) and (2), we get

$$2^{50} \equiv 4 \pmod 7$$

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

Example 10. *Find the remainder if* 3^{40} *is divided by* 23.

Solution. $3^1 \equiv 3 \pmod{23}$

$$3^2 \equiv 9 \pmod{23}$$
$$3^3 \equiv 27 \pmod{23}$$

Or $3^3 \equiv 4 \pmod{23} \quad \ldots(1)$

Raising to power 3, we get

$$(3^3)^3 \equiv 4^3 \pmod{23}$$

Or $3^9 \equiv 64 \pmod{23}$

Or $3^9 \equiv -5 \pmod{23}$

Squaring, we get

$$3^{18} \equiv 25 \pmod{23}$$

Or $3^{18} \equiv 2 \pmod{23}$

Again squaring, we get

$$3^{36} \equiv 4 \pmod{23} \quad \ldots(2)$$

Multiplying (1) and (2), we have

$$3^{39} \equiv 16 \pmod{23}$$

Multiplying both sides by 3, we ha

$3^{40} \equiv 48 \pmod{23}$

Or $3^{40} \equiv 2 \pmod{23}$

$\therefore$ 2 is the remainder when 3^{40} is

Example 11. If $ca \equiv cb \pmod n$ *and*

Solution. Since $ca \equiv cb \pmod n$

$\therefore$ $n \mid (ca - cb)$

$\Rightarrow$ $n \mid c(a - b)$

But $gcd(c, n) = 1$,

$\therefore$ by Gauss theorem,

$n \mid (a - b)$

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

Hence the solution.

Example 12. Show that for any

Solution. Let $a = 3k + r, 0 \le r <$

If $r = 0$, then $a = 3k$

$\Rightarrow$ $a^3 = 27k^3 \equiv 0 \pmod$

If $r = 1$, then $a = 3k + 1$

$\therefore$ $a^3 = 27k^3 + 1 + 27$

$\Rightarrow$ $a^3 \equiv 1 \pmod 9$

If $a = 3k + 2$, then

$a^3 = 27k^3 + 8 + 5$

$\Rightarrow$ $a^3 \equiv 8 \pmod 9$

$\therefore$ $a^3 = 0, 1$ or 8 (

Multiplying both sides by 3, we have

$3^{40} \equiv 48 \pmod{23}$

Or $3^{40} \equiv 2 \pmod{23}$

$\therefore$ 2 is the remainder when 3^{40} is divided by 23.

Example 11. If $ca \equiv cb \pmod{n}$ *and* $gcd\,(c, n) = 1$, *then* $a \equiv b \pmod{n}$.

Solution. Since $ca \equiv cb \pmod{n}$

$\therefore \quad n \mid (ca - cb)$

$\Rightarrow \quad n \mid c\,(a - b)$

But $gcd\,(c, n) = 1$,

$\therefore$ by Gauss theorem,

$n \mid (a - b)$

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

Hence the solution.

Example 12. Show that for any integer a, $a^3 \equiv 0, 1$ *or* $8 \pmod{9}$.

Solution. Let $a = 3k + r, 0 \le r < 3$.

If $r = 0$, then $a = 3k$

$\Rightarrow \quad a^3 = 27k^3 \equiv 0 \pmod{9}$

If $r = 1$, then $a = 3k + 1$

$\therefore \quad a^3 = 27k^3 + 1 + 27k^2 + 9k$

$\Rightarrow \quad a^3 \equiv 1 \pmod{9}$

If $a = 3k + 2$, then

$a^3 = 27k^3 + 8 + 54k^2 + 36k$

$\Rightarrow \quad a^3 \equiv 8 \pmod{9}$

$\therefore \quad a^3 = 0, 1$ or $8 \pmod{9}$.

Example 13. *If* $a \equiv b \pmod{n_1}$ *and* $a \equiv c \pmod{n_2}$, *prove that* $b \equiv c \pmod{n}$, *where integer* $n = gcd\,(n_1, n_2)$.

Solution. Since $a \equiv b \pmod{n_1}$

$\Rightarrow \quad n_1 \mid (a-b)$

and $\quad a \equiv c \pmod{n_2}$

$\Rightarrow \quad n_2 \mid (a-c)$

But $gcd\,(n_1, n_2) = n$

$\Rightarrow \quad n \mid n_1$ and $n \mid n_2$

$\therefore \quad n_1 \mid (a-b)$

$\Rightarrow \quad n \mid (a-b)$

and $\quad n_2 \mid (a-c)$

$\Rightarrow \quad n \mid (a-c)$

Since $\quad n \mid (a-b)$ and $n \mid (a-c)$

$\Rightarrow \quad n \mid \{(a-c)-(a-b)\}$

$\Rightarrow \quad n \mid (a-c-a+b)$

$\Rightarrow \quad n \mid (b-c)$

$\Rightarrow \quad b \equiv c \pmod{n}$

Hence the solution.

LINEAR CONGRUENCE

A polynomial congruence of degree 1 is called a **linear congruence**.

Any linear congruence can be written in the form $ax \equiv b \bmod m$ where a is not congruent to $0 \bmod m$.

SOLUTION OF LINEAR CONGRUENCE

An integer x_1 *is said to be a solution of the linear congruence* $ax \equiv b \pmod{m}$ *if*

$$ax_1 \equiv b \pmod{m}$$

i.e if $m \mid (ax_1 - b)$

Note

A linear congruence may or may not have a solution.

Theorem 6. The linear congruence $ax \equiv b \pmod{m}$ ***has a solution if and only if*** $gcd\,(a, m)$ ***divides*** b.

Proof. Let $d = gcd\,(a, m)$ divides b. ....(1)

Then there exists an integer b_1 such that

$b = db_1$ (by definition of divisibility)

Also since $d = gcd\,(a, m)$ ....(2)

$\therefore$ $\exists$ integers h and k such that

$ah + mk = d$

Multiplying both sides of (2) by b_1, we get

$b_1 ah + b_1 km = db_1$

Or $\quad ahb_1 + mkb_1 = db_1 \qquad (\because db_1 = b)$

Or $\quad ahb_1 + mkb_1 = b$

Or $\quad ahb_1 - b = -mkb_1$

Or $\quad a(hb_1) - b = -mkb_1$

which is divisible by m.

$\therefore \quad a(hb_1) \equiv b \pmod{m}$

Comparing with $ax \equiv b \pmod{m}$, we have

$x = hb_1$ is a solution.

Conversely. Let the linear congruence $ax \equiv b \pmod{m}$ have a solution say x_1.

$\therefore \quad ax_1 \equiv b \pmod{m}$

$\Rightarrow \quad m \mid (ax_1 - b)$

$\therefore$ $\exists$ an integer u such that

$ax_1 - b = mu$ ....(3)

Or $\quad ax_1 - mu = b$

Again, since $d = gcd\,(a, m)$

$\Rightarrow \quad d \mid a$ and $d \mid m$

$\therefore$ $\exists$ integers a_1 and m_1 such that

$a = da_1$ and $m = dm_1$,

where $gcd\,(a_1, m_1) = 1$.

Putting the values of a and m in (3), we get

Or $\quad d\,a_1 x_1 - d\,m_1 u = b$

Or $\quad d\,(a_1 x_1 - m_1 u) = b$

$\quad d \mid b$ (by definition of divisibility)

Theorem 7. ***If gcd $(a, m) = 1$, the congruence $ax \equiv b \pmod m$ has a unique solution.***

Proof. Since $gcd\,(a, m) = 1$.

Then, there exist integers h and k such that

$$ah + mk = 1$$

Multiplying (1) by b, we get

$$abh + mbk = b$$

Or $\quad a\,(bh) - b = -mbk$

Or $\quad m \mid \{a\,(bh) - b\}$

$\therefore \quad a\,(bh) \equiv b \pmod m$

$\therefore$ bh is a solution of the congruence $ax \equiv b \pmod m$.

Therefore the congruence $ax \equiv b \pmod m$ has a solution.

Uniqueness

If possible let $x_1, x_2\ (0 \le x_1 \le (m-1), 0 \le x_2 \le (m-1))$ be two solutions of

$$ax \equiv b \pmod m.$$

$\therefore \quad ax_1 \equiv b \pmod m$

and $\quad ax_2 \equiv b \pmod m$

Subtracting, we get

$$a\,(x_1 - x_2) \equiv 0 \pmod m$$

$\therefore \quad m \mid a\,(x_1 - x_2)$

But $\quad gcd\,(a, m) = 1$

i.e $\quad gcd\,(m, a) = 1$

Therefore by Gauss theorem,

$$m \mid (x_1 - x_2) \text{ where } 0 \le x_1 - x_2 \le (m-1) < m.$$

$\therefore \quad x_1 - x_2 = 0$

Or $\quad x_1 = x_2$

Therefore the congruence $ax \equiv b \pmod m$ always has a unique solution if $gcd\,(a, m) = 1$.

Example 14. Find the number of solutions of $3x \equiv 5 \pmod 7$.

Solution. The given congruence is $3x \equiv 5 \pmod 7$.

Comparing with $ax \equiv b \pmod m$,

we have

$$a = 3, b = 5 \text{ and } m = 7$$

$$d = gcd\,(a, m) = gcd\,(3, 7) = 1$$

which divides $b = 5$.

Hence the congruence $3x \equiv 5 \pmod 7$ has one and only one incongruent solution $(mod\ 7)$.

Note

If $gcd\,(a, m) = d$ and $d \mid b$, then the congruence $ax \equiv b \pmod m$ has exactly d incongruent solution $mod\ m$.

Example 15. Find the number of solutions of $4x \equiv 5 \pmod 6$.

Solution. The given congruence is $4x \equiv 5 \pmod 6$

Comparing with $ax \equiv b \pmod m$,

we have

$$a = 4, b = 5, m = 6, d = gcd\,(a.\ m) = gcd\,(4, 6) = 2$$

which does not divide $b = 5$.

Therefore the congruence $4x \equiv 5 \pmod 6$ has no solution.

Example 16. Find the number of solutions of $10x \equiv 15 \pmod{35}$.

Solution. The given congruence is $10x \equiv 15 \pmod{35}$.

Comparing with $ax \equiv b \pmod m$,

we have

$$a = 10, b = 15, m = 35$$

$$d = gcd\,(a, m) = gcd\,(10, 35) = 5$$

which divides $b = 15$.

Hence the congruence $10x \equiv 15 \pmod{35}$ has $d = 5$ solutions incongruent $(mod\ 35)$.

Example 17. Solve the congruence $3x + 2 \equiv 0 \pmod 7$.

Solution. The given congruence is

$$3x + 2 \equiv 0 \pmod 7$$

Or $\quad 3x \equiv -2 \pmod 7$

Comparing with $ax \equiv b \pmod m$, we have

$a = 3, b = -2, m = 7$

$d = gcd\,(a, m) = gcd\,(3, 7) = 1$

which divides $b = -2$.

Therefore the solution of the given congruence exists and is unique.

Now $3x \equiv -2 \pmod 7$

Also $0 \equiv 14 \pmod 7$

Adding (1) and (2), we get

$3x \equiv 12 \pmod 7$

Or $x \equiv 4 \pmod 7$

$\therefore\ x \equiv 4 \pmod 7$ is a solution of the congruence

$3x + 2 \equiv 0 \pmod 7$

Note

In (2), we write 0 on the L.H.S. and a suitable multiple of m on the R.H.S., so that on adding the two congruences we get the value of x.

Example 18. *Solve* $3x \equiv 1 \pmod{125}$

Solution. The given congruence is

$3x \equiv 1 \pmod{125}$

Comparing with $ax \equiv b \pmod{125}$, we get

$a = 3, b = 1, m = 125$

$d = gcd\,(a, m) = gcd\,(3, 125) = 1$

which divides $b = 1$.

Hence the given congruence has one and only one incongruent solution.

Now $3x \equiv 1 \pmod{125}$ ....(1)

Also $0 \equiv 125 \pmod{125}$ ....(2)

Adding (1) and (2), we get

$3x \equiv 126 \pmod{125}$

Or $x \equiv 42 \pmod{125}$

[$\because$ If $ca \equiv cb \pmod m$ and $gcd\,(c, m) = 1$, then $a \equiv b \pmod m$]

Therefore $x \equiv 42 \pmod{125}$ is the incongruent solution of

$3x \equiv 1 \pmod{125}$.

Example 19. *Find all solutions x where $0 \le x \le 15$ of the equation $3x \equiv 6 \pmod{15}$.*

Solution. Given congruence is

$3x \equiv 6 \pmod{15}$

Here $a = 3, b = 6, m = 15$

$d = gcd(a, m)$

$= gcd(3, 15)$

$= 3$ which divides $b = 6$.

Hence the congruence $3x \equiv 6 \pmod{15}$ has $d = 3$ solutions incongruent $(mod\ 15)$.

Since $3x \equiv 6 \pmod{15}$ ....(1)

Also, $0 \equiv 15 \pmod{15}$ ....(2)

Adding, (1) and (2), we have

$3x \equiv 21 \pmod{15}$

$\Rightarrow \quad x \equiv 7 \pmod{15}$.

Here $k = 0, 1, 2$

$\therefore \quad x = x_0 + k\dfrac{m}{d}$

$= 7 + k\dfrac{15}{3}$

$= 7 + 5k$

$= 7, 12, 17.$

Since $0 \le x \le 15$

$\therefore \ x = 7, 12.$

Example 20. Solve the congruence $3x \equiv 5 \pmod{11}$.

Solution. The given congruence is $3x \equiv 5 \pmod{11}$

Comparing with $ax \equiv b \pmod{m}$, we get

$a = 3, b = 5, m = 11$

$d = gcd(a, m) = gcd(3, 11) = 1$

which divides $b = 5$.

Hence the congruence has one and only one incongruent solution.

Now $3x \equiv 5 \pmod{11}$ ....(1)

Also $0 \equiv 22 \pmod{11}$ ....(2)

Adding (1) and (2), we get

$3x \equiv 27 \pmod{11}$

Or $\quad x \equiv 9 \pmod{11}$

Therefore $x \equiv 9 \pmod{11}$ is the only incongruent solution of

$$3x \equiv 5 \pmod{11}.$$

Example 21. *Solve the congruence* $7x \equiv 4 \pmod{10}$.

Solution. The given congruence is $7x \equiv 4 \pmod{10}$

Comparing with $ax \equiv b \pmod{m}$,

we have

$$a = 7, b = 4, m = 10$$

$$d = gcd\,(a, m) = gcd\,(7, 10) = 1$$

which divides $b = 4$.

Hence the congruence has one and only incongruent solution.

Now $7x \equiv 4 \pmod{10}$ ...(1)

Also, $0 \equiv 10 \pmod{10}$ ...(2)

Adding (1) and (2), we get

$$7x \equiv 14 \pmod{10}$$

Or $x \equiv 2 \pmod{10}$

Therefore $x \equiv 2 \pmod{10}$ is the only incongruent solution of

$$7x \equiv 4 \pmod{10}.$$

Example 22. *Solve the congruence* $259x \equiv 5 \pmod{11}$.

Solution. The given congruence is

$$259x \equiv 5 \pmod{11} \quad \text{...(1)}$$

Comparing with $ax \equiv b \pmod{m}$,

we have

$$a = 259, b = 5, m = 11$$

$$d = gcd\,(a, m) = gcd\,(259, 11) = 1$$

which divides $b = 5$.

Therefore the given congruence has only one solution.

Now $259 \equiv 6 \pmod{11}$ ($\because$ 6 is the remainder obtained on dividing 259 by 11)

$\therefore$ $259x \equiv 6x \pmod{11}$

Or $6x \equiv 259x \pmod{11}$ ...(2)

From (1) and (2), we get (due to transitive property)

$$6x \equiv 5 \pmod{11} \quad \text{...(3)}$$

Also, $0 \equiv 55 \pmod{11}$ ...(4)

Adding (3) and (4), we get

$$6x \equiv 60 \pmod{11}$$

Or $x \equiv 10 \pmod{11}$

Hence $x \equiv 10$ is a solution of (3) and hence of (1).

Example 23. Solve the congruence $15x \equiv 12 \pmod{21}$.

Solution. The given congruence is

$$15x \equiv 12 \pmod{21} \quad \ldots(1)$$

Comparing with $ax \equiv b \pmod{m}$,

we get

$$a = 15, b = 12, m = 21$$

$$d = gcd\,(a, m)$$

$$= gcd\,(15, 21)$$

$$= 3$$

which divides 12.

Therefore, the given congruence has 3 solutions incongruent (*mod* 21).

The given congruence is

$$3 \cdot 5x = 3 \cdot 4 \pmod{3 \cdot 7}$$

$\therefore$ $5x \equiv 4 \pmod{7}$ [$\because$ If $ax \equiv bx \pmod{mx}$, then $a \equiv b \pmod{m}$] ...(2)

Since $5x \equiv 4 \pmod{7}$ ...(3)

Also, $0 \equiv 21 \pmod{7}$

Adding (2) and (3), we get

$$5x \equiv 25 \pmod{7}$$

Or $x \equiv 5 \pmod{7}$

$\therefore$ $x \equiv 5 \pmod{7}$ is a solution of $5x \equiv 4 \pmod{7}$

and hence is also a solution of congruence (1).

Therefore, all the three incongruent *mod* (21) is a solution of $15x \equiv 12 \pmod{21}$ are given by

$$x_0 + km_1 \text{ where } k = 0, 1, 2, \ldots\ldots, (d-1)$$

and $m_1 = \dfrac{m}{d}$

Here $x_0 = 5, d = 3, m_1 = \dfrac{21}{3} = 7$

$\therefore$ 3 solutions of the given congruence are

$$x = x_0 + km_1$$
$$= 5 + 7k, \text{ where } k = 0, 1, 2.$$
$$x \equiv 5, 12, 19 \pmod{21}.$$

Example 24. *Solve the congruence* $15x \equiv 12 \pmod{36}$.

Solution. The given congruence is

$$15x \equiv 12 \pmod{36}$$

Comparing with $ax \equiv b \pmod{m}$, we get

$$a = 15, b = 12, m = 36$$
$$d = gcd\,(a, m) = gcd\,(15, 36) = 3$$

which divides $b = 12$.

Therefore the given congruence has 3 solutions incongruent $(mod\ 36)$.

Since $15x \equiv 12 \pmod{36}$

$\therefore$ $5x \equiv 4 \pmod{12}$

Also $0 \equiv 36 \pmod{12}$

Adding (2) and (3), we get

$$5x \equiv 40 \pmod{12}$$

Or $x \equiv 8 \pmod{12}$

$\therefore$ $x = 8$ is a solution of (2) and hence of (1).

[Putting $x = 8$ in (1), we get

$$15 \cdot 8 \equiv 12 \pmod{36}$$

Or $120 \equiv 12 \pmod{36}$

Or $108 \equiv 0 \pmod{36}$

which is true.]

$\therefore$ $x = 8 = x_0$ is a solution of (1).

Hence all the three solutions of (1) are given by

$$x = x_0 + k\frac{m}{d}$$
$$= 8 + k\frac{36}{3}$$
$$= 8 + 12k \text{ where } k = 0, 1, 2$$

$\therefore$ $x \equiv 8, 20, 32 \pmod{36}$.

Example 25. Find the least positive incongruent solution of $7x \equiv 5 \pmod{256}$

Solution. The given congruence is $7x \equiv 5 \pmod{256}$ ....(1)

Comparing with $ax \equiv b \pmod{m}$,

we have

$a = 7, b = 5$ and $m = 256$

$d = gcd\,(a, m) = gcd\,(7, 256) = 1$

which divides $b = 5$.

Therefore the given congruence has one and only one solution at incongruent mod 256).

Since $m = 256$ is large,

we put the *g.c.d.* of $(7, 256) = 1$ in the form $1 = 7u + 256v$

$256 = 7 \cdot 36 + 4$ ($\because$ 4 is the remainder obtained on dividing 256 by 7) ....(2)

$7 = 4 \cdot 1 + 3$ ($\because$ 3 is the remainder obtained on dividing 7 by 4) ....(3)

$4 = 3 \cdot 1 + 1$ ....(4)

From (4), $d = 1 = 4 - (7 - 4)$

$= 4 - 7 + 4$

$= 2 \cdot 4 - 7$

Putting $4 = 256 - 7 \cdot 36$ from (2), we get

$d = 1 = 2\,(256 - 7 \cdot 36) - 7$

Or $1 = 2\,(256) - 2\,(7 \cdot 36) - 7$

$= 2 \cdot 256 - 7 \cdot 72 - 7$

Or $1 = 2\,(256) - 73 \cdot 7$

Multiplying by $5 = b$, we get

$5 = 10\,(256) - 7\,(365)$

Using this value of 5, congruence (1) becomes

$7x \equiv 10\,(256) - 7\,(365) \pmod{256}$

Also $0 \equiv 10\,(256) \pmod{256}$

Subtracting these congruence, we get

$7x \equiv -7\,(365) \pmod{256}$

canceling 7, [$\because$ $gcd\,(7, 256) = 1$], we have

$x \equiv -365 \pmod{256}$

Also $0 \equiv 512 \pmod{256}$

Adding $x \equiv 147 \pmod{256}$

$\therefore \quad x \equiv 147 \pmod{256}$

give the least positive solution incongruent *mod* 256.

Example 26. *Solve the linear congruence* $25x \equiv 15 \pmod{29}$.

Solution. The given congruence is

$$25x \equiv 15 \pmod{29}$$

Comparing with $ax \equiv b \pmod{m}$,

we have

$$a = 25, b = 15, m = 29$$

$$d = gcd\,(a, m) = gcd\,(25, 29) = 1$$

which divides $b = 15$.

Hence the congruence has one and only one incongruent solution

Now $25x \equiv 15 \pmod{29}$

Also $0 \equiv 435 \pmod{29}$

Adding (1) and (2), we get

$$25x \equiv 450 \pmod{29}$$

Or $\quad x \equiv 18 \pmod{29}$

$\therefore \quad x \equiv 18 \pmod{29}$ is the only incongruent solution of $25x \equiv 15 \pmod{29}$.

Example 27. *Solve the linear congruence* $5x \equiv 2 \pmod{26}$.

Solution. The given congruence is

$$5x \equiv 2 \pmod{26}$$

Comparing with $ax \equiv b \pmod{m}$,

we have

$$a = 5, b = 2, m = 26$$

$$d = gcd\,(a, m) = gcd\,(5, 26) = 1$$

which divides $b = 2$.

Hence the congruence has one and only one incongruent solution.

Now $5x \equiv 2 \pmod{26}$

Also $0 \equiv 78 \pmod{26}$

Adding (1) and (2), we get

$$5x \equiv 80 \pmod{26}$$

Or $x \equiv 16 \pmod{26}$

Thus $x \equiv 16 \pmod{26}$ is the only incongruent solution of $5x \equiv 2 \pmod{26}$.

Example 28. Solve the linear congruence $6x \equiv 15 \pmod{21}$.

Solution. The given congruence is

$$6x \equiv 15 \pmod{21}$$

Comparing with $ax \equiv b \pmod{m}$, we have

$$a = 6, b = 15, m = 21$$

$$d = gcd(a, m) = gcd(6, 21) = 3$$

which divides $b = 15$.

Therefore the given congruence has 3 solutions incongruent $(mod\ 21)$.

Since $6x \equiv 15 \pmod{21}$ ....(1)

Also $0 \equiv 21 \pmod{21}$ ....(2)

Adding (1) and (2), we have

$$6x = 36 \pmod{21}$$

Or $x \equiv 6 \pmod{21}$ is a solution of $6x \equiv 15 \pmod{21}$

Therefore, all the three incongruent $(mod\ 21)$ solutions of $6x \equiv 15 \pmod{21}$ are given by

$$x_0 + km_1, \text{ where } k = 0, 1, 2, \ldots\ldots, (d-1)$$

where $m_1 = \dfrac{m}{d}$

and $x_0 = 6, d = 3$

$\Rightarrow$ $m_1 = \dfrac{21}{3} = 7$

$\therefore$ 3 solutions of the given congruence are

$$x = x_0 + km_1$$

$$= 6 + 7k \text{ where } k = 0, 1, 2$$

$\therefore$ $x \equiv 6, 13, 20 \pmod{21}$.

Example 29. Solve the linear congruence $36x \equiv 8 \pmod{102}$

Solution. The given congruence is

$$36x \equiv 8 \pmod{102}$$

Comparing with $ax \equiv b \pmod{m}$,
we have

$$a = 36, b = 8, m = 102$$

$$d = gcd(a, m) = gcd(36, 102) = 6$$

which does not divide $b = 8$.

Thus the given congruence has no solution.

Example 30. *Solve the linear congruence* $34x \equiv 60 \pmod{98}$.

Solution. The given congruence is $34x \equiv 60 \pmod{98}$

Comparing with $ax \equiv b$,
we have

$$a = 34, b = 60, m = 98$$

$$d = gcd(a, m) = gcd(34, 98) = 2$$

which divides $b = 60$.

Therefore, the given congruence has 2 solutions incongruent $(mod\ 98)$

Since $34x \equiv 60 \pmod{98}$

Also $0 = 1470 \pmod{98}$ ....(1)

Adding (1) and (2), we have ....(2)

$$34x \equiv 1530 \pmod{98}$$

Or $x \equiv 45 \pmod{98}$

$\therefore$ $x \equiv 45 \pmod{98}$ is a solution of $34x \equiv 60 \pmod{98}$

Therefore, all the two incongruent $(mod\ 98)$ is a solution of $34x \equiv 60 \pmod{98}$ are given by

$$x_0 + km_1, \text{ where } k = 0, 1, 2, \ldots\ldots, (d-1)$$

and $m_1 = \dfrac{m}{d}$,

Here $x_0 = 45, d = 2,$

$$m_1 = \frac{98}{2} = 49$$

$\therefore$ 2 solutions of the given congruence are

$$x = x_0 + km_1$$

$$= 45 + 49k \text{ where } k = 0, 1$$

$\therefore$ $x = 45, 94 \ mod\ (98)$.

Example 31. Solve the linear congruence $140x \equiv 133 \pmod{301}$

Solution. The given congruence is

$$140x \equiv 133 \pmod{301}$$

Comparing with $ax \equiv b, \pmod{m}$,

we have

$$a = 140, b = 133, m = 301$$

$$d = gcd\,(a, m) = gcd\,(140, 301) = 7$$

which divides $b = 133$.

Therefore, the given congruence has 7 solutions incongruent (*mod* 301).

Since $140x = 133 \pmod{301}$ ....(1)

Also $0 \equiv 2107 \pmod{301}$ ....(2)

Adding (1) and (2), we get

$$140x \equiv 2240 \pmod{301}$$

Or $x \equiv 16 \pmod{301}$

$\therefore\ x \equiv 16 \pmod{301}$ is a solution of given congruence.

Therefore all the 7 incongruent (*mod* 301) is a solution of $140x \equiv 133 \pmod{301}$ are given by $x_0 + km_1$ where

$$k = 0, 1, 2, \ldots\ldots, (d - 1)$$

and $m_1 = \dfrac{m}{d}$

Here $x_0 = 16, d = 7,$

$$m_1 = \frac{301}{7} = 43$$

$\therefore$ 7 solutions of the given congruence are

$$x = x_0 + km_1$$

$$= 16 + 43k, \text{ where } k = 0, 1, 2, 3, 4, 5, 6.$$

$\therefore$ $x = 16, 59, 102, 145, 188, 231, 274 \pmod{301}$.

Example 32. Find all solutions of $5x + 3y = 52$ *in positive integers.*

Solution. The given equation can be put into the form

$$5x \equiv 52 \pmod{3}.$$ [1 is the remainder after dividing 52 by 3]

$\Rightarrow$ $5x \equiv 1 \pmod{3}$

Since $5x \equiv 1 \pmod 3$

Also $0 \equiv 9 \pmod 3$

Adding these two, we get

$$5x \equiv 10 \pmod 3$$

Or $x \equiv 2 \pmod 3$

Hence $3y = 52 - 5x$

$= 52 - 10 \pmod 3$ $(\because x = 2)$

$= 42 \pmod 3$

Or $y \equiv 14 \pmod 3$

If $x \equiv 5 \pmod 3$,

then $3y \equiv 52 - 25 \equiv 27 \pmod 3$,

so that $y \equiv 9 \pmod 3$.

If $x \equiv 8 \pmod 3$,

then $3y \equiv 52 - 40 \equiv 12 \pmod 3$

i.e $y \equiv 4 \pmod 3$.

Hence we have the following solution in positive integers :

$(8, 4)$; $(5, 9)$; $(2, 14)$.

Example 33. *Solve the linear congruence*

$$3x - 7y \equiv 11 \pmod{13}.$$

Solution. Given congruence is

$$3x - 7y \equiv 11 \pmod{13}$$

comparing with $ax + by \equiv c \pmod m$, we have ....(1)

$$a = 3, b = -7, m = 13$$

Here $d = (a, b, m) = (3, -7, 13) = 1$ and $1 \mid 11$

Therefore the given congruence is solvable.

Congruence (1) can be written as

$$3x \equiv 11 + 7y \pmod{13}$$

$\Rightarrow$ $3x \equiv 24 - 5y \pmod{13}$

i.e. $x \equiv 8 - 2y \pmod{13}$ [$\because 24 \equiv 11 \pmod{13}$ and $7 \equiv -6 \pmod{13}$]

Now each incongruent value of y modulo 13 will give exactly incongruent value of x modulo 13.

Therefore the incongruent solu

$(8, 0), (6, 1), (4, 2), (2$

$(5, 8), (3, 9), (1, 10),$

[$\because$ For $y = 5$, $x \equiv 8 - 10$ (mo

$\equiv -2 \pmod{1}$

$\equiv 11 \pmod{13}$

and so on.

Example 34. Prove that for any

Solution. Divide a by 7, then

$a \equiv 0$ or 1 or 2 or 3

$\Rightarrow$ $a^3 \equiv 0$ or 1 or 6 (m

Since $2^3 = 8 \equiv 1 \pmod 7$,

$3^3 = 27 \equiv 6 \pmod 7$

$4^3 = 64 \equiv 1 \pmod 7$

$5^3 = 125 \equiv 6 \pmod$

$6^3 = 216 \equiv 6 \pmod$

Example 35. Prove that for a

Solution. Divide a by 5, then

$a \equiv 0$ or 1 or 2 or

$\Rightarrow$ $a^2 \equiv 0$ or 1 or 4 (

$\Rightarrow$ $a^4 \equiv 0$ or 1 (mod

since $3^2 = 9 \equiv 4 \pmod$

and $4^2 = 16 \equiv 1$ (mo

Example 36. Show that if t

Solution. Divide a by 6.

Let k be the quotient a

$\therefore$ $a = 6k + r$ wher

But $r = 0$ or 1 or 2

$\therefore$ $2 \nmid a$ and $3 \nmid$

$r \neq 0, \neq 2, \neq 3,$

Therefore the incongruent solution are the ordered pair of integers
(8, 0), (6, 1), (4, 2), (2, 3), (0, 4), (11, 5), (9, 6), (7, 7),
(5, 8), (3, 9), (1, 10), (12, 11) and (10, 12).

[For $y = 5$, $x \equiv 8 - 10 \pmod{13}$
$\equiv -2 \pmod{13}$
$\equiv 11 \pmod{13}$]

and so on.

Example 34. Prove that for any integer a, $a^3 \equiv 0$ *or* 1 *or* $6 \pmod 7$.

Solution. Divide a by 7, then

$a \equiv 0$ or 1 or 2 or 3 or 4 or 5 or $6 \pmod 7$

$\Rightarrow$ $a^3 \equiv 0$ or 1 or $6 \pmod 7$.

Since $2^3 = 8 \equiv 1 \pmod 7$,

$3^3 = 27 \equiv 6 \pmod 7$,

$4^3 = 64 \equiv 1 \pmod 7$

$5^3 = 125 \equiv 6 \pmod 7$

$6^3 = 216 \equiv 6 \pmod 7$.

Example 35. Prove that for any integer a, $a^4 \equiv 0$ *or* $1 \pmod 5$.

Solution. Divide a by 5, then

$a \equiv 0$ or 1 or 2 or 3 or $4 \pmod 5$

$\Rightarrow$ $a^2 \equiv 0$ or 1 or $4 \pmod 5$

$\Rightarrow$ $a^4 \equiv 0$ or $1 \pmod 5$, $[\because 4^2 = 16 \equiv 1 \pmod 5]$

since $3^2 = 9 \equiv 4 \pmod 5$

and $4^2 = 16 \equiv 1 \pmod 5$.

Example 36. Show that if the integer a is not divisible by 2 *or* 3, *then* $a^2 \equiv 1 \pmod{24}$.

Solution. Divide a by 6.

Let k be the quotient and r be the least non-negative remainder.

$\therefore$ $a = 6k + r$ where

$r \equiv 0$ or 1 or 2 or 3 or 4 or 5

But $2 \nmid a$ and $3 \nmid a$

$\therefore$ $r \neq 0, \neq 2, \neq 3, \neq 4$

$\therefore$ $r = 1$ or 5 so that

$a = 6k + 1$ or $6k + 5$

i.e $a = 6k \pm 1$ type

$\Rightarrow$ $a^2 = 36k^2 \pm 12k + 1$

$= 12k(3k \pm 1) + 1$ ...(1)

$\Rightarrow$ $a^2 - 1 = 12k(3k \pm 1)$

If k is odd, then $3k \pm 1$ is even so that $24 \mid 12k(3k \pm 1)$

$\therefore$ in each case,

$12k(3k \pm 1) \equiv 0 \pmod{24}$

$\Rightarrow$ $a^2 - 1 \equiv 0 \pmod{24}$ by (1)

$\Rightarrow$ $a^2 \equiv 1 \pmod{24}$

CHINESE THEOREM

Theorem 8. State and prove Chinese remainder theorem.

Statement. *Let $m_1, m_2, \ldots, m_r$ be positive integers such that $(m_i, m_j) = 1$ for $i \neq j$. Then, the system of linear congruences*

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2},$$
$$\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots$$
$$x \equiv a_r \pmod{m_r}$$

has a simultaneous solution which is unique modulo $m_1, m_2, \ldots, m_r$.

Proof. Let us write

$$m = m_1 m_2 \ldots\ldots m_r$$

and $$M_k = \frac{m}{m_k} = m_1 m_2 \ldots\ldots m_{k-1} m_{k+1} \ldots\ldots m_r$$

Since $(m_i, m_j) = 1$ for $i \neq j$,

therefore $(M_k, m_k) = 1$ and

$$M_k \equiv 0 \pmod{m_i} \text{ for } i \neq k$$

$\Rightarrow$ $M_k x \equiv 1 \pmod{m_k}$

has a unique solution modulo m_k.

Therefore there exists $b_k \in Z$ such that

$$M_k b_k \equiv 1 \pmod{m_k}$$ ...(1)

Since $M_k \equiv 0 \pmod{m_i}$ for $i \neq k$

$\therefore \quad a_k M_k b_k \equiv 0 \pmod{m_i}$ for $i \neq k$

$\Rightarrow \quad x_0 = a_1 M_1 b_1 + a_2 M_2 b_2 + \ldots\ldots + a_r M_r b_r$ ....(2)

$\equiv a_k M b_k \pmod{m_k}$

Since $M_k b_k \equiv 1 \pmod{m_k}$ by (1),

therefore (2) gives

$x_0 \equiv a_k \pmod{m_k}$

Hence x_0 is a simultaneous solution of given congruences.

Uniqueness

Let x_0 and y_0 be two solutions of given congruences.

$\therefore \quad x_0 \equiv a_k \pmod{m_k}$

and $\quad y_0 \equiv a_k \pmod{m_k} \quad \forall\ k = 1, 2, \ldots\ldots, r$

$\Rightarrow \quad x_0 \equiv y_0 \pmod{m_k} \quad \forall\ k = 1, 2, \ldots\ldots, r$

$\Rightarrow \quad x_0 \equiv y_0 \pmod{m_1, m_2, \ldots\ldots, m_r}$ $[\because (m_i, m_j) = 1$ for $i \neq j]$

Hence the solution of given congruences is unique modulo $m_1 m_2 \ldots\ldots m_r$.

Example 37. Solve the system of congruences

$x \equiv 2 \pmod{3}; x \equiv 3 \pmod{5}; x \equiv 2 \pmod{7}$.

Solution. Given congruences are

$$\left.\begin{aligned} x &\equiv 2 \pmod{3}, \\ x &\equiv 3 \pmod{5} \\ \text{and} \quad x &\equiv 2 \pmod{7} \end{aligned}\right\} \quad \ldots(1)$$

Since 3, 5 and 7 are relatively prime in pairs, therefore congruences (1) has unique solution modulo $3 \cdot 5 \cdot 7 = 105$ *i.e* $m = 105$

Hence $m_1 = 3, m_2 = 5, m_3 = 7,$

$a_1 = 2, a_2 = 3, a_3 = 2$

and $\quad M_1 = \dfrac{m}{m_1} = \dfrac{105}{3} = 35,$

$M_2 = \dfrac{m}{m_2} = \dfrac{105}{5} = 21$

$$M_3 = \frac{m}{m_3} = \frac{105}{7} = 15$$

We solve the linear congruences

$35x \equiv 1 \pmod 3$,

$21x \equiv 1 \pmod 5$,

$15x \equiv 1 \pmod 7$

Solving the above congruences, we get

$35x \equiv 1 \pmod 3$

Also $0 \equiv 69 \pmod 3$

Adding----------

$35x \equiv 70 \pmod 3$

$\Rightarrow x \equiv 2 \pmod 3$

$21x \equiv 1 \pmod 5$

Also $0 \equiv 20 \pmod 5$

Adding----------

$21x \equiv 21 \pmod 5$

$\Rightarrow x \equiv 1 \pmod 5$

Again $15x \equiv 1 \pmod 7$

Also $0 \equiv 14 \pmod 7$

Adding----------

$15x \equiv 15 \pmod 7$

$\Rightarrow x \equiv 1 \pmod 7$

Thus the solutions of the above congruences are $b_1 = 2, b_2 = 1, b_3 = 1$ respectively.

$\therefore \quad x_0 = a_1 M_1 b_1 + a_2 M_2 b_2 + a_3 M_3 b_3$

$= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1$

$= 140 + 63 + 30$

$= 233 \pmod{105}$

Therefore unique solution is given by

$x \equiv 233 \pmod{105}$.

Example 38. A certain integer between 1 *and* 1200 *leaves the remainder* 1, 2, 6 *when divided by* 9, 11, 13 *respectively. What is the integer ?*

Solution. Let us consider congruences

$x \equiv 1 \pmod 9$, ...(1)

$x \equiv 2 \pmod{11}$ ....(2)

and $x \equiv 6 \pmod{13}$ ....(3)

From (1), we get $x = 1 + 9k, k \in Z$

It will satisfy (2) if

$1 + 9k \equiv 2 \pmod{11}$

Or $9k \equiv 1 \pmod{11}$

Also $0 \equiv 44 \pmod{11}$

Adding ----------

$9k \equiv 45 \pmod{11}$

$\Rightarrow \quad k \equiv 5 \pmod{11}$

i.e $k = 5 + 11r; r \in Z$

$\therefore \quad x = 1 + 9k$

$= 1 + 9(5 + 11r)$

$= 46 + 99r$

It will satisfy (3) if

$46 + 99r \equiv 6 \pmod{13}$ [$\because 46 \equiv 7 \pmod{13}$ and $99 \equiv 8 \pmod{13}$]

Or $7 + 8r \equiv 6 \pmod{13}$

Or $8r \equiv -1 \pmod{13}$

Since $8r \equiv -1 \pmod{13}$

Also $0 \equiv 65 \pmod{13}$

Adding ----------

$8r \equiv 64 \pmod{13}$

Or $r \equiv 8 \pmod{13}$

Therefore $r = 8 + 13s; s \in Z$

$\therefore \quad x = 46 + 99(8 + 13s)$

$= 46 + 792 + 1287s$

$= 838 + 1287s\ ;\ s \in Z$

Taking $s = 0$,

$x = 838$ is the required integer.

Example 39. *Solve the following system of congruences* $x \equiv 3\ (mod\ 5)$ *and* $x \equiv 5\ (mod\ 7)$.

Solution. Given congruences are

$x \equiv 3\ (mod\ 5)$ ....(1)

and $x \equiv 5\ (mod\ 7)$ ....(2)

Since $3 \equiv 5\ (mod\ (5, 7))$,

therefore (1) and (2) have a unique solution modulo $[5, 7] = 35$

Now from (1), we have

$x = 3 + 5k;\ k \in Z$

It will satisfy (2) if

$3 + 5k \equiv 5\ (mod\ 7)$

Or $5k \equiv 2\ (mod\ 7)$

Also $0 \equiv 28\ (mod\ 7)$

Adding ----------

$5k \equiv 30\ (mod\ 7)$

Or $k \equiv 6\ (mod\ 7)$

Or $k = 6 + 7m;\ m \in Z$

$\therefore$ $x = 3 + 5\ (6 + 7m)$

$= 33 + 35m$

Therefore solution of given congruence is

$x \equiv 33\ (mod\ 35)$.

Example 40. *Find the least positive integer which when divided by* 5, 6, 7 *leaves positive integers* 3, 1, 4 *respectively.*

Solution. Consider the congruences

$x \equiv 3\ (mod\ 5)$, ...(1)

$x \equiv 1\ (mod\ 6)$, ...(2)

$x \equiv 4\ (mod\ 7)$ ....(3)

Since $x \equiv 3$ is incongruent solution of (1),

$\therefore$ $x = 3 + 5k$ is any solution of (1) $\forall$ $k \in Z$.

It will be a solution of (2) if

$3 + 5k \equiv 1 \pmod 6$

i.e if $5k \equiv -2 \pmod 6$

i.e if $k \equiv 2 \pmod 6$

[$\because$ $5k \equiv -2 \pmod 6$

Also $0 \equiv 12 \pmod 6$

$\Rightarrow$ $5k \equiv 10 \pmod 6$

Or $k \equiv 2 \pmod 6$]

$\therefore$ $x = 3 + 10$ *i.e*

$x = 13$ is a solution of (1) and (2).

$\therefore$ $x = 13 + 5 \cdot 6t$ is any solution of (1) and (2) $\forall\ t \in Z$.

It will be solution of (3) if

$13 + 30t \equiv 4 \pmod 7$

i.e if $-1 + 2t \equiv 4 \pmod 7$

i.e if $2t \equiv 5 \pmod 7$

i.e if $t \equiv 6 \pmod 7$

$\therefore$ $x = 13 + 5 \cdot 6 \cdot 6$

i.e $x = 193$ is solution of (1), (2) and (3).

Therefore the required least positive integer = 193.

Example 41. *Find all integers that give the remainders 1, 2, 3 when divided by 3, 4, 5 respectively.*

Solution. Consider the congruences

$x \equiv 1 \pmod 3$, ...(1)

$x \equiv 2 \pmod 4$, ...(2)

$x \equiv 3 \pmod 5$ ...(3)

Since $x = 1$ is incongruent solution of (1).

$\therefore$ $x = 1 + 3k$ is any solution of (1) $\forall\ k \in Z$.

It will be a solution of (2) if

$1 + 3k \equiv 2 \pmod 4$

i.e if $3k \equiv 1 \pmod 4$

i.e if $k \equiv 3$

$\therefore$ $x = 1 + 3 \cdot 3$

i.e $x = 10$ is a solution of (1) and (2).

$\Rightarrow$ $x = 10 + 3 \cdot 4t$ is any solution of (1) and (2).

It will be solution of (3) if

$$10 + 12t \equiv 3 \pmod 5$$

i.e if $2t \equiv 3 \pmod 5$

i.e if $t \equiv 4$

$\therefore$ $x = 10 + 3 \cdot 4 \cdot 4$

i.e $x = 58$ is a solution of (1), (2) and (3)

$\therefore$ $x \equiv 58 \pmod{3 \cdot 4 \cdot 5}$

i.e $x \equiv 58 \pmod{60}$

i.e $x \equiv -2 \pmod{60}$

$\Rightarrow$ $x = -2 + 60j \ \forall\ j \in Z$

Therefore all solutions of (1), (2) and (3) are given by

$x = 60j - 2$ where j is any integer.

Example 42. Solve the set of congruences

$$x \equiv 1 \pmod 4,\ x \equiv 0 \pmod 3,\ x \equiv 5 \pmod 7.$$

Solution. The given congruences are

$$x \equiv 1 \pmod 4,$$
$$x \equiv 0 \pmod 3,$$
$$x \equiv 5 \pmod 7$$

Since $x = 1$ is incongruent solution of (1),

$\therefore x = 1 + 4k$ is any solution of (1) $\forall\ k \in Z$.

It will be solution of (2) if

$$1 + 4k \equiv 0 \pmod 3$$

i.e if $k \equiv -1 \pmod 3$

i.e if $k = 2$.

$\therefore$ $x = 1 + 4 \cdot 2$ *i.e*

$x = 9$ is solution of (1) and (2)

$\Rightarrow$ $x = 9 + 4 \cdot 3t$ is any solution of (1) and (2) $\forall\ t \in Z$.

It will be solution of (3) if

$$9 + 12t \equiv 5 \pmod 7$$

i.e if $2 + 5t \equiv 5 \pmod 7$

i.e if $5t \equiv 3 \pmod 7$

i.e if $t = 2$

$\therefore \quad x = 9 + 12 \cdot 2$

$\Rightarrow \quad x \equiv 33 \pmod{84}$

$\Rightarrow \quad x \equiv 33 + 84j \ \forall\, j \in Z$

Therefore all solutions of (1), (2) and (3) are given by

$$x = 84j + 33$$

where j is any integer.

Example 43. *Solve the congruence* $x^3 + 4x + 8 \equiv 0 \pmod{15}$.

Solution. The given congruence is

$$x^3 + 4x + 8 \equiv 0 \pmod{15} \quad \text{....(1)}$$

Since $15 = 3 \times 5$ where $(3, 5) = 1$

Therefore the congruence (1) is equivalent to

$$x^3 + 4x + 8 \equiv 0 \pmod 3 \quad \text{....(2)}$$

$$x^3 + 4x + 8 \equiv 0 \pmod 5 \quad \text{....(3)}$$

The possible solution of (2) lies in the set $\{0, 1, 2\}$.

Since $f(0) = 8 \not\equiv 0 \pmod 3$

$f(1) = 13 \not\equiv 0 \pmod 3$

$f(2) = 24 \equiv 0 \pmod 3$

$\therefore \quad x \equiv 2 \pmod 3$ is a solution of (2).

Again the possible solutions of (3) lie in the set $\{0, 1, 2, 3, 4\}$.

Since $f(0) = 8 \not\equiv 0 \pmod 5$

$f(1) = 13 \not\equiv 0 \pmod 5$

$f(2) = 24 \not\equiv 0 \pmod 5$

$f(3) = 47 \not\equiv 0 \pmod 5$

$f(4) = 88 \not\equiv 0 \pmod 5$

Therefore the congruence (3) has no solution.

Since $5 \nmid 15$.

therefore the given congruence $x^3 + 4x + 8 \equiv 0 \pmod{15}$ has no solution.

Example 44. *Find the missing digit of the number* 423124 .... 2819 *so that it is divisible by* 11.

Solution. Let the missing digit be x.

Therefore the number 423124 x 2819 must be divisible by 11.

Since $9 - 1 + 8 - 2 + x - 4 + 2 - 1 + 3 - 2 + 4 = 16 + x$.

Therefore the given number is divisible by 11 iff $11 \mid 16 + x$

where $0 \le x < 10$ and $x \in Z$.

$\therefore$ We must have $x = 6$.

Hence the missing digit is 6.

Example 45. *Show that any integer satisfies atleast one of the following five congruences*

$x \equiv 0 \pmod 2$, $x \equiv 0 \pmod 3$,

$x \equiv 1 \pmod 4$, $x \equiv 5 \pmod 6$,

$x \equiv 7 \pmod{12}$.

Solution. We know that any even integer satisfies

$x \equiv 0 \pmod 2$

For modulo 12, all odd integers can be classified into six classes

$12k + 1, 12k + 3, 12k + 5,$

$12k + 7, 12k + 9, 12k + 11,$

where k is any integer.

Clearly, the classes $12k + 3$, $12k + 9$ satisfy $x \equiv 0 \pmod 3$

The classes $12k + 1$, $12k + 5$ satisfy $x \equiv 1 \pmod 4$ and the classes $12k + 7$, $12k + 11$ satisfy

$x \equiv 7 \pmod{12}$, $x \equiv 5 \pmod 6$ respectively.

Complete and reduced residue systems

Definition. *If* $x \equiv y \pmod m$, *then* y *is called a* **residue** *of* x *modulo* m.

A set $\{x_1, x_2, \ldots, x_m\}$ *is called a* **complete residue system** *(CRS) modulo* m *if for every integer* y *there is one and only one* x_i *such that* $y \equiv x_i \pmod m$.

Definition. *A* **reduced residue system** *(RRS) modulo* m *is a set of integers* r_i *such that* $(r_i, m) = 1$, $r_i \not\equiv r_j \pmod m$.

If $i \not\equiv j$ *and such that every* x

Note

1. There are infinitely
2. A set of m integers
   two integers in the
3. For fixed integers a
   arithmetic progressi

This set is called a resid

Example 46. *Show that* {1
$m > 2$.

Solution. Since $1^2 - (m - 1$

Therefore given set is

Theorem 9. *If* $a_1, a_2, \ldots, a$
$aa_1 + b, aa_2 + b, \ldots, aa_m +$
m.

Proof. Since we know tha
modulo m if and only if k

So we have only to pr

$$aa_i + b \not\equiv aa_j +$$

Let, if possible

$$aa_i + b \equiv aa_j +$$

$$\Rightarrow \quad aa_i \equiv aa_j \pmod{}$$

But $(a, m) = 1$

Therefore, $a_i \equiv a_j$ (mo
which is a contradicti
Hence $aa_i + b$ is a co

$r_i \neq r_j$ and such that every x prime to x is congruent modulo m to some number r_i of the set.

Note

1. There are infinitely many complete residue system modulo m.
2. A set of m integers form a complete residue system modulo m if and only if no two integers in the set are congruent modulo m.
3. For fixed integers a and $m > 0$, the set of all integers x satisfy $x \equiv a \pmod{m}$ is the arithmetic progression ....., $a-3m$, $a-2m$, $a-m$, $a+m$, $a+2m$, $a+3m$,.... This set is called a residue class or congruence class, modulo m.

Example 46. Show that $\{1^2, 2^2, \ldots\ldots, m^2\}$ *is not a complete residue system modulo m if* $m > 2$.

Solution. Since $1^2 - (m-1)^2 = 1 - m^2 - 2m + 1$

$$= 2m - m^2$$
$$\equiv 0 \pmod{m}$$

Therefore given set is not a complete residue system modulo m.

Theorem 9. If $a_1, a_2, \ldots, a_m$ ***is a complete residue system modulo m and*** $(a, m) = 1$, ***then*** $aa_1 + b, aa_2 + b, \ldots\ldots, aa_m + b$, ***b is any integer are also a complete residue system modulo m.***

Proof. Since we know that a set of k integers $a_1, a_2, \ldots\ldots, a_k$ is a complete residue system modulo m if and only if $k = m$ and $a_i \not\equiv a_j \pmod{m}$, $i \neq j$.

So we have only to prove that

$$aa_i + b \not\equiv aa_j + b \pmod{m}, \; i \neq j.$$

Let, if possible

$$aa_i + b \equiv aa_j + b \pmod{m}$$

$$\Rightarrow \quad aa_i \equiv aa_j \pmod{m}$$

But $(a, m) = 1$

Therefore, $a_i \equiv a_j \pmod{m}$,

which is a contradiction, because $a_1, \ldots\ldots, a_m$ is a complete residue system of m.

Hence $aa_i + b$ is a complete residue system modulo m.

TESTS OF DIVISIBILITY

Theorem 10. Let $N = a_m 10^m + a_{m-1} 10^{m-1} + \ldots + a_1 10 + a_0$ *be the decimal expression of positive integer* $N, 0 \le a_k < 10$ *and let* $S = a_0 + a_1 + \ldots + a_m$. *Prove that* $9 \mid N$ *iff* $9 \mid S$.

Proof. Let $f(x) = \sum_{k=0}^{m} a_k x^k$

Since $10 \equiv 1 \pmod 9$

$\therefore \quad f(10) \equiv f(-1) \pmod 9$

$\Rightarrow \quad \sum_{k=0}^{m} a_k 10^k \equiv \sum_{k=0}^{m} a_k \pmod 9$

$\Rightarrow \quad N \equiv S \pmod 9$

Hence $N \equiv 0 \pmod 9$ iff $S \equiv 0 \pmod 9$

i.e $9 \mid N$ iff $9 \mid S$.

Theorem 11. Let $N = a_m 10^m + a_{m-1} 10^{m-1} + \ldots + a_1 10 + a_0$ *be the decimal representation of positive integer* $N, 0 \le a_k < 10$ *and let*

$$T = a_0 - a_1 + a_2 - \ldots\ldots + (-1)^m a_m .$$

Prove that $11 \mid N$ *iff* $11 \mid T$.

Proof. Let $f(x) = \sum_{k=0}^{m} a_k x^k$

Since $10 \equiv -1 \pmod{11}$

$\therefore \quad f(10) \equiv f(-1) \pmod{11}$

$\Rightarrow \quad \sum_{k=0}^{m} a_k (10)^k \equiv \sum_{k=0}^{m} a_k (-1)^k \pmod{11}$

$\Rightarrow \quad N \equiv T \pmod{11}$

Hence $N \equiv 0 \pmod{11}$ iff $T \equiv 0 \pmod{11}$

i.e $11 \mid N$ iff $11 \mid T$.

Example 47. Show that 670, 04

Solution. Since $7 + (-0) + 1 +$

and $11 \mid 11 \Rightarrow 11 \mid 670$

Example 48. Show that 176, 5

Solution. Since $1 + 7 + 6 + 5$

and $9 \mid 27 \Rightarrow 9 \mid 176,$

Example 49. Find the missin

by 11.

Solution. Suppose the missi

$9, 555, 5x4, 35$

Since $3 - 5 + 3 - 4 + x$

Given number is divisi

$11 \Leftrightarrow 11 \mid x - 12$

$\Leftrightarrow 11 \mid x - 1.$

Also $0 \le x < 10$, then

Example 50. Show that 2

Solution. Since $6 - 5 + 1$

and $11 \mid 0$

$\therefore \quad 11 \mid 22354156$

Example 51. Show that

Solution. Since $1 + 7 +$

and $9 \mid 27$

$\therefore \quad 9 \mid 17621512$

Example 52. Find the

Solution. Clearly $9^9 \equiv$

$\therefore \quad 9^9 = 10k +$

$= 9^{10k+}$

$= (9^{10}$

$\equiv 81 \ (m$

Example 47. Show that 670, 040, 107 *is divisible by* 11.

Solution. Since $7+(-0)+1+(-0)+4+(-0)+0+(-7)+6=11$

and $11 \mid 11 \Rightarrow 11 \mid 670,040,107.$

Example 48. Show that 176, 521, 221 *is divisible by* 9.

Solution. Since $1+7+6+5+2+1+2+2+1=27$

and $9 \mid 27 \Rightarrow 9 \mid 176,521,221.$

Example 49. Find the missing digit of the number 9, 555, 5 – 4, 353 *so that it is divisible by* 11.

Solution. Suppose the missing digit is x, then we have

9, 555, 5 x 4, 353 should be divisible by 11.

Since $3-5+3-4+x-5+5-5+5-9=x-12$;

Given number is divisible by

$11 \Leftrightarrow 11 \mid x-12$

$\Leftrightarrow 11 \mid x-1.$

Also $0 \le x < 10$, then $x=1$ *i.e* the missing digit is one.

Example 50. Show that 22354156 *is divisible by* 11.

Solution. Since $6-5+1-4+5-3+2-2=0$

and $11 \mid 0$

$\therefore$ $11 \mid 22354156$

Example 51. Show that the number 176215122 *is divisible by* 9.

Solution. Since $1+7+6+2+1+5+1+2+2=27$

and $9 \mid 27$

$\therefore$ $9 \mid 176215122.$

Example 52. Find the last two digits of numbers 9^{9^9}.

Solution. *Clearly* $9^9 \equiv 9 \pmod{10}$

$\therefore$ $9^9 = 10k+9,\ k \in Z$ ...(1)

$\Rightarrow$ $9^{9^9} = 9^{10k+9}$

$= (9^{10})^k \cdot 9^9$

But $9^2 \equiv 81 \pmod{100}$

$\Rightarrow \quad 9^4 \equiv 81^2 \equiv 61 \pmod{100}$

$\Rightarrow \quad 9^8 \equiv 61^2 \equiv 21 \pmod{100}$

$\Rightarrow \quad 9^9 \equiv 189 \equiv 89 \pmod{100}$

$\Rightarrow \quad 9^{10} \equiv 801 \equiv 1 \pmod{100}$

From (1), (2) and (3), we have

$$9^{9^9} \equiv 89 \times 1 \pmod{100}$$

Or $\quad 9^{9^9} \equiv 89 \pmod{100}$

Thus the last two digits of 9^{9^9} are 89.

Example 53. *Prove that an integer is divisible by 3 iff the sum of its digits is divisible by 3.*

Solution. Let

$$N = a_m 10^m + a_{m-1} 10^{m-1} + \ldots\ldots + 10^2 a_2 + 10a_1 + a_0$$

be the decimal expansion of the positive integer N, $0 \le a_k < 10$.

Let $\quad f(x) = \sum_{k=0}^{m} a_k x^k$

Since $\quad 10 \equiv 1 \pmod 3$

$\therefore \quad f(10) \equiv f(1) \pmod 3$

i.e $\quad \sum_{k=0}^{m} a_k 10^k \equiv \sum_{k=0}^{m} a_k \pmod 3$

i.e $\quad N \equiv \sum_{k=0}^{m} a_k \pmod 3$

Hence $N \equiv 0 \pmod 3$ iff

$$\sum_{k=0}^{m} a_k \equiv 0 \pmod 3$$

i.e $\quad 3 \mid N$ iff $3 \mid \sum_{k=0}^{m} a_k$.

Example 54. Prove that an integer is divisible by 4 iff the number formed by its tens and units digits is divisible by 4.

Solution. Let $N = a_m\ 10^m + a_{m-1}\ 10^{m-1} + \ldots + a_1\ 10 + a_0$ be the decimal expression of the positive integer N, $0 \le a_k < 10$.

Since $10^k \equiv 0\ (mod\ 4)$ for $k \ge 2$

$$\Rightarrow \quad a_k\ 10^k \equiv 0\ (mod\ 4) \text{ for } 2 \le k \le m$$

$$\Rightarrow \quad \sum_{k=2}^{m} a_k\ 10^k \equiv 0\ (mod\ 4)$$

$$\Rightarrow \quad N = \sum_{k=0}^{m} a_k\ 10^k$$

$$\equiv a_1\ 10 + a_0\ (mod\ 4)$$

$$\Rightarrow \quad N \equiv 0\ (mod\ 4) \text{ iff } a_1\ 10 + a_0 \equiv 0\ (mod 4)$$

i.e. $4 \mid N$ iff the number formed by its tens and units digits is divisible by 4.

Example 55. Find the last two digits of number 2^{1000}.

Solution. We have

$$2^{10} = 1024 \equiv 24\ (mod\ 100) \qquad \ldots(1)$$

$$\Rightarrow \quad 2^{20} \equiv 576 \equiv 76\ (mod\ 100)$$

Now $76^2 \equiv 76\ (mod\ 100)$ ...(2)

and hence by induction, for any positive integer k,

$$76^k \equiv 76\ (mod\ 100)$$

From (1) and (2), we get

$$2^{1000} \equiv 76^{50} \equiv 76\ (mod\ 100)$$

Thus the last two digits of 2^{1000} are 76.

Example 56. Find the missing digit of the number 423124 .... 2819 so that it is divisible by 11.

Solution. Let the missing digit be x.

Therefore the number 423124 x 2819 must be divisible by 11.

Since $9-1+8-2+x-4+2-1+3-2+4=16+x$.

Therefore the given number is divisible by 11 iff $11 \mid 16+x$

where $0 \le x < 10$ and $x \in Z$.

$\therefore$ We must have $x=6$.

Hence the missing digit is 6.

❑❑❑

4

CHAPTER

FERMAT NUMBE

The number $F_$

thought they might

Here we can ea

which F_n is known

For $n = 5, 6, \ldots$

FERMAT'S FACT

Question. Explain

Solution. Let n be

square of two integ

$$n = x^2$$

If $n = ab, a \geq$

$$n = \left($$

We want to fi

$$n = x^2$$

Or $x^2 - n$

By inspection

$$k^2 - n$$

Let $m \geq \sqrt{n}$ su

4
CHAPTER

FERMAT'S THEOREM

Fermat's Factorization Method

FERMAT NUMBER

The number $F_n = 2^{2^n} + 1$ are called the Fermat's numbers after Pierre Fermat who thought they might all be prime.

Here we can easily show that F_n is prime for $n = 0, 1, \ldots, n$, there are the only n for which F_n is known to be prime.

For $n = 5, 6, \ldots, 21$, F_n is composite.

FERMAT'S FACTORIZATION METHOD

Question. Explain Fermat's factorization method.

Solution. Let n be any odd positive integer such that it can be written as the difference of square of two integers *i.e*

$$n = x^2 - y^2 = (x - y)(x + y)$$

If $n = ab$, $a \geq b \geq 1$, then we can write

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

We want to find the integral value of x and y which satisfy

$$n = x^2 - y^2$$

Or $\quad x^2 - n = y^2$

By inspection, we observe the following numbers

$$k^2 - n, (k+1)^2 - n, (k+2)^2 - n, \ldots\ldots$$

Let $m \geq \sqrt{n}$ such that $m^2 - n$ is square.

If n can be factorized, then it is not expressible as difference of squares of two numbers and then n has no factor other than n and 1.

Hence, n is prime.

Order of a modulo m

If $(a, m) = 1$, λ is the smallest positive integer such that $a^{\lambda} \equiv 1 \pmod{m}$

i.e $a^{\lambda} \equiv 1 \pmod{m}$, $a^k \not\equiv 1 \pmod{m}$, $0 < k < 1$.

Then λ is called the order of a modulo m.

Pseudo Prime

Any integer n is called a pseudo prime if $2^n \equiv 2 \pmod{n}$.

e.g. the number 341 is a pseudo prime because

$$2^{341} \equiv 2 \pmod{341}$$

Absolutely Pseudo Primes

A composite number n is called an absolute pseudo prime if

$$a^n \equiv a \pmod{n}, \ \forall\ a.$$

Note

1. The absolutely pseudo prime is also known as Chemichael number.
2. The least absolutely pseudo prime number is 561.

Theorem 1. Let n be a composite square free integer. Also let $n = p_1 p_2 \ldots\ldots p_r$, p_i are distinct primes. If $(p_1 - 1) \mid (n - 1)$ for $i = 1, 2, \ldots\ldots, r$ then n is an absolutely pseudo primes.

Proof. Let a be an integer such that

$$(a, n) = 1.$$

Then $(a, p_i) = 1 \ \forall\ i$

Therefore, by Fermat's theorem, we have

$$a^{p_i - 1} \equiv 1 \pmod{p_i} \ \forall\ i = 1, 2, \ldots\ldots, r$$

$$\Rightarrow \quad p_i \mid (a^{p_i - 1} - 1) \ \forall\ i = 1, 2, \ldots\ldots, r$$

$$\Rightarrow \quad p_i \mid (a^{n-1} - 1) \ \forall\ i = 1, 2, \ldots\ldots, r \qquad (\because p_i - 1 \mid n - 1)$$

$$\Rightarrow \quad p_1 p_2 \ldots\ldots p_r \mid a^{n-1} - 1$$

$$\Rightarrow \quad n \mid a^{n-1} - 1$$

$$\Rightarrow \quad a^{n-1} \equiv 1 \pmod{n} \text{ when } (a, n) = 1$$

$\Rightarrow \quad a^n \equiv a \pmod{n} \ \forall\ a \in Z.$

Hence n is an absolute pseudo prime.

Example 1. Show that 561 is an absolute pseudo prime.

Solution. Clearly $561 = 3 \cdot 11 \cdot 17$.

If a is an integer such that

$(a, 561) = 1$, then

$(a, 3) = 1$, $(a, 11) = 1$ and $(a, 17) = 1$.

Therefore by Fermat's theorem

$$a^2 \equiv 1 \pmod{3},$$

$$a^{10} \equiv 1 \pmod{11},$$

$$a^{16} \equiv 1 \pmod{17}$$

$$\Rightarrow \quad a^{560} \equiv (a^2)^{280} \equiv 1 \pmod{3},$$

$$a^{560} \equiv (a^{10})^{56} \equiv 1 \pmod{11}$$

and $\quad a^{560} = (a^{16})^{35} \equiv 1 \pmod{17}$

Combining these three congruences, we get

$$a^{560} \equiv 1 \pmod{561} \text{ when } (a, 561) = 1$$

$$\Rightarrow \quad a^{561} \equiv a \pmod{561} \ \forall\ a \in Z$$

Hence 561 is an absolute pseudo prime.

Example 2. Show that 341 is a pseudo prime but not an absolute pseudo prime.

Solution. Since $2^{341} \equiv 2 \pmod{341}$

Therefore 341 is a pseudo prime.

Since 31 is a prime and $11 \nmid 31$, therefore by Fermat's theorem, we have

$$11^{30} \equiv 1 \pmod{31}$$

$$\Rightarrow \quad (11^{30})^{11} \equiv (1)^{11} \pmod{31}$$

$$\Rightarrow \quad 11^{330} \equiv 1 \pmod{31} \qquad \ldots(1)$$

Also $\quad 11^2 = 121 \equiv -3 \pmod{31}$ $\qquad \ldots(2)$

$$\Rightarrow \quad 11^8 \equiv 81 \equiv 19 \pmod{31} \qquad \ldots(3)$$

From (2) and (3), we have

$$11^{10} \equiv -57 \equiv 5 \pmod{31} \qquad \ldots(4)$$

Or $\quad 11^{11} \equiv 55 \equiv 24 \pmod{31}$

From (1) and (4), we get

$$11^{341} \equiv 24 \pmod{31}$$

$$\Rightarrow \quad 31 \nmid 11^{341} - 11$$

$$\Rightarrow \quad 11 \times 31 \nmid 11^{341} - 11$$

$$\Rightarrow \quad 341 \nmid 11^{341} - 11$$

$$\Rightarrow \quad 11^{341} \not\equiv 11 \pmod{341}$$

Hence 341 is not an absolute pseudo prime.

Example 3. *Factorize* 10541 *by Fermat's factorization method.*

Solution. Here $n = 10541$

Clearly $102^2 < 10541 < 103^2$

Thus, we have considered the values of $k^2 - 10541$ for $k \geq 103$

We have

$$103^2 - 10541 = 10609 - 10541 = 68$$

$$104^2 - 10541 = 10816 - 10541 = 275$$

$$105^2 - 10541 = 11025 - 10541 = 484 = 22^2$$

$$\Rightarrow \quad 10541 = 105^2 - 22^2$$

$$= (105 + 22)(105 - 22)$$

$$= 127 \times 83$$

which are the required factors.

Example 4. *Use Fermat's method to factor* 340663.

Solution. Here $n = 340663$

Clearly $583^2 < 340663 < 584^2$

Thus we consider the values of k in the range

$$584 < k < \frac{340663 + 1}{2} = 170032$$

which makes $k^2 - 340663$ a perfect square.

$$584^2 - 340663 = 341056 - 340663 = 393$$

$$585^2 - 340663 = 34225 - 340663 = 1562$$

$$586^2 - 340663 = 343396 - 340663 = 2733$$

$$587^2 - 340663 = 344569 - 340663 = 3906$$

$$588^2 - 340663 = 345744 - 340663 = 5081$$

$$589^2 - 340663 = 346921 - 340663 = 6258$$

$$590^2 - 340663 = 348100 - 340663 = 7437$$

$$591^2 - 340663 = 349281 - 340663 = 8618$$

$$592^2 - 340663 = 350464 - 340663 = 9801 = (99)^2$$

Therefore

$$340663 = 592^2 - 99^2$$

$$= (592 + 99)(592 - 99)$$

$$= 691 \times 493$$

which are the required factors.

Example 5. *Factor the numbers* $2^{11} - 1$ *by Fermat's factorization method.*

Solution. We have

$$2^{11} - 1 = (2^5)^2 \cdot 2 - 1$$

$$= (32)^2 \cdot 2 - 1$$

$$= (1024) \cdot 2 - 1$$

$$= 2048 - 1$$

$$= 2047$$

Clearly $45^2 < 2047 < 46^2$

Thus we consider the values of k in the range

$$46 < k < \frac{2047 + 1}{2} = 1024$$

which makes $k^2 - 2047$ a perfect square.

$$46^2 - 2047 = 2116 - 2047 = 69$$

$$47^2 - 2047 = 2269 - 2047 = 162$$

$$48^2 - 2047 = 2304 - 2047 = 257$$

$$49^2 - 2047 = 2401 - 2047 = 354$$

$$50^2 - 2047 = 2500 - 2047 = 453$$

$$51^2 - 2047 = 2601 - 2047 = 554$$

$$52^2 - 2047 = 2704 - 2047 = 657$$

$$53^2 - 2047 = 2809 - 2047 = 762$$

$54^2 - 2047 = 2916 - 2047 = 869$

$55^2 - 2047 = 3025 - 2047 = 978$

$56^2 - 2047 = 3136 - 2047 = 1089 = 33^2$

$\Rightarrow \quad 2047 = 56^2 - 33^2$

$= (56 + 33)(56 - 33)$

$= 89 \times 23$

which are the required factors.

Theorem 2. ***State and prove Fermat's theorem.***

Or

State and prove Fermat's little theorem.

Statement. If p is a prime number and gcd $(a, p) = 1$, ***then*** $a^{p-1} \equiv 1 \pmod{p}$.

Proof. Since $gcd\ (a, p) = 1$,

therefore if the number a, $2a$, $3a$,....., $(p-1)\,a$ are divided by p, the remainders are 1, 2, 3,...., $(p-1)$, though not necessarily in this order.

Let $r_1, r_2, \ldots\ldots, r_{p-1}$ be the remainders obtained on dividing $a, 2a, \ldots\ldots, (p-1)a$ respectively by p.

Then as mentioned above $r_1, r_2, \ldots\ldots, r_{p-1}$ are precisely $1, 2, \ldots\ldots, p-1$ placed in some order so that the product $r_1 r_2 \ldots\ldots r_{p-1}$ = the product $1 \cdot 2 \ldots\ldots (p-1) \ldots\ldots (1)$

Now $a \equiv r_1 \pmod{p}$

$2a \equiv r_2 \pmod{p}$

.....

.....

$(p-1)\,a \equiv r_{p-1} \pmod{p}$

Multiplying these congruence relations, we get

$a \cdot 2a \cdot 3a \ldots\ldots (p-1) \cdot a \equiv r_1 r_2 \ldots\ldots r_{p-1} \pmod{p}$

Or $1 \cdot 2 \cdot 3 \ldots\ldots (p-1)\, a^{p-1} \equiv 1 \cdot 2 \cdot 3 \ldots\ldots (p-1) \pmod{p}$ [by (1)]

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

Since p is prime, therefore

$gcd\ (p, 1) = 1$, $gcd\ (p, 2) = 1, \ldots\ldots$,

$gcd\ (p, (p-1)) = 1$,

and hence $gcd\ (p, (p-1)!) = 1$.

Therefore cancelling $(p-1)!$ from both sides of (2), we get

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

Theorem 3. ***If p is a prime, then*** $a^p \equiv a \pmod{p}$ ***for any integer a.***

Proof. Since p is a prime, either $p \mid a$ or $gcd\ (a, p) = 1$.

Therefore if $p \mid a$, then

$a \equiv 0 \pmod{p}$

$\Rightarrow \quad a^p \equiv 0 \pmod{p}$

Hence $a^p \equiv a \pmod{p}$.

Now, suppose $gcd\ (a, p) = 1$.

The integers a, $2a$,....., $(p-1)\,a$ are mutually incongruent

$p-1$ integers coprime to p.

But then $1, 2, \ldots\ldots, p-1$ is a reduced residue system (mod p).

Hence for each j, $1 \le j \le p-1$, there exists a unique i, $1 \le i \le p-1$ such that

$ja \equiv i \pmod{p}$

Therefore,

$a \cdot 2a \ldots\ldots (p-1)\, a \equiv 1 \cdot 2 \ldots\ldots (p-1) \pmod{p}$

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

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

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

Multiplying both sides by a, we have

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

2nd ***Proof (Alternatively)***

By induction for any integers $a_1, a_2, \ldots\ldots, a_n$

$(a_1 + a_2 + \ldots + a_n)^p \equiv (a_1^p + a_2^p + \ldots\ldots + a_n^p) \pmod{p}$

Putting $a_1 = a_2 = \ldots\ldots = a_n = 1$ in (1), we get

$(1 + 1 + \ldots\ldots + 1)^p \equiv (1^p + 1^p + \ldots\ldots 1^p) \pmod{p}$

Or $n^p \equiv n \pmod{p}$ for every natural number n.

Replacing n by a, we have

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

Corollary. *If n is odd and $2^{n-1} \not\equiv 1 \pmod{n}$ then n must be composite.*

Proof. If possible let n be prime.

Therefore by Fermat's theorem, we have

$$2^{n-1} \equiv 1 \pmod{n}$$

which contradicts the given hypothesis.

Hence n is composite.

Example 6. *Show that* $5^{38} \equiv 4 \pmod{11}$.

Solution. Since we know that

$$a^p \equiv a \pmod{p}, \text{ then}$$

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

$$\therefore \quad 5^{38} = 5^{3 \cdot 11 + 5} = (5^{11})^3 \cdot 5^5$$

$$= 5^3 \cdot 5^5 \pmod{11}$$

$$= 5^8 \pmod{11}$$

$$= (5^2)^4 \pmod{11}$$

$$= 3^4 \pmod{11}$$

$$= 81 \pmod{11}$$

$$= 4 \pmod{11}$$

Example 7. *Give an example to show that the converse of Fermat's theorem is not true.*

Solution. ***Example is***

Let $p = 561$ and a be any integer such that $(a, p) = 1$.

Since $561 = 3 \cdot 11 \cdot 17$

$\therefore \quad (a, 561) = 1$

$\Rightarrow \quad (a, 3) = 1, (a, 11) = 1, (a, 17) = 1$

Then $a^2 \equiv 1 \pmod{3}$,

$a^{10} \equiv 1 \pmod{11}$,

$a^{16} \equiv 1 \pmod{17}$

Raising power 280, 56 and 35 respectively, we get

$a^{560} \equiv 1 \pmod{3}$,

$a^{560} \equiv 1 \pmod{11}$,

$a^{560} \equiv 1 \pmod{17}$

But 3, 11, 17 are mutually coprime

$\therefore \quad a^{560} \equiv 1 \pmod{3 \cdot 11 \cdot 17}$

$\therefore \quad a^{560} \equiv 1 \pmod{561}$

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

But p is not prime number.

Therefore converse of Fermat's theorem may not be true.

Example 8. *Prove that* $\frac{1}{3}n^3 + \frac{1}{5}n^5 + \frac{7}{15}n$ *is an integer for every integer* n.

Solution. By Fermat's theorem, we have

$$n^3 \equiv n \pmod{3} \text{ and}$$

$$n^5 \equiv n \pmod{5}$$

$$\Rightarrow \quad 3 \mid n^3 - n \text{ and } 5 \mid n^5 - n$$

$$\Rightarrow \quad \frac{n^3 - n}{3} \text{ and } \frac{n^5 - n}{5} \text{ are integers}$$

$$\Rightarrow \quad \frac{n^3 - n}{3} + \frac{n^5 - n}{5} \text{ is an integer}$$

$$\Rightarrow \quad \frac{n^3}{3} + \frac{n^5}{5} - \left(\frac{n}{3} + \frac{n}{5}\right) \text{is an integer}$$

$$\Rightarrow \quad \frac{1}{3}n^3 + \frac{1}{5}n^5 - \frac{8}{15}n \text{ is an integer}$$

$$\Rightarrow \quad \left(\frac{1}{3}n^3 + \frac{1}{5}n^5 - \frac{8}{15}n\right) + n \text{ is an integer.}$$

$$\Rightarrow \quad \frac{1}{3}n^3 + \frac{1}{5}n^5 + \frac{7}{15}n \text{ is an integer.}$$

Example 9. *Prove that* 42 *divides* $n^7 - n$ *for every integer* n.

Solution. Since $42 = 6 \cdot 7$ and

$$n^7 - n = n(n^6 - 1)$$

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

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

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

Since $(n-1), n, (n+1)$ are three consecutive integers,

$\therefore \quad 3 \mid (n-1)\, n\, (n+1)$

i.e $\quad 6 \mid (n-1)\, n\, (n+1)$

$\Rightarrow \quad 6 \mid (n-1)\, n\, (n+1)\, (n^4 + n^2 + 1)$

$\Rightarrow \quad 6 \mid n^7 - n$

Also by Fermat's theorem,

$$n^7 \equiv n \pmod 7 \qquad \ldots(1)$$

$\Rightarrow \quad 7 \mid n^7 - n$

Since $(6, 7) = 1$

Therefore by (1) and (2), we get

$$6 \cdot 7 \mid n^7 - n$$

$\Rightarrow \quad 42 \mid n^7 - n$ for every integer n.

Lemma

If p and q are distinct primes with $a^p \equiv a \pmod q$ and $a^q \equiv a \pmod p$, then

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

Proof. Since we know that

$$a^p \equiv a \pmod p$$

$\therefore \quad (a^p)^q \equiv a^p \pmod q$

and $a^p \equiv a \pmod q$ by hypothesis

$\Rightarrow \quad a^{pq} \equiv a \pmod q$

$\Rightarrow \quad q \mid a^{pq} - a$

Similarly $(a^q)^p \equiv a^q \pmod p$ ....(1)

and $\quad a^q \equiv a \pmod p$

$\Rightarrow \quad a^{pq} \equiv a \pmod p$

$\Rightarrow \quad p \mid a^{pq} - a$

Since p and q are distinct primes, ...(2)

$\therefore$ (1) and (2) $\Rightarrow pq \mid a^{pq} - a$

Or $\quad a^{pq} \equiv a \pmod{pq}$.

e.g. $\quad 2^{340} \equiv 1 \pmod{341}$,

where $341 = 11 \cdot 31$ is not a prime

But $\quad 2^{341} \equiv 2 \pmod{341}$.

For, $\quad 2^{11} \equiv 2 \pmod{31}$

Since $\quad 2^{11} = 2^{5 \cdot 2 + 1}$

$$= (2^5)^2 \cdot 2$$

$$= (32)^2 \cdot 2$$

$$\equiv 2 \pmod{31}$$

and $\quad 2^{31} \equiv 2 \pmod{11}$,

as $\quad 2^{31} \equiv 2^{5 \cdot 6 + 1} \equiv (2^5)^6 \cdot 2$

$$\equiv (32)^6 \cdot 2$$

$$\equiv (-1)^6 \cdot 2$$

$$\equiv 2 \pmod{31}$$

Therefore by above lemma

$$2^{341} \equiv 2 \pmod{341}.$$

Hence converse of Fermat's theorem is false.

Example 10. *Show that $5^{10} - 3^{10}$ is divisible by 11.*

Solution. Here $gcd\ (5, 11) = 1$ and $gcd\ (3, 11) = 1$.

Hence $\quad 5^{10} - 3^{10} = 5^{11-1} - 1 - (3^{11-1} - 1)$

$$\equiv 0 \pmod{11}.$$

Since by Fermat's theorem

$$5^{11-1} - 1 = 0 \pmod{11} \text{ and}$$

$$3^{11-1} - 1 \equiv 0 \pmod{11}.$$

$\therefore \quad 5^{10} - 3^{10} \equiv 0 \pmod{11}$

$\Rightarrow \quad 11 \mid (5^{10} - 3^{10})$

Example 11. *If n and a are coprime to 91, prove that $n^{12} - a^{12}$ is divisible by 91.*

Solution. Since $gcd\ (n, 91) = 1$ and

$gcd\ (a, 91) = 1$

$\therefore \quad gcd\ (n, 13) = 1$ and

$gcd\ (a, 13) = 1$ [$\because$ 13 is a divisor of 91

Therefore by Fermat's theorem,

$$n^{12} \equiv 1 \pmod{13}$$

and $a^{12} \equiv 1 \pmod{13}$

Subtracting, we get

$$n^{12} - a^{12} \equiv 0 \pmod{13}$$

Therefore $n^{12} - a^{12}$ is divisible by 13.

Again, since n and a are both co-prime to 91, therefore n and a are both coprimes to 7. ....(1)

($\because$ 7 is a factor of 91)

Also, 7 is a prime,

$\therefore$ by Fermat's theorem,

$$n^6 \equiv 1 \pmod{7}$$

and $a^6 \equiv 1 \pmod{7}$

Raising both congruences to power 2, we get

$$n^{12} \equiv 1 \pmod{7}$$

and $a^{12} \equiv 1 \pmod{7}$

Subtracting this congruence, we get

$$n^{12} - a^{12} \equiv 0 \pmod{7}$$

$\therefore$ $n^{12} - a^{12}$ is divisible by 7.

Hence from (1) and (2), we get ....(2)

$n^{12} - a^{12}$ is divisible by 91 ($= 13 \times 7$).

Example 12. *If gcd* $(a, 133) = gcd\ (b, 133) = 1$, *show that*

$133 \mid a^{18} - b^{18}$.

Solution. Since $gcd\ (a, 133) = 1$

and $gcd\ (b, 133) = 1$.

But $133 = 19 \times 7$

$\therefore$ $gcd\ (a, 19) = 1$ and $gcd\ (b, 19) = 1$.

But 19 is a prime number,

$\therefore$ by Fermat's theorem

$$a^{18} \equiv 1 \pmod{19}$$ and

$$b^{18} \equiv 1 \pmod{19}$$

Subtracting, we get

$$a^{18} - b^{18} \equiv 0 \pmod{19}$$

Again since a and b are both comprimes to 133. ....(1)

$\therefore$ a and b are coprimes to 7.

($\because$ 7 is a factor of 133)

$\therefore$ by Fermat's theorem,

$$a^6 \equiv 1 \pmod{7}$$

and $b^6 \equiv 1 \pmod{7}$

Raising both congruences to power 3, we get

$$a^{18} \equiv 1 \pmod{7}$$

and $b^{18} \equiv 1 \pmod{7}$

Subtracting, we get

$$a^{18} - b^{18} \equiv 0 \pmod{7}$$ ....(2)

From (1) and (2), we get

$a^{18} - b^{18}$ is divisible by 133 ($= 19 \times 7$)

i.e $133 \mid a^{18} - b^{18}$.

Example 13. *Prove that* $a^{11} - a$ *is divisible by* 11 *for any integer* a.

Solution. Since 11 is a prime number, also we know that

$$a^p \equiv a \pmod{p}$$ if p is a prime number

$\therefore$ $a^{11} \equiv a \pmod{11}$

Hence $a^{11} - a$ is divisible by 11.

Example 14. *Show that* $a^7 \equiv a \pmod{42}$ $\forall$ a.

Solution. Since 7 is prime, therefore by Fermat's theorem, we have

$$a^7 \equiv a \pmod{7}$$ ....(1)

i.e $7 \mid (a^7 - a)$

Also $a^7 - a = a\ (a^6 - 1)$

$= a\ (a^3 - 1)\ (a^3 + 1)$

$= a\ (a - 1)\ (a^2 + a + 1)\ (a + 1)\ (a^2 - a + 1)$

$= (a-1)\,a\,(a+1)\,(a^2+a+1)\,(a^2-a+1)$

Now $(a-1)\,a\,(a+1)$ is a product of three consecutive integers so it is divisible by 3 *i.e* by 6.

Thus $6 \mid (a^7 - a)$ ...(1)

Since $gcd\,(6, 7) = 1$,

therefore from (1) and (2), we have

$(6 \cdot 7) \mid (a^7 - a)$

$\Rightarrow \quad 42 \mid (a^7 - a)$

Hence $a^7 - a$ is divisible by 42.

Example 15. *Show that* $2^{48} \equiv 1 \pmod{105}$

Solution. Here $2^{48} = (2^4)^{12}$

$= (16)^2 \cdot (16)^4 \cdot (16)^6$

By Fermat's theorem,

$(16)^2 \equiv 1 \pmod 3$

$(16)^4 \equiv 1 \pmod 5$

$(16)^6 \equiv 1 \pmod 7$

Hence $2^{48} \equiv (16)^2 \cdot (16)^4 \cdot (16)^6 \equiv 1 \pmod{105}$.

Example 16. *Show that* $30 \mid a^{4b+1} - a$.

Solution. $a^{4b+1} - a = a\,(a^{4b} - 1)$

$\Rightarrow \quad a \mid a^{4b+1} - a$

and $\quad a^4 - 1 \mid a^{4b+1} - a$

$\Rightarrow \quad a\,(a^4 - 1) \mid a^{4b+1} - a$

Now $\quad a^4 - 1 \equiv 0 \pmod 5$ and also

$a\,(a^2 - 1) = a\,(a-1)\,(a+1)$

and $\quad 3 \nmid (a-1)\,a\,(a+1)$

Hence the result follows.

Example 17. *Show that* $a^{12} - 1$ *is divisible by 7 when* $gcd\,(a, 7) = 1$.

Solution. Since 7 is prime and $gcd\,(a, 7) = 1$, therefore by

Fermat's theorem, we have

$a^{7-1} \equiv 1 \pmod 7$

$\Rightarrow \quad a^6 \equiv 1 \pmod 7$

$\Rightarrow \quad 7 \mid (a^6 - 1)$

$\Rightarrow \quad 7 \mid (a^6 - 1)\,(a^6 + 1)$

$\Rightarrow \quad 7 \mid (a^{12} - 1)$

Hence $a^{12} - 1$ is divisible by 7.

Example 18. *Employ Fermat's theorem to prove that, if p is odd prime, then*

$1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots\ldots + (p-1)^{p-1} \equiv -1 \pmod p$

Solution. Since p is a prime number and 1, 2, 3....., $(p-1)$ are all less than p.

$\therefore \quad gcd\,(1, p) = 1,$

$gcd\,(2, p) = 1,$

$gcd\,(3, p) = 1,$

.....,

$gcd\,(p-1, p) = 1.$

Therefore putting, $a = 1, 2, 3, \ldots\ldots, (p-1)$ in Fermat's theorem,

$a^{p-1} \equiv 1 \pmod p$, we have

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

$2^{p-1} \equiv 1 \pmod p,$

$3^{p-1} \equiv 1 \pmod p$

.....

and $\quad (p-1)^{p-1} \equiv 1 \pmod p$

Adding up all these $(p-1)$ congruences, we get

$1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots\ldots + (p-1)^{p-1} \equiv (p-1) \pmod p$

Also $\quad 0 \equiv p \pmod p$

Subtracting these congruences, we get

$1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots\ldots + (p-1)^{p-1} \equiv -1 \pmod p$

Or $\quad 1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots\ldots + (p-1)^{p-1} + 1 \equiv 0 \pmod p$

Example 19. Prove that $576 \mid 5^{2n+2} - 24n - 25$.

Solution. We have

$$5^{2n+2} - 24n - 25 = 25^{n+1} - 24n - 25$$
$$= 25(1+24)^n - 24n - 25$$
$$= 25(1 + 24 \cdot n + \text{multiple of } 24^2) - 24n - 25$$
$$= (25 + 25 \cdot n \cdot 24 + \text{multiple of } 24^2) - 24n - 25$$
$$= 25 + 25 \cdot 24n + \text{ multiple of } 24^2) - 24n - 25$$
$$= 25 \cdot 24n - 24n + \text{multiple of } 24^2$$
$$= 24n(25-1) + \text{ multiple of } 24^2$$
$$= 24n \cdot 24 + \text{ multiple of } 24^2$$
$$= 576n + \text{ multiple of } 24^2$$
$$= 576 + \text{multiple of } 576$$
$$= 576(n+5)$$
$$= \text{multiple of } 576.$$

$\therefore \quad 576 \mid 5^{2n+2} - 24n - 25.$

Example 20. *For* $n \geq 1$, *show that* $27 \mid 2^{5n+1} + 5^{n+2}$

Or

Prove that 27 *divides* $2^{5n+1} + 5^{n+2}$.

Solution.

$$2^{5n+1} + 5^{n+2} = 2 \cdot (2^5)^n + 5^2 \cdot 5^n$$
$$= 2(32)^n + 25 \cdot 5^n$$
$$\equiv 2 \cdot 5^n + 25 \cdot 5^n \qquad [\because 32 \equiv 5 \pmod{27}]$$
$$\equiv (2+25) \cdot 5^n \pmod{27}$$
$$\equiv 27 \cdot 5^n \pmod{27}$$
$$\equiv 0 \pmod{27}$$

Hence $27 \mid 2^{5n+1} + 5^{n+2}$.

Example 21. *Prove that* $2^{15} - 2^3$ *divides* $a^{15} - a^3$ *for any integer* a.

Solution. We have

$$2^{15} - 2^3 = 2^3(2^{12} - 1)$$
$$= 8(2^6 - 1)(2^6 + 1)$$
$$= 8 \cdot 63 \cdot 65$$
$$= 5 \cdot 7 \cdot 8 \cdot 9 \cdot 13$$

By Fermat's theorem, we have

$$a^5 \equiv a \pmod{5},$$
$$a^7 \equiv a \pmod{7}$$
and $\quad a^{13} \equiv a \pmod{13}$

Now $\quad a^5 \equiv a \pmod{5}$

$\Rightarrow \quad a^{15} \equiv a^3 \pmod{5}$ ...(1)

$$a^7 \equiv a \pmod{7}$$

$\Rightarrow \quad a^{14} \equiv a^2 \pmod{7}$

$\Rightarrow \quad a^{15} \equiv a^2 \pmod{7}$ ...(2)

and $\quad a^{13} \equiv a \pmod{13}$ ...(3)

$\Rightarrow \quad a^{15} \equiv a^2 \pmod{13}$

If $8 \mid a$ then $8 \mid a^{15} - a^3$

and if $8 \nmid a$ then by Euler's theorem.

$$a^{\phi(8)} \equiv 1 \pmod{8}$$

$\Rightarrow \quad a^4 \equiv 1 \pmod{8}$

$\Rightarrow \quad a^{12} \equiv 1 \pmod{8}$

$\Rightarrow \quad a^{15} \equiv a^3 \pmod{8}$ ...(4)

$\therefore$ in either case $a^{15} \equiv a^3 \pmod{8}$

If $9 \mid a$ then $9 \mid a^{15} - a^3$

and if $9 \nmid a$ then Euler's theorem

$$a^{\phi(9)} \equiv 1 \pmod{9}$$

$\Rightarrow \quad a^6 \equiv 1 \pmod{9}$

$\Rightarrow \quad a^{12} \equiv 1 \pmod{9}$

$\Rightarrow \quad a^{15} \equiv a^3 \pmod{9}$

$\therefore$ in either case $a^{15} \equiv a^3 \pmod 9$ ...(3)

Since 5, 7, 8, 9, 13 are relatively prime in pairs, therefore from (1), (2), (3), (4) and (5), we get

$$a^{15} \equiv a^3 \bmod (5 \cdot 7 \cdot 8 \cdot 9 \cdot 13)$$

Or $a^5 \equiv a^3 \bmod (2^{15} - 2^3)$

$\therefore$ $2^{15} - 2^3 \mid a^{15} - a^3$ for any integer a.

Example 22. *For $n \geq 1$, show that*

$$(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}$$

Solution. We prove the result by induction on n.

For $n = 1$,

$$(-13)^{1+1} \equiv (-13)^1 + (-13)^{1-1} \pmod{181}$$

iff $169 \equiv -13 + 1 \pmod{181}$

iff $169 \equiv -12 \pmod{181}$

which is true.

Therefore the result is true for $n = 1$.

Let the result be true for $n = k$.

$\therefore$ $(-13)^{k+1} \equiv (-13)^k + (-13)^{k-1} \pmod{181}$ ...(1)

Now $(-13)^{k+2} \equiv (-13)(-13)^{k+1}$

$\equiv (-13)[(-13)^k + (-13)^{k-1}] \pmod{181}$ [by (1)]

$\equiv (-13)^{k+1} + (-13)^k \pmod{181}$

Therefore the result is true for $n = k + 1$.

Hence by induction result is true for all $n \in N$.

Example 23. *Show that $61 \mid 2^{48} + 3^3$.*

Solution. Since $2^6 \equiv 2 \pmod{61}$

$\therefore$ $(2^6)^4 \equiv 3^4 \pmod{61}$

But $3^4 \equiv 20 \pmod{61}$

Hence $2^{24} \equiv 20 \pmod{61}$

$\Rightarrow$ $2^{18} \equiv 400 \pmod{61}$

$\Rightarrow$ $2^{48} \equiv -3^3 \pmod{61}$

$\Rightarrow$ $2^{48} + 3^3 \equiv 0 \pmod{61}$

$\Rightarrow$ $61 \mid 2^{48} + 3^3$.

Example 24. *If m,n are primes, then show that $m^{n-1} + n^{m-1} - 1$ is a multiple of mn.*

Solution. We have $m \mid m^{n-1}$ ...(1)

Since m and n are primes,

therefore $gcd\ (m, n) = 1$.

So by Fermat's theorem,

$$n^{m-1} \equiv 1 \pmod m$$

i.e $m \mid (n^{m-1} - 1)$ ...(2)

From (1) and (2), we have

$m \mid (m^{n-1} + n^{m-1} - 1)$ ...(3)

Again $n \mid n^{m-1}$

Also by Fermat's theorem

$$m^{n-1} \equiv 1 \pmod n$$

i.e $n \mid (m^{n-1} - 1)$

$\therefore$ $n \mid (n^{m-1} + m^{n-1} - 1)$ ...(4)

From (3) and (4), we have

$$m^{n-1} + n^{m-1} - 1 \equiv 0 \pmod n$$

$\therefore$ $m^{n-1} + n^{m-1} - 1 \equiv 0 \pmod{\text{L.C.M. of } m \text{ and } n}$

$\equiv 0 \pmod{mn}$

Thus $mn \mid (m^{n-1} + n^{m-1} - 1)$.

Hence $m^{n-1} + n^{m-1} - 1$ is a multiple of mn.

Example 25. *Find the remainder when 2^{100} is divided by 11 and 2^{105} is divided by 11.*

Solution. $2^{100} = (2^{10})^{10}$

But $2^{10} \equiv 1 \pmod{11}$ by Fermat's theorem.

Hence $(2^{10})^{10} \equiv 1 \pmod{11}$

Thus the remainder is 1.

Now $2^{105} = 2^{100+5}$

$= (2^{100}) \cdot 2^5$

$= (2^{100}) \cdot 32$

$= 1\,(10) = 10\,(mod\ 11)$

The remainder in this case is 10.

Example 26. *What is the last digit in the ordinary decimal representation of* 3^{400} *?*

Solution. Here $3^4 \equiv 1\,(mod\ 5)$ by Fermat's theorem.

Also $3^4 \equiv 1\,(mod\ 2)$.

Hence $3^4 \equiv 1\,(mod\ 5)$ with

$3^4 \equiv 1\,(mod\ 2)$

$\Rightarrow \quad 3^4 \equiv 1\,(mod\ 10)$

and hence $3^{4n} \equiv 1\,(mod\ 10)$ for any $n \geq 1$.

Thus 1 is the last digit.

Example 27. *If* $(a, 35) = 1$, *show that* $a^{12} \equiv 1\,(mod\ 35)$.

Solution. Since $35 = 7 \cdot 5$

As $\quad gcd\,(a, 35) = 1$

$\Rightarrow \quad gcd\,(a, 5) = 1.$

Since 7 is a prime number so by Fermat's theorem

$$a^6 \equiv 1\,(mod\ 7) \qquad \ldots(1)$$

Also 5 is a prime number so by Fermat's theorem

$$a^4 \equiv 1\,(mod\ 5) \qquad \ldots(2)$$

Raising congruence (1) to power 2 and congruence (2) to power 3, we have

$a^{12} \equiv 1\,(mod\ 7)$

and $\quad a^{12} \equiv 1\,(mod\ 5)$

Hence $a^{12} \equiv 1\,(mod\ 7)$ with

$a^{12} \equiv 1\,(mod\ 5)$

$\Rightarrow \quad a^{12} \equiv 1\,(mod\ 35).$

Example 28. *Prove that* $n^{16} - 1$ *is divisible by* 17 *if* $gcd\,(n, 17) = 1$.

Solution. Since $gcd\,(n, 17) = 1$ and 17 is a prime number.

Therefore by Fermat's theorem,

$n^{16} \equiv 1\,(mod\ 17)$

Or $\quad 17 \mid (n^{16} - 1)$

i.e $\quad (n^{16} - 1)$ is divisible by 17.

Example 29. *Show that* $111^{333} + 333^{111}$ *is divisible by* 7.

Solution. Since $111^{333} + 333^{111} \equiv (-1)^{333} + 4^{111}\,(mod\ 7)$

$\because \quad 111 \equiv -1\,(mod\ 7)$

and $\quad 333 \equiv 4\,(mod\ 7)$

$\Rightarrow \quad 111^{333} + 333^{111} \equiv -1 + (4^3)^{37}\,(mod\ 7)$

$\equiv -1 + (64)^{37}\,(mod\ 7)$

$\equiv -1 + 1^{37}\,(mod\ 7)\,[\because 64 \equiv 1\,(mod\ 7)]$

$\equiv -1 + 1\,(mod\ 7)$

$\equiv 0\,(mod\ 7)$

$\Rightarrow \quad 7 \mid 111^{333} + 333^{111}.$

Example 30. *Show that the integer* $53^{103} + 103^{53}$ *is divided by* 39.

Solution. Since

$(53)^{103} + (103)^{53} \equiv (14)^{103} + (-14)^{53}\,(mod\ 39)$

$[\because 53 \equiv 14\,(mod\ 39)$ and $103 \equiv -14\,(mod\ 39)]$

$\equiv 14^{103} - 14^{53}\,(mod\ 39)$

$\equiv 14^{53}\,[14^{50} - 1]\,(mod\ 39)$

$= 14^{53}\,[(14^2)^{25} - 1]\,(mod\ 39)$

$= 14^{53}\,[(196)^{25} - 1]\,(mod\ 39)$

$= 14^{53}\,(1 - 1)\,(mod\ 39) \qquad [\because 196 \equiv 1\,(mod\ 39)]$

$\equiv 0\,(mod\ 39).$

$\Rightarrow \quad 39 \mid 53^{103} + 103^{53}.$

Example 31. *Find the remainder when* 4444^{4444} *is divided by* 9.

Solution. We have

$4444 = 9 \cdot 493 + 7$

$\equiv 7\,(mod\ 9)$

$\equiv -2 \pmod 9$

$\therefore \quad 4444^{4444} \equiv (-2)^{4444} \pmod 9$

Now $(-2)^3 \equiv 1 \pmod 9$ —(1)

$\Rightarrow \quad (-2)^{3 \cdot 1481} \equiv 1 \pmod 9$

$\Rightarrow \quad (-2)^{3 \cdot 1481} \cdot (-2) \equiv -2 \pmod 9$

$\Rightarrow \quad (-2)^{3 \cdot 1481 + 1} \equiv -2 \pmod 9$

$\Rightarrow \quad (-2)^{4444} \equiv -2 \pmod 9$

$\Rightarrow \quad (-2)^{4444} \equiv 7 \pmod 9$ —(2)

From (1) and (2), we get

$4444^{4444} \equiv 7 \pmod 9$

Therefore 4444^{4444} leaves remainder 7 when divided by 9.

Example 32. *Find the remainder when* $1! + 2! + 3! + \ldots\ldots + 100!$ *is divided by* 12.

Solution. Since $4! = 24 \equiv 0 \pmod{12}$

and for any $k \geq 4$,

$k! = 1 \cdot 2 \cdot 3 \cdot 4 \ldots\ldots (k-1)\, k$

$= 4!\, 5 \cdot 6 \ldots\ldots k$

$\Rightarrow \quad k! \equiv 0 \pmod{12}$

$\therefore \quad 1! + 2! + 3! + 4! + \ldots\ldots + 100! \equiv (1! + 2! + 3!) \pmod{12}$

$\Rightarrow \quad 1! + 2! + 3! + 4! + \ldots\ldots + 100! \equiv 9 \pmod{12}$

Thus, $1! + 2! + \ldots\ldots + 100!$ leaves remainder 9 when divided by 12.

Example 33. *Obtain the necessary and sufficient condition that a positive integer n can be divided by* 7.

Solution. Since, we have

$1000 \equiv -1 \pmod 7$

We can write

$$n = a_0 + a_1 (1000) + a_2 (1000)^2 + \ldots\ldots + a_{k-1} (1000)^{k-1},\ 0 < a_i < 1000$$

Then, we get the required condition

$$(a_0 + a_1 + \ldots\ldots) - (a_1 + a_3 + \ldots\ldots) = \sum_{i=0}^{k-1} (-1)^i a_i \equiv 0 \pmod 7$$

For example

$n = 637693 = 693 + 637\ (1000)$

$\Rightarrow \quad a_0 = 693,\ a_1 = 637$

Since $a_0 - a_1 = 693 - 637 = 56 \equiv 0 \pmod 7$

Hence 637693 is a multiple of 7.

Example 34. *Find the remainder when the sum* $S = 1! + 2! + 3! + \ldots\ldots + 1000!$ *is divisible by* 8.

Solution. We know that $k!$ is divisible by 8 for all $k \geq 4$, we have

$S = 1! + 2! + 3! + \ldots\ldots + 1000!$

$= 1! + 2! + 3! \pmod 8$

$= 1 + 2 + 6 \pmod 8$

$= 9 \pmod 8$

$\equiv 1 \pmod 8$

Hence the required remainder is 1.

Example 35. *Show that* $x^2 + y^2 = z^2$ *has no solution consisting of only primes i.e no prime solution.*

Solution. Let, if possible, $x = a,\ y = b,\ z = c$ form a prime solution.

If $a = 2$, from $c^2 - b^2 = a^2$, we get

$(c - b)(c + b) = 4$

$\Rightarrow \quad c + b = 4,\ c - b = 1$

i.e $\quad c = \dfrac{5}{2}$ which is not possible.

Thus a and b are both odd.

Then $\quad a^2 \equiv 1 \pmod 4$

$b^2 \equiv 1 \pmod 4$

Hence $a^2 + b^2 \equiv 2 \equiv c^2 \pmod 4$

and $\quad 2 \mid c,$

which is a contradiction.

This contradiction shows that a, b, c all are not prime.

Example 36. *Find the remainder when the sum* $1^5 + 2^5 + 3^5 + \ldots\ldots + 99^5 + 100^5$ *is divided by* 4.

Solution. Since $1^5 + 2^5 + 3^5 + 4^5 + \ldots\ldots + 100^5$

$\equiv 1^5+2^5+3^5+0^5+1^5+2^5+3^5+0^5+\ldots\ldots+1^5+2^5+3^5+0^5 \pmod 4$

i.e $1^5+2^5+3^5+\ldots\ldots+100^5$

$\equiv 25(1^5+2^5+3^5) \pmod 4$ $[\because 4 \equiv 0 \pmod 4)\ 5 \equiv 1 \pmod 4$ etc.$]$

$\equiv 1[1^5+2^5+(-1)^5] \pmod 4$ $[\because 3 \equiv -1 \pmod 4$ and $25 \equiv 1 \pmod 4]$

$\equiv (1+32-1) \pmod 4$

$\equiv 32 \pmod 4$

$\equiv 0 \pmod 4$

Therefore the remainder is 0 when

$1^5+2^5+3^5+\ldots\ldots+100^5$

is divided by 4.

Example 37. *Find the remainder when* 2^{50} *and* 41^{65} *is divided by* 7.

Solution. $2^{50} = 2^2(2^6)^8 = 4 \cdot (64)^8$

i.e $2^{50} = 4(64)^8$

Taking *(mod* 7*)*, we get

$2^{50} \equiv 4(1)^8 \pmod 7$

$\Rightarrow$ $2^{50} \equiv 4 \pmod 7$

$\Rightarrow$ the remainder is 4 when 2^{50} divided by 7.

Since $(41)^{65} \equiv (-1)^{65} \pmod 7$

$[\because 41 \equiv -1 \pmod 7)]$

$\Rightarrow$ $41^{65} \equiv 6 \pmod 7$

$[\because -1 \equiv 6 \pmod 7)]$

$\Rightarrow$ $41^{65} \equiv 6 \pmod 7$

Therefore the remainder is 6 when 41^{65} is divided by 7.

Example 38. *For* $n \geq 1$*, show that* $(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}$

Solution. We shall prove this result by applying induction on n.

When $n = 1$, result will be true for $n = 1$

i.e if $(-13)^{1+1} \equiv (-13)^1 + (-13)^0 \pmod{181}$

i.e if $169 \equiv -13 + 1 \pmod{181}$

i.e if $169 \equiv -12 \pmod{181}$

i.e if $181 \mid 169 - (-12)$

i.e if $181 \mid 181$.

which is true.

Therefore the result is true for $n = 1$.

Let us assume that the result is true for $n = k$

i.e $(-13)^{k+1} \equiv (-13)^k + (-13)^{k-1} \pmod{181}$

Now we prove that the result is true for $n = k+1$

i.e we prove that

$(-13)^{k+2} \equiv (-13)^{k+1} + (-13)^k \pmod{181}$

Since $(-13)^{k+2} = -13(-13)^{k+1}$

$\equiv -13[(-13)^k + (-13)^{k-1}] \pmod{181}$

$\equiv [(-13)^{k+1} + (-13)^k] \pmod{181}$

i.e $(-13)^{k+2} \equiv (-13)^{k+1} + (-13)^k \pmod{181}$

Therefore the result is true for $n = k+1$.

Hence by induction the result is true $\forall\ n \geq 1$.

Example 39. *Find the remainder when* 5^{11} *is divided by* 7.

Solution. Since $(5, 7) = 1$ and 7 is prime,

therefore we have

$5^6 \equiv 1 \pmod 7$

$5^4 \equiv 2 \pmod 7$

$\therefore$ $5^{11} = 5^6 \times 5^4 \times 5 \pmod 7$

$= 1 \times 2 \times 5 \pmod 7$

$= 10 \pmod 7$

$= 3 \pmod 7$

Hence the required remainder is 3.

Example 40. *Find the remainder when* 72^{1001} *is divided by* 31.

Solution. Here we have

$72 \equiv 10 \pmod{31}$

$\therefore$ $72^{1001} \equiv 10^{1001} \pmod{31}$

Since $(10, 31) = 1$ and 31 is prime, therefore by Fermat's theorem, we have

$$10^{30} \equiv 1 \pmod{31}$$

$$\Rightarrow \quad 10^{990} \equiv 1 \pmod{31}$$

Further, $10^2 \equiv 7 \pmod{31}$

$$10^4 \equiv -13 \pmod{31}$$

$$10^8 \equiv 14 \pmod{31}$$

Again $72^{1001} = 10^{1001} \pmod{31}$

$$= 10^{990} \times 10^8 \times 10^2 \times 10 \pmod{31}$$

$$= 1 \times 14 \times 7 \times 10 \pmod{31}$$

$$= 5 \times 10 \pmod{31}$$

$$= 19 \pmod{31}$$

Hence, the required remainder is 19.

Example 41. *Prove that if a is an odd integer, then*

$$a^2 \equiv 1 \pmod{8}.$$

Solution. Since a is an odd integer, so let

$$a = 2k + 1$$

$$\Rightarrow \quad a^2 = (2k+1)^2$$

$$= 4k^2 + 1 + 4k$$

$$\Rightarrow \quad a^2 = 4k(k+1) + 1$$

Taking $(mod\ 8)$, we get

$$a^2 \equiv 0 + 1 \pmod{8}$$

[$\because$ one of k and $k+1$ is even so $2 \mid k(k+1)$]

$$\Rightarrow \quad a^2 \equiv 1 \pmod{8}$$

$$\Rightarrow \quad 8 \mid 4k(k+1).$$

Example 42. *Prove that if the integer a is not divisible by 2 or 3, then $a^2 \equiv 1 \pmod{24}$.*

Solution. Divide a by 6.

Let k be the quotient and r be the least non-negative remainder.

$\therefore \quad a = 6k + r, r = 0$ or 1 or 2 or 3 or 4 or 5

But $\quad 2 \nmid a$, and $3 \nmid a$,

$\therefore \quad r \neq 0, \neq 2, \neq 3, \neq 4,$

$\therefore \quad r = 1$ or 5 so that

$a = 6k + 1$ or $6k + 5$

i.e $\quad a = 6k \pm 1$ type.

$\Rightarrow \quad a^2 = 36k^2 \pm 12k + 1$

$= 12k(3k \pm 1) + 1$

$\Rightarrow \quad a^2 - 1 = 12k(3k \pm 1)$ —(1)

If k is even, then $24 \mid 12k(3k \pm 1)$

If k is odd, then $3k \pm 1$ is even so that

$24 \mid 12k(3k \pm 1)$

Therefore in each case,

$12k(3k \pm 1) \equiv 0 \pmod{24}$

$\Rightarrow \quad a^2 - 1 \equiv 0 \pmod{24}$ by (1)

$\Rightarrow \quad a^2 \equiv 1 \pmod{24}.$

Example 43. *Show that 1729 is an pseudo prime.*

Solution. Here, we have

$$1729 = 7 \times 13 \times 19$$

If $(a, 1729) = 1$, then

$$(a, 7) = 1, (a, 13) = 1, (a, 19) = 1.$$

Then by Fermat's theorem, we have

$$a^6 \equiv 1 \pmod{7},$$

$$a^{12} \equiv 1 \pmod{13},$$

$$a^{18} \equiv 1 \pmod{19}$$

which gives

$$a^{1728} \equiv (a^6)^{288} \equiv 1 \pmod{7}$$

$$= (a^{12})^{144} \equiv 1 \pmod{13}$$

$$\equiv (a^{18})^{96} \equiv 1 \pmod{19}$$

$$\equiv 1 \pmod{7 \cdot 13 \cdot 19}$$

$$\equiv 1 \pmod{1729}$$

Hence, 1729 is an absolute pseudo prime.

Example 44. *Prove that $(a+b)^p \equiv a^p + b^p \pmod{p}$, where p is prime number.*

Solution. Since

$$(a+b)^p = a^p + pa^{p-1}b + \frac{p(p-1)}{2!}a^{p-2}b^2 + \ldots + pab^{p-1} + b^p$$

i.e $$(a+b)^p = a^p + b^p + p\left[a^{p-1}b + \frac{p-1}{2}a^{p-1}b^2 + \ldots + ab^{p-1}\right]$$

Taking $(mod\ p)$, we get

$$(a+b)^p \equiv a^p + b^p + 0\ (mod\ p)$$

i.e $$(a+b)^p \equiv a^p + b^p\ (mod\ p).$$

Example 45. *Show that $3m^n - 1$ is never perfect square $\forall\ m, n \in N$.*

Solution. If possible let $3m^n - 1$ be a perfect square, say

$$3m^n - 1 = t^2 \quad \ldots(1)$$

Divide t by 3,

let k be the quotient and r be the least non-negative remainder.

$$\therefore \quad t = 3k + r;\ r = 0 \text{ or } 1 \text{ or } 2 \quad \ldots(2)$$

Taking $(mod\ 3)$ in (1) and (2), we get

$$0 - 1 \equiv t^2\ (mod\ 3) \text{ and}$$

$$t \equiv r\ (mod\ 3)$$

$$\Rightarrow \quad t^2 \equiv -1\ (mod\ 3) \text{ and}$$

$$t^2 \equiv r^2\ (mod\ 3)$$

$$\Rightarrow \quad r^2 \equiv -1\ (mod\ 3)$$

where $r = 0$ or 1 or 2

which is impossible.

$\therefore$ $3m^n - 1$ is never a perfect square.

Example 46. *If $7 \nmid a$ then prove that either $a^3 + 1$ or $a^3 - 1$ is divisible by 7.*

Solution. Since $7 \nmid a$, therefore by Fermat's theorem, we have

$$a^6 \equiv 1\ (mod\ 7)$$

$$\Rightarrow \quad 7 \mid (a^6 - 1)$$

$$\Rightarrow \quad 7 \mid (a^3 - 1)(a^3 + 1)$$

$$\Rightarrow \quad 7 \mid a^3 - 1 \text{ or } 7 \mid a^3 + 1$$

which shows that if $7 \nmid a$, then either $a^3 + 1$ or $a^3 - 1$ is divisible by 7.

Example 47. *If p is a prime other than 2 or 5 then show that p divides infinitely many of integers 9, 99, 999, 9999,.....*

Solution. Since $p \neq 2$ or 5

Therefore $(p, 10) = 1$ and hence by Fermat's theorem

$$10^{p-1} \equiv 1\ (mod\ p)$$

$$\Rightarrow \quad (10^{p-1})^n \equiv 1\ (mod\ p) \text{ for any positive integer } n$$

$$\Rightarrow \quad 10^k \equiv 1\ (mod\ p) \text{ where } k = n(p-1)$$

$$\Rightarrow \quad p \mid 10^k - 1 \text{ for infinitely many } k \text{ of form } n(p-1)$$

$$\Rightarrow p \text{ divides infinitely of integers } 9, 99, 999, \ldots\ldots$$

WILSON'S THEOREM

Theorem 4. State and prove Wilson's theorem.

Statement. If p is prime, then $(p-1)! \equiv -1\ (mod\ p)$.

Proof. Suppose p is a prime.

Let a be an integer such that

$$1 \leq a \leq p - 1.$$

Then $gcd\ (a.\ p) = 1$.

Hence the congruence

$$ax \equiv 1\ (mod\ p)$$

has a unique solution $(mod\ p)$ say b.

$$\therefore \quad ab \equiv 1\ (mod\ p)$$

Also if $b \equiv a\ (mod\ p)$, then

$$a^2 \equiv 1\ (mod\ p)$$

$$\Rightarrow \quad p \mid a^2 - 1$$

$$\Rightarrow \quad p \mid a - 1 \text{ or } p \mid a + 1$$

$$\Rightarrow \quad a \equiv 1\ (mod\ p) \text{ or } a \equiv -1\ (mod\ p)$$

Thus for each integer $b \in \{2, 3, \ldots\ldots, p-2\}$ there is an integer $c \in \{2, 3, \ldots\ldots, p-2\}$ such that $bc \equiv 1\ (mod\ p)$

Therefore, by pairing b's $(1 < b < p-1)$ with c's $(1 < c < p-1)$ such that

$bc \equiv 1\ (mod\ p)$, we get

$$1 \cdot 2 \cdot 3 \ldots\ldots\ldots\ldots (p-1) \equiv 1 \cdot (p-1)\ (mod\ p)$$

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

$$\Rightarrow \quad (p-1)! \equiv -1\ (mod\ p)$$

Hence the Proof.

Note

General form of Wilson's Theorem

If $x_1, x_2, \ldots, x_{\phi(m)}$ is the reduced residue system modulo prime p, then

$$x_1 x_2 \ldots x_{\phi(m)} + 1 \equiv 0 \pmod{p},$$

where p is prime.

Theorem 5. ***State and prove converse of Wilson's theorem.***

Statement. *If* $(p-1)! \equiv -1 \pmod{p}$ *and* $p > 1$, *then* p *is a prime.*

Proof. If possible let p be not prime.

$\therefore$ p is composite ($\because p > 1$)

So let $p = p_1 p_2$ where

$$1 < p_1 < p,\ 1 < p_2 < p.$$

Or $\quad 1 < p_1 \le p-1,\ 1 < p_2 \le p-1$

Since $1 < p_1 \le p-1$, therefore, p_1 is one of the factors in the value of $(p-1)!$ and therefore, p_1 divides $(p-1)!$ ...(1)

Also $\quad p = p_1 p_2$ ...(2)

$\Rightarrow \quad p_1 \mid p$

But $(p-1)! \equiv -1 \pmod{p}$ (given) ...(3)

$\therefore \quad p \mid (p-1)! + 1$

From (2) and (3), we have

$$p_1 \mid (p-1)! + 1 \quad \ldots(4)$$

From (4) and (1), we have

$$p_1 \mid (p-1)! + 1 - (p-1)!$$

$\Rightarrow \quad p_1 \mid 1$

$\Rightarrow \quad p_1 = 1$

But this is not possible as $p_1 > 1$.

$\therefore$ p is a prime number.

Note

Wilson's theorem and its converse provide a necessary and sufficient condition for determining primality; namely an integer $n > 1$ is prime if and only if

$$(n-1)! \equiv -1 \pmod{n}.$$

However the characterization of prime numbers offered by Wilson's theorem is not of much practical value to test the primality of n, since there is no known fast method to calculate $n!$

Example 48. *Find the remainder when* 2 (26)! *is divided by* 29.

Solution. By Wilson's theorem,

$$(p-1)! \equiv -1 \pmod{p} \text{ if } p \text{ is prime number}$$

$\Rightarrow \quad (p-1)(p-2)(p-3)! \equiv -1 \pmod{p}$

$\Rightarrow \quad (p^2 - 3p + 2)(p-3)! \equiv -1 \pmod{p}$

$\Rightarrow \quad 2(p-3)! \equiv -1 \pmod{p}$

Taking $p = 29$, we get

$$2(29-3)! \equiv -1 \pmod{29}$$

$\Rightarrow \quad 2(26)! \equiv 28 \pmod{29}$ [$\because 28 \equiv -1 \pmod{29}$]

Therefore remainder is 28 when 2 (26)! is divided by 29.

Example 49. *Find the remainder when* 2 (28)! *is divided by* 31.

Solution. By Wilson's theorem, we have

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

Therefore,

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

$\therefore \quad 2(p-2)! \equiv 2 \pmod{p}$

Or $\quad 2(p-2)(p-3)! \equiv 2 \pmod{p}$

i.e $\quad 2(p-3)! \equiv -1 \pmod{p}$

Putting $p = 31$, we get

$$2(28)! \equiv -1 \pmod{31}$$

Or $\quad 2(28)! \equiv 30 \pmod{31}$

Hence the required remainder is 30.

Example 50. *If* p, n *be positive integers,* $p > 0, n > 0$, *show that* p *is prime if and only if* $(n-1)!(p-n)! \equiv (-1)^n \pmod{p}$.

Solution. We know that

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

and $\quad (n-1)! = (-1)^{n-k}(p-1)\ldots(p-n+1) \pmod{p}$

Then, from Wilson's theorem, we have

$$(n-1)!(p-n)! \equiv (-1)^{n-1}(p-1)!$$

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

Example 51. *Given a prime number p, prove that*
$(p-1)! \equiv (p-1) \pmod{1+2+3+\ldots\ldots+(p-1)}$

Solution. *Since p is prime number,* therefore by Wilson's theorem, we have

$$(p-1)! \equiv -1 \pmod p$$
$$\Rightarrow \quad (p-1)(p-2)! \equiv -1 \pmod p$$
$$\Rightarrow \quad (0-1)(p-2)! \equiv -1 \pmod p$$
$$\Rightarrow \quad (p-2)! \equiv 1 \pmod p$$
$$\Rightarrow \quad p \mid (p-2)! - 1$$
$$\Rightarrow \quad p \mid 2\,[(p-2)! - 1]$$
$$\Rightarrow \quad p(p-1) \mid 2(p-1)((p-2)! - 1)$$
$$\Rightarrow \quad \frac{p(p-1)}{2} \Big| (p-1)((p-2)! - 1)$$
$$\Rightarrow \quad \frac{p(p-1)}{2} \Big| (p-1)! - (p-1)$$
$$\Rightarrow \quad (p-1)! \equiv (p-1) \bmod \frac{p(p-1)}{2}$$
$$\Rightarrow \quad (p-1)! \equiv (p-1) \pmod{1+2+3+\ldots\ldots+(p-1)}$$

Example 52. *Prove that for any odd prime p,*

$$1^2 \cdot 3^2 \cdot 5^2 \ldots\ldots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$$

Solution. By Wilson's theorem, we have

$$(p-1)! \equiv -1 \pmod p$$
$$\Rightarrow \quad [(p-1)!]^2 \equiv 1 \pmod p$$
$$\Rightarrow \quad 1^2 \cdot 2^2 \cdot 3^2 \ldots\ldots (p-1)^2 \equiv 1 \pmod p$$
$$\Rightarrow \quad [1^2 \cdot 3^2 \ldots\ldots (p-2)^2][2^2 \cdot 4^2 \ldots\ldots (p-1)^2] \equiv 1 \pmod p \qquad \ldots(1)$$

But we know that

$$2^2 \cdot 4^2 \cdot 6^2 \ldots\ldots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$$

Therefore (1) becomes

$$1^2 \cdot 3^2 \cdot 5^2 \ldots\ldots (p-2)^2 (-1)^{\frac{p+1}{2}} \equiv 1 \pmod p$$
$$\Rightarrow \quad 1^2 \cdot 3^2 \cdot 5^2 \ldots\ldots (p-2)^2 (-1)^{p+1} \equiv (-1)^{\frac{p+1}{2}} \pmod p$$
$$\Rightarrow \quad 1^2 \cdot 3^2 \cdot 5^2 \ldots\ldots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$$

Example 53. *If p is an odd prime, show that*

$$2^2 \cdot 4^2 \cdot 6^2 \ldots\ldots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p.$$

Solution. By Wilson's theorem, we have

$$(p-1)! \equiv -1 \pmod p$$
$$\Rightarrow \quad \left(1 \cdot 2 \ldots\ldots j \ldots\ldots \frac{p-1}{2}\right)\left(\frac{p+1}{2} \cdot \frac{p+3}{2} \ldots\ldots (p-1)\right)$$
$$\equiv -1 \pmod p$$
$$\Rightarrow \quad \left(1 \cdot 2 \ldots\ldots j \ldots\ldots \frac{p-1}{2}\right)\left(\left(p - \frac{p-1}{2}\right)\left(p - \frac{p-3}{2}\right)\ldots\ldots (p-j) \ldots (p-1)\right)$$
$$\equiv -1 \pmod p$$
$$\Rightarrow \quad \prod_{j=1}^{\frac{p-1}{2}} j(p-j) \equiv -1 \pmod p$$
$$\Rightarrow \quad \prod_{j=1}^{\frac{p-1}{2}} (p_j - j^2) \equiv -1 \pmod p$$
$$\Rightarrow \quad \prod_{j=1}^{\frac{p-1}{2}} -j^2 \equiv -1 \pmod p$$
$$\Rightarrow \quad (-1)^{\frac{p-1}{2}} \prod_{j=1}^{\frac{p-1}{2}} j^2 \equiv -1 \pmod p$$
$$\Rightarrow \quad \prod_{j=1}^{\frac{p-1}{2}} j^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$$

$$\Rightarrow \quad 1^2 \cdot 2^2 \cdots \left(\frac{p-1}{2}\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p} \qquad \ldots(1)$$

Since p is an odd prime, therefore by Fermat's theorem, we have

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

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

$$\Rightarrow \quad 2^2 \cdot 2^2 \cdots \left(\frac{p-1}{2}\right) \text{times} \equiv 1 \pmod{p} \qquad \ldots(2)$$

From (1) and (2), we get

$$(1^2 \cdot 2^2)(2^2 \cdot 2^2) \cdots \left[\left(\frac{p-1}{2}\right)^2 \cdot 2^2\right] \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$$

Or $$2^2 \cdot 4^2 \cdots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$$

Example 54. *If p is an odd prime, show that*

$$1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} \equiv p + (p-1)\,! \pmod{p^2}$$

Solution. By Wilson's theorem, we have

$$(p-1)\,! + 1 \equiv 0 \pmod{p}$$

$$\Rightarrow \quad \frac{(p-1)\,! + 1}{p} \in Z$$

Let $$\frac{(p-1)\,! + 1}{p} \equiv r \pmod{p}$$

$$\Rightarrow \quad (p-1)\,! + 1 \equiv pr \pmod{p^2}$$

$$\Rightarrow \quad (p-1)\,! \equiv pr - 1 \pmod{p^2}$$

Also for $1 \le a \le p-1$, by Fermat's theorem, we have

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

$$\Rightarrow \quad \frac{a^{p-1} - 1}{p} \in Z$$

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

$$\Rightarrow \quad a^{p-1} \equiv p\, r_a + 1 \pmod{p^2} \qquad \ldots(3)$$

Now $$[(p-1)\,!]^{p-1} = 1^{p-1} \cdot 2^{p-1} \cdots (p-1)^{p-1}$$

$$\equiv (pr_1 + 1)(pr_2 + 1) \cdots (pr_{p-1} + 1) \pmod{p^2}$$

$$\equiv 1 + p(r_1 + r_2 + \ldots + r_{p-1}) \pmod{p^2} \qquad \text{[using (2)]}$$

From (1), we have $\ldots(3)$

$$[(p-1)\,!]^{p-1} \equiv (pr - 1)^{p-1} \pmod{p^2}$$

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

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

$$\equiv 1 + pr \pmod{p^2}$$

From (3) and (4), we have $\ldots(4)$

$$1 + p(r_1 + r_2 + \ldots + r_{p-1}) \equiv 1 + pr \pmod{p^2}$$

$$\Rightarrow \quad pr_1 + pr_2 + pr_3 + \ldots + pr_{p-1} \equiv pr \pmod{p^2}$$

$$\Rightarrow \quad (1^{p-1} - 1) + (2^{p-1} - 1) + \ldots + ((p-1)^{p-1} - 1)$$

$$\equiv (p-1)\,! + 1 \pmod{p^2} \qquad \text{[using (2) and (1)]}$$

$$\Rightarrow \quad 1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} \equiv p - 1 + (p-1)\,! + 1 \pmod{p^2}$$

$$\Rightarrow \quad 1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} \equiv p + (p-1)\,! \pmod{p^2}$$

Theorem 6. ***The quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$, where p is an odd prime, has a solution if and only if $p \equiv 1 \pmod{4}$.***

Or

Let p be an odd prime. The congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.

Or

If p is an odd prime, prove that the congruence $x^2 + 1 \equiv 0 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.

Proof. Suppose $x^2 \equiv -1 \pmod{p}$ has a solution, say a.

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

and $\gcd(a, p) = 1$.

Also $a^{p-1} \equiv 1 \pmod{p}$ by Fermat's theorem

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

Since p is odd, $\frac{p-1}{2}$ is an integer and $a^2 \equiv -1 \pmod p$

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

But last equation is true only when $\frac{p-1}{2}$ is even say

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

$\Rightarrow \quad p - 1 = 4k$

$\Rightarrow \quad p = 4k + 1$

$\Rightarrow \quad p \equiv 1 \pmod 4$

Conversely, suppose $p \equiv 1 \pmod 4$, then

$p = 4k + 1$ for some integers.

Now $(p-1)! \equiv -1 \pmod p$ by Wilson's theorem.

$\Rightarrow \quad 1 \cdot 2 \ldots\ldots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \frac{p+3}{2} \ldots\ldots (p-1) \equiv -1 \pmod p$ ....(1)

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

$\frac{p+3}{2} \equiv -\frac{p-3}{2} \pmod p$

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

Using this in (1), we have

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

$$\Rightarrow \quad (-1)^{2k} \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod p \qquad \left(\because \frac{p-1}{2} = 2k\right)$$

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

$\Rightarrow \quad \left(\frac{p-1}{2}\right)!$ is a solution of $x^2 \equiv -1 \pmod p$.

Theorem 7. ***Let p be an odd prime with p ≡ 3 (mod 4).***

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

Proof. Since $-1 \equiv (p-1)!$

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

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

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

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

Example 55. *If p is prime, show that* $2(p-3)! + 1$ *is a multiple of p.*

Solution. Since p is prime, by Wilson's theorem, we have

$(p-1)! + 1 \equiv 0 \pmod p$

$\Rightarrow \quad (p-1)(p-2)(p-3)! + 1 \equiv 0 \pmod p$

$\Rightarrow \quad (p^2 - 3p + 2)(p-3)! + 1 \equiv 0 \pmod p$

$\Rightarrow \quad 2(p-3)! + 1 + (p^2 - 3p)(p-3)! \equiv 0 \pmod p$

$\Rightarrow \quad 2(p-3)! + 1 + p(p-3)(p-3)! \equiv 0 \pmod p$

$\Rightarrow \quad 2(p-3)! + 1 \equiv 0 \pmod p$

$[\because \quad p(p-3)(p-3)! \equiv 0 \pmod p]$

Example 56. *Apply Wilson's theorem to show that*
$18! + 1 \equiv 0 \pmod{19}$
Or $18! \equiv -1 \pmod{19}$

Solution. Since 19 is prime, therefore by Wilson's theorem, we have
$(19-1)! + 1 \equiv 0 \pmod{19}$
$\Rightarrow \quad 18! + 1 \equiv 0 \pmod{19}$.

Example 57. *Apply Wilson's theorem to show that*
$18! + 1 \equiv 0 \pmod{23}$

Solution. Since 23 is prime, therefore by Wilson's theorem, we have
$(23-1)! + 1 \equiv 0 \pmod{23}$
$\Rightarrow \quad 22! + 1 \equiv 0 \pmod{23}$
$\Rightarrow \quad 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18! + 1 \equiv 0 \pmod{23}$
$\Rightarrow \quad (23-1)(23-2)(23-3)(23-4) \cdot 18! + 1 \equiv 0 \pmod{23}$
$\Rightarrow \quad (-1)(-2)(-3)(-4) \cdot 18! + 1 \equiv 0 \pmod{23}$
$\Rightarrow \quad 24 \cdot 18! + 1 \equiv 0 \pmod{23}$
$\Rightarrow \quad (23+1) \cdot 18! + 1 \equiv 0 \pmod{23}$
$\Rightarrow \quad 23 \cdot 18! + 18! + 1 \equiv 0 \pmod{23}$
$\Rightarrow \quad 18! + 1 \equiv 0 \pmod{23}$.

Example 58. *Apply Wilson's theorem to show that*
$18! + 1 = 0 \pmod{437}$.

Or

Show that $\underline{|18} \equiv -1 \pmod{437}$.

Solution. Since
$18! + 1 \equiv 0 \pmod{19}$
and $18! + 1 \equiv 0 \pmod{23}$
$\Rightarrow \quad 18! + 1 \equiv 0 \pmod{\text{L.C.M. of 19 and 23}}$
$\Rightarrow \quad 18! + 1 \equiv 0 \pmod{19 \times 23}$
$\Rightarrow \quad 18! + 1 \equiv 0 \pmod{437}$.

Example 59. *Apply Wilson's theorem to show that*
(i) $10! - 32 \equiv 0 \pmod{11}$
(ii) $10! - 32 \equiv 0 \pmod{13}$
Then show that $10! - 32 \equiv 0 \pmod{143}$.

Solution. Since 11 is prime, therefore by Wilson's theorem, we have
$(11-1)! + 1 \equiv 0 \pmod{11}$
$\Rightarrow \quad 10! + 1 \equiv 0 \pmod{11}$
$\Rightarrow \quad 10! + 1 - 33 \equiv 0 \pmod{11}$
$\Rightarrow \quad 10! - 32 \equiv 0 \pmod{11}$.

Again 13 is prime, therefore by Wilson's theorem, we have
$12! + 1 \equiv 0 \pmod{13}$
$\Rightarrow \quad 12 \cdot 11 \cdot 10! + 1 \equiv 0 \pmod{13}$
$\Rightarrow \quad (13-1)(13-2)\,10! + 1 \equiv 0 \pmod{13}$
$\Rightarrow \quad (-1)(-2) \cdot 10! + 1 \equiv 0 \pmod{13}$
$\Rightarrow \quad 2(10!) + 1 \equiv 0 \pmod{13}$
$\Rightarrow \quad 2(10!) - 65 + 1 \equiv 0 \pmod{13}$
$\Rightarrow \quad 2(10!) - 64 \equiv 0 \pmod{13}$
$\Rightarrow \quad 10! - 32 \equiv 0 \pmod{13}$
$[\because gcd(2, 13) = 1]$

Now $10! - 32 \equiv 0 \pmod{11}$ and
$10! - 32 \equiv 0 \pmod{13}$
$\Rightarrow \quad 10! - 32 \equiv 0 \pmod{\text{L.C.M. of 13 and 11}}$
$\Rightarrow \quad 10! - 32 \equiv 0 \pmod{143}$.

Example 60. *Show that* $16! + 86$ *is divisible by* 323.

Solution. We have $323 = 17 \times 19$ where both 17 and 19 are primes.

Since 17 is a prime, therefore by Wilson's theorem
$(17-1)! + 1 \equiv 0 \pmod{17}$
$\Rightarrow \quad 16! + 86 - 85 \equiv 0 \pmod{17}$

$\Rightarrow \quad 16! + 86 \equiv 0 \pmod{17}$ ...(1)

$[\because 85 \equiv 0 \pmod{17}]$

Again 19 is a prime, so by Wilson's theorem

$(19-1)! + 1 \equiv 0 \pmod{19}$

$\Rightarrow \quad 18! + 1 \equiv 0 \pmod{19}$

$\Rightarrow \quad [(19-1)(19-2)] \cdot 16! + 1 \equiv 0 \pmod{19}$

$\Rightarrow \quad (19^2 - 3 \times 19 + 2) \cdot 16! + 1 \equiv 0 \pmod{19}$

$\Rightarrow \quad (19^2 - 3 \times 19) \cdot 16! + 2(16!) + 1 = 0 \pmod{19}$

$\Rightarrow \quad 2(16!) + 1 \equiv 0 \pmod{19}$ ...(2)

$[\because (19^2 - 3 \times 19) \cdot 16! \equiv 0 \pmod{19}]$

Also $171 \equiv 0 \pmod{19}$ ...(3)

Adding the congruences (2) and (3), we have

$2(16!) + 172 \equiv 0 \pmod{19}$

$\Rightarrow \quad 16! + 86 \equiv 0 \pmod{19}$, ...(4)

Cancelling 2 because $gcd\,(2, 19) = 1$.

Thus from (1) and (4), we have

$16! + 86 \equiv 0 \pmod{17}$ and

$16! + 86 \equiv 0 \pmod{19}$

$\Rightarrow \quad 16! + 86 \equiv 0 \pmod{\text{L.C.M. of 17 and 19}}$

$\Rightarrow \quad 16! + 86 \equiv 0 \pmod{17 \times 19}$

$\Rightarrow \quad 16! + 86 \equiv 0 \pmod{323}$.

Example 61. *If p is an odd prime and $gcd\,(a, p) = 1$, then prove either*

$a^{(p-1)/2} \equiv 1 \pmod{p}$ *or* $a^{(p-1)/2} \equiv -1 \pmod{p}$.

Solution. Since p is odd, therefore $p - 1$ is even and so $\left(\frac{p-1}{2}\right)$ is a positive integer.

Now $a^{p-1} - 1 = [a^{(p-1)/2}]^2 - 1^2$

$= [a^{(p-1)/2} - 1][a^{(p-1)/2} + 1]$ ...(1)

Since p is prime and $gcd\,(a, p) = 1$, therefore by Fermat's theorem, we have

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

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

$\Rightarrow \quad p \mid [a^{(p-1)/2} - 1][a^{(p-1)/2} + 1]$ by (1)

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

Or $\quad p \mid [a^{(p-1)/2} + 1]$

$[\because p$ is prime and so $p \mid ab \Rightarrow p \mid a$ or $p \mid b]$

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

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

Example 62. *Prove that* $28! + 233 \equiv 0 \pmod{899}$.

Solution. We have $899 = 29 \times 31$, where both 29 and 31 are prime.

Since 29 is prime, therefore by Wilson's theorem, we have

$(29-1)! + 1 \equiv 0 \pmod{29}$

$\Rightarrow \quad 28! + 1 \equiv 0 \pmod{29}$

$\Rightarrow \quad 28! + 1 + 8 \cdot 29 \equiv 0 \pmod{29}$

$\Rightarrow \quad 28! + 1 + 232 \equiv 0 \pmod{29}$

$\Rightarrow \quad 28! + 233 \equiv 0 \pmod{29}$

Again 31 is prime, therefore by Wilson's theorem, we have

$(31-1)! + 1 \equiv 0 \pmod{31}$

$\Rightarrow \quad 30! + 1 \equiv 0 \pmod{31}$

$\Rightarrow \quad 30 \cdot 29 \cdot 28! + 1 \equiv 0 \pmod{31}$

$\Rightarrow \quad (31-1)(31-2) \cdot 28! + 1 \equiv 0 \pmod{31}$

$\Rightarrow \quad (-1)(-2) \cdot 28! + 1 \equiv 0 \pmod{31}$

$\Rightarrow \quad 2 \cdot 28! + 1 \equiv 0 \pmod{31}$

$\Rightarrow \quad 2 \cdot 28! + 31 \cdot 15 + 1 \equiv 0 \pmod{31}$

$\Rightarrow \quad 2 \cdot 28! + 465 + 1 \equiv 0 \pmod{31}$

$\Rightarrow \quad 2 \cdot 28! + 466 \equiv 0 \pmod{31}$

$\Rightarrow \quad 28! + 233 \equiv 0 \pmod{31}$

[$\because$ gcd (2, 31) = 1]

Now $28! + 233 \equiv 0 \pmod{29}$

and $28! + 233 \equiv 0 \pmod{31}$

$\Rightarrow$ $28! + 233 \equiv 0 \pmod{\text{L.C.M. of 29 and 31}}$

$\Rightarrow$ $28! + 233 \equiv 0 \pmod{899}$.

Example 63. *If p is prime, prove that $a^p (p-1)! + a$ is divisible by p.*

Solution. Since p is prime,

therefore by Wilson's theorem.

$$(p-1)! \equiv -1 \pmod{p} \quad \text{...(1)}$$

Again since p is prime,

$$\therefore \quad a^p \equiv a \pmod{p} \quad \text{...(2)}$$

Multiplying congruences (1) and (2), we have

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

$\therefore$ $a^p (p-1)! + a$ is divisible by p.

Example 64. *If p is prime show that $2(p-3)! + 1$ is a multiple of p.*

Solution. By Wilson's theorem, $(p-1)! + 1 \equiv 0 \pmod{p}$ where p is prime.

i.e $1 + (p-1)(p-2)(p-3)! \equiv 0 \pmod{p}$

Or $1 + (p^2 - 3p + 2)(p-3)! \equiv 0 \pmod{p}$

Or $1 + (p^2 - 3p)(p-3)! + 2(p-3)! \equiv 0 \pmod{p}$ ...(1)

Or $1 + p(p-3)(p-3)! + 2(p-3)! \equiv 0 \pmod{p}$

But $p(p-3)(p-3)!$ is divisible by p. ...(2)

i.e $p(p-3)(p-3)! \equiv 0 \pmod{p}$

From (1) and (2), we get

$$1 + 2(p-3)! \equiv 0 \pmod{p}$$

i.e $1 + 2(p-3)!$ is a multiple of p.

❑❑❑

CHAPTER 5

NUMBER-THEORETIC FUNCTIONS

THE FUNCTIONS τ AND σ

Definition. *For each positive integer n, let $\tau(n)$ denote the number of positive divisors of n and $\sigma(n)$ denote the sum of these divisors i.e. $\tau : N \to N$ and $\sigma : N \to N$ are functions defined respectively as*

$$\tau(n) = \sum_{\substack{d \mid n \\ d \geq 1}} 1$$

$$\sigma(n) = \sum_{\substack{d \mid n \\ d \geq 1}} d$$

Note

The notation, $\sum_{d \mid n} 1$, in particular says that we are to add together as many 1's as there are positive divisors of n.

Illustration 1. The integer 10 has the four positive divisors 1, 2, 5, 10, whence

$$\tau(10) = \sum_{d \mid 10} 1 = 1 + 1 + 1 + 1 = 4$$

and $$\sigma(10) = \sum_{d \mid 10} d$$

$$= 1 + 2 + 5 + 10 = 18.$$

Illustration 2. Let $n = 5$. Then

$$\tau(5) = 2 \text{ and } \sigma(5) = 1 + 5 = 6.$$

In fact we have

$\tau(n) = 2 \Leftrightarrow n$ is a prime

and $\sigma(n) = n + 1 \Rightarrow n$ is a prime

Illustration 3. Let $n = 12$.

Since 12 has the positive divisors 1, 2, 3, 4, 6, 12,

$\therefore$ we have

$\tau(12) = 6$ and

$\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28.$

For the first few integers,

$\tau(1) = 1, \tau(2) = 2, \tau(3) = 2,$

$\tau(4) = 3, \tau(5) = 2$ and

$\tau(6) = 4$ and so on.

and $\sigma(1) = 1, \sigma(2) = 1 + 2 = 3,$

$\sigma(3) = 1 + 3 = 4, \sigma(4) = 1 + 2 + 4 = 7, \sigma(5) = 1 + 5 = 6$

and $\sigma(6) = 1 + 2 + 3 + 6 = 12.$

Note

We interpret the symbol $\sum_{d \mid n} f(d)$

as "sum the values $f(d)$ as d runs over all the positive divisors of the positive integer n".

e.g. $\sum_{d \mid 20} f(d) = f(1) + f(2) + f(4) + f(5) + f(10) + f(20)$

Theorem 1. ***If $n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}$ is the prime factorization of $n > 1$, then the positive divisors of n are precisely those integers d of the form***

$$d = p_1^{a_1} p_2^{a_2} \ldots\ldots p_r^{a_r}$$

where $0 \le a_i \le k_i$ $(i = 1, 2, \ldots\ldots, r)$.

Proof. Since $d = 1$ when

$a_1 = a_2 = \ldots\ldots = a_r = 0,$

n itself occurs when $a_1 = k_1$,

$a_2 = k_2, \ldots\ldots, a_r = k_r$.

Suppose that d divides n nontrivially, say

$n = dd'$, where $d > 1, d' > 1$.

Let us express both d and d' as product of (not necessarily distinct) primes :

$d = q_1 q_2 \ldots\ldots q_s,$

$d' = t_1 t_2 \ldots\ldots t_u$

with q_i, t_j prime.

Then $p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r} = q_1 q_2 \ldots\ldots q_s t_1 t_2 \ldots\ldots t_u$ are two prime factorizations of the positive integer n.

By the uniqueness of the prime factorization, each prime q_i must be one of the p_j.

Collecting the equal primes into a single integral power, we get

$$d = q_1 q_2 \ldots\ldots q_s = p_1^{a_1} p_2^{a_2} \ldots\ldots p_r^{a_r}$$

where the possibility that $a_i = 0$ is allowed.

Conversely, every number

$$d = p_1^{a_1} p_2^{a_2} \ldots\ldots p_r^{a_r} \quad (0 \le a_i \le k_i)$$ is a divisor of n.

Thus we can write

$$n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}$$

$$= (p_1^{a_1} p_2^{a_2} \ldots\ldots p_r^{a_r})(p_1^{k_1 - a_1} p_2^{k_2 - a_2} \ldots\ldots p_r^{k_r - a_r})$$

$$= dd'$$

with $d' = p_1^{k_1 - a_1} p_2^{k_2 - a_2} \ldots\ldots p_r^{k_r - a_r}$ with

$k_i - a_i \ge 0 \ \forall\ i.$

Then $d' > 0$ and $d \mid n$.

Theorem 2. ***If $n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}$ is the prime factorization of $n > 1$, then***

(i) $\tau(n) = (k_1 + 1)(k_2 + 1) \ldots\ldots (k_r + 1)$ *and*

(ii) $\sigma(n) = \dfrac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \dfrac{p_2^{k_2+1} - 1}{p_2 - 1} \ldots\ldots \dfrac{p_r^{k_r+1} - 1}{p_r - 1}$.

Proof. We prove both the parts by induction on r, the number of distinct prime divisors of n and shall be given simultaneously.

Therefore let $r = 1$

i.e n has only one prime divisor say p.

Then $n = p^k$ for some integer k.

The positive divisors of n are $1, p, p^2, \ldots\ldots, p^k$, $k+1$ in number.

Hence $\tau(n) = k+1$; and

$$\sigma(n) = 1 + p + p^2 + \ldots\ldots + p^k$$

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

[$\because 1 + p + p^2 + \ldots\ldots + p^k$ is a G.P. series with $a = 1$ and $r = p > 1$ and $n = k + 1$

$$\therefore \quad S_n = \frac{a(r^n - 1)}{r - 1} = \frac{1(p^{k+1} - 1)}{p - 1} = \frac{p^{k+1} - 1}{p - 1}$$]

Further, suppose that the results (i) and (ii) hold when an integer has $r-1, r \geq 1$ distinct prime factors; and that $n (> 1)$ is an integer with r distinct prime factors *i.e.*

$n = p_1^{k_1} p_2^{k_2} \ldots\ldots\ldots\ldots p_r^{k_r}$, p_i are distinct primes and integers $k_i \geq 1$.

Let $\quad n' = p_1^{k_1} p_2^{k_2} \ldots\ldots p_{r-1}^{k_{r-1}}$.

Then $\quad n = n' p_r^{k_r}$;

since p_i are distinct primes,

$$gcd(n', p_r^{k_r}) = 1.$$

Also any divisor of n' is a divisor of n_i so any divisor of n is of the form

$$d' p_r^s, \; 0 \leq s \leq k_i, \; 1 \leq d', \; d' \mid n'.$$

$$\therefore \quad \tau(n) = \sum_{\substack{d \mid n \\ d \geq 1}} 1$$

$$= \sum_{d' \mid n'} 1 + \sum_{d' p_r \mid n'} 1 + \sum_{d' p_r^2 \mid n'} 1 + \ldots\ldots\ldots + \sum_{d' p_r^{k_r} \mid n'} 1$$

$$= \tau(n') + \tau(n') + \ldots\ldots + \tau(n'), \; k_r + 1 \text{ summands}$$

$$= \tau(n')(k_r + 1)$$

By induction hypothesis

$$\tau(n') = (k_1 + 1) \ldots\ldots (k_{r-1} + 1)$$

$$\tau(n) = (k_1 + 1) \ldots\ldots (k_r + 1).$$

$\therefore$ Also $\quad \sigma(n) = \sum_{\substack{d \mid n \\ d \geq 1}} d$

$$= \sum_{d' \mid n'} d' + \sum_{d' \mid n'} d' p_r + \ldots\ldots + \sum_{\substack{d' \mid n' \\ d' \geq 1}} d' p_r^{k_r}$$

$$= \left(\sum_{\substack{d' \mid n' \\ d' \geq 1}} d' \right) + \left(\sum_{\substack{d' \mid n' \\ d' \geq 1}} d' \right) p_r + \ldots\ldots + \left(\sum_{\substack{d' \mid n' \\ d' \geq 1}} d' \right) p_r^{k_r}$$

$$= \left(\sum_{\substack{d' \mid n' \\ d' \geq 1}} d' \right) (1 + p_r + \ldots\ldots + p_r^{k_r})$$

$$= \sigma(n') \frac{(p_r^{k_r+1} - 1)}{p_r - 1}$$

[$\because 1 + p_r + \ldots\ldots + p_r^{k_r}$ is a G.P. series with $a = 1, r = p_r > 1$ and $n = k_r + 1$ so

$$S_n = \frac{a(r^n - 1)}{r - 1} = \frac{1(p_r^{k_r+1} - 1)}{p_r - 1} = \frac{p_r^{k_r+1} - 1}{p_r - 1}$$]

By induction hypothesis

$$\sigma(n') = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdot \ldots\ldots \cdot \frac{p_{k-1}^{k_{r-1}+1} - 1}{p_{r-1} - 1}.$$

Hence $\quad \sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdot \ldots\ldots \cdot \frac{p_r^{k_r+1} - 1}{p_r - 1}$.

Illustration 4. The number $180 = 2^2 \cdot 3^2 \cdot 5$ has $\tau(180) = (2+1)(2+1)(1+1) = 18$ positive divisors.

These are integers of the form

$$2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3}$$

where $a_1 = 0, 1, 2,$

$a_2 = 0, 1, 2$ and

$a_3 = 0, 1.$

Thus we get

1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180.

The sum of integers is

$$\sigma(180) = \frac{2^3-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{5^2-1}{5-1}$$

$$= \frac{7}{1} \cdot \frac{26}{2} \cdot \frac{24}{4}$$

$$= 7 \cdot 13 \cdot 6$$

$$= 546$$

Theorem 3. ***Prove that*** $\prod_{d \mid n} d = n^{\tau(n) \mid 2}$ ***where n is an integer*** > 1.

Proof. We know that if d is an integer such that $d \mid n$, then there exists an integer d' such that $n = dd'$

$\Rightarrow$ $d' \mid n$ and $d' = \frac{n}{d}$.

Thus divisor d of n are in pairs $\left(d, \frac{n}{d}\right)$

$\Rightarrow$ Product of all divisors of

$$n = \left(\prod_{d \mid n} d\right)^2 = n^{\tau(n)}$$

Or $\prod_{d \mid n} d = n^{\tau(n) \mid 2}$,

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 $n^{\tau(n) \mid 2}$ is an integer and if $\tau(n)$ is odd, n is a perfect sqaure, so that $n^{\tau(n) \mid 2} = (n^{1/2})^{\tau(n)}$ is again an integer.

Thus $\prod_{d \mid n} d = n^{\tau(n) \mid 2}$

MULTIPLICATIVE FUNCTION

Definition. *A number-theoretic function f is said to be* ***multiplicative*** *if $f(m \cdot n) = f(m) f(n)$ whenever $\gcd(m, n) = 1$.*

Note

1. Multiplicative functions completely determined once their values at prime powers are known. In fact, if $n > 1$ is a given positive integer, then we can write $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ in canonical form because the $p_i^{k_i}$ are relatively prime in pairs, the multiplicative ensures that $f(n) = f(p_1^{k_1}) f(p_2^{k_2}) \ldots f(p_r^{k_r})$.
2. If f is a multiplicative function that does not vanish identically then there exists an integer n such that $f(n) \neq 0$

But $f(n) = f(n \cdot 1) = f(n) f(1)$ being non-zero.

Or $f(1) = 1$ [Cancelling both sides by $f(n)$]

Thus $f(1) = 1$ for any multiplicative function not identically zero.

Theorem 4. Prove that $\tau(n)$ ***is multiplicative function.***

Or

Show that the function is multiplicative function where $\tau(n)$ ***denotes the number of positive divisors.***

Proof. Let a and b be two coprime positive integers.

To prove that $\tau(ab) = \tau(a)\, \tau(b)$.

If $a = 1, b = 1$, then

$ab = 1$

Therefore

$\tau(a) = \tau(1) = 1,$

$\tau(b) = \tau(1) = 1$

and $\tau(ab) = \tau(1) = 1$

$\Rightarrow$ $\tau(a) = \tau(b) = \tau(ab) = 1$

Also $\tau(a)\, \tau(b) = 1 \cdot 1 = 1$

which shows that

$\tau(ab) = \tau(a)\, \tau(b)$

If $a = 1$ and $b \neq 1$, then $ab = b$

$\Rightarrow$ $\tau(ab) = \tau(b)$

$\Rightarrow \quad \tau(ab) = 1 \cdot \tau(b) \qquad [\because a = 1 \Rightarrow \tau(a) = \tau(1) = 1]$

$\Rightarrow \quad \tau(ab) = \tau(a)\,\tau(b)$

Similarly if $a \neq 1$ and $b = 1$,

then $\tau(ab) = \tau(a)\,\tau(b)$.

If $a \neq 1$ and $b \neq 1$, then $a > 1$ and $b > 1$ so that

$a = p_1^{a_1} p_2^{a_2} \ldots\ldots p_r^{a_r}$ and

$b = q_1^{b_1} q_2^{b_2} \ldots\ldots q_s^{b_s}$

where $p_1, p_2, \ldots\ldots, p_r ; q_1, q_2, \ldots\ldots, q_s$ are distinct primes.

$\therefore \quad ab = p_1^{a_1} p_2^{a_2} \ldots\ldots p_r^{a_r} q_1^{b_1} q_2^{b_2} \ldots\ldots q_s^{b_s}$

$\Rightarrow \quad \tau(ab) = (a_1 + 1)(a_2 + 1) \ldots\ldots (a_r + 1)(b_1 + 1)(b_2 + 1) \ldots\ldots (b_s + 1)$

$= [(a_1 + 1)(a_2 + 1) \ldots\ldots (a_r + 1)] \cdot [(b_1 + 1)(b_2 + 1) \ldots\ldots (b_s + 1)]$

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

Hence in each case,

$\tau(ab) = \tau(a)\,\tau(b)$

which shows that $\tau(n)$ is multiplicative function.

Theorem 5. Prove that $\sigma(n)$ is multiplicative function.

Proof. Let a and b be two coprime positive integers.

If $a = 1$ and $b = 1$, then $ab = 1$.

Therefore

$\sigma(a) = \sigma(1) = 1,$

$\sigma(b) = \sigma(1) = 1$

and $\sigma(ab) = \sigma(1) = 1$

$\therefore \quad \sigma(a) = \sigma(b) = \sigma(ab) = 1$

Also $\sigma(a)\,\sigma(b) = 1 \cdot 1 = 1 = \sigma(ab)$

which shows that

$\sigma(ab) = \sigma(a)\,\sigma(b).$

If $a = 1$ and $b \neq 1$, then

$\sigma(ab) = \sigma(b).$

$\Rightarrow \quad \sigma(ab) = 1 \cdot \sigma(b)$

$\Rightarrow \quad \sigma(ab) = \sigma(a)\,\sigma(b) \qquad [\because \sigma(a) = \sigma(1) = 1]$

Similarly if $a \neq 1$ and $b = 1$, then

$\sigma(ab) = \sigma(a)\,\sigma(b).$

If $a \neq 1$ and $b \neq 1$, then $a > 1$ and $b > 1$ so that

$a = p_1^{a_1} p_2^{a_2} \ldots\ldots p_r^{a_r}$ and

$b = q_1^{b_1} q_2^{b_2} \ldots\ldots q_s^{b_s}$

where $p_1, p_2, \ldots\ldots, p_r ; q_1, q_2, \ldots\ldots, q_s$ are distinct primes.

Therefore

$ab = p_1^{a_1} p_2^{a_2} \ldots\ldots p_r^{a_r} q_1^{b_1} q_2^{b_2} \ldots\ldots q_s^{b_s}$

$$\Rightarrow \quad \sigma(ab) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdot \ldots\ldots \cdot \frac{p_r^{a_r+1} - 1}{p_r - 1} \cdot \frac{q_1^{b_1+1} - 1}{q_1 - 1} \cdot \frac{q_2^{b_2+1} - 1}{q_2 - 1} \cdot \ldots\ldots \cdot \frac{q_s^{b_s+1} - 1}{q_s - 1}$$

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

Hence in each case,

$\sigma(ab) = \sigma(a)\,\sigma(b)$

which shows that $\sigma(n)$ is multiplicative function.

Lemma

If $\gcd(m, n) = 1$, then the set of positive divisors of mn consists of all products $d_1 d_2$, where $d_1 \mid m$, $d_2 \mid n$ and $\gcd(d_1, d_2) = 1$; furthermore, these products are all distinct.

Proof. Let us assume that $m > 1$ and $n > 1$.

Let $m = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}$ and $n = q_1^{j_1} q_2^{j_2} \ldots\ldots q_s^{j_s}$ be their respective prime factorization, where the primes $p_1, \ldots\ldots, p_r, q_1, \ldots\ldots, q_s$ are all distinct.

The prime factorization of mn is

$mn = p_1^{k_1} \ldots\ldots p_r^{k_r} q_1^{j_1} \ldots\ldots q_s^{j_s}.$

Hence, any positive divisor d of mn will be uniquely expressed in the form

$d = p_1^{a_1} p_2^{a_2} \ldots\ldots p_r^{a_r} q_1^{b_1} \ldots\ldots q_s^{b_s} ; 0 \leq a_i \leq k_i, 0 \leq b_i \leq j_i$

Thus we can write $d = d_1 d_2$,

where $d_1 = p_1^{a_1} \ldots\ldots p_r^{a_r}$ divides m and $d_2 = q_1^{b_1} \ldots\ldots q_s^{b_s}$ divides n.

Since no p_i is equal to any q_j,

so we must have

$$gcd\,(d_1, d_2) = 1.$$

Hence the Proof.

Theorem 6. ***If f is a multiplicative function and F is defined by*** $F(n) = \sum_{d \mid n} f(d)$, ***then F is also multiplicative.***

Proof. Let m and n be relatively prime positive integers *i.e.*

$$gcd\,(m, n) = 1.$$

Then m and n have canonical representations

$$n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r},$$

$$m = q_1^{j_1} q_2^{j_2} \ldots\ldots q_s^{j_s},$$

where k_r and j_s are positive exponents and $p_1, p_2, \ldots\ldots, p_r$ and $q_1, q_2, \ldots\ldots, q_j$ are all distinct primes.

In fact the positive divisors d_1 of n are just the numbers

$$d_1 = p_1^{g_1} p_2^{g_2} \ldots\ldots p_r^{g_r}$$

for all possible selections of g's, $0 \le g_l \le k_l$.

Similarly all the positive divisors d_2 of m are given by

$$d_2 = q_1^{h_1} q_2^{h_2} \ldots\ldots q_s^{h_s}, 0 \le h_l \le j_l.$$

Now we observe that d_1 runs through all positive divisors of n and d_2 runs through all positive divisors of m, and hence their product mn runs through the values

$$d = d_1 d_2 = p_1^{g_1} p_2^{g_2} \ldots\ldots p_r^{g_r} q_1^{h_1} q_2^{h_2} \ldots\ldots q_s^{h_s}, 0 \le g_l \le k_l, 0 \le h_l \le j_l.$$

But these are just all the positive divisors of

$$mn = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r} q_1^{j_1} q_2^{j_2} \ldots\ldots q_s^{j_s}.$$

Equivalently,

$$\sum_{d_1 \mid n} \sum_{d_2 \mid m} f(d_1 d_2) = \sum_{d \mid mn} f(d).$$

Clearly $gcd\,(d_1, d_2) = 1$.

Hence $F(mn) = \sum_{d \mid mn} f(d)$

$$= \sum_{d_1 \mid n} \sum_{d_2 \mid m} f(d_1 d_2)$$

$$= \sum_{d_1 \mid n} \sum_{d_2 \mid m} f(d_1) f(d_2)$$

$$= \sum_{d_1 \mid n} f(d_1) \sum_{d_2 \mid m} f(d_2)$$

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

Hence the Proof.

Alternative Proof

In order to get the required result we first state and prove the following lemma.

Statement of lemma

If $(m, n) = 1$ and $d \mid mn$ then $d = d_1 d_2$ such that

$$d_1 \mid m, d_2 \mid n \text{ and } (d_1, d_2) = 1.$$

Proof of lemma

For $m = 1$ and $n = 1$, there is nothing to prove.

Therefore let $m > 1$ and $n > 1$

Let $m = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}$ and

$$n = q_1^{j_1} q_2^{j_2} \ldots\ldots q_s^{j_s}$$

be the prime factorization of m and n.

Since $(m, n) = 1$,

therefore, all p_i's are different from q_j's and hence prime factorization of mn is given by

$$mn = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r} q_1^{j_1} q_2^{j_2} \ldots\ldots q_s^{j_s}$$

Hence any positive divisor d of mn is uniquely expressed as

$$d = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \ldots\ldots q_s^{\beta_s}$$

where $0 \le \alpha_i \le k_i$; $0 \le \beta_i \le j_i$

Therefore $d = d_1 d_2$ where

$d_1 = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$ divides m

and $d_2 = q_1^{\beta_1} q_2^{\beta_2} \ldots\ldots q_s^{\beta_s}$ divides n

Since no p_i is equal to any q_j,

therefore $(d_1, d_2) = 1$

Proof of main theorem

Let $(m, n) = 1$

Then $$F(mn) = \sum_{d \mid mn} f(d)$$

$$= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1 d_2)$$

Since $d \mid mn$ and $d = d_1 d_2$ where $d_1 \mid m$, $d_2 \mid n$, therefore

$$(d_1, d_2) = 1$$

$$\Rightarrow \quad f(d_1 d_2) = f(d_1) f(d_2) \qquad (\because\ f \text{ is multiplicative})$$

$$\therefore \quad F(mn) = \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1) f(d_2)$$

$$= \left(\sum_{d_1 \mid m} f(d_1) \right) \left(\sum_{d_2 \mid n} f(d_2) \right)$$

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

Hence F is multiplicative function.

Note

Illustration 5. Let $m = 8$ and $n = 3$, we have

$$F(8 \cdot 3) = \sum_{d \mid 24} f(d)$$

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

$$= f(1 \cdot 1) + f(2 \cdot 1) + f(1 \cdot 3) + f(4 \cdot 1) + f(2 \cdot 3) + f(8 \cdot 1) + f(4 \cdot 3) + f(8 \cdot 3)$$

$$= f(1) f(1) + f(2) f(1) + f(1) f(3) + f(4) f(1) +$$
$$f(2) f(3) + f(8) f(1) + f(4) f(3) + f(8) f(3)$$

$$= [f(1) + f(2) + f(4) + f(8)]\,[f(1) + f(3)]$$

$$= \sum_{d \mid 8} f(d) \cdot \sum_{d \mid 3} f(d)$$

$$= F(8)\, F(3).$$

Corollary. *Prove that the fiunctions* τ *and* σ *are multiplicative function.*

Proof. We know that the constant function $f(n) = 1$ is multiplicative, as is the identity function $f(n) = n$.

Then by the theorem, "If f is multiplicative function and F is defined by $F(n) = \sum_{d \mid n} f(a)$ then F is also multiplicative" and from the definition, we have

$$\tau(n) = \sum_{d \mid n} 1 \quad \text{and}$$

$$\sigma(n) = \sum_{d \mid n} d$$

Thus the result follows from the above quoted theorem.

Theorem 7. ***Let n be an integer > 1. Then*** $\tau(n)$ ***is an odd integer if and only if n is a perfect square.***

Or

Number of positive divisors of a number is odd if and only if the number is perfect square.

Proof. Let number of divisors of n be odd and

$$n = p_1^{a_1} p_2^{a_2} \ldots\ldots p_r^{a_r}$$

where p_i's are distinct primes.

Since $\tau(n)$ = odd number

$\Rightarrow$ $(a_1 + 1)(a_2 + 1) \ldots\ldots (a_r + 1)$ = odd number

$\Rightarrow$ $a_1 + 1$ = odd number,

$a_2 + 1$ = odd number,

$a_r + 1$ = odd number

$\Rightarrow$ a_1 = even number

a_2 = even number,

---

a_r = even number say,

$a_1 = 2k_1$,

$a_2 = 2k_2$,

$a_r = 2k_r$

$\therefore \quad n = p_1^{2k_1} p_2^{2k_2} \ldots\ldots p_r^{2k_r}$

$= (p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r})^2$

$\Rightarrow$ n is a perfect square.

Conversely, let n be a perfect square, say, $n = m^2$.

Since $n > 1$

$\therefore \quad m > 1$

Let $m = q_1^{b_1} q_2^{b_2} \ldots\ldots q_s^{b_s}$ where q_i's are distinct primes

$\therefore \quad n = (q_1^{b_1} q_2^{b_2} \ldots\ldots q_s^{b_s})^2$

$= q_1^{2b_1} q_2^{2b_2} \ldots\ldots q_s^{2b_s}$

$\Rightarrow \quad \tau(n) = (2b_1 + 1)(2b_2 + 1) \ldots\ldots (2b_s + 1)$

= (odd number) (odd number) ..... (odd number)

= odd number

$\Rightarrow$ Number of positive divisors of n is odd.

Theorem 8. ***Let n be an integer > 1. Then σ (n) is odd if and only if n is a perfect square or twice a perfect square.***

Proof. Since we know that

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \ldots\ldots \frac{p_r^{k_r+1} - 1}{p_r - 1}$$

$$= (1 + p_1 + \ldots\ldots + p_1^{k_1})(1 + p_2 + \ldots\ldots + p_2^{k_2}) \ldots\ldots (1 + p_r + p_r^2 + \ldots\ldots + p_r^{k_r})$$

$\therefore$ $\sigma(n)$ is odd

$\Leftrightarrow \quad (1 + p_1 + \ldots\ldots + p_1^{k_1})(1 + p_2 + \ldots\ldots + p_2^{k_2}) \ldots\ldots (1 + p_r + \ldots\ldots + p_r^{k_r})$ is odd

$\Leftrightarrow \quad 1 + p_i + \ldots\ldots + p_i^{k_i}$ is odd ~~$\forall$~~ $i = 1, 2, \ldots\ldots, r$.

$\Leftrightarrow$ k_i is even for all i, if all p_i are odd and if one of p_i say $p_1 = 2$ then k_i is even for all $i = 2, 3, \ldots\ldots, r$.

$\Leftrightarrow \quad k_i = 2m_i$ for some integers m_i for all $i = 1, 2, \ldots\ldots, r$.

Or $\quad k_i = 2m_i'$ for some integers m_i' for all $i = 2, 3, \ldots\ldots, r$

and k_i is any integer ≥ 1.

$\Leftrightarrow \quad n = (p_1^{m_1} \ldots\ldots p_r^{m_r})^2$

Or $\quad n = 2^{k_1} (p_2^{m_2'} \ldots\ldots p_r^{m_r'})^2$

Now, if k_1 is even, then

$$n = (2^{k_1/2} p_2^{m_2'} \ldots\ldots p_r^{m_r'})^2 \text{ ; and}$$

if k_1 is odd say $k_1 = 2m_1' + 1$, then

$$n = 2 (2^{m_1'} p_2^{m_2'} \ldots\ldots p_r^{m_r'})^2$$

Hence $\sigma(n)$ is odd

$\Leftrightarrow$ n is a perfect square or twice a perfect square.

Example 1. *Show that the sum of the divisors of an integer is odd iff n is of the form k^2 or $2k^2$.*

Solution. Let n be of the form k^2.

Then $\quad \sigma(n) = (k^{2+1} - 1)/(k - 1)$

$= k^2 + k + 1$

and is always odd whether k is even or odd.

Now let us assume

$$n = \sum_{j=1}^{m} k_j^2$$

Then $\quad \sigma(n) = \prod_{j=1}^{m} (k_j^2 + k_j + 1)$

is odd since $k_j^2 + k_j + 1$ is odd and the product of odd numbers is odd.

Conversely, let $\sigma(n)$ be odd.

Then $\sigma(n) = \prod_{j=1}^{m} (1 + p_j + p_j^2 + \ldots\ldots + p_j^{e_j})$ is odd

$\Rightarrow$ $1 + p_j + p_j^2 + \ldots\ldots + p_j^{e_j}$ is odd

$\Rightarrow$ $p_j + p_j^2 + \ldots\ldots + p_j^{e_j}$ is odd

$\Rightarrow$ e_j is even for each p_j whether p_j is odd or even

$\Rightarrow$ $p_j^{e_j}$ is of the form k^2 or $2k^2$ $\forall$ j.

$\Rightarrow$ n is of the form k^2 or $2k^2$.

THE MOBIUS FUNCTION

Definition. *The Mobius function* μ *is defined as*

$$\mu : N \to \{-1, 0, 1\} \text{ i.e}$$

$$\mu(n) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } p^2 \mid n \text{ for some prime } p \\ \text{or if } n \text{ has a square factor} \\ (-1)^r \text{ if } n = p_1 p_2 \ldots\ldots p_r, \text{ where} \\ p_i \text{ are distinct primes.} \end{cases}$$

Note

(1) If p is prime, then

$$\mu(p^k) = \begin{cases} 1 & \text{for } k = 1 \\ 0 & \text{for } k \geq 2 \end{cases}$$

(2) $\mu(n) = 0$ if n is not a square-free integer, where as

$\mu(n) = (-1)^r$ if n is square-free with r prime factors.

e.g. $\mu(30) = \mu(2.3.5) = (-1)^3 = -1$.

The first few values of μ are

$\mu(1) = 1, \mu(2) = -1, \mu(3) = -1,$

$\mu(4) = 0, \mu(5) = -1, \mu(6) = 1, \ldots\ldots$

If p is a prime number, then it is clear that $\mu(p) = -1$.

Definition. *An integer indivisible by the square of any integer* $n \neq 1$ *is said to be square free.*

Theorem 9. Prove that Mobius function is multiplicative function.

Or

Show that the function μ ***is a multiplicative function.***

Or

Prove that $\mu(n)$ ***is multiplicative.***

Or

Prove that Mobius function μ ***is multiplicative.***

Proof. Let a and b be two relatively prime positive integers.

Case I

When $a = 1$ and $b = 1$, then $ab = 1$.

$\therefore$ $\mu(a) = \mu(b) = \mu(ab) = \mu(1) = 1$

so that $\mu(a)\,\mu(b) = 1 \cdot 1 = 1 = \mu(ab)$.

Case II

When $a = 1$ and $b \neq 1$, then $ab = b$

$\Rightarrow$ $\mu(ab) = \mu(b)$

$\Rightarrow$ $\mu(ab) = 1 \cdot \mu(b)$

$\Rightarrow$ $\mu(ab) = \mu(a)\,\mu(b)$ $\quad [\because \mu(a) = \mu(1) = 1]$

Similarly, when $a \neq 1$ and $b = 1$, then

$\mu(ab) = \mu(a)\,\mu(b)$.

Case III

When $a \neq 1$ and $b \neq 1$.

Sub-case (i)

When a or b is divisible by some square p^2 (say), then

$\mu(a) = 0$ or $\mu(b) = 0$

$\Rightarrow$ $\mu(a)\,\mu(b) = 0$ in each case.

Also $p^2 \mid a$ or $p^2 \mid b$

$\Rightarrow$ $p^2 \mid ab \Rightarrow \mu(ab) = 0$

$\therefore$ $\mu(ab) = \mu(a)\,\mu(b)$.

Sub-case (ii)

When a and b are not divisible by square of any prime number, then

$a = p_1 p_2 \ldots\ldots p_r$ and

$b = q_1 q_2 \ldots\ldots q_s$

where $p_1, p_2, \ldots\ldots, p_r$ and $q_1, q_2, \ldots\ldots, q_s$ are distinct primes.

$\therefore$ $\mu(a) = (-1)^r$ and

$\mu(b) = (-1)^s$

$\Rightarrow$ $\mu(a)\,\mu(b) = (-1)^r (-1)^s = (-1)^{r+s}$

Also $ab = p_1 p_2 \ldots\ldots p_r q_1 q_2 \ldots\ldots q_s$

$\Rightarrow$ $\mu(ab) = (-1)^{r+s} = \mu(a)\,\mu(b)$

Therefore in each case,

$\mu(ab) = \mu(a)\,\mu(b)$

Hence mobius function is multiplicative function.

Theorem 10. ***The function*** μ ***is a multiplicative function.***

Or

Prove that $\mu(n)$ ***is multiplicative.***

Proof. Let us assume that a and b are relative prime *i.e.*

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

Then $p^2 \mid ab$ only if either $p^2 \mid a$ or $p^2 \mid b$, and in either case

$\mu(a) \cdot \mu(b) = \mu(ab) = 0.$

If a and b are assumed to be both square-free, that

$a = p_1 p_2 \ldots\ldots p_r,$

$b = q_1 q_2 \ldots\ldots q_s,$

$ab = p_1 p_2 \ldots\ldots p_r q_1 \ldots\ldots q_s$

where the primes p_i and q_j are all different.

Hence $\mu(a) = (-1)^r,$

$\mu(b) = (-1)^s$ and

$\mu(ab) = (-1)^{r+s}$

$= (-1)^r (-1)^s$

$= \mu(a)\,\mu(b).$

Hence the Proof.

Theorem 11. ***Prove that*** $\phi(n) = n \sum_{d \mid n} \frac{\mu(d)}{d}$.

Proof. Let us define a as the divisors of $p_1, p_2, \ldots\ldots\ldots, p_s$, including one, which are

composed of an even number of prime factors and b as the divisors of the same number composed of an odd number of prime factors.

Then a and b together represent all square-free divisors (*i.e* divisors not divisible by a square except 1) of n,

the formula for $\phi(n)$:

$$\phi(n) = n - \sum_i \frac{n}{p_i} + \sum_{i,j} \frac{n}{p_i p_j} - \sum_{i,j,k} \frac{n}{p_i p_j p_k} + \ldots\ldots + (-1)^s \frac{n}{p_1 p_2 \ldots\ldots p_s}$$

can be be expressed thus

$$\phi(n) = n \sum_a \frac{1}{a} - n \sum_b \frac{1}{b},$$

the suffixes a and b indicating that the respective summations are extended over all divisors a and b.

In view of Mobius function, we find

$\mu(1) = 1;$

$\mu(n) = 0$ if n is divisible by square > 1,

$\mu(n) = +1$ if n is square free and contains an even number of primes;

$\mu(n) = -1$ if n is square free and contains an odd number of primes.

Then $\phi(n)$ can be exhibited thus :

$$\phi(n) = n \sum_{d \mid n} \frac{\mu(d)}{d}$$

where the summation extends all divisors of n, keeping this fact in mind that corresponding to divisors which are divisible by squares > 1 are zeros, and the other terms correspond to square- free divisors denoted by a and b, but by definition

$\mu(a) = +1$ and $\mu(b) = -1.$

Theorem 12. ***For each integer*** $n \geq 1$

$$\sum_{d \mid n} \mu(d) = \begin{cases} \mathbf{1} & \textbf{if } n = 1 \\ \mathbf{0} & \textbf{if } n > 1. \end{cases}$$

Proof. If $n = 1$,

then $\sum_{d \mid n} \mu(1) = \mu(1) = 1$ by definition.

Therefore, let $n \geq 2$.

By fundamental theorem of arithmetic

$n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}$ where p_i are distinct primes and $k_i \geq 1$.

$$\therefore \quad \sum_{d \mid n} \mu(d) = \mu(1) + \sum_{i=1}^{r} \mu(p_i) + \sum_{\substack{i \leq 1 \\ i,j=1}} \mu(p_i p_j) + \ldots\ldots$$

$$+ \mu(p_1 p_2 \ldots\ldots p_r) + 0 + \ldots\ldots + 0;$$

the remaining all terms vanish since they contain square factors.

$$\Rightarrow \quad \sum_{d \mid n} \mu(d) = 1 + r(-1) + \binom{r}{2}(-1)^2 + \ldots\ldots + (-1)^r$$

$$= 1 + \binom{r}{1}(-1) + \binom{r}{2}(-1)^2 + \ldots\ldots + (-1)^r$$

$$= \sum_{j=0}^{r} (-1)^j \binom{r}{j}$$

$$= (1-1)^r = 0, \text{ in case } r > 0.$$

Hence the Proof.

Note

Let us take $n = 10$.

The positive divisors of 10 are 1, 2, 5, 10 and the desired sum is

$$\sum_{d \mid 10} \mu(d) = \mu(1) + \mu(2) + \mu(5) + (10)$$

$$= 1 + (-1) + (-1) + 1$$

$$= 1 - 1 - 1 + 1$$

$$= 0.$$

Theorem 13. ***State and prove Mobius Inversion Formula.***

Statement. *Let F and f be two number-theoretic functions related by the formula*

$$F(n) = \sum_{d \mid n} f(d)$$

Then $f(n) = \sum_{d \mid n} \mu(d)\, F\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) F(d)$.

Proof. $\sum_{d \mid n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d \mid n} \left(\mu(d) \sum_{c \mid \left(\frac{n}{d}\right)} f(c) \right)$

$$= \sum_{d \mid n} \left(\sum_{c \mid \left(\frac{n}{d}\right)} \mu(d) f(c) \right) \quad \ldots(1)$$

Since $d \mid n$ and $c \mid \left(\frac{n}{d}\right)$ if and only if $c \mid n$ and $d \mid \left(\frac{n}{c}\right)$.

Using this, the last expression in (1) becomes

$$\sum_{d \mid n} \left(\sum_{c \mid \left(\frac{n}{d}\right)} \mu(d) f(c) \right) = \sum_{c \mid n} \left(\sum_{d \mid \left(\frac{n}{c}\right)} f(c) \mu(d) \right)$$

$$= \sum_{c \mid n} \left(f(c) \sum_{d \mid \left(\frac{n}{c}\right)} \mu(d) \right) \quad \ldots(2)$$

Using the theorem, "For each positive integer $n \geq 1$,

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

where d runs through the positive divisors of $n > 1$," we have

$$\sum_{d \mid \left(\frac{n}{c}\right)} \mu(d) = \begin{cases} 1 & \text{if } \frac{n}{c} = 1 \ \ i.e \text{ if } n = c \\ 0 & \text{if } \frac{n}{c} > 1 \end{cases}$$

Now putting the value of $\sum_{d \mid \left(\frac{n}{c}\right)} \mu(d) = 1$ in the right hand sides of (2), we get

$$\sum_{c \mid n} \left(f(c) \sum_{d \mid \left(\frac{n}{c}\right)} \mu(d) \right) = \sum_{c = n} f(c) \cdot 1 = f(n)$$

$$\therefore \sum_{d \mid n} \left(\sum_{c \mid \left(\frac{n}{d}\right)} \mu(d) f(c) \right) = f(n)$$

But $$\sum_{d \mid n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d \mid n} \left(\sum_{c \mid \left(\frac{n}{d}\right)} \mu(d) f(c) \right)$$

$$\therefore \sum_{d \mid n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) F(d) = f(n)$$

Hence the Proof.

Note

1. Let us take $n = 10$.

Then $$\sum_{d \mid 10} \left(\sum_{c \mid \left(\frac{10}{d}\right)} \mu(d) f(c) \right)$$

$$= \mu(1)[f(1) + f(2) + f(5) + f(10)] + \mu(2)[f(1) + f(5)] + \mu(5)[f(1) + f(2)] + \mu(10) f(1)$$

$$= f(1)[\mu(1) + \mu(2) + \mu(5) + \mu(10)] + f(2)[\mu(1) + \mu(5)] + f(5)[\mu(1) + \mu(2)] + f(10)\mu(1)$$

$$= \sum_{c \mid 10} \left(\sum_{d \mid \left(\frac{10}{c}\right)} f(c) \mu(d) \right)$$

2. The function τ and σ may both be described as "sum functions"

$$\tau(n) = \sum_{d \mid n} 1 \text{ and}$$

$$\sigma(n) = \sum_{d \mid n} d$$

The Mobius inversion formula tells us that these formulas may be inverted to give

$$1 = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \tau(d) \text{ and}$$

$$n = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \sigma(d) \text{ which are valid } \forall\ n \geq 1.$$

Theorem 14. *If F is a multiplicative function and*

$$F(n) = \sum_{d \mid n} f(d),$$

then f is also multiplicative.

Proof. Let m and n be relatively prime positive integers.
We know that any divisor d of mn can be uniquely written as

$$d = d_1 d_2,$$

where $d_1 \mid m$, $d_2 \mid n$ and

$$gcd(d_1, d_2) = 1.$$

Then, using the inversion formula, we have

$$f(mn) = \sum_{d \mid mn} \mu(d)\ F\left(\frac{mn}{d}\right)$$

$$= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} \mu(d_1 d_2) F\left(\frac{mn}{d_1 d_2}\right)$$

$$= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} \mu(d_1)\mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right)$$

$$= \sum_{d_1 \mid m} \mu(d_1) F\left(\frac{m}{d_1}\right) \sum_{d_2 \mid n} \mu(d_2) F\left(\frac{n}{d_2}\right)$$

$$= f(m) f(n)$$

which shows that f is multiplicative.

Hence the Proof.

Definition. *For $n \geq 1$, we define the sum*

$$M(n) = \sum_{k=1}^{n} \mu(k).$$

Then $M(n)$ is the difference between the number of square free positive integers $k \leq n$ with an even number of prime factors and those with an odd number of prime factors.

e.g. $M(9) = 2 - 4 = -2.$

THE MANGOLDT FUNCTION Λ

The Mangoldt function $\Lambda(n)$ is defined by

$$\Lambda(n) = \begin{cases} \log p \text{ if } n = p^k, \text{ where } p \text{ is a prime and } k \geq 1 \\ 0 \text{ otherwise.} \end{cases}$$

Example 2. *Prove that* $\mu(n) \log n = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \Lambda(d)$.

Solution. We know that

$$\frac{1}{\zeta(s)} = \sum \frac{\mu(n)}{n^s}$$

Now $$-\frac{d}{ds}\left\{\frac{1}{\zeta(s)}\right\} = \frac{\zeta'(s)}{\zeta^2(s)} = -\frac{1}{\zeta(s)}\left\{-\frac{\zeta'(s)}{\zeta(s)}\right\}$$

Or $$-\frac{d}{ds}\sum \frac{\mu(n)}{n^s} = -\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$$

Or $$\sum_{n=1}^{\infty} \frac{\mu(n) \log n}{n^s} = -\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

which gives

$$-\mu(n) \log n = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \Lambda(d).$$

Theorem 15. ***Prove that*** $\Lambda(n) = -\sum_{d \mid n} \mu(d) \log d$.

Proof. Now $$-\frac{\zeta'(s)}{\zeta(s)} = \zeta(s) \frac{d}{ds}\left\{\frac{1}{\zeta(s)}\right\}$$

Using the theorem,

$$"-\frac{\zeta'(s)}{\zeta(s)} = \sum_{1}^{\infty} \Lambda(n) n^{-s} \ (s > 1),"$$

we have

$$\sum \frac{\Lambda(n)}{n^s} = -\sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{n=1}^{\infty} \frac{\mu(n) \log n}{n^s}$$

which proves that

$$\Lambda(n) = -\sum_{d \mid n} \mu(d) \log d$$

Theorem 16. ***Prove that*** $-\frac{\zeta'(s)}{\zeta(s)} = \sum_{1}^{\infty} \Lambda(n) n^{-s} \ (s > 1)$.

Proof. Since we know that

$$\zeta(s) = \sum_{1}^{\infty} \frac{1}{n^s} \qquad \ldots(1)$$

Differentiating it term by term with respect to s, we get

$$\zeta'(s) = -\sum_{1}^{\infty} \frac{\log n}{n^s} \ (\Lambda > 1) \qquad \ldots(2)$$

Also $$\prod_{p \leq P} \frac{1}{1 - p^{-s}} = \sum_{p} n^{-s} = \zeta(s)$$

The summation on the right hand side extending over numbers formed from the primes upto P.

Differentiating

$$\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}}$$

with respect to s, we get

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{p} \log p \sum_{m=1}^{\infty} p^{-ms}$$

We know that the double series $\sum \sum p^{-ms} \log p$ is absolutely convergent where $s > 1$.

It assumes the form

$$\sum_{p, m} p^{-ms} \log p = \sum \Lambda(n) m^{-s} \text{ in view of definition of } \Lambda(n).$$

Hence $$-\frac{\zeta'(s)}{\zeta(s)} = \sum \Lambda(n) n^{-s}.$$

Definition. *An arithmetic function f is called a* ***multiplicative arithmetic*** *function if for each pair of co-prime integers m and n.*

$$f(mn) = f(m)\, f(n).$$

Note

If f is a multiplicative arithmetic function and $m_1 \ldots\ldots m_r$ is a finite set of pairwise relatively prime integers, then

$$f(m_1 m_2 \ldots\ldots m_r) = f(m_1)\, f(m_2) \ldots\ldots f(m_r)$$

and if there is at least one positive integer n such that $f(n) \neq 0$, then $f(1) = 1$.

Also a multiplicative arithmetic function is completely determined by its values at prime powers.

Example 3. Prove that $1 = \sum_{d \mid n} \mu(d)\, \tau\left(\frac{n}{d}\right)$.

Solution. As $(\tau(n), f)$ where $f(n) = 1 \ \forall\ n$, is a Mobius pair, by inversion formula, we have

$$f(n) = \sum_{d \mid n} \mu(d)\, \tau\left(\frac{n}{d}\right)$$

$$\Rightarrow \quad 1 = \sum_{d \mid n} \mu(d)\, \tau\left(\frac{n}{d}\right)$$

Example 4. Let $f(n) = \prod_{d \mid n} g(d)$, *then show that*

$$g(n) = \prod_{d \mid n} (f(d))^{\mu\left(\frac{n}{d}\right)}$$

Solution. Since $f(n) = \prod_{d \mid n} g(d)$

Taking log on both sides, we get

$$\log f(n) = \sum_{d \mid n} \log g(d)$$

By inversion formula

$$\log g(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \log f(d)$$

$$= \sum_{d \mid n} \log (f(d))^{\mu\left(\frac{n}{d}\right)}$$

$$= \log \prod_{d \mid n} f(d)^{\mu\left(\frac{n}{d}\right)}$$

Now taking antilogs, we have

$$g(n) = \prod_{d \mid n} f(d)^{\mu\left(\frac{n}{d}\right)}.$$

Example 5. Prove that $\frac{\phi(n)}{n} = \sum_{d \mid n} \frac{\mu(d)}{d}$.

Solution. We know that (n, ϕ) is a Mobius pair and

$$n = \sum_{d \mid n} \phi(d)$$

Therefore by inversion formula

$$\phi(n) = \sum_{d \mid n} \mu(d) \cdot \frac{n}{d}$$

Dividing both sides by n, we get

$$\frac{\phi(n)}{n} = \sum_{d \mid n} \frac{\mu(d)}{n} \cdot \frac{n}{d}$$

$$\Rightarrow \quad \frac{\phi(n)}{n} = \sum_{d \mid n} \frac{\mu(d)}{d}.$$

Theorem 17. ***The functions ϕ, τ, σ and μ are all multiplicative arithmetic functions.***

Proof. Let $m > 1$ and $n > 1$ be two co-prime integers and

$$m = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r} \text{ and}$$

$$n = q_1^{s_1} q_2^{s_2} \ldots\ldots q_t^{s_t}$$

be their unique factorizations into primes.

Since $\gcd(m, n) = 1$,

$$p_1, p_2, \ldots\ldots, p_r ; q_1, q_2, \ldots\ldots, q_t \text{ are all distinct.}$$

Now $\quad mn = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r} q_1^{s_1} q_2^{s_2} \ldots\ldots q_t^{s_t}$

$$\therefore \quad \phi(mn) = \phi(p_1^{k_1})\, \phi(p_2^{k_2}) \ldots\ldots \phi(p_r^{k_r}).$$

$$\phi(q_1^{s_1})\, \phi(q_2^{s_2}) \ldots\ldots \phi(q_t^{s_t})$$

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

$$\tau(mn) = (k_1 + 1)(k_2 + 1) \ldots\ldots (k_r + 1).$$
$$(s_1 + 1)(s_2 + 1) \ldots\ldots (s_t + 1)$$
$$= \tau(m)\,\tau(n);$$

$$\sigma(mn) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \ldots\ldots \frac{p_r^{k_r+1} - 1}{p_r - 1} \cdot$$
$$\frac{q_1^{s_1+1} - 1}{q_1 - 1} \cdot \frac{q_2^{s_2+1} - 1}{q_2 - 1} \ldots\ldots \frac{q_t^{s_t+1} - 1}{q_t - 1}$$
$$= \sigma(m)\,\sigma(n)$$

and $$\mu(mn) = \begin{cases} (-1)^{r+t} \text{ if } k_i = s_j = 1 \ \forall\ i = 1, 2, \ldots\ldots, r, \\ j = 1, 2, \ldots\ldots, t \\ 0 \text{ if } k_i, s_j > 1 \text{ for at least one } i \text{ or } j \end{cases}$$
$$= \mu(m)\,\mu(n)$$

Thus by definition of multiplicative arithmetic functions ϕ, τ, σ and μ are multiplicative.

Example 6. *Prove that* $\sum_{d \mid n} \frac{1}{d} = \frac{\sigma(n)}{n}$ *for every positive integer n.*

Solution. Let $d_1, d_2, \ldots\ldots, d_r$ be the all positive divisors of n.

Then $\frac{n}{d_1}, \frac{n}{d_2}, \ldots\ldots, \frac{n}{d_r}$ are also the all positive divisors of n.

$$\therefore \quad \sum_{d \mid n} \frac{1}{d} = \frac{1}{n/d_1} + \frac{1}{n/d_2} + \ldots\ldots + \frac{1}{n/d_r}$$
$$= \frac{d_1}{n} + \frac{d_2}{n} + \ldots\ldots + \frac{d_r}{n}$$
$$= \frac{d_1 + d_2 + \ldots\ldots + d_r}{n}$$
$$= \frac{\sigma(n)}{n}$$

Example 7. *Evaluate* $\tau(180)$ *and* $\sigma(180)$

Solution. $180 = 2^2 \cdot 3^2 \cdot 5^1$

$$\therefore \quad \tau(180) = (2 + 1)(2 + 1)(1 + 1)$$
$$= (3)(3)(2)$$
$$= 18$$

$$\sigma(180) = \frac{2^3 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1}$$
$$= 7 \cdot \frac{26}{2} \cdot \frac{24}{4}$$
$$= 7 \cdot 13 \cdot 6$$
$$= 546.$$

Example 8. *Prove that* $\prod_{d \mid n} d = n^{\frac{1}{2}\tau(n)}$

Or

Prove that $\prod_{d \mid n} d = n^{\frac{r(n)}{2}}$

Solution. For $n = 1$, the result is obvious, so let us take $n > 1$.

Let $d_1, d_2, \ldots\ldots, d_r$ be all positive divisors of n so that $\tau(n) = r$.

Therefore $$\prod_{d \mid n} d = d_1\, d_2 \ldots\ldots d_r \qquad \ldots(1)$$

Since $\frac{n}{d_1}, \frac{n}{d_2}, \ldots\ldots, \frac{n}{d_r}$ are also all positive divisors of n

Therefore $$\prod_{d \mid n} d = \frac{n}{d_1} \cdot \frac{n}{d_2} \ldots\ldots \frac{n}{d_r}$$

i.e $$\prod_{d \mid n} d = \frac{n^r}{d_1\, d_2 \ldots\ldots d_r} \qquad \ldots(2)$$

Multiplying (1) and (2), we get

$$\left(\prod_{d \mid n} d\right)^2 = (d_1\, d_2 \ldots\ldots d_r)\, \frac{n^r}{(d_1\, d_2 \ldots\ldots d_r)}$$
$$= n^r$$

$$\Rightarrow \quad \prod_{d \mid n} d = n^{\frac{1}{2}r}$$

$$\Rightarrow \quad \prod_{d \mid n} d = n^{\frac{1}{2}\tau(n)}$$

Example 9. *Evaluate* τ *and* σ *for* $n = 3000$.

Solution. Since $3000 = 2^3 \cdot 3^1 \cdot 5^3$,
therefore we have

$$\tau(3000) = (3+1)(1+1)(3+1)$$
$$= 4 \cdot 2 \cdot 4$$
$$= 32$$

$$\text{Again, } \sigma(3000) = \left(\frac{2^4-1}{2-1}\right) \cdot \left(\frac{3^2-1}{3-1}\right) \cdot \left(\frac{5^4-1}{5-1}\right)$$
$$= \left(\frac{16-1}{1}\right) \cdot \left(\frac{9-1}{2}\right) \cdot \left(\frac{625-1}{4}\right)$$
$$= 15 \cdot 4 \cdot 156$$
$$= 9360.$$

Example 10. *Show that* $\tau(n) = \tau(n+1) = \tau(n+2)$ *for* $n = 4503$.

Solution. We can write

$$n = 4503 = 3 \times 19 \times 79$$
$$\tau(n) = \tau(4503)$$
$$= (1+1)(1+1)(1+1)$$
$$= 8$$

Again, $n + 1 = 4504 = 2^3 \cdot 563$

Thus, $\tau(n+1) = (3+1)(1+1) = 8$

Also, $n + 2 = 4505 = 5 \times 17 \times 53$

Thus, $\tau(n+2) = (1+1)(1+1)(1+1)$
$= 8$

Hence, from (1), (2) and (3), we conclude that

$$\tau(n) = \tau(n+1) = \tau(n+2).$$

Example 11. *If* $f(n) = n^2 + 2$ *and* $n = 6$, *then show that*

$$\sum_{d \mid 6} f(d) = \sum_{d \mid 6} f\left(\frac{6}{d}\right)$$

Solution. The divisors of 6 are given by

$$d = 1, 2, 3, 6$$

$$\therefore \quad \frac{6}{d} = 6, 3, 2, 1$$

$$\Rightarrow \quad \sum_{d \mid 6} f(d) = (1^2+2) + (2^2+2) + (3^2+2) + (6^2+2)$$
$$= 58$$

$$\text{Also} \quad \sum_{d \mid 6} f\left(\frac{6}{d}\right) = (6^2+2) + (3^2+2) + (2^2+2) + (1^2+2)$$
$$= 58$$

$$\text{Hence, } \sum_{d \mid 6} f(d) = \sum_{d \mid 6} f\left(\frac{6}{d}\right)$$

Example 12. *Find a positive integer* n *such that*

$$\mu(n) + \mu(n+1) + \mu(n+2) = 3.$$

Solution. We know that

$$\mu(n) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } n \text{ is divisible by some square} > 1 \\ (-1)^r \text{ if } n = p_1 p_2 \ldots p_r \text{ where } p_i\text{'s are distinct primes} \end{cases}$$

Therefore max. of value of $\mu(n) = 1$.

Since $\mu(n) + \mu(n+1) + \mu(n+2) = 3$

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

But $n = 1$ is not possible as

$$\mu(n+1) = \mu(1+1) = \mu(2) = -1$$

Therefore n must contain even number of primes.

$n+1$ must contain even number of primes

$n+2$ must contain even number of primes.

One such number is 33,

since $33 = 3 \times 11, 34 = 2 \times 17, 35 = 5 \times 7.$

Another such number is 93,

since $93 = 3 \times 31, 94 = 2 \times 47, 95 = 5 \times 19.$

Example 13. *For each positive integer n, show that*

$$\mu(n)\,\mu(n+1)\,\mu(n+2)\,\mu(n+3) = 0.$$

Solution. Divide n by 4.

Let k be the quotient and r be the least non-negative remainder.

$\therefore$ $n = 4k + r$ where $r = 0, 1, 2$ or 3

$\Rightarrow$ $n = 4k$ or $4k+1$ or $4k+2$ or $4k+3$

$\Rightarrow$ $n = 4k$ or $n+3 = 4k+4$ or $n+2 = 4k+4$ or $n+1 = 4k+4$

$\Rightarrow$ $4 \mid n$

Or $4 \mid n+3$

Or $4 \mid n+2$

Or $4 \mid n+1$

$\Rightarrow$ $\mu(n+0)$ or $\mu(n+3) = 0$

Or $\mu(n+2) = 0$ or $\mu(n+1) = 0$

Therefore one of $\mu(n), \mu(n+1), \mu(n+2), \mu(n+3)$ is 0 for each n

$\Rightarrow$ $\mu(n)\,\mu(n+1)\,\mu(n+2)\,\mu(n+3) = 0$ for each positive integer n.

Example 14. *If n is a positive integer such that $n \geq 3$, then*

$$\sum_{k=1}^{n} \mu(k!) = 1.$$

Solution. We prove this result by using the principle of mathematical induction.

For $n = 3$, we have

$$\sum_{k=1}^{3} \mu(k!) = \mu(1!) + \mu(2!) + \mu(3!)$$

$$= \mu(1) + \mu(2) + \mu(6)$$

$$= 1 + (-1) + \mu(2 \cdot 3)$$

$$= (-1)^2$$

$$= 1$$

$\Rightarrow$ result is true for $n = 3$.

Suppose, result is true for $n = m$ *i.e*

$$\sum_{k=1}^{m} \mu(k!) = 1$$

To show, result is true for $n = m+1$.

For this, we shall show that

$$\sum_{k=1}^{m+1} \mu(k!) = 1$$

Consider $\sum_{k=1}^{m+1} \mu(k!) = \sum_{k=1}^{m} \mu(k!) + \mu[(m+1)!]$

$$= 1 + 0$$

[$\because$ in $(m+1)!$, there will be one factor 2^2]

$$= 1$$

$\Rightarrow$ result is true for $n = m+1$.

Hence, by principle of mathematical induction, the result is true for all $n \geq 3$.

Example 15. *If f is a multiplicative function which does not vanish identically then show that $f(1) = 1$.*

Solution. Since f does not vanish identically,

therefore there exists $n \in Z$ such that

$$f(n) \neq 0.$$

Since f is multiplicative and $(n, 1) = 1$

$\therefore$ $f(n) = f(n \cdot 1)$

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

Cancelling $f(n) \neq 0$ from both sides, we get

$$1 = f(1)$$

Hence $f(1) = 1$.

Example 16. *Let f and g be multiplicative functions such that $f(p^k) = g(p^k)$ for each prime p and $k \geq 1$. Prove that $f = g$.*

Solution. Let n be any arbitrary positive integer with

$$n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}$$

as prime factorization of n.

Then $f(n) = f(p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r})$

$= f(p_1^{k_1}) f(p_2^{k_2}) \ldots f(p_r^{k_r})$

[$\because$ f is multiplicative and $p_1, p_2, \ldots, p_r$ are relatively prime in pairs]

$= g(p_1^{k_1}) g(p_2^{k_2}) \ldots g(p_r^{k_r})$

[$\because$ $f(p^k) = g(p^k)$ for each prime p]

$= g(p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r})$ ($\because$ g is multiplicative)

$= g(n)$

Hence $f = g$.

Example 17. *Show that* $\sigma(12n-1) \equiv 0 \pmod{12}$ *for* $n \geq 1$.

Or

Show that $\sigma(12n-1)$ *is divisible by* $12n \geq 1$.

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

be all positive divisors of $12n-1$ in the ascending order.

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

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

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

Since $d_1 \mid 12n-1$, therefore,

$(d_1, 12) = 1$

$\Rightarrow$ $(d_1, 3) = 1$

Therefore by Fermat's theorem, we have

$d_1^2 \equiv 1 \pmod{3}$ ...(2)

Also d_1 is odd number, say $d_1 = 2k+1$

$\therefore$ $d_1^2 = (2k+1)^2 = 4k^2 + 4k + 1$

$\Rightarrow$ $d_1^2 \equiv 1 \pmod{4}$ ...(3)

Therefore from (2) and (3), we get

$d_1^2 \equiv 1 \pmod{3 \cdot 4}$

$\Rightarrow$ $d_1^2 \equiv 1 \pmod{12}$

$\Rightarrow$ $d_1^2 - 1 = 12k_1$

$\therefore$ $\frac{d_1^2 - 1 + 12n}{d_1} = \frac{12k_1 + 12n}{d_1} = \frac{12(k_1 + n)}{d_1}$

[which is an integer, since d_1 and $\frac{12n-1}{d_1}$ are integers]

$\therefore$ $d_1 \mid 12(k_1 + n) \Rightarrow d_1 \mid k_1 + n$ [$\because (d_1, 12) = 1$]

$\Rightarrow$ $\frac{k_1 + n}{d_1}$ is an integer

$\Rightarrow$ $12\frac{(k_1 + n)}{d_1}$ is multiple of 12

$\Rightarrow$ $\frac{12k_1 + 12n}{d_1}$ is multiple of 12

$\Rightarrow$ $\frac{d_1^2 - 1 + 12n}{d_1}$ is a multiple of 12.

$\Rightarrow$ $\frac{d_1^2 - 1 + 12n}{d_1} \equiv 0 \pmod{12}$

Similarly $\frac{d_2^2 - 1 + 12n}{d_2} \equiv 0 \pmod{12}$ and so on.

Therefore from (1), we get

$\sigma(12n-1) \equiv 0 \pmod{12}$

$\Rightarrow$ $12 \mid \sigma(12n-1)$ $\forall$ $n \geq 1$.

Example 18. *Show that* $\sigma(24n-1) \equiv 0 \pmod{24}$ $\forall$ $n \geq 1$.

Or

Show that $\sigma(24n-1)$ *is divisible by* 24 $\forall$ $n \geq 1$.

Solution. Let $d_1, d_2, \ldots, \frac{24n-1}{d_2}, \frac{24n-1}{d_1}$

be the divisors of $24n-1$ in ascending order.

$$\therefore \quad \sigma(24n-1) = d_1 + d_2 + \ldots\ldots + \frac{24n-1}{d_2} + \frac{24n-1}{d_1}$$

$$= \left(d_1 + \frac{24n-1}{d_1}\right) + \left(d_2 + \frac{24n-1}{d_2}\right) + \ldots\ldots$$

$$= \frac{d_1^2 - 1 + 24n}{d_1} + \frac{d_2^2 - 1 + 24n}{d_2} + \ldots\ldots \quad \ldots(1)$$

Since $d_1 \mid 24n-1$ and $3 \mid 24$ and $(24n-1, 24) = 1$

$\therefore \quad (d_1, 3) = 1$

Therefore by Fermat's theorem, we have

$$d_1^2 \equiv 1 \pmod 3 \quad \ldots(2)$$

$(\because 24n-1$ is odd$)$

Also d_1 is odd.

say, $d_1 = 2k+1$

$$\Rightarrow \quad d_1^2 = (2k+1)^2$$

$$= 4k^2 + 4k + 1$$

$$= 4k^2 + 4k + 1$$

$$= 4k(k+1) + 1$$

$$\equiv 0 + 1 \pmod 8 \quad [\because \text{one of } k \text{ and } k+1 \text{ is even}]$$

$$i.e \quad d_1^2 \equiv 1 \pmod 8 \quad \ldots(3)$$

Since $(3, 8) = 1$

Therefore from (2) and (3), we have

$$d_1^2 \equiv 1 \pmod{3 \cdot 8}$$

$$\Rightarrow \quad d_1^2 - 1 \equiv 0 \pmod{24}$$

$$\Rightarrow \quad d_1^2 - 1 = 24k_1$$

$$\therefore \quad \frac{d_1^2 - 1 + 24n}{d_1} = \frac{24k_1 + 24n}{d_1} = \frac{24(k_1 + n)}{d_1},$$

which is an integer.

$[\because d_1$ and $\frac{24n-1}{d_1}$ are integers$]$

$$d_1 \mid 24(k_1 + n)$$

$$\therefore \quad d_1 \mid k_1 + n$$

$$\Rightarrow \quad \frac{k_1 + n}{d_1} \text{ is an integer} \qquad [\because (d_1, 24) = 1]$$

$$\Rightarrow \quad 24\frac{(k_1 + n)}{d_1} \text{ is multiple of 24.}$$

$$\Rightarrow \quad \frac{d_1^2 - 1 + 24n}{d_1} \text{ is multiple of 24.}$$

$$\Rightarrow \quad \frac{d_1^2 - 1 + 24n}{d_1} \equiv 0 \pmod{24}$$

Similarly $\frac{d_2^2 - 1 + 24n}{d_2} \equiv 0 \pmod{24}$ and so on.

Therefore from (1), we get

$$\sigma(24n-1) \equiv 0 \pmod{24} \ \forall\ n \geq 1$$

$$\Rightarrow \quad \sigma(24n-1) \text{ is divisible by } 24 \ \forall\ n \geq 1.$$

Example 19. Show that $\sigma(4n+3) \equiv 0 \pmod 4$.

Solution. Let d be a divisor of $4n+3$.

Then $(d, 4) = 1$

$\therefore \quad d = 4k+1$ or $4k+3$

Let $4n+3 = de$ for some $e \in Z$ $\qquad [\because d \mid 4n+3]$

If $d = 4k+1$ then $e = 4k' + 3$

and if $d = 4k+3$ then $e = 4k' + 1$

Hence in either case $4 \mid d + e$.

Since $4n+3$ is not a perfect square, therefore, number of positive divisors of $4n+3$ is even and hence all divisors of $4n+3$ may be paired in above manner to get

$$4 \mid \sigma(4n+3)$$

Or $\quad \sigma(4n+3) \equiv 0 \pmod 4$

Example 20. Find the form of all positive integers n satisfying $\tau(n) = 10$. *What is the smallest positive integer for which this is true ?*

Solution. We have

$\tau(n) = 10 = 10 \times 1$ or 5×2

Let $n = p_1^{a_1} p_2^{a_2}$

$\Rightarrow \quad \tau(n) = (a_1 + 1)(a_2 + 1)$

Since $\tau(n) = (a_1 + 1)(a_2 + 1) = 10 \times 1$

$\Rightarrow \quad a_1 + 1 = 10$ and $a_2 + 1 = 1$

$\Rightarrow \quad a_1 = 9$ and $a_2 = 0$

$\therefore \quad n = p_1^{a_1} p_2^{a_2}$

$= p_1^9 p_2^0$

i.e $n = p_1^9$

Now $\tau(n) = (a_1 + 1)(a_2 + 1) = 5 \times 2$

$\Rightarrow \quad a_1 + 1 = 5$ and $a_2 + 1 = 2$

$\Rightarrow \quad a_1 = 4$ and $a_2 = 1$

$\therefore \quad n = p_1^4 p_2^1$

i.e $n = p_1^4 p_2$

To obtain the smallest positive integer for which $\tau(n) = 10$.

Choose the two smallest primes *i.e* 2 and 3 so that the smallest such positive integer

$= 2^4 \cdot 3^1 = 48.$

Example 21. Show that there is no positive integer n satisfying $\sigma(n) = 10$.

Solution. We have $\sigma(n) = 10$.

We know that $\sigma(n) > n$ for $n > 1$

$\Rightarrow \quad 10 > n$ where $n > 1$

i.e $1 < n < 10$

$\Rightarrow \quad 2 \le n \le 9$

$\Rightarrow \quad n = 2$ or 3 or 4 or 5 or 6 or 7 or 8

$\sigma(2) = 1 + 2 = 3 \neq 10$

$\sigma(3) = 1 + 3 = 4 \neq 10$

$\sigma(4) = 1 + 2 + 4 = 7 \neq 10$

$\sigma(5) = 1 + 5 = 6 \neq 10$

$\sigma(6) = 1 + 2 + 3 + 6 = 12 \neq 10$

$\sigma(7) = 1 + 7 = 8 \neq 10$

$\sigma(8) = 1 + 2 + 4 + 8 = 15 \neq 10$

Hence there is no positive integer n satisfying $\sigma(n) = 10$.

THE GREASTEST INTEGER FUNCTION

Definition. *Let x be a real number, denoted by* $[x]$, *the largest integer less than or equal to x, i.e. the largest integer that does not exceed x.*

e.g. $[5] = 5, [6.23] = 6,$

$\left[\frac{1}{3}\right] = 0, [\pi] = 3, [-\pi] = -4$

In general, for each $j \in Z$, $[j] = j$ *and for non-integral* $x > 0$, $[-x] = -[x] - 1$.

Note

(1) The equality $[x] = x$ holds if and only if x is an integer.

(2) For each real number x, we can write

$x = [x] + \theta$

for a suitable choice of θ, with $0 \le \theta < 1$.

It then follows that

$x - 1 < [x] \le x$

θ is called fractional part of x and $[x]$, its integral part.

Theorem 18. ***Let x and y be any real numbers. Then the following hold :***

(i) $[x] \le x < [x] + 1$

(ii) $[x + n] = [x] + n$ ***for any integer n.***

(iii) $[x] + [y] \le [x + y] \le [x] + [y] + 1$

(iv) $[x] + [-x] = 0$ ***or*** -1, ***according as x is an integer or not.***

(v) $\left[\frac{x}{n}\right] = \left[\frac{[x]}{n}\right]$ ***for any positive integer n.***

Proof.

(i) Since for any real number x

$$x = [x] + \theta,\ 0 \le \theta < 1$$

$$\therefore \quad [x] \le x < [x] + 1$$

(ii) Since $x = [x] + \theta,\ 0 \le \theta < 1$

$$\therefore \quad x + n = [x] + \theta + n$$

$$\Rightarrow \quad [x + n] = [x] + n$$

(iii) Let $x = [x] + \theta_1,\ 0 \le \theta_1 < 1$

and $\quad y = [y] + \theta_2,\ 0 \le \theta_2 < 1$

$$\therefore \quad x + y = [x] + [y] + \theta_1 + \theta_2$$

$$\Rightarrow \quad [x+y] = \begin{cases} x+y & \text{if } \theta_1 + \theta_2 < 1 \\ x+y+1 & \text{if } \theta_1 + \theta_2 \ge 1 \end{cases} \quad \ldots(1)$$

$$\therefore \quad [x+y] \le [x] + [y] + 1$$

Also $\quad [x] + [y] \le x + y$

$$\Rightarrow \quad [[x] + [y]] \le [x+y] \quad \ldots(2)$$

$$\Rightarrow \quad [x] + [y] \le [x+y]$$

Combining (1) and (2), we have

$$[x] + [y] \le [x+y] \le [x] + [y] + 1.$$

(iv) We now show that

$$[x] + [-x] = \begin{cases} 0 & \text{if } x \text{ is an integer} \\ -1 & \text{if otherwise.} \end{cases}$$

If x is an integer, then

$$[x] = x \text{ and } [-x] = -x$$

$$\therefore \quad [x] + [-x] = 0.$$

Suppose x is not an integer, then

$$x = [x] + \theta,\ 0 \le \theta < 1$$

And $\quad [-x] = [-[x] - \theta]$

$$= -[x] - 1$$

$$\therefore \quad [x] + [-x] = -1.$$

(v) By division algorith, we have

$$[x] = nq + r,\ 0 \le r < n$$

Also, $\quad x = [x] + \theta,\ 0 \le \theta < 1$

$$\therefore \quad \left[\frac{x}{n}\right] = \left[\frac{[x] + \theta}{n}\right]$$

$$= \left[\frac{nq + r + \theta}{n}\right]$$

Since $\quad r < n \Rightarrow r \le n - 1$

$$\Rightarrow \quad r + \theta < n$$

Therefore,

$$\left[\frac{x}{n}\right] = q$$

Also $\left[\dfrac{[x]}{n}\right] = \left[q + \dfrac{r}{n}\right] = q$, the result follows.

Theorem 19. ***Prove that*** $\left[\dfrac{[x/a]}{b}\right] = \left[\dfrac{x}{ab}\right]$.

Proof. Set $[x/a] = s$

$$[s/b] = t.$$

Then $\quad x = as + r_1,\ 0 \le r_1 < a$

and $\quad s = bt + r_2,\ 0 \le r_2 < b$

so that $x = t\,ab + ar_2 + r_1$

and $\quad \left[\dfrac{x}{ab}\right] = t + \left[\dfrac{ar_2 + r_1}{ab}\right]$.

However, max (r_2) is $b - 1$ and max (r_1) is $a - 1$,

and hence max $(ar_2 + r_1) = a\,(b-1) + a - 1$

$$= ab - 1.$$

Consequently, $\left[\dfrac{x}{ab}\right] = t = \left[\dfrac{s}{b}\right] = \left[\dfrac{x/a}{b}\right]$

which proves the required result.

Example 22. *Let x and y be any real numbers such that*

(i) $[x+y]=[x]+[y]$ *and*

(ii) $[-x-y]=[-x]+[-y]$, *then one of x or y is an integer and conversely.*

Solution. Let $x=[x]+\theta_1$ and

$$y=[y]+\theta_2\ ;\ 0<\theta_1,\theta_2<1. \qquad \ldots(1)$$

i.e both x and y are non integers.

By hypothesis in (i),

$$\theta_1+\theta_2<1$$

$$\therefore \quad 0<\theta_1+\theta_2<1$$

Also, $-x=-[x]-\theta_1$ and

$$-y=-[y]-\theta_2 \text{ [from (1)]}$$

$$\Rightarrow \quad [-x-y]=[-[x]-\theta_1-[y]-\theta_2]$$

$$=[-[x]-[y]-[\theta_1+\theta_2]] \qquad \ldots(2)$$

$$=-[x]-[y]-1$$

Moreover,

$$[-x]=-[x]-1,$$

$$[-y]=-[y]-1 \qquad \ldots(3)$$

$$\Rightarrow \quad [-x]+[-y]=-[x]-[y]-2$$

But $\quad [-x-y]=[-x]+[-y]$

$\therefore$ (2) and (3) implies that x and y both cannot be non-integers *i.e* only one of x or y must be integers and other a fraction.

Conversely, if x is an integer and y is any real number, say

$$y=[y]+\theta,\ 0\le\theta<1,$$

then $\quad [x+y]=[x+[y]+\theta]$

$$=x+[y]$$

$$\Rightarrow \quad [x+y]=[x]+[y]$$

and $\quad [-x-y]=[-x-[y]-\theta]$

$$=-x-[y]-1.$$

Also $\quad [-x]+[-y]=-x-[y]-1$

$$\therefore \quad [-x-y]=[-x]+[-y]$$

We proceed similarly if y is an integer and x is not an integer.

Theorem 20. ***If n is a positive integer and p a prime, then the exponent of the highest power of p that divides $n!$ is***

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

where the series is finite, because $[n/p^k]=0$ for $p^k>n$.

Proof. Let us suppose that the first n positive integers divisible by p are $p, 2p, \ldots\ldots, mp$ where m is the largest integer such that $mp\le n$.

In other words, m is the largest integer less than or equal to $\frac{n}{p}$ which is to say $m=[n/p]$.

Thus there are exactly $[n/p]$ multiples of p occuring in the product that defines $n!$ namely

$$p, 2p, \ldots\ldots, \left[\frac{n}{p}\right]p \qquad \ldots(1)$$

The exponent of p in the prime factorization of $n!$ is obtained by adding to the number of integers in equation (1), the number of integers among $1, 2, \ldots\ldots, n$ divisible by p^2, and then the number divisible by p^3, and so on.

By using the above arguments, the integers between 1 and n that are divisible by p^2 are

$$p^2, 2p^2, \ldots\ldots\ldots, \left[\frac{n}{p^2}\right]p^2 \qquad \ldots(2)$$

which are $\left[\frac{n}{p^2}\right]$ in number.

Similarly, $\left[\frac{n}{p^3}\right]$ are again divisible by p :

$$p^3, 2p^3, \ldots\ldots, \left[\frac{n}{p^3}\right]p^3 \qquad \ldots(3)$$

Repeating the above process a finite number of times, we conclude that the total number of times p divides $n!$ is

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

Note

$n! = \prod_{p \le n} p^{\sum_{k=1}^{\infty} [n/p^k]}$ is known as Legendre's formula.

Example 23. *Find the number of zeros with which the decimal representation of 50! terminates.*

Solution. Since the number of times 10 enters into the product 50! so it is enough to find the exponents of 2 and 5 in the prime factorization of 50!

By direct calculation, we have

$$[50/2] + [50/2^2] + [50/2^3] + [50/2^4] + [50/2^5]$$
$$= 25 + 12 + 6 + 3 + 1$$
$$= 47$$

The above theorem tells us that 2^{47} divides 50!, but 2^{48} does not.

Similarly $[50/5] + [50/5^2] = 10 + 2 = 12$ and so the highest power of 5 dividing 50! is 12. This means that 50! ends with 12 zeros.

Theorem 21. ***If n and r are positive integers with $1 \le r < n$, then the bionormal coefficient***

$$\binom{n}{r} = \frac{n!}{r!\,(n-r)!}$$ ***is also an integer.***

Proof. We know that if a and b are arbitrary real numbers, then

$$[a+b] \ge [a] + [b].$$

In particular, for each prime factor p of $r!\,(n-r)!$,

$$\left[\frac{n}{p^k}\right] \ge \left[\frac{r}{p^k}\right] + \left[\frac{(n-r)}{p^k}\right],$$

$k = 1, 2, \ldots\ldots$

Adding these inequalities, we get

$$\sum_{k \ge 1} \left[\frac{n}{p^k}\right] \ge \sum_{k \ge 1} \left[\frac{r}{p^k}\right] + \sum_{k \ge 1} \left[\frac{(n-r)}{p^k}\right] \quad \ldots(1)$$

The L.H.S. of equation (1) gives the exponent of the highest power of the prime p that divides $n!$, whereas the R.H.S. equals the highest power of this prime contained in $r!\,(n-r)!$.

Hence, p appears in the numerator of $n!/r!\,(n-r)!$ at least as many times as it occurs in the denominator.

Since this holds true for every prime divisor of the denominator, $r!\,(n-r)!$ must divide $n!$, making $n! \mid r!\,(n-r)!$ an integer.

Corollary. *For a positive integer r, the product of any r consecutive positive integers is divisible by r!.*

Proof. The product of r consecutive positive integers, the largest of which is n, is

$$n(n-1)(n-2)\ldots\ldots(n-r+1)$$

Now we have

$$n(n-1)(n-2)\ldots\ldots(n-r+1)$$
$$= \left(\frac{n!}{r!\,(n-r)!}\right) r!$$

Since $n!/r!\,(n-r)!$ is an integer by the theorem, "*If n and r are positive integers with* $1 \le r < n$, *then the bionomial coefficient* $\binom{n}{r} = \frac{n!}{r!\,(n-r)!}$ *is also an integer*".

It follows that $r!$ must divide the product $n(n-1)\ldots(n-r+1)$

Thus for a positive integer r, the product of any r consecutive positive integers is divisible by $r!$.

Theorem 22. ***Let f and F be number-theoretic functions such that***

$$F(n) = \sum_{d \mid n} f(d)$$

Then, for any positive integer N,

$$\sum_{n=1}^{N} F(n) = \sum_{k=1}^{N} f(k) \left[\frac{N}{k}\right].$$

Proof. Since we know that

$$\sum_{n=1}^{\infty} F(n) = \sum_{n=1}^{N} \sum_{d \mid n} f(d) \quad \ldots(1)$$

Now we shall collect terms with equal values of $f(d)$ in this double sum.

Let $k \le N$ be a fixed positive integer.

Then the term $f(k)$ appears in $\sum_{d \mid n} f(d)$ if and only if k is a divisor of n,

since each integer has itself as a divisor, the right-hand side of equation (1) includes $f(k)$, at least once.

Now in order to calculate the number of sums $\sum_{d \mid n} f(d)$ in which $f(k)$ occurs as a term, it is sufficient to obtain the number of integers among 1, 2,....., N, which are divisible by k.

There are exactly $[N/k]$ of them :

$k, 2k, 3k, \ldots\ldots, \left[\frac{N}{k}\right]k.$

Thus, for each k such that

$1 \le k \le N$,

$f(k)$ is a term of the sum $\sum_{d \mid n} f(d)$ for $[N/k]$ different positive integers less than or equal to N.

Thus we may rewrite the double sum in equation (1) as

$$\sum_{d=1}^{N} \sum_{d \mid n} f(d) = \sum_{k=1}^{N} f(k) \left[\frac{N}{k}\right]$$

Hence the Proof.

Corollary 1. *If N is a positive integer, then*

$$\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \left[\frac{N}{n}\right]$$

Proof. Since $\tau(n) = \sum_{d \mid n} 1$,

so writing τ for F and taking f to be the constant function $f(n) = 1 \ \forall\ n$,

we get the required result.

Corollary 2. *If N is a positive integer, then*

$$\sum_{n=1}^{N} \sigma(n) = \sum_{n=1}^{N} n \left[\frac{N}{n}\right].$$

Proof. Since, $\sigma(n) = \sum_{d \mid n} d$

so writing σ for F and taking f to be the function

$f(n) = 1 \ \forall\ n$,

we get the required result.

e.g. Let $N = 6$.

The definition of τ gives that $\sum_{n=1}^{6} \tau(n) = 14$

From Corollary 1,

$$\sum_{n=1}^{\infty} \left[\frac{6}{n}\right] = [6] + [3] + [2] + \left[\frac{3}{2}\right] + \left[\frac{6}{5}\right] + [1]$$
$$= 6 + 3 + 2 + 1 + 1 + 1$$
$$= 14$$

Also $\sum_{n=1}^{6} \sigma(n) = 33$

By corollary 2, we have

$$\sum_{n=1}^{6} n \left[\frac{6}{n}\right] = 1\,[6] + 2\,[3] + 3\,[2] + 4\left[\frac{3}{2}\right] + 5\left[\frac{6}{5}\right] + 6\,[1]$$
$$= 1 \cdot 6 + 2 \cdot 3 + 3 \cdot 2 + 4 \cdot 1 + 5 \cdot 1 + 6 \cdot 1$$
$$= 33.$$

Example 24. *Prove that $\frac{n!}{a_1! \cdot a_2! \cdot a_3!}$ is an integer where $a_i \ge 0$ and $n = a_1 + a_2 + a_3$.*

Solution. In order to prove the required result we shall show that every prime divides the numerator to at least as high as exponent as it divides the denominator.

Suppose p is a prime that divides $n!$.

Then its exponent is at most $\sum_{j=1}^{\infty} \left[\frac{n}{p^j}\right]$.

The power of p that divides $a_i!$ is $\sum_{j=1}^{\infty} \left[\frac{a_i}{p^j}\right]$ at most.

To complete, we must show that

$$\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] \ge \sum_{j=1}^{\infty} \left(\left[\frac{a_1}{p^j}\right] + \left[\frac{a_2}{p^j}\right] + \left[\frac{a_3}{p^j}\right]\right)$$

$$\left[\frac{a_1}{p^j}\right]+\left[\frac{a_2}{p^j}\right]+\left[\frac{a_3}{p^j}\right]$$

$$\left[\frac{a_1+a_2+a_3}{p^j}\right]=\left[\frac{n}{p^j}\right] \forall j$$

$$\Rightarrow \sum_{j=1}^{\infty}\left(\left[\frac{a_1}{p^j}\right]+\left[\frac{a_2}{p^j}\right]+\left[\frac{a_3}{p^j}\right]\right)\le\sum_{j=1}^{\infty}\left[\frac{n}{p^j}\right]$$

which gives the required result.

Example 25. *Evaluate the exponent of* 3 *in* 40.

Solution. Since $\left[\frac{40}{3}\right]=13$;

$$\left[\frac{40}{3^2}\right]=4,\left[\frac{40}{3^3}\right]=1$$

and $\left[\frac{40}{3^4}\right]=0$

$\therefore$ the required exponent $=13+4+1=18$.

Example 26. *Evaluate the exponent of* 7 *in* 1000.

Solution. Since $(1000)_7=2626$ is the reresentation of 1000 to base 7, therefore we have

$$e=\frac{1000-(2+6+2+6)}{6}$$

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

$$=\frac{984}{6}=164$$

$\therefore$ $7^{164}\mid(1000)!$ and

$7^{165}\nmid(1000)!$

Example 27. *Find the highest power of* 3 *contained in* 100!

Solution. Here $\left[\frac{100}{3}\right]=33$ is the number that 3 is contained in 100; and the integers are

6, 9,....., 99.

Of these, some contain the factor 3 again viz., 9, 18, 27, 99 and their number is

$$\left[\frac{100}{3^2}\right]=11.$$

Again we see that some 9, 18, 27,.....,99 contain the factor 3 a third time., viz. 27, 54, 81 and their number is

$$\left[\frac{100}{3^3}\right]=3.$$

One number only, 81, contains the factor 3 four times.

Hence the highest power required is $33+11+3+1=48$.

Example 28. *What is the highest power of* 2 *dividing* 533! ? ; *the highest power of* 3 ? ; *the highest power of* 6 ? ; *the highest power of* 12 ? ; *the highest power of* 70 ?

Solution. The highest power of 2 dividing 533! is

$$\left[\frac{533}{2}\right]+\left[\frac{533}{2^2}\right]+\left[\frac{533}{2^3}\right]+\left[\frac{533}{2^4}\right]+\left[\frac{533}{2^5}\right]+\left[\frac{533}{2^6}\right]+\left[\frac{533}{2^7}\right]+\left[\frac{533}{2^8}\right]+\left[\frac{533}{2^9}\right]$$

$$=266+133+66+33+16+8+4+2+1$$

$$=529.$$

To find the highest power of 3 that divides 533!, we compute

$$\left[\frac{533}{3}\right]=177,\left[\frac{177}{3}\right]=59,$$

$$\left[\frac{59}{3}\right]=19,$$

$$\left[\frac{19}{3}\right]=6,\left[\frac{6}{3}\right]=2,\left[\frac{2}{3}\right]=0.$$

Adding we find that

$3^{263}\mid 533!$ and $e_3=263$ but

$3^{264}\mid 533!$

To find the highest power of 6 that divides 533!, we compute e_3 and e_2 since $6=3\times 2$, and hence

$$e_6=\min(529, 263)=263.$$

Similarly, since $12 = 2^2 \times 3$,

$$e_{12} = \min\left(\left[\frac{529}{2}\right], 263\right) = 263$$

Now $e_5 = \left[\frac{533}{5}\right] + \left[\frac{533}{5^2}\right] + \ldots\ldots$

$$= 106 + \left[\frac{106}{5}\right] + \ldots\ldots$$

$$= 106 + 21 + \left[\frac{21}{5}\right] + \ldots\ldots\ldots$$

$$= 106 + 21 + 4 + \left[\frac{4}{5}\right].$$

$$= 106 + 21 + 4 + 0$$

$$= 137.$$

To find e_7, we compute

$$\left[\frac{533}{7}\right] = 76, \left[\frac{76}{7}\right] = 10, \left[\frac{10}{7}\right] = 1$$

and thus $e_7 = 76 + 10 + 1 = 87$.

Example 29. *Find the highest power of* 5 *dividing* 1000!

Solution. The highest power of 5 dividing 1000! is

$$\left[\frac{1000}{5}\right] + \left[\frac{1000}{5^2}\right] + \left[\frac{1000}{5^3}\right] + \left[\frac{1000}{5^4}\right] + \left[\frac{1000}{5^5}\right]$$

$$= 200 + 40 + 8 + 1 + 0$$

$$= 249.$$

Example 30. *Find the highest power of* 7 *dividing* 2000!

Solution. The highest power of 7 dividing 2000! is

$$\left[\frac{2000}{7}\right] + \left[\frac{2000}{7^2}\right] + \left[\frac{2000}{7^3}\right] + \left[\frac{2000}{7^4}\right]$$

$$= 285 + 40 + 5 + 0$$

$$= 330.$$

Example 31. *Prove that the highest power of* n *which is contained in* $(n^j - 1)!$ *is* $(n^j - nj + j - 1)/(n-1)$.

Solution. $e_n = [(n^j - 1)/n] + [(n^j - 1)/n^2] + \ldots + [(n^j - 1)/n^j - 1]$

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

$$= \frac{n^j - 1}{n - 1} - (j - 1), \text{ and etc.}$$

Thus the highest power of n which is contained in $(n^j - 1)!$ is

$$(n^j - nj + j - 1)/(n - 1)$$

Example 32. *Find the highest power of* 3 *dividing* (533)!

Solution. Highest power of 3 dividing (533)!

$$= \left[\frac{533}{3}\right] + \left[\frac{533}{3^2}\right] + \left[\frac{533}{3^3}\right] + \left[\frac{533}{3^4}\right] + \left[\frac{533}{3^5}\right] + \left[\frac{533}{3^6}\right] + \ldots$$

$$= \left[\frac{533}{3}\right] + \left[\frac{533}{9}\right] + \left[\frac{533}{27}\right] + \left[\frac{533}{81}\right] + \left[\frac{533}{243}\right] + \left[\frac{533}{729}\right]$$

$$= 177 + 59 + 19 + 6 + 2 + 0$$

$$= 263$$

Example 33. *Find the highest power of* 9 *that divides* (365)!

Solution. ***Highest power of 3 in*** (365)!

$$= \left[\frac{365}{3}\right] + \left[\frac{365}{3^2}\right] + \left[\frac{365}{3^3}\right] + \left[\frac{365}{3^4}\right] + \left[\frac{365}{3^5}\right] + \left[\frac{365}{3^6}\right] + \ldots$$

$$= \left[\frac{365}{3}\right] + \left[\frac{365}{9}\right] + \left[\frac{365}{27}\right] + \left[\frac{365}{81}\right] + \left[\frac{365}{243}\right] + \left[\frac{365}{729}\right]$$

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

$$= 179.$$

Therefore highest power of 9 (*i.e* 3^2) in (365)!

$$= 89$$

Example 34. *Find the highest power of* 6 *that divides* (245)!

Solution. $6 = 2 \times 3$

Highest power of 2 in (245)!

$$= \left[\frac{245}{2}\right] + \left[\frac{245}{4}\right] + \left[\frac{245}{8}\right] + \left[\frac{245}{16}\right] + \left[\frac{245}{32}\right] + \left[\frac{245}{64}\right] + \left[\frac{245}{128}\right] + \left[\frac{245}{256}\right]$$

$$= 122 + 61 + 30 + 15 + 7 + 3 + 1 + 0$$

$$= 239$$

Highest power of 3 in (245) !

$$= \left[\frac{245}{3}\right] + \left[\frac{245}{9}\right] + \left[\frac{245}{27}\right] + \left[\frac{245}{81}\right] + \left[\frac{245}{243}\right] + \left[\frac{245}{729}\right]$$

$$= 81 + 27 + 9 + 3 + 1 + 0$$

$$= 121$$

Therefore highest power of 6 in (245) !

$$= Min\ \{239, 121\}$$

$$= 121.$$

Example 35. *Find the highest power of* 12 *that divide* (270) !

Solution. Since $12 = 2^2 \times 3$

Highest power of 2 in (270) !

$$= \left[\frac{270}{2}\right] + \left[\frac{270}{4}\right] + \left[\frac{270}{8}\right] + \left[\frac{270}{16}\right] + \left[\frac{270}{32}\right] + \left[\frac{270}{64}\right] + \left[\frac{270}{128}\right] + \left[\frac{270}{256}\right] + \left[\frac{270}{512}\right]$$

$$= 135 + 67 + 33 + 16 + 8 + 4 + 2 + 1 + 0$$

$$= 266$$

Therefore highest power of 4 in (270) ! = 133

Highest power of 3 in (270) !

$$= \left[\frac{270}{3}\right] + \left[\frac{270}{9}\right] + \left[\frac{270}{27}\right] + \left[\frac{270}{81}\right] + \left[\frac{270}{343}\right] + \left[\frac{270}{729}\right]$$

$$= 90 + 30 + 10 + 3 + 1 + 0$$

$$= 134$$

Therefore highest power of 12 in (270) !

$$= Min\ \{133, 134\}$$

$$= 133.$$

Example 36. *Find the highest power of* 15 *that divides* (736) !

Solution. Since $15 = 3 \times 5$

Highest power of 3 in (736) !

$$= \left[\frac{736}{3}\right] + \left[\frac{736}{9}\right] + \left[\frac{736}{27}\right] + \left[\frac{736}{81}\right] + \left[\frac{736}{243}\right] + \left[\frac{736}{729}\right]$$

$$= 245 + 81 + 27 + 9 + 3 + 1$$

$$= 366$$

Highest power of 5 in (736) !

$$= \left[\frac{736}{5}\right] + \left[\frac{736}{25}\right] + \left[\frac{736}{125}\right] + \left[\frac{736}{625}\right]$$

$$= 147 + 29 + 5 + 1$$

$$= 182$$

Therefore highest power of 15 in (736) !

$$= Min\ \{366, 182\}$$

$$= 182.$$

Example 37. *Find the highest power of* 5 *dividing* $\underline{|1000}$ *and the highest power of* 7 *dividing* $\underline{|2000}$.

Solution. The highest power of 5 dividing

$$\underline{|1000} = \left[\frac{1000}{5}\right] + \left[\frac{1000}{5^2}\right] + \left[\frac{1000}{5^3}\right] + \left[\frac{1000}{5^4}\right] + \left[\frac{1000}{5^5}\right] + \ldots\ldots$$

$$= \left[\frac{1000}{5}\right] + \left[\frac{1000}{25}\right] + \left[\frac{1000}{125}\right] + \left[\frac{1000}{625}\right] + \left[\frac{1000}{3125}\right]$$

$$= 200 + 40 + 8 + 1 + 0$$

$$= 249$$

The highest power of 7 dividing

$$\underline{|2000} = \left[\frac{2000}{7}\right] + \left[\frac{2000}{7^2}\right] + \left[\frac{2000}{7^3}\right] + \left[\frac{2000}{7^4}\right] + \ldots\ldots$$

$$= \left[\frac{2000}{7}\right] + \left[\frac{2000}{49}\right] + \left[\frac{2000}{343}\right] + \left[\frac{2000}{2401}\right]$$

$$= 285 + 40 + 5 + 0$$

$$= 330.$$

Example 38. *Find the number of zeros at the end of* $\lfloor 13$.

Solution. $10 = 2 \times 5$

Highest power of 2 in $\lfloor 13$

$$= \left[\frac{13}{2}\right] + \left[\frac{13}{4}\right] + \left[\frac{13}{8}\right] + \left[\frac{13}{16}\right]$$

$$= 6 + 3 + 1 + 0 = 10$$

Highest power of 5 in $\lfloor 13$

$$= \left[\frac{13}{5}\right] + \left[\frac{13}{25}\right]$$

$$= 2 + 0 = 2$$

Therefore highest power of 10 in $\lfloor 13$

$$= Min\{10, 2\}$$

$$= 2$$

Hence there are two zeros at the end of $\lfloor 13$.

Example 39. *Find the number of zeros with which the decimal representation of* 50! *terminates.*

Solution. Highest exponent of 2 dividing 50!

$$= \left[\frac{50}{2}\right] + \left[\frac{50}{2^2}\right] + \left[\frac{50}{2^3}\right] + \left[\frac{50}{2^4}\right] + \left[\frac{50}{25}\right]$$

$$= 25 + 12 + 6 + 3 + 1$$

$$= 47$$

and highest exponent of 5 dividing 50!

$$= \left[\frac{50}{5}\right] + \left[\frac{50}{5^2}\right]$$

$$= 10 + 2$$

$$= 12.$$

Hence 50! ends with min {47, 12}

$$= 12 \text{ zeros.}$$

AN APPLICATION TO THE CALENDAR

In this section we are to determine the day of the week for a given date after the year 1600 in Gregorian calender. Since the leap year is added at the end of February, let us adopt the convenient fiction that each year ends at the end of February.

According to this plan, in the Gregorian year $Y + 1$ are, for convenience, counted as the eleventh and twelfth months of the year Y.

Another convenience is to
by the number 0, 1,....., 6.

Sun	Mon	Tue	V
0	1	2	

The number of days in a c
whereas in leap years there

$$366 \equiv 2 \pmod 7, \text{ d}$$

Since Februarζ 28 is the 3
and $365 \equiv 1 \pmod 7$,
February 28 always falls
Thus if a particular Marc
will be one more, modulo 7,
But if it follows a leap ye
e.g. If D_{1600} is the wee
1601, 1602 and 1603 has
$D_{1600} + 3$ respectively;
$D_{1600} + 5 \pmod 7$

Thus the weekday nur
congruence $D_Y \equiv D_{1600} + ($
between March 1, 1600 an
Let us find L, number
To do this, we count
number of century years, a

Formula to find out
given by

$$L = \left[\frac{Y}{4}\right] - \left[\frac{Y}{100}\right.$$

Example 40. *Obtain the*
Solution. Let us compute

$$L = \left[\frac{1995}{4}\right] -$$

$$= 498 - 19$$

$$= 95$$

Another convenience is to designate the days of the week, Sunday through Saturday, by the number 0, 1,....., 6.

Sun	Mon	Tue	Wed	Thu	Fri	Sat
0	1	2	3	4	5	6

The number of days in a common year is $365 \equiv 1 \pmod 7$,
whereas in leap years there are
$366 \equiv 2 \pmod 7$, days.

Since February 28 is the 365^{th} day of the year
and $365 \equiv 1 \pmod 7$,
February 28 always falls on the same weekday as the previous March 1.

Thus if a particular March 1 immediately follows February 28, its weekday number will be one more, modulo 7, than the weekday number of the previous March!

But if it follows a leap year, February 29, its week day number will be increased by two.

e.g. If D_{1600} is the weekday number for March 1, 1600, then March 1 in the years 1601, 1602 and 1603 has numbers congruent modulo 7 to $D_{1600}+1$ and $D_{1600}+2$, $D_{1600}+3$ respectively; but the number corresponding to March 1, 1604 is $D_{1600}+5 \pmod 7$

Thus the weekday number D_Y for March 1 of any year $Y > 1600$ will satisfy the cobgruence $D_Y \equiv D_{1600} + (Y-1600) + L \pmod 7$ where L is the number of leap year days between March 1, 1600 and March 1 of the year Y.

Let us find L. number of leap year days between 1600 and the year Y.

To do this, we count the number of these years that are divisible by 4, deduct the number of century years, and then add back the number of century years divisible by 400.

Formula to find out the number of leap years between 1600 and every year Y is given by

$$L = \left[\frac{Y}{4}\right] - \left[\frac{Y}{100}\right] + \left[\frac{Y}{400}\right] - 388.$$

Example 40. *Obtain the number of leap years between* 1600 *and* 1995.

Solution. Let us compute

$$L = \left[\frac{1995}{4}\right] - \left[\frac{1995}{100}\right] + \left[\frac{1995}{400}\right] - 388$$

$$= 498 - 19 + 4 - 388$$

$$= 95$$

Note

Number of years n in the internal $1600 < n \le Y$ that are divisible by 4 is given by

$$\left[\frac{Y-1600}{4}\right]=\left[\frac{Y}{4}-400\right]=\left[\frac{Y}{4}\right]-400$$

Likewise, the number of elapsed century years is

$$\left[\frac{Y-1600}{100}\right]=\left[\frac{Y}{100}-16\right]=\left[\frac{Y}{100}\right]-16$$

whereas among those there are

$$\left[\frac{Y-1600}{400}\right]=\left[\frac{Y}{400}-4\right]=\left[\frac{Y}{400}\right]-4$$

century years that are divisible by 400.

Taken together, these statements yield

$$L=\left(\left[\frac{Y}{4}\right]-400\right)-\left(\left[\frac{Y}{100}\right]-16\right)+\left(\left[\frac{Y}{400}\right]-4\right)$$

$$=\left[\frac{Y}{4}\right]-\left[\frac{Y}{100}\right]+\left[\frac{Y}{400}\right]-388.$$

Example 41. *Find the number of leap years between* 1600 *and* 2075.

Solution. Here

$$L=\left[\frac{2075}{4}\right]-\left[\frac{2075}{100}\right]+\left[\frac{2075}{400}\right]-388$$

$$=518-20+5-388$$

$$=115.$$

Note

The formula to find out the week day number n for first of any month is as follows:

$$n \equiv Dy + [(2{\cdot}6)\, m - 0{\cdot}2] - 2 \pmod 7$$

Here m = number of month,

n = number of week day and

$$Dy \equiv 3 - 2c + y + \left[\frac{c}{4}\right] + \left[\frac{y}{4}\right] \pmod 7$$

c = number of centuries,

y = number of years within the century.

e.g.

$$D_{1990} \equiv 3 - (2 \times 19) + 90 + \left[\frac{19}{4}\right] + \left[\frac{90}{4}\right]$$

$$\equiv 3 - 38 + 90 + 4 + 22$$

$$\equiv 81$$

$$\equiv 4 \pmod 7$$

Example 42. *Find the day n for December* 1, 1990.

Solution. Here

$$n \equiv Dy + [(2{\cdot}6)\, m - 0{\cdot}2] - 2 \pmod 7$$

$$\equiv 4 + [(2{\cdot}6)\, 10 - 0{\cdot}2] - 2 \pmod 7$$

$$\equiv 4 + [26 - 0{\cdot}2] - 2 \pmod 7$$

$$\equiv 4 + 25 - 2 \pmod 7$$

$$\equiv 6 \pmod 7$$

So the day is Saturday.

Note

Designate the days of the week as follows :

Sun	Mon	Tue	Wed	Thurs	Fri	Sat
0	1	2	3	4	5	6

Designate the months of a year as follows :

March	April	May	June	July	Aug	Sept	Oct	Nov	Dec	Jan	Feb
1	2	3	4	5	6	7	8	9	10	11	12

Example 43. *Prove that an integer $n > 1$ is prime if and only if $\lfloor n-2 \equiv 1 \pmod n$.*

Solution. Using Wilson's theorem we may get

$$(n-2)\,!\,(n-1) - (n-1) \equiv 0 \pmod n$$

Then, $(n-1)\,[(n-2)\,! - 1] \equiv 0 \pmod n$

But, since $(n-1, n) = 1$.

Therefore $(n-2)\,! - 1 \equiv 0 \pmod n$

$\Rightarrow \quad (n-2)\,! \equiv 1 \pmod n$.

Theorem 23. ***Let m, y, c be as above then week day number is given by***

$$n \equiv d + [(2{\cdot}6)\, m - 0{\cdot}2] - 2c + y + \left[\frac{c}{4}\right] + \left[\frac{y}{4}\right] \pmod 7$$

where d = ***date.***

Example 44. *Find the day of the week on 14 December, 2020.*

Solution. Here

$$n \equiv 14 + [(2\cdot6)\ 11 - 0\cdot2] - 2 \times 20 + 19 + \left[\frac{20}{4}\right] + \left[\frac{19}{4}\right] \pmod 7$$

$$\equiv 14 + 28 - 40 + 19 + 5 + 4$$

$$\equiv 2 \pmod 7$$

Hence 14 December, 2020 is Tuesday.

Example 45. *Find the day of the week for the important dates below :*

(a) November 19, 1863 *(b) April* 18, 1906

(c) November 11, 1918 *(d) October* 24, 1929

(e) June 6, 1944 *(f) February* 15, 1898

Solution. Do yourself.

Ans is :

(a) Thursday (b) Wednesday

(c) Monday (d) Thursday

(e) Tuesday (f) Tuesday.

AN APPLICATION OF CRYPTOGRAPHY

"Cryptography is the art of achieving security by enclosing messages to make them non-readable".

It is the science of making communications through secret codes. In the language of cryptography the codes are called *ciphers*.

(i) Plain text

The original message, that is to be encrypted, is known as plain text.

(ii) Cipher text

The coded message is known as the *cipher text*.

(iii) Encryption

The process of converting plain text into cipher text is known as *encryption* or *enciphering*.

(iv) Decryption

The process of converting cipher text into plaintext is known as *decryption* or *deciphering*.

(v) Cryptography

The art of devising the ciphers, is called *cryptography*.

(vi) Cryptanalysis

The art of breaking the cipher is known as *cryptanalysis*.

(vii) Cryptology

The cryptography and crypanalysis together are called *cryptology*.

Encryption Techniques

Mainly there are two techniques used by which a plain text message can be converted into the corresponding cipher text.

These are as follows :

(i) Substitution cipher (ii) Transposition cipher.

(i) **Substitution Cipher**

In the substitution cipher technique, character of a plain text symbols but disguise them. Following are some techniques using the substitution cipher.

(a) Caesar cipher

This substitution technique was first purposed by the Julius Caesar and is so named as Caesar Cipher.

In this technique, each alphabet in the message is replaced by the third forthcoming alphabet in the series.

Scheme :

Plain text	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Cipher text	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V

T	U	V	W	X	Y	Z
W	X	Y	Z	A	B	C

e.g.

The plain text message Encryption with Caesar Cipher becomes

HQFUBSWLRQZLWK FDHUDU FLSKHU

Plain text	E	N	C	R	Y	P	T	I	O	N		W	I	T	H		C	A	E	S
Cipher text	H	Q	F	U	B	S	W	L	R	Q		Z	L	W	K		F	D	H	V

A	R		C	I	P	H	E	R
D	U		F	L	S	K	H	U

The plain text *RETURN HOME* is transformed to cipher text

UHWXUQKRPH

The Caesar cipher can be described by congruences by assigning numerical values to the alphabets as

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16

Q	R	S	T	U	V	W	X	Y	Z
17	18	19	20	21	22	23	24	25	26

(b) Modified Caesar Cipher

Caesar cipher technique is not so good in practice.

In the modified version of Caesar Cipher each alphabet in the plain text message is replaced by any alphabet.

Now an alphabet '*A*' can be replaced by either '*E*' or by '*F*' or by '*G*' and so on.

When we decide the replacement scheme, it would be constant and remain same for all other alphabets in that message. Since there may be only 26 alphabets in English language, so there are only 25 possibilities of replacement.

(c) Mono-Alphabetic Cipher

The main disadvantage with Caesar Cipher technique is its predictability and Brute-force attack to break the code.

An attack is said to be a Brute-force attack if an attacker attempts to use all possible permutations and combinations for breaking the code and the attacker is assured of a success.

In Mono-Alphabetic Cipher, we do not use the uniform substitution scheme for all the alphabets in a given text message, but we use a random substitution scheme.

In other words, in a given text message, each '*A*' can be replaced by any other alphabet '*B*' through '*Z*', each '*B*' can be replaced by other random alphabet like *A*, *C*, *D* through *Z* except itself.

Thus we can replace an alphabet by one of the other 25 alphabets at random.

This increases the possibilities of permutations or combinations by 26! (*i.e* $26 \times 25 \times 24 \times \ldots\ldots \times 3 \times 2 \times 1$) or 4×1026.

Thus, due to 4×1026 and so, this scheme becomes hard to break.

Definition. *If P is a digit of plain text and C be the corresponding digit of cipher text then the congruence* $C \equiv aP + b \pmod{26}$ *is defined as* ***linear cipher***.

Example 46. *Find the corresponding decrypting congruence of the linear cipher* $C \equiv aP + b \pmod{26}$ *where a and b are integers with* $(a, b) = 1$.

Solution. Given linear cipher is

$$C \equiv aP + b \pmod{26}$$

$\Rightarrow$ $C - aP - b = 26k$ for some $k \in Z$

$\Rightarrow$ $aP = C - b - 26k$

$\equiv C - b \pmod{26}$

Let a' be an integer such that

$$a' \equiv 1 \pmod{26} \quad \ldots(1)$$

Then from (1), we get

$$aa'P \equiv a'(C - b) \pmod{26}$$

Or $P \equiv a'(C - b) \pmod{26}$

Example 47. *Decrypt the message* TZSVIW JQBVMIJ HLMVOOVI *which was produced using linear cipher* $C \equiv 3P + 7 \pmod{26}$

Solution. Given linear cipher is

$$C \equiv 3P + 7 \pmod{26}$$

$\Rightarrow$ $C - 3P - 7 = 26k$ for some $k \in Z$

$\Rightarrow$ $3P = C - 7 - 26k$

$\equiv C - 7 \ (26)$

Since $3 \cdot 9 \equiv 1 \pmod{26}$, $\quad \ldots(1)$

therefore from (1), we get

$$3 \cdot 9P \equiv 9C - 63 \pmod{26}$$

Or $P \equiv 9C - 63 \pmod{26}$

Or $P \equiv 9C - 11 \pmod{26}$ $\quad [\because 63 \equiv 11 \pmod{26}] \quad \ldots(2)$

Numerical equivalent of given cipher text is

20 26 19 22 09 23 10 17 02 22 13 09 10 08 12 13 22 15 15 22 09

Using (2), numerical equivalent plain text is

13 15 04 05 18 14 01 12 07 05 02 18 01 09 19 02 05 20 20 05 18

Therefore Plain text : *MODERN ALGEBRA IS BETTER.*

❑❑❑

CHAPTER 6

EULER'S GENERALIZATION OF FERMAT'S THEOREM

Q 1. Define Euler's ϕ-function.

Or

Define Euler's Phi-function.

Solution. The number of positive integers less than or equal to n and are relatively prime to n is called ***Euler's function*** and is denoted by $\phi(n)$.

e.g. $\phi(1) = 1$ ($\because$ 1 is the only integer ≤ 1 and co-prime to 1)

$\phi(2) = 1$ ($\because$ 1 is the only integer ≤ 2 and co-prime to 2)

$\phi(3) = 2$ ($\because$ 1 and 2 are the only integers ≤ 3 and co-prime to 3)

Note

If p is a prime number, then 1, 2, 3,....., $(p-1)$ are all less than p and coprime to p and $(p-1)$ in total.

$\therefore \quad \phi(p) = p - 1.$

Example 1. *Evaluate $\phi(m)$ for $m = 1, 2, 3,\ldots\ldots, 12$.*

Solution. By definition,

$\phi(1) = 1, \phi(2) = 1$

$\phi(3) = 2$ since $gcd(1, 3) = 1$, $gcd(2, 3) = 1$

$\phi(4) = 2$ since $gcd(1, 4) = 1$, $gcd(3, 4) = 1$.

$\phi(5) = 4$ since $gcd(1, 5) = 1$, $gcd(2, 5) = 1$,

$gcd(3, 5) = 1$ and $gcd(4, 5) = 1$.

$\phi(6) = 2$ since $gcd(1, 6) = 1$, $gcd(5, 6) = 1$

$\phi(7) = 6$ since $gcd(1, 7) = 1$, $gcd(2, 7) = 1$,

$gcd(3, 7) = 1$, $gcd(4, 7) = 1$,

$gcd(5, 7) = 1$, $gcd(6, 7) = 1$

$\phi(8) = 4$ since $gcd(1, 8) = 1$, $gcd(3, 8) = 1$,

$gcd(5, 8) = 1$, $gcd(7, 8) = 1$

Similarly $\phi(9) = 6$,

$\phi(10) = 4$,

$\phi(11) = 10$,

$\phi(12) = 4$.

Theorem 1. ***If p is a prime and $k > 0$, then***

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

Proof. Number of integers from 1 to p^k which are not co-prime to p^k are $p.1, p.2,\ldots\ldots, p.p^{k-1}$.

Total number of such integers which are not coprime to $p^k = p^{k-1}$.

$\therefore \quad \phi(p^k)$ = Number of integers co-prime to p^k and $< p^k$

$= p^k - p^{k-1}$

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

Note

We have

$\phi(9) = \phi(3^2)$

$= 3^2 - 3 = 6$,

the six integers less than and relatively prime to 9 being 1, 2, 4, 5, 7, 8.

Similarly $\phi(16) = \phi(2^4)$

$= 2^4 - 2^3$

$= 16 - 8$

$= 8$

Note

If p is a positive prime and n is any positive integer, then

$$\phi(1) + \phi(p) + \phi(p^2) + \ldots\ldots + \phi(p^{n-1}) + \phi(p^n) = p^n.$$

Proof. We know that $\phi(1) = 1$.

Also we know that

$$\phi(p^k) = p^k - p^{k-1}, \text{ we get}$$
$$\phi(p) = p^1 - p^0 = p - 1$$
$$\phi(p^2) = p^2 - p$$
$$\phi(p^3) = p^3 - p^2$$
$$\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots$$
$$\phi(p^{k-1}) = p^{k-1} - p^{k-2}$$
$$\phi(p^k) = p^k - p^{k-1}$$

Adding all the above relations, we get

$$\phi(1) + \phi(p) + \phi(p^2) + \ldots\ldots + \phi(p^n) = p^n.$$

Lemma

Given integers a, b, c,

$$gcd\,(a, bc) = 1 \text{ if and only if}$$
$$gcd\,(a, b) = 1 \text{ and } gcd\,(a, c) = 1.$$

Proof. First suppose that

$$gcd\,(a, bc) = 1$$

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

Then by definition of gcd $d \mid a$ and $d \mid b$,

whence $d \mid a$ and $d \mid bc$.

This implies that

$$gcd\,(a, bc) \geq d,$$

which shows that $d = 1$

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

Conversely, $gcd\,(a, b) = 1 = gcd\,(a, c)$.

Let us assume that $gcd\,(a, bc) = d_1 > 1$.

Then d_1 must have a prime divisor p.

Since $d_1 \mid bc$,

It follows that $p \mid bc$

$\Rightarrow$ $p \mid b$ or $p \mid c$.

If $p \mid b$, then we have

$gcd\,(a, b) \geq p$,

which leads to a contradiction.

Similarly, if $p \mid c$, then we have

$gcd\,(a, c) \geq p$,

which again leads to a contradiction.

Thus $d_1 = 1$

Hence the Proof.

Theorem 2. ***The function ϕ is multiplicative function.***

Or

If m and n are relatively prime positive integers, then prove that $\phi(mn) = \phi(m)\,\phi(n)$.

Or

Show that the Euler's PHI-function is multiplicative function.

Or

Prove that Euler's ϕ function is a multiplicative function.

Proof. Since $\phi(1) = 1$, the result is trivially true, if either $m = 1$ or $n = 1$.

Thus we can suppose that $m > 1$ and $n > 1$.

Then $\phi(mn)$ is the number of integers in the set

$$\{0, 1, 2, \ldots\ldots, mn - 1\} \quad \ldots(1)$$

which are prime to mn.

The mn integer in the set (1), in view of the theorem of division algorithm, be uniquely represented in the form $mq + r$ such that

$$0 \leq q \leq (n - 1) \text{ and } 0 \leq r \leq (m - 1).$$

Since we know that

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

where a, b, k are integers, so we have

$$gcd\,(mq + r, m) = gcd\,(r, m).$$

Thus $gcd\,(mq + r, m) = 1$ iff $gcd\,(r, m) = 1$.

The definition of $\phi(m)$ claims that there exist $\phi(m)$ values of r satisfying the condition that $gcd\,(r, m) = 1$.

Let these $\phi(m)$ values be denoted by $r_1, r_2, \ldots\ldots, r_{\phi(m)}$.

Now consider the n distinct integers ...(2)

$$x_q = mq + r_1 \; (q = 0, 1, 2, \ldots\ldots, n - 1)$$

each of which is a prime to m.

This claims that no two of these have the same principal remainder with respect to n.

For this suppose that x_{q_1} and x_{q_2} $(q_1 \neq q_2)$ have the same remainder.

Then $n \mid (x_{q_1} - x_{q_2})$

Now from (2), we have

$$x_{q_1} = mq_1 + r_1$$

and $$x_{q_2} = mq_2 + r_1$$

Subtracting (3) and (4), we get

$$x_{q_1} - x_{q_2} = m(q_1 - q_2)$$

Since $n \mid (x_{q_1} - x_{q_2})$

$\Rightarrow$ $n \mid m(q_1 - q_2)$

But $gcd(n, m) = 1$

$\therefore$ $n \mid (q_1 - q_2)$

But $0 \leq q_1 \leq n - 1 < n$

$\Rightarrow$ $0 \leq q_1 < n$

and $0 \leq q_2 < n$

$\therefore$ $q_1 - q_2 < n$

(As we know that if $a \mid b$ and $b < a$, then $b = 0$)

$\therefore$ $q_1 = q_2$

which leads to a contradiction.

Thus x_{q_1} and x_{q_2} have different principal remainders with respect to n.

It follows in view of the theorem of division algorithm that n integers denoted by (2) can in some order, be expressed in the form

$nk_s + s$ $(s = 0, 1, 2, \ldots\ldots, n-1)$ where $k_0, k_1, \ldots\ldots, k_{n-1}$ are non-negative integers.

Now $gcd(a + kb, b) = gcd(a, b)$

implies that

$$gcd(nk_s + s, n) = 1 \text{ iff } gcd(s, n) = 1.$$

Thus there exists $\phi(n)$ integers in the set (2) which are prime to n.

Therefore there are $\phi(n)$ integers in the set (1) with principal remainder r_1 with respect to m which are prime to m and n, and therefore prime to mn.

$[\because gcd(r, m) = 1$ and $gcd(r, n) = 1 \Rightarrow gcd(r, mn) = 1]$

By applying the same argument to each of the other integers $r_2, r_3, \ldots\ldots, r_{\phi(m)}$ in place of r_1 it follows that there are $\phi(m)\,\phi(n)$ integers in the set (1) which are prime to mn.

Hence $\phi(mn) = \phi(m)\,\phi(n)$

Justification

The formula $\phi(mn) = \phi(m)\,\phi(n)$ is applicable only when

$$gcd(m, n) = 1.$$

e.g. we have

$\phi(20) = 8$ since 1,3,7,9,11,13,17, 19 are the only eight integers which are less than 20 and are relatively prime to 20.

Now $20 = 10 \cdot 2$ and 10 and 2 are not relatively prime.

We have

$$\phi(10) = 4 \text{ and } \phi(2) = 1$$

Thus we see that

$$\phi(20) = \phi(10 \cdot 2) \neq \phi(10) \cdot \phi(2)$$

i.e $8 \neq 4 \cdot 1$

Also we can write

$20 = 4 \cdot 5$ where 4 and 5 are relatively prime.

We have

$$\phi(5) = 4 \text{ and } \phi(4) = 2$$

Thus we see that

$$\phi(20) = \phi(4 \cdot 5) = \phi(4) \cdot \phi(5)$$

i.e $8 = 2 \cdot 4 = 8$ which is true.

Theorem 3. ***If the integer $n > 1$ has the prime factorization***

$$n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r} \text{ then}$$

$$\phi(n) = (p_1^{k_1} - p_1^{k_1 - 1})(p_2^{k_2} - p_2^{k_2 - 1}) \ldots\ldots (p_r^{k_r} - p_r^{k_r - 1})$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\ldots\left(1 - \frac{1}{p_r}\right).$$

Or

For any positive integer $n > 1$, prove that

$$\phi(n) = n \prod_{p_i \mid n} \left(1 - \frac{1}{p_i}\right).$$

Proof. Since $p_1, p_2, \ldots\ldots, p_r$ are distinct prime factors of n

$$\therefore \quad n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}$$

$$\therefore \quad \phi(n) = \phi(p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r})$$

$$= \phi(p_1^{k_1}) \phi(p_2^{k_2}) \ldots\ldots \phi(p_r^{k_r})$$

[$\because p_1, p_2, \ldots\ldots, p_r$ are distinct primes and hence are co-prime to each other and $\phi(ab) = \phi(a)\phi(b)$ if a and b are co-prime to each other]

Thus $$\phi(n) = p_1^{k_1}\left(1 - \frac{1}{p_1}\right) p_2^{k_2}\left(1 - \frac{1}{p_2}\right) \ldots\ldots p_r^{k_r}\left(1 - \frac{1}{p_r}\right)$$

$$= p_1^{k_1} \cdot p_2^{k_2} \ldots\ldots p_r^{k_r}\left(1 - \frac{1}{p_1}\right) \ldots\ldots \left(1 - \frac{1}{p_r}\right)$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots\ldots \left(1 - \frac{1}{p_r}\right) \qquad (\because n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r})$$

Example 2. *Find the number of positive integers < 3600 that are relatively prime to 3600.*

Solution. Since $3600 = 2^4 \cdot 3^2 \cdot 5^2$

$$\phi(3600) = \phi(2^4 \times 3^2 \times 5^2)$$

$$= \phi(2^4)\,\phi(3^2)\,\phi(5^2)$$

$$= 2^4\left(1 - \frac{1}{2}\right) \cdot 3^2\left(1 - \frac{1}{3}\right) \cdot 5^2\left(1 - \frac{1}{5}\right)$$

$$\left[\because \phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right) \ldots\ldots \left(1 - \frac{1}{p_m}\right)\right]$$

$$= 2^4 \cdot 3^2 \cdot 5^2\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$$

$$= 3600 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5}$$

$$= 960.$$

Theorem 4. *Let n be any integer > 2. Then $\phi(n)$ is even.*

Proof. Let us first assume that n is a power of 2.

Let us take $n = 2^k$, with $k \geq 2$.

By the theorem, "If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}$, then

$$\phi(n) = (p_1^{k_1} - p_1^{k_1 - 1})(p_2^{k_2} - p_2^{k_2 - 1}) \ldots\ldots (p_r^{k_r} - p_r^{k_r - 1})$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots\ldots \left(1 - \frac{1}{p_r}\right).$$

we have

$$\phi(n) = \phi(2^k)$$

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

$$= 2^{k-1}$$

$$= \text{an even integer.}$$

If n is not a power of 2, then it is divisible by an odd prime p.

Therefore we may write $n = p^k m$ where $k \geq 1$

and $\quad gcd(p^k, m) = 1.$

Since ϕ is a multiplicative function so we have

$$\phi(n) = \phi(p^k)\,\phi(m)$$

$$= p^{k-1}\,\phi(m)$$

which again is even because $2 \mid p - 1$.

Alternative Proof

By fundamental theorem of arithmetic,

$$n = 2^{k_0} p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}, \; p_i \text{ are distinct odd primes,}$$

integers $k_i \geq 0$, $0 \leq i \leq r$.

Now if $k_i \geq 1$ at least for one i, then $\phi(p_i^{k_i}) = p_i^{k_i} - p_i^{k_i - 1}$, is always an even integer.

Since ϕ is a multiplicative function, so

$$\phi(n) = \phi(2^{k_0})\,\phi(p_1^{k_1}) \ldots\ldots \phi(p_r^{k_r})$$

$$= (2^{k_0} - 2^{k_0-1})(p_1^{k_1} - p_1^{k_1-1}) \ldots\ldots (p_r^{k_r} - p_r^{k_r-1})$$

and $n > 2$, either $k_0 \geq 2$ or at least one $k_i \geq 1$;

consequently $\phi(n)$ is even.

Theorem 5. Prove that $\phi(n)$ is an even integer for $n > 2$.

Proof. Two cases arise :

Case I When n is a power of 2.

Let $n = 2^k$ where $k \geq 2$

Then $\phi(n) = 2^k\left(1 - \frac{1}{2}\right)$ $(\because n > 2)$

$= 2^{k-1}$

which is clearly an even integer.

Case II When n is not a power of 2.

Let $n = p^k m$ where p is an odd prime and $(p^k, m) = 1$

$\therefore \quad \phi(n) = \phi(p^k m)$

$= \phi(p^k)\,\phi(m)$

$= (p^k - p^{k-1})\,\phi(m)$

$= p^{k-1}(p-1)\,\phi(m)$

which is also an even integer as $(p-1)$ is even.

Example 3. *Evaluate* $\phi(450)$.

Solution. Since $450 = 2 \cdot 3^2 \cdot 5^2$

$\therefore \quad \phi(450) = \phi(2)\,\phi(3^2)\,\phi(5^2)$

$= 1 \cdot (3^2 - 3)(5^2 - 5)$

$= 1 \cdot 6 \cdot 20$

$= 120.$

Example 4. *Calculate* $\phi(36{,}000)$.

Solution. Since $36000 = 2^6 \cdot 3^2 \cdot 5^4$

$\therefore \quad \phi(36000) = \phi(2^6) \cdot \phi(3^2)\,\phi(5^4)$

$= 2^6\left(1 - \frac{1}{2}\right) \cdot 3^2\left(1 - \frac{1}{3}\right) \cdot 5^4\left(1 - \frac{1}{5}\right)$

$\left[\because \phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_m}\right)\right]$

$= 2^6 \cdot 3^2 \cdot 5^4\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$

$= 36000 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5}$

$= 9600.$

Example 5. Calculate $\phi(5040)$.

Solution. Since $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 9$

$\therefore \quad \phi(5040) = \phi(2^4) \cdot \phi(3^2) \cdot \phi(5) \cdot \phi(9)$

$= 2^4\left(1 - \frac{1}{2}\right) \cdot 3^2\left(1 - \frac{1}{3}\right) \cdot 4 \cdot 6$ $(\because \phi(5) = 4 \text{ and } \phi(9) = 6)$

$= 2^4 \cdot 3^2 \cdot 4 \cdot 6 \cdot \frac{1}{2} \cdot \frac{2}{3}$

$= 1152.$

Example 6. Calculate $\phi(1001)$.

Solution. Since $1001 = 7 \cdot 11 \cdot 13$

$\therefore \quad \phi(1001) = \phi(7) \cdot \phi(11) \cdot \phi(13)$

But $\phi(7) = 6$ as $gcd(1, 7) = 1$, $gcd(2, 7) = 1$,

$gcd(3, 7) = 1$, $gcd(4, 7) = 1$, $gcd(5, 7) = 1$ and $gcd(6, 7) = 1$

$\phi(11) = 10$ as $gcd(1, 11) = 1$, $gcd(2, 11) = 1$,

$gcd(3, 11) = 1$, $gcd(4, 11) = 1$,

$gcd(5, 11) = 1$, $gcd(6, 11) = 1$, $gcd(7, 11) = 1$, $gcd(8, 11) = 1$, $gcd(9, 11) = 1$,

$gcd(10, 11) = 1$

Similarly $\phi(13) = 12$

$\therefore \quad \phi(1001) = 6 \times 10 \times 12$

$= 720.$

Example 7. If n has distinct odd prime factors, prove that $2^k \mid \phi(n)$.

Solution. Let $n = 3 \cdot 5$ then

$\phi(n) = \phi(3 \cdot 5)$

$$= \phi(3)\,\phi(5)$$
$$= 2 \cdot 4$$
$$= 2^2 \cdot 2$$

and hence $2^2 \mid \phi(n)$.

Again $n = 3 \cdot 5 \cdot 7$.

Hence $\phi(n) = \phi(3 \cdot 5 \cdot 7)$

$$= \phi(3)\,\phi(5)\,\phi(7)$$
$$= 2 \cdot 4 \cdot 6$$
$$= 2^3 \cdot 6 \text{ and so}$$

$2^3 \mid \phi(n)$.

Now let $n = p_1 p_2 \ldots\ldots p_k$.

Then $\phi(n) = p_1 p_2 \ldots\ldots p_k \left(\frac{p_1 - 1}{p_1}\right) \ldots\ldots \left(\frac{p_k - 1}{p_k}\right)$

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

By hypothesis $p_1, p_2, \ldots\ldots, p_k$ are all distinct prime, and hence

$$p_1 - 1, p_2 - 1, \ldots\ldots, p_k - 1$$

are all even, that is, each of $p_1 - 1, p_2 - 1, \ldots\ldots, p_k - 1$ containts a factor of 2.

Therefore the product $(p_1 - 1)(p_2 - 1) \ldots\ldots (p_k - 1)$ contains a factor of 2^k.

Therefore, the assertion

$2^k \mid \phi(n)$ follows.

Example 8. *For positive integers m and n, where*

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

show that $\phi(m)\,\phi(n) = \phi(mn)\,\frac{\phi(d)}{d}$.

Solution. $\dfrac{\phi(mn)}{\phi(m)\,\phi(n)}$

$$= mn \prod_{p \mid mn} \left(1 - \frac{1}{p}\right) \Bigg| m \prod_{p \mid m} \left(1 - \frac{1}{p}\right) n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

$$= \prod_{p \mid m_1 n_1 d^2} \left(1 - \frac{1}{p}\right) \Bigg| \prod_{p \mid m_1 d} \left(1 - \frac{1}{p}\right) \prod_{p \mid n_1 d} \left(1 - \frac{1}{p}\right)$$

$$= \frac{\prod_{p \mid m_1} \left(1 - \frac{1}{p}\right) \prod_{p \mid n_1} \left(1 - \frac{1}{p}\right) \prod_{p \mid d^2} \left(1 - \frac{1}{p}\right)}{\prod_{p \mid m_1} \left(1 - \frac{1}{p}\right) \prod_{p \mid d} \left(1 - \frac{1}{p}\right) \prod_{p \mid n_1} \left(1 - \frac{1}{p}\right) \prod_{p \mid d} \left(1 - \frac{1}{p}\right)}$$

$$= \prod_{p \mid d} \left(1 - \frac{1}{p}\right) \Bigg| \prod_{p \mid d} \left(1 - \frac{1}{p}\right) \prod_{p \mid d} \left(1 - \frac{1}{p}\right)$$

$$= 1 \Bigg| \prod_{p \mid d} \left(1 - \frac{1}{p}\right)$$

$$= d \mid d \prod_{p \mid d} \left(1 - \frac{1}{p}\right)$$

$$= d \mid \phi(d)$$

$$\Rightarrow \quad \frac{\phi(mn)}{\phi(m)\,\phi(n)} = \frac{d}{\phi(d)}$$

$$\Rightarrow \quad \phi(m)\,\phi(n) = \phi(mn)\,\frac{\phi(d)}{d}$$

Example 9. *Find all solutions of* $\phi(n) = 24$.

Solution. Here $24 = 2 \times 12, 4 \times 6, 8 \times 3, 24 \times 1$.

Now $2 \times 12 = \phi(3)\,\phi(13)$

$$= \phi(39),$$

so $n = 39$.

Also $2 \times 12 = \phi(4)\,\phi(13)$

$$= \phi(52),$$

and hence $n = 52$.

Again $\phi(6) = 2$ and so

$$n = 13 \times 6 = 78.$$

Thus $\phi(n) = 24 \Rightarrow n = 39, 52, 78$

Now $\phi(7) = 6$ but $\phi(5) = 4$,

$\phi(8) = 4$, $\phi(10) = 4$, $\phi(12) = 4$.

Hence $\phi(n) = 4 \times 6 = \phi(5)\,\phi(7)$

$\Rightarrow \quad n = 35, 56, 70, 84.$

There exist no integer n, such that

$$\phi(n) = 3.$$

Therefore to consider the factor 8×3 is out of question.

Hence all solutions are

35, 39, 45, 52, 56, 70, 72, 78, 84, 90.

Example 10. *Show that the equation $\phi(n) = \phi(n+2)$ is satisfied by $n = 2(2p-1)$ where p and $2p-1$ are both odd primes.*

Solution. Let p and $2p-1$ be odd primes and $n = 2(2p-1)$.

Then
$$\begin{aligned}\phi(n) &= \phi(2(2p-1)) \\ &= \phi(2)\,\phi(2p-1) \\ &= (2-1)(2p-1-1) \\ &= 1 \cdot (2p-2) \\ &= 2(p-1)\end{aligned}$$

and
$$\begin{aligned}\phi(n+2) &= \phi(4p-2+2) \\ &= \phi(4p) \\ &= \phi(2^2 p) \\ &= \phi(2^2)\,\phi(p) \\ &= (2^2-2)(p-1) \\ &= 2(p-1)\end{aligned}$$

From (1) and (2), we get

$$\phi(n) = \phi(n+2).$$

Example 11. *If n and $n+2$ both primes, then show that*

$$\phi(n+2) = \phi(n) + 2.$$

Solution. We have

$$\begin{aligned}\phi(n+2) &= (n+2-1) \quad [\because \phi(p) = p-1 \text{ if } p \text{ is prime}] \\ &= (n+1)\end{aligned}$$

Also $\phi(n) + 2 = n - 1 + 2 = n + 1$

From (1) and (2), we get

$$\phi(n+2) = \phi(n) + 2.$$

Example 12. *If n is an odd integer, then $\phi(2n) = \phi(n)$.*

Solution. Since it is given that n is an odd integer, therefore, it is relatively prime to 2, i.e. $(2, n) = 1$.

Thus,
$$\begin{aligned}\phi(2n) &= \phi(2)\,\phi(n) \\ &= (2-1)\,\phi(n) \\ &= \phi(n).\end{aligned}$$

Example 13. *If every prime that divides n, also divides m, then*

$$\phi(mn) = n\,\phi(m).$$

Solution. We know that every prime divisor of n is also a prime divisor of m, therefore, we can write

$$n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}$$

and
$$m = p_1^{l_1} p_2^{l_2} \ldots\ldots p_r^{l_r} p_{r+1}^{l_{r+1}} \ldots\ldots p_t^{l_t}$$

where all p_i are prime, k_i, l_i are integers greater than or equal to 1 and $t \geq r$.

Now,
$$\begin{aligned}\phi(mn) &= \phi(p_1^{k_1+l_1} p_2^{k_2+l_2} \ldots\ldots p_r^{k_r+l_r} p_{r+1}^{l_{r+1}} \ldots p_t^{l_t}) \\ &= \phi(p_1^{k_1+l_1}) \cdot \phi(p_2^{k_2+l_2}) \ldots\ldots \phi(p_r^{k_r+l_r}) \cdot \phi(p_{r+1}^{l_{r+1}}) \ldots \phi(p_t^{l_t}) \\ &= (p_1^{k_1+l_1} - p_1^{k_1+l_1-1})(p_2^{k_2+l_2} - p_2^{k_2+l_2-1}) \\ &\qquad \ldots\ldots (p_r^{k_r+l_r} - p_r^{k_r+l_r-1}) \phi(p_{r+1}^{l_{r+1}}) \ldots \phi(p_t^{l_t}) \\ &= p_1^{k_1} \cdot p_2^{k_2} \ldots\ldots p_r^{k_r} (p_1^{l_1} - p_1^{l_1-1})(p_2^{l_2} - p_2^{l_2-1}) \\ &\qquad \ldots\ldots (p_r^{l_r} - p_r^{l_r-1}) \phi(p_{r+1}^{l_{r+1}}) \ldots \phi(p_t^{l_t}) \\ &= n\,\phi(p_1^{l_1})\,\phi(p_2^{l_2}) \ldots \phi(p_t^{l_t}) \\ &= n\,\phi(m).\end{aligned}$$

Note

Taking $m = n$, we get

$$\phi(n^2) = n\,\phi(n).$$

Example 14. *Find all integers n such that $10 \mid \phi(n)$.*

Solution. Let $n = 11^k$ where k is a positive integer.

Then
$$\begin{aligned}\phi(n) &= \phi(11^k) \\ &= 11^k - 11^{k-1} \\ &= 11^{k-1}(11-1)\end{aligned}$$

There exist no integer n, such that

$$\phi(n) = 3.$$

Therefore to consider the factor 8×3 is out of question.

Hence all solutions are

35, 39, 45, 52, 56, 70, 72, 78, 84, 90.

Example 10. *Show that the equation $\phi(n) = \phi(n+2)$ is satisfied by $n = 2(2p-1)$ whenever p and $2p-1$ are both odd primes.*

Solution. Let p and $2p-1$ be odd primes and $n = 2(2p-1)$.

Then $\phi(n) = \phi(2(2p-1))$

$$= \phi(2)\,\phi(2p-1)$$
$$= (2-1)(2p-1-1)$$
$$= 1 \cdot (2p-2)$$
$$= 2(p-1)$$

and $\phi(n+2) = \phi(4p-2+2)$ ...(1)

$$= \phi(4p)$$
$$= \phi(2^2 p)$$
$$= \phi(2^2)\,\phi(p)$$
$$= (2^2-2)(p-1)$$
$$= 2(p-1) \quad \text{...(2)}$$

From (1) and (2), we get

$$\phi(n) = \phi(n+2).$$

Example 11. *If n and $n+2$ both primes, then show that*

$$\phi(n+2) = \phi(n) + 2.$$

Solution. We have

$$\phi(n+2) = (n+2-1) \quad [\because \phi(p) = p-1 \text{ if } p \text{ is prime}] \quad \text{...(1)}$$
$$= (n+1) \quad \text{...(2)}$$

Also $\phi(n) + 2 = n - 1 + 2 = n + 1$

From (1) and (2), we get

$$\phi(n+2) = \phi(n) + 2.$$

Example 12. *If n is an odd integer, then $\phi(2n) = \phi(n)$.*

Solution. Since it is given that n is an odd integer, therefore, it is relatively prime to 2

i.e. $(2, n) = 1$.

Thus, $\phi(2n) = \phi(2)\,\phi(n)$

$$= (2-1)\,\phi(n)$$
$$= \phi(n).$$

Example 13. *If every prime that divides n, also divides m, then*

$$\phi(mn) = n\,\phi(m).$$

Solution. We know that every prime divisor of n is also a prime divisor of m, therefore, we can write

$$n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}$$

and $m = p_1^{l_1} p_2^{l_2} \ldots\ldots p_r^{l_r} p_{r+1}^{l_{r+1}} \ldots\ldots p_t^{l_t}$

where all p_i are prime, k_i, l_i are integers greater than or equal to 1 and $t \geq r$.

Now, $\phi(mn) = \phi(p_1^{k_1+l_1} p_2^{k_2+l_2} \ldots\ldots p_r^{k_r+l_r} p_{r+1}^{l_{r+1}} \ldots\ldots p_t^{l_t})$

$$= \phi(p_1^{k_1+l_1}) \cdot \phi(p_2^{k_2+l_2}) \ldots\ldots \phi(p_r^{k_r+l_r}) \cdot \phi(p_{r+1}^{l_{r+1}}) \ldots\ldots \phi(p_t^{l_t})$$
$$= (p_1^{k_1+l_1} - p_1^{k_1+l_1-1})(p_2^{k_2+l_2} - p_2^{k_2+l_2-1})$$
$$\ldots\ldots (p_r^{k_r+l_r} - p_r^{k_r+l_r-1})\,\phi(p_{r+1}^{l_{r+1}}) \ldots\ldots \phi(p_t^{l_t})$$
$$= p_1^{k_1} \cdot p_2^{k_2} \ldots\ldots p_r^{k_r} (p_1^{l_1} - p_1^{l_1-1})(p_2^{l_2} - p_2^{l_2-1})$$
$$\ldots\ldots (p_r^{l_r} - p_r^{l_r-1})\,\phi(p_{r+1}^{l_{r+1}}) \ldots\ldots \phi(p_t^{l_t})$$
$$= n\,\phi(p_1^{l_1})\,\phi(p_2^{l_2}) \ldots\ldots \phi(p_t^{l_t})$$
$$= n\,\phi(m).$$

Note

Taking $m = n$, we get

$$\phi(n^2) = n\,\phi(n).$$

Example 14. *Find all integers n such that $10 \mid \phi(n)$.*

Solution. Let $n = 11^k$ where k is a positive integer.

Then $\phi(n) = \phi(11^k)$

$$= 11^k - 11^{k-1}$$
$$= 11^{k-1}(11-1)$$

$$= 11^{k-1} \cdot 10$$

i.e $10 \mid \phi(n)$.

Therefore there are infinitely many integers of the form $n = 1 \overbrace{1 \ldots 1}^{k}$; $k \geq 1$ for which $10 \mid \phi(n)$.

Theorem 6. ***Prove that*** $\phi(mn) = n\,\phi(m)$ ***if every prime that divides*** n ***also divides*** m.

Proof. Let us assume that

$$n = \prod_{i=1}^{j} p_i^{g_i}$$

Then $m = \prod_{i=1}^{s} p_i^{h_i} \prod_{k=1}^{m} q_k^{l_k}$.

Now $\phi(nm) = \phi\left(\prod_{i=1}^{j} p_i^{g_i+h_i} \prod_{k=1}^{m} q_k^{l_k}\right)$

$$= \prod_{i=1}^{j} p_i^{g_i+h_i-1} \prod_{k=1}^{m} q_k^{l_k-1} \prod_{i=1}^{j} (p_i - 1) \prod_{k=1}^{m} (q_k - 1).$$

$$= \prod_{i=1}^{j} p_i^{g_i} \prod_{i=1}^{j} p_i^{h_i-1} (p_i - 1) \prod_{k=1}^{m} q_k^{l_k-1} (q_k - 1)$$

$$= \prod_{i=1}^{j} p_i^{g_i} \phi\left(\prod_{i=1}^{j} p_i^{h_i}\right) \phi\left(\prod_{k=1}^{m} q_k^{l_k}\right)$$

$$= \prod_{i=1}^{j} p_i^{g_i} \phi\left(\prod_{i=1}^{j} p_i^{h_i} \prod_{k=1}^{m} q_k^{l_k}\right)$$

$$= n\phi(m).$$

Example 15. *If* p *and* q *are any two positive integers, show that* $(pq)!$ *are divisible by* $(p!)^q\, q!$ *and by* $(q!)^p \cdot p!$

Solution. (by induction).

Suppose that

$$(p!)^{q-1} \cdot (q-1)! \mid (p(q-1))!$$

Moreover,

$$\frac{(pq)!}{(p!)^q \cdot q!} \div \frac{(p(q-1))!}{(p!)^{q-1}(q-1)!} = \frac{(pq)!}{(pq-p)!} \cdot \frac{(q-1)!}{p!\,q!}$$

$$= \frac{pq(pq-1)(pq-2)\ldots\text{to } p \text{ factors}}{pq(p-1)!}$$

$$= \frac{(pq-1)(pq-2)\ldots p-1 \text{ factors}}{(p-1)!}$$

= integer.

But $\frac{p!}{p!1!}$ is an integer; and so on.

Example 16. *Assuming the result* $\sum_{d \mid n} \phi(d) = n$, *show that* $\sum (-1)^d \phi(d) = n - 2m$, *where* m *is the greatest odd divisor of* n.

Solution.

$$\sum (-1)^d \phi(d) = \phi(d_1) + \phi(d_2) - \phi(d_3) + \phi(d_4) - \ldots\ldots$$

where d_1, d_3, d_5 are odd divisors of n.

$$= \phi(d_1) + \phi(d_2) + \phi(d_3) + (d_4) + \ldots\ldots - 2\phi(d_1) - 2\phi(d_2) - \ldots\ldots$$

$$= n - 2m.$$

Example 17. *For what values of* m *is* $\phi(m)$ *odd ?*

Solution. If $m > 2$, $\phi(m)$ is even

($\because$ if $m > 2$, then $\phi(m)$ is even)

Also $\phi(1) = 1$

and $\phi(2) = 1$

$\therefore$ Only for $m = 1$, $m = 2$, $\phi(m)$ is odd.

Example 18. *Prove that* $\phi(m^2) = m\,\phi(m)$ *for every positive* n.

Solution. Since n is a positive integer.

$\therefore$ $n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}$

where $p_1, p_2, \ldots\ldots, p_r$ are distinct primes

$\therefore$ $m^2 = p_1^{2k_1} \cdot p_2^{2k_2} \ldots\ldots p_r^{2k_r}$

$\therefore$ $\phi(m^2) = m^2\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\ldots\left(1 - \frac{1}{p_r}\right)$ $\left[\because \phi(n) = \phi(p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r})\right]$

$$= m\left[m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\ldots\left(1 - \frac{1}{p_r}\right)\right]$$

Or $\phi(m^2) = m\phi(m)$.

Example 19. If n is a composite number, then $\phi(n) \le n - \sqrt{n}$.

Solution. Let $n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}$, where p_1 is the smallest prime.

Then $$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

$$\le n\left(1-\frac{1}{p_1}\right)$$

$$\le n\left(1-\frac{1}{\sqrt{n}}\right) = n - \sqrt{n}$$

Hence $\phi(n) \le n - \sqrt{n}$.

Lemma

Let $n > 1$ ***and gcd*** $(a, n) = 1$. ***If*** $a_1, a_2, \ldots\ldots, a_{\phi(n)}$ ***are the positive integers less than and relatively prime to n, then***

$aa_1, aa_2, \ldots\ldots, aa_{\phi(n)}$ ***are congruent modulo n to***

$a_1, a_2, \ldots\ldots\ldots, a_{\phi(n)}$ ***in some order.***

Proof. Let us assume that no two of the integers

$$aa_1, aa_2, \ldots\ldots, aa_{\phi(n)}$$

are congruent modulo n.

For if $aa_i \equiv aa_j \pmod n$, with $1 \le i \le j \le \phi(n)$,

then the cancellation law gives

$$a_i \equiv a_j \pmod n,$$

and thus $a_i = a_j$, a contradiction.

Furthermore, since $gcd(a_i, n) = 1$ for all i and

$$gcd(a, n) = 1,$$

then by lemma, "*given integers a, b, c, gcd* $(a, bc) = 1$ *if and only if gcd* $(a, b) = 1$ *and gcd* $(a, c) = 1$," each of the aa_i is relatively prime to n.

Fixing on a particular aa_i, there exists a unique integer b, where $0 \le k < n$, for which

$$aa_i \equiv b \pmod n.$$

Since $gcd(b, n) = gcd(aa_i, n) = 1$

b must be one of the integers $a_1, a_2, \ldots\ldots, a_{\phi(n)}$.

This proves that the numbers $aa_1, aa_2, \ldots\ldots, aa_{\phi(n)}$ and the numbers $a_1, a_2, \ldots\ldots, a_{\phi(n)}$ are identical (modulo n) in a certain order.

Theorem 7. State and prove Euler's Theorem.

Statement. If $n \ge 1$ ***and gcd*** $(a, n) = 1$, ***then*** $a^{\phi(n)} \equiv 1 \pmod n$.

Proof. Let us take $n > 1$.

Let $a_1, a_2, \ldots\ldots, a_{\phi(n)}$ be the positive integers less than n that are relatively prime to n.

Since $gcd(a, n) = 1$,

it follows from the lemma, "*Let* $n > 1$ *and gcd* $(a, n) = 1$. *If* $a_1, a_2, \ldots\ldots, a_{\phi(n)}$ *are the positive integers less than n and relatively prime to n, then* $aa_1, aa_2, \ldots\ldots, aa_{\phi(n)}$ *are congruent modulo n to* $a_1, a_2, \ldots\ldots, a_{\phi(n)}$ *in some order*",

$aa_1, aa_2, \ldots\ldots, aa_{\phi(n)}$ are congruent, not necessarily in order of appearance, to

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

Then $$aa_1 \equiv r_1 \pmod n$$

$$aa_2 \equiv r_2 \pmod n$$

$$\vdots \qquad \vdots$$

$$aa_{\phi(n)} \equiv r_{\phi(n)} \pmod n,$$

where $r_1, r_2, \ldots\ldots, r_{\phi(n)}$ are the integers $a_1, a_2, \ldots\ldots, a_{\phi(n)}$ in some order so that

the product $r_1 r_2 \ldots\ldots r_{\phi(n)}$ = the product $a_1 a_2 \ldots\ldots a_{\phi(n)}$ ...(1)

Multiplying the above congruence, we get

$$aa_1 \cdot aa_2 \ldots\ldots aa_{\phi(n)} \equiv r_1 r_2 \ldots\ldots r_{\phi(n)} \pmod n$$

Or $$(a_1 a_2 \ldots\ldots a_{\phi(n)})a^{\phi(n)} \equiv a_1 a_2 \ldots\ldots a_{\phi(n)} \pmod n \quad \text{[by using (1)]} \quad \ldots(2)$$

Since each a_i is relatively prime to n, so their product is also relatively prime to n i.e.

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

Cancelling $a_1 a_2 \ldots\ldots a_{\phi(n)}$ from each side of (2), we get

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

Corollary. *If p is a prime and* $p \nmid a$, *then* $a^{p-1} \equiv 1 \pmod p$.

Proof. If $p \nmid a$,

$gcd\,(a, p) = 1.$

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

But $\quad \phi(p) = p - 1$

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

Note Euler's theorem is helpful in reducing large powers modulo n.

Example 20. *Find the remainder if* 8^{103} *is divided by* 103.

Solution. *Since 103 is prime, therefore by Fermat's theorem*

$$8^{103} \equiv 8 \pmod{103}.$$

Hence if we divide 8^{103} by 103, remainder is 8.

Theorem 8. ***State and prove Gauss Theorem***

Statement. For each positive integer $n \geq 1$,

$$n = \sum_{d \mid n} \phi(d),$$

the sum being extended over all positive divisors of n.

Proof. By induction on number of distinct prime factors of n, suppose first that $n = p^r$

A divisor d of n is of the from p^r, $0 \leq r \leq k$

$\Rightarrow$ $1, p, p^2, \ldots\ldots, p^k$ are all the divisors of n. Thus

$$\sum_{d \mid n} \phi(d) = \phi(1) + \phi(p) + \ldots\ldots + \phi(p^k)$$

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

$$= p^k.$$

Thus the result is true for all integers n that contains only one factor.

Let us suppose that the result is true for all the integers $m > 1$ that contain $r-1$ distinct prime factors *i.e* if

$$m = q_1^{k_1} q_2^{k_2} \ldots\ldots q_{r-1}^{k_{r-1}} \;\forall\; i,\ 1 \leq i \leq r-1,$$

q_i primes and integers $k_i \geq 1$,

then $\quad \sum_{d \mid n} \phi(d) = m.$

Let $\quad n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r} \;\forall\; i,\ 1 \leq i \leq r,$

p_r are primes and integer $k_i \geq 1$.

Let $\quad n' = p_1^{k_1} p_2^{k_2} \ldots\ldots p_{r-1}^{k_{r-1}}$, then

$n = n'\, p_r^{k_r}$, $gcd\,(n', p_r^{k_r}) = 1$.

Any divisor d of n is of the form $d' \cdot p_r^t$ where d' is a divisor of n' and $1 \leq r \leq k_r$

Therefore, if $d_1, d_2, \ldots\ldots, d_s$ are all divisors of n', then

$d_1, d_2, \ldots\ldots, d_s, p_r d_1, p_r d_2 \ldots\ldots p_r d_s, \ldots\ldots, p_r^{k_r} d_s$

are all the divisors of n.

$$\therefore \sum_{d \mid n} \phi(d) = \sum_{i=1}^{s} \phi(d_i) + \sum_{i=1}^{s} \phi(p_r d_i) + \ldots\ldots + \sum_{i=1}^{s} \phi(p_r^{k_r} d_i)$$

$$= \sum_{i=1}^{r} [\phi(d_i) + \phi(p_r d_i) + \ldots\ldots + \phi(p_r^{k_r} d_i)]$$

$$= \sum_{i=1}^{r} [\phi(d_i) + \phi(p_r)\phi(d_i) + \ldots\ldots + \phi(p_r^{k_r})\phi(d_i)]$$

$$= \sum_{i=1}^{r} [\phi(d_i)(1 + \phi(p_r) + \ldots\ldots + \phi(p_r^{k_r})]$$

$$= \left[\sum_{i=1}^{r} \phi(d_i)\right] \cdot p_r^{k_r}$$

$= n'\, p_r^{k_r}$, since by induction hypothesis

$\Rightarrow \quad n' = \sum_{i=1}^{r} \phi(d_i)$

$= n.$

Hence the Proof.

Theorem 9. ***For*** $n > 1$, ***the sum of positive integers less than n and relatively prime to n is*** $\frac{1}{2} n \phi(n)$.

Proof. Let $a_1, a_2, \ldots\ldots, a_{\phi(n)}$ be the positive integer less than n and relatively prime to n.

Now since $gcd(a, n) = 1$ if and only if $gcd(n - a, n) = 1$, the numbers $n - a_1, n - a_2, \ldots\ldots, n - a_{\phi(n)}$ are equal in some order to $a_1, a_2, \ldots\ldots, a_{\phi(n)}$.

Thus, $a_1 + a_2 + \ldots + a_{\phi(n)} = (n - a_1) + (n - a_2) + \ldots + (n - a_{\phi(n)})$

$= \phi(n)\, n - (a_1 + a_2 + \ldots\ldots + a_{\phi(n)})$

Hence $a_1 + a_2 + \ldots\ldots + a_{\phi(n)} = \phi(n)\, n - (a_1 + a_2 + \ldots\ldots + a_{\phi(n)})$

$\Rightarrow \quad (a_1 + a_2 + \ldots\ldots + a_{\phi(n)}) + (a_1 + a_2 + \ldots\ldots + a_{\phi(n)}) = \phi(n)\, n$

$\Rightarrow \quad 2(a_1 + a_2 + \ldots\ldots + a_{\phi(n)}) = \phi(n)\, n$

$a_1 + a_2 + \ldots\ldots + a_{\phi(n)} = \frac{1}{2} n\, \phi(n)$

which proves the theorem.

Theorem 10. ***For any positive integer*** n, $\phi(n) = n \sum_{d \mid n} \frac{\mu(d)}{d}$.

Proof. We know that (n, ϕ) is a Mobius pair and $n = \sum_{d \mid n} \phi(d)$

Therefore by inversion formula

$$\phi(n) = \sum_{d \mid n} \mu(d) \cdot \frac{n}{d}$$

$$\Rightarrow \quad \frac{\phi(n)}{n} = \sum_{d \mid n} \frac{\mu(d)}{n} \cdot \frac{n}{d}$$

$$\Rightarrow \quad \frac{\phi(n)}{n} = \sum_{d \mid n} \frac{\mu(d)}{d}$$

$$\Rightarrow \quad \phi(n) = n \sum_{d \mid n} \frac{\mu(d)}{d}.$$

Example 21. *Find the value of* $\sum_{d \mid n} \phi(d)$ *for* $n = 12$.

Solution. Here $n = 12$

All its divisors are 1, 2, 3, 4, 6 and 12.

$$\therefore \sum_{d \mid n} \phi(d) = \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12)$$

$= 1 + 1 + 2 + 2 + 2 + 4$

$= 12.$

Example 22. *If* n *is a composite number, then* $\phi(n) \le n - \sqrt{n}$.

Solution. Let $n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}$, where p_1 is the smallest prime.

Then, $\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right)$

$\le n\left(1 - \frac{1}{p_1}\right)$ ...(1)

Since p_1 is the smallest prime dividing composite number n, therefore $p_1 \le \sqrt{n}$.

$\Rightarrow \quad \frac{1}{p_1} \ge \frac{1}{\sqrt{n}}$

$\Rightarrow \quad -\frac{1}{p_1} \le -\frac{1}{\sqrt{n}}$

$\Rightarrow \quad n\left(1 - \frac{1}{p_1}\right) \le n\left(1 - \frac{1}{\sqrt{n}}\right)$ ...(2)

From (1) and (2), we get

$$\phi(n) \le n\left(1 - \frac{1}{p_1}\right) \le n\left(1 - \frac{1}{\sqrt{n}}\right)$$

i.e $\quad \phi(n) \le n - \sqrt{n}$

Example 23. *If* p *and* $2p + 1$ *are both primes and* $n = 4p$, *then show that*

$$\phi(n + 2) = \phi(n) + 2.$$

Solution. We have

$$\phi(n + 2) = \phi(4p + 2)$$

$$= \phi(2(2p + 1))$$

$$= \phi(2)\, \phi(2p + 1)$$

$$= (2 - 1)(2p + 1 - 1)$$

$$= 2p \quad \ldots(1)$$

Also $\quad \phi(n) + 2 = \phi(4p) + 2$

$$= \phi(2^2 p) + 2$$

$$= \phi(2^2)\,\phi(p) + 2$$
$$= (2^2 - 2)(p-1) + 2$$
$$= 2(p-1) + 2$$
$$= 2p - 2 + 2$$
$$= 2p$$

From (1) and (2), we get

$$\phi(n+2) = \phi(n) + 2.$$

Example 24. *Show that if n is an odd integer then $\phi(2n) = \phi(n)$.*

Solution. Since n is an odd integer,

$\therefore \quad (2, n) = 1$

Therefore

$$\phi(2n) = \phi(2)\,\phi(n)$$
$$= 1\,\phi(n)$$
$$= \phi(n).$$

Hence if n is an odd integer, then

$$\phi(2n) = \phi(n). \qquad [\because \phi(2) = 1]$$

Example 25. *If $\phi(n) \mid n-1$ then prove that n is a square-free integer.*

Solution. If possible let $n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}$ be the prime factorization of n with $k_1 \geq 2$.

$$\therefore \quad \phi(n) = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right)$$
$$= p_1^{k_1 - 1} p_2^{k_2 - 1} \ldots\ldots p_r^{k_r - 1}(p_1 - 1)(p_2 - 1)\ldots\ldots(p_r - 1)$$

$$\Rightarrow \quad p_1 \mid \phi(n) \qquad [\because k_1 \geq 2 \Rightarrow k_1 - 1 \geq 1]$$

Also $\phi(n) \mid n-1$

Therefore

$$p_1 \mid n-1$$

$$\Rightarrow \quad p_1 \mid n - (n-1) \qquad (\because p_1 \mid n)$$

$$\Rightarrow \quad p_1 \mid 1$$

which is not possible.

Therefore $k_1 \neq 2 \Rightarrow k_1 = 1$.

Similarly $k_2 = k_3 = \ldots\ldots = k_r = 1$.

Therefore $n = p_1 p_2 \ldots\ldots p_r$ and hence n is square free.

Example 26. *Prove that there are infinitely many integers n for which $\phi(n) = \frac{n}{3}$.*

Solution. Let $n = 2^k 3^j$,

then $\phi(n) = \phi(2^k 3^j)$

$$= 2^{k-1} 3^{j-1}(2-1)(3-1)$$
$$= 2^{k-1} 3^{j-1}(1)(2)$$
$$= 2^k 3^{j-1}$$
$$= 2^k 3^j \cdot 3^{-1}$$
$$= n \cdot 3^{-1}$$

$$\Rightarrow \quad \phi(n) = \frac{n}{3} \qquad (\because n = 2^k 3^j)$$

Therefore there are infinitely many integers $n = 2^j 3^k$; $j, k \in N$ for which $\phi(n) = \frac{n}{3}$.

Example 27. *Find the number of positive integers ≤ 7200 that are relatively prime to 3600.*

Solution. Since $7200 = 2 \times 3600$,

therefore number of positive integers ≤ 7200 that are relatively prime to

$$3600 = 2\,\phi(3600)$$
$$= 2 \times 960 \qquad (\because \phi(3600) = 960)$$
$$= 1920.$$

Example 28. *Find the positive integral values of x, y, z satisfying the equation*

$$\phi(x-5) + \phi(3y-5) + \phi(5z-18) = 3.$$

Solution. Since $\phi(n) \geq 1 \ \forall\ n \in N$ and the right hand side of given equation is 3, therefore each term on L.H.S. of given equation must be 1.

Therefore

$$\phi(x-5) = 1$$

$$\Rightarrow \quad x - 5 = 1 \text{ or } 2$$

$\Rightarrow$ $x = 6$ or 7.

$\Rightarrow$ $\phi(3y-5) = 1$

$\Rightarrow$ $3y - 5 = 1$ or 2

$\Rightarrow$ $y = 2$ or $\frac{7}{3}$

and $\phi(5z-8) = 1$

$\Rightarrow$ $5z - 18 \equiv 1$ or 2

$\Rightarrow$ $z = \frac{19}{5}$ or 4.

Here $y = \frac{7}{3}$ and $z = \frac{19}{5}$ are not possible since $x, y, z \in N$.

Therefore $x = 6$ or 7,

$y = 2, z = 4$.

Example 29. *If m and n are relatively prime positive integers, then show that*

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$$

Solution. Since $(m, n) = 1$

Therefore by Euler's theorem, we have

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

and $$n^{\phi(m)} \equiv 1 \pmod{m}$$

$\Rightarrow$ $m \mid n^{\phi(m)} - 1$ and

$n \mid m^{\phi(n)} - 1$

$\Rightarrow$ $mn \mid (n^{\phi(m)} - 1)(m^{\phi(n)} - 1)$

$\Rightarrow$ $mn \mid m^{\phi(n)} n^{\phi(m)} - m^{\phi(n)} - n^{\phi(m)} + 1$

Also $mn \mid m^{\phi(n)} n^{\phi(m)}$ [$\because \phi(m) \geq 1, \phi(n) \geq 1$]

Therefore

$$mn \mid -m^{\phi(n)} - n^{\phi(m)} + 1$$

$\Rightarrow$ $$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{(mn)}.$$

Example 30. *Find the units digit of 3^{100} by means of Euler's theorem.*

Solution. Since $(3, 10) = 1$,

therefore by Euler's theorem

$$3^{\phi(10)} \equiv 1 \pmod{10}$$

$\Rightarrow$ $3^4 \equiv 1 \pmod{10}$

$\Rightarrow$ $(3^4)^{25} \equiv (1)^{25} \pmod{10}$

$\Rightarrow$ $3^{100} \equiv 1 \pmod{10}$

Hence units digit of 3^{100} is 1.

Example 31. *Prove that n divides $\phi(2^n - 1)$ for any $n > 1$.*

Solution. Since $2^n - 1 \mid 2^n - 1$

$\therefore$ $2^n \equiv 1 \pmod{(2^n - 1)}$

$\Rightarrow$ order of 2 modulo $(2^n - 1)$ is n.

Also as $(2, 2^n - 1) = 1$,

therefore by Euler's theorem, we have

$$2^{\phi(2^n - 1)} \equiv 1 \pmod{(2^n - 1)}$$

$\therefore$ $n \mid \phi(2^n - 1)$

Hence n divides $\phi(2^n - 1)$ for any $n > 1$.

Example 32. *Use Euler's theorem to show that $a^{37} \equiv a \pmod{1729}$ for any integer a.*

Solution. $1729 = 7 \cdot 13 \cdot 19$

If $7 \mid a$ then $7 \mid a^{37}$

$\Rightarrow$ $7 \mid a^{37} - a$

$\Rightarrow$ $a^{37} \equiv a \pmod{7}$

If $7 \nmid a$ then $(a, 7) = 1$ and hence by Euler's theorem

$$a^{\phi(7)} \equiv 1 \pmod{7}$$

$\Rightarrow$ $a^6 \equiv 1 \pmod{7}$

$\Rightarrow$ $a^{36} \equiv 1 \pmod{7}$

$\Rightarrow$ $a^{37} \equiv a \pmod{7}$

Therefore in either case

$$a^{37} \equiv a \pmod{7}$$

If $13 \mid a$ then $13 \mid a^{37}$

$\Rightarrow$ $13 \mid a^{37} - a$

$\Rightarrow \quad a^{37} \equiv a \pmod{13}$

If $13 \nmid a$ then $(a, 13) = 1$ and hence by Euler's theorem,

$\Rightarrow \quad a^{\phi(13)} \equiv 1 \pmod{13}$

$\Rightarrow \quad a^{12} \equiv 1 \pmod{13}$

$\Rightarrow \quad a^{36} \equiv 1 \pmod{13}$

$\Rightarrow \quad a^{37} \equiv a \pmod{13}$

$\therefore$ in either case

$$a^{37} \equiv a \pmod{13}$$

Again if $19 \mid a$ then $19 \mid a^{37}$

$\Rightarrow \quad 19 \mid a^{37} - a$

$\Rightarrow \quad a^{37} \equiv a \pmod{19}$

and if $19 \nmid a$ then by Euler's theorem

$$a^{\phi(19)} \equiv 1 \pmod{13}$$

$\Rightarrow \quad a^{18} \equiv 1 \pmod{13}$

$\Rightarrow \quad a^{36} \equiv 1 \pmod{13}$

$\Rightarrow \quad a^{37} \equiv a \pmod{13}$

Therefore in either case

$$a^{37} \equiv a \pmod{13}$$

Since 7, 13 and 19 are relatively co-prime in pairs therefore from (1), (2) and (3), we get ...(3)

$$a^{37} \equiv a \pmod{7 \cdot 13 \cdot 19}$$

i.e. $\quad a^{37} \equiv a \pmod{1729}$.

Example 33. *Use Euler's theorem to show that* $a^{33} \equiv a \pmod{4080}$ *for any odd integer* a.

Solution. $4080 = 3 \cdot 5 \cdot 16 \cdot 17$

If $3 \mid a$ then $3 \mid a^{33}$

$\Rightarrow \quad 3 \mid a^{33} - a$

$\Rightarrow \quad a^{33} \equiv a \pmod{3}$

If $3 \nmid a$ then $(a, 3) = 1$ and hence by Euler's theorem,

$$a^{\phi(3)} \equiv 1 \pmod{3}$$

$\Rightarrow \quad a^{2} \equiv 1 \pmod{3}$

$\Rightarrow \quad a^{32} \equiv 1 \pmod{3}$

$\Rightarrow \quad a^{33} \equiv a \pmod{3}$

Therefore in either case

$$a^{33} \equiv a \pmod{3}$$

Similarly $a^{33} \equiv a \pmod{5}$ ...(1)

Since 17 is prime, therefore by Fermat's theorem ...(2)

$$a^{16} \equiv 1 \pmod{17}$$

$\Rightarrow \quad a^{32} \equiv 1 \pmod{17}$

$\Rightarrow \quad a^{33} \equiv a \pmod{17}$

Since a is odd, therefore $(a, 16) = 1$ and hence by Euler's theorem, ...(3)

$$a^{\phi(16)} \equiv 1 \pmod{16}$$

$\Rightarrow \quad a^{8} \equiv 1 \pmod{16}$

$\Rightarrow \quad a^{32} \equiv 1 \pmod{16}$

$\Rightarrow \quad a^{33} \equiv a \pmod{16}$ ...(4)

Since 3, 5, 16 and 17 are relatively prime in pairs, therefore from (1), (2), (3) and (4), we get

$$a^{33} \equiv a \pmod{3 \cdot 5 \cdot 16 \cdot 17}$$

$$a^{33} \equiv a \pmod{4080}$$

Example 34. *Use Euler's theorem to show that for any integer* $n \geq 0$, $51 \mid 10^{32n+9} - 7$.

Solution. Clearly

$$10^2 \equiv -2 \pmod{51}$$

$\Rightarrow \quad (10^2)^4 \equiv (-2)^4 \pmod{51}$

$\Rightarrow \quad 10^8 \equiv 16 \pmod{51}$

$\Rightarrow \quad 10^9 \equiv 160 \pmod{51}$

Or $\quad 10^9 \equiv 7 \pmod{51}$ ...(1)

since $(10, 51) = 1$, therefore by Euler's theorem,

$$10^{\phi(51)} \equiv 1 \pmod{51}$$

where $\phi(51) = \phi(3 \times 17)$

$$= 51\left(1-\frac{1}{3}\right)\left(1-\frac{1}{17}\right)$$

$$= 51 \times \frac{2}{3} \times \frac{16}{17}$$

$$= 32$$

$\therefore$ $10^{32} \equiv 1 \pmod{51}$

From (1) and (2), we get

$10^{32n+9} \equiv 7 \pmod{51}$

$\Rightarrow$ $51 \mid 10^{32n+9} - 7$.

Example 35. *Show that if* $(a, n) \equiv (a-1, n) = 1$, *then*

$1 + a + a^2 + \ldots\ldots + a^{\phi(n)-1} \equiv 0 \pmod{n}$.

Solution. Since $(a, n) = 1$

Therefore by Euler's theorem, we have

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

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

$\Rightarrow$ $n \mid (a-1)(a^{\phi(n)-1} + \ldots\ldots + a^2 + a + 1)$

$\Rightarrow$ $n \mid a^{\phi(n)-1} + \ldots\ldots + a^2 + a + 1$

$\Rightarrow$ $1 + a + a^2 + \ldots\ldots + a^{\phi(n)-1} \equiv 0 \pmod{n}$. $[\because (a-1, n) = 1]$

Example 36. *Show that* $\sum_{d=1}^{n} \phi(d)\left[\frac{n}{d}\right] = \frac{n(n+1)}{2}$ *for any positive integer* n.

Solution. Let $f(n) = \sum_{d=1}^{n} \phi(d)\left[\frac{n}{d}\right]$ so that

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

$$= \sum_{d=1}^{n} \phi(d)\left[\frac{n-1}{d}\right] \quad \left(\because \left[\frac{n-1}{n}\right] = 0\right)$$

Therefore $f(n) - f(n-1) = \sum_{d=1}^{n} \phi(d)\left\{\left[\frac{n}{d}\right] - \left[\frac{n-1}{d}\right]\right\}$

$$= \sum_{\substack{d=1 \\ d \mid n}} \phi(d) \cdot 1 + \sum_{\substack{d=1 \\ d \nmid n}} \phi(d) \cdot 0$$

$$\left[\because \left[\frac{n}{d}\right] - \left[\frac{n-1}{d}\right] = \begin{cases} 1 & \text{if } d \mid n \\ 0 & \text{if } d \nmid n \end{cases}\right]$$

$$= \sum_{d \mid n} \phi(d) = n$$

i.e. $f(n) - f(n-1) = n$.

Putting $n = 2, 3, \ldots\ldots, n$, we get

$f(2) - f(1) = 2$,

$f(3) - f(2) = 3$,

$f(4) - f(3) = 4$

.....

.....

$f(n) - f(n-1) = n$

Adding vertically, we get

$f(n) - f(1) = 2 + 3 + \ldots\ldots + n$

$\Rightarrow$ $f(n) = f(1) + 2 + 3 + \ldots\ldots + n$

$= 1 + 2 + \ldots\ldots + n$ $(\because f(1) = \phi(1)[1] = 1)$

$\Rightarrow$ $f(n) = \frac{n(n+1)}{2}$

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

❑❑❑

10. The value of $\left(0.5\overline{8} \div 0.\overline{53}\right) \times \frac{5}{33} + \frac{10}{21} \div 1\frac{1}{14}$ of $\frac{5}{3} - \frac{5}{3} \times \frac{1}{10}$ is:

$\left(0.5\overline{8} \div 0.\overline{53}\right) \times \frac{5}{33} + \frac{10}{21} \div 1\frac{1}{14}$ of $\frac{5}{3} - \frac{5}{3} \times \frac{1}{10}$ का मान ज्ञात कीजिए?

PRIMITIVE ROOTS AND INDICES

CHAPTER 7

Definition. *Let $n > 1$ be an integer and a another integer. A positive integer k is called the* **exponent** *of a modulo m if k is the smallest positive integer such that*

$$a^k \equiv 1 \pmod{n}.$$

e.g. the exponent of 3 modulo 5 is 4,

since $3^1 \equiv 3 \pmod 5$,

$3^2 \equiv 4 \pmod 5$,

$3^3 \equiv 2 \pmod 5$,

and $3^4 \equiv 1 \pmod 5$.

Order of an integer modulo *n*

Definition. *Let $n > 1$ be any integer.*

Also let a be any integer such that $(a, n) = 1$. Then, the order of a modulo n is the smallest positive integer k such that $a^k \equiv 1 \pmod n$

e.g, the order of 2 modulo 7 is 3, because

$2^1 \equiv 2 \pmod 7$

$2^2 \equiv 4 \pmod 7$

$2^3 \equiv 1 \pmod 7$.

Theorem 1. ***Let the integer a have order k modulo n. Then $a^h \equiv 1 \pmod n$ if and only if $k \mid h$; particular $k \mid \phi(n)$.***

Proof. Let us suppose that $k \mid h$;

Then by definition of divisibility,

$h = jk$ for some integer j.

Since $a^k \equiv 1 \pmod n$

$\Rightarrow \quad (a^k)^j \equiv 1^j \pmod n$

$\Rightarrow \quad a^{jk} \equiv 1 \pmod n$

$\Rightarrow \quad a^h \equiv 1 \pmod n$

Conversely, let h be any positive integer satisfying

$a^h \equiv 1 \pmod n$.

By the division algorithm there exists q and r such that

$h = qk + r$, where $0 \le r < k$.

$\therefore \quad a^h \equiv a^{qk+r} \equiv a^{qk} \cdot a^r \equiv (a^k)^q \cdot a^r$

But by hypothesis both $a^h \equiv 1 \pmod n$ and

$a^k \equiv 1 \pmod n$,

which implies that

$1 = 1^q \cdot a^r \pmod n$ ....(1)

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

But $0 \le r < k$,

and k is the exponent of $a \pmod n$,

so (1) holds only where $r = 0$.

$\therefore \quad h = qk$

$\Rightarrow \quad k \mid h$ by definition of divisibility.

Hence the Proof.

Note

Let us obtain the order of 2 modulo 13.

Since $\phi(13) = 12$,

the order of 2 must be one of integers 1, 2, 3, 4, 6, 12.

From $2^1 \equiv 2, 2^2 \equiv 4$,

$2^3 \equiv 8, 2^4 \equiv 3, 2^6 \equiv 12, 2^{12} \equiv 1 \pmod{13}$

Thus we see that 2 has order 12 modulo 13.

Theorem 2. ***If the integer a has order k modulo n, then $a^i \equiv a^j \pmod n$ if and only if $i \equiv j \pmod k$.***

Proof. Let $a^i \equiv a^j \pmod n$, where $i \ge j$.

Since a is relatively prime to n,

so we have $a^{i-j} \equiv 1 \pmod n$. ....(1)

Congruence (1) holds only if

$$k \mid i-j.$$

which implies that

$$i \equiv j \pmod{k}.$$

Conversely, let $i \equiv j \pmod{k}$.

Then we have $i = j + qk$ for some integer q.

By the definition of k,

$$a^k \equiv 1 \pmod{n}, \text{ so that}$$

$$a^i \equiv a^{j+qk} \equiv a^j a^{qk}$$

$$\Rightarrow \quad a^i = a^j (a^k)^q \equiv a^j \pmod{n}$$

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

which proves the theorem.

Corollary. *If a has order k modulo n, then the integers $a, a^2, \ldots\ldots, a^k$ are incongruent modulo n.*

Proof. If $a^i \equiv a^j \pmod{n}$ for $1 \le i \le j \le k$, then the theorem ensures that $i \equiv j \pmod{k}$.

But this is impossible unless $i = j$.

Theorem 3. If a has order k modulo n and a has order h modulo m then show that a has order [h, k] modulo [m, n].

Proof. Let a has order r modulo $[m, n]$ and $l = [h, k]$.

Then $a^r \equiv 1 \pmod{([m, n])}$

$\Rightarrow \quad a^r \equiv 1 \pmod{n}$

and $\quad a^r \equiv 1 \pmod{m}$

$\Rightarrow \quad k \mid r$ and $h \mid r$

$\Rightarrow \quad [h, k] \mid r$

$\Rightarrow \quad l \mid r$ ....(1)

Since $k \mid l$ and $a^k \equiv 1 \pmod{n}$, ...(2)

therefore $a^l \equiv 1 \pmod{n}$

Also $h \mid l$ and $a^h \equiv 1 \pmod{m}$ ....(3)

$\therefore \quad a^l \equiv 1 \pmod{m}$

From (2) and (3), we have

$$a^l \equiv 1 \pmod{[m, n]} \quad \text{....(4)}$$

$\Rightarrow \quad r \mid l$

From (1) and (4), we get

$$r = l$$

Therefore order of a modulo $[m, n]$ is $[h, k]$.

Theorem 4. If the integer a has order k modulo n and $h > 0$, then a^h has order $k / gcd(h, k)$ modulo n.

Proof. Let $d = gcd(h, k)$.

$\Rightarrow \quad d \mid h$ and $d \mid k$ (by definition)

$\Rightarrow \quad h = h_1 d$ and $k = k_1 d$, with $gcd(h_1, k_1) = 1$.

Let a^h has exponent $t \pmod{n}$

$\Rightarrow \quad a^{ht} \equiv 1 \pmod{n}$

$\Rightarrow \quad k \mid ht$

Now $\quad k \mid ht \Rightarrow k_1 d \mid h_1 dt$

$\Rightarrow \quad k_1 \mid h_1 t \qquad (\because gcd(h_1, k_1) = 1)$

$\Rightarrow \quad k_1 \mid t$ ....(1)

$\Rightarrow \quad \frac{k}{d} \mid t$

Also $\quad (a^h)^{\frac{k}{d}} = (a^h)^{k_1}$

$$= (a^{h_1 d})^{k_1}$$

$$= (a^{k_1 d})^{h_1}$$

$$= (a^k)^{h_1}$$

$$\equiv 1 \pmod{n} \quad \text{....(2)}$$

$\therefore \quad t \mid \frac{k}{d}$

From (1) and (2), we get

$$t = \frac{k}{d} = \frac{k}{gcd(h, k)}$$

Hence the Proof.

Corollary. *Let a have order k modulo n. Then a^h also has order k if and only if $(h, k) = 1$.*

Proof. Do yourself.

Definition. *If $\gcd(a, n) = 1$ and a is of order $\phi(n)$ modulo n, then a is a primitive root of the integer n.*

If an integer a has exponent $\phi(n)$ modulo n, n a positive integer, then we say that a is a ***primitive root*** *modulo n or a is a primitive root belonging to n.*

Or

Note

$1^n = 1$ for all integers n, hence 1 can never be a primitive root of any integer > 2.

Example 1. *Show that 3 is a primitive root of 7.*

Solution. $3^1 \equiv 3 \pmod 7$,

$3^2 \equiv 2 \pmod 7$,

$3^3 \equiv 6 \pmod 7$,

$3^4 \equiv 4 \pmod 7$,

$3^5 \equiv 5 \pmod 7$,

and $3^6 \equiv 1 \pmod 7$

$\Rightarrow$ 3 is a primitive root $(mod\ 7)$

Example 2. *List all primitive roots modulo 8.*

Solution. Since $\phi(8) = 4$ and 1, 3, 5, 7 are coprime to 8.

Hence possible primitive roots can be 3, 5 or 7.

As $3^2 \equiv 1 \pmod 8$,

$5^2 \equiv 1 \pmod 8$,

$7^2 \equiv 1 \pmod 8$

None of 3, 5, 7 is a primitive root $(mod\ 8)$

Example 3. *List all primitive roots modulo 6.*

Solution. Since $\phi(6) = 2$ and any integer $(mod\ 6)$ is congruent to one of 0, 1, 2, 3, 4, 5.

Therefore the primitive roots $(mod\ 6)$ will be amongst 2, 3, 4, 5.

But then

$2^2 \equiv 4 \pmod 6$,

$3^2 \equiv 3 \pmod 6$,

and $4^2 \equiv 2 \pmod 6$.

$5^2 \equiv 1 \pmod 6$

Thus 5 is the only primitive root $(mod\ 6)$.

Example 4. Show that if $F_n = 2^{2n} + 1$, $n > 1$ is a prime, then 2 is not a primitive root of Fn.

Solution. Clearly 2 is a primitive root of $5 = F_1$.

From the factorization

$$2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1),$$ we have

$$2^{2^{n+1}} \equiv 1 \pmod{F_n}$$

which implies that the order of 2 modulo F_n does not exceed 2^{n+1}. But if F_n is assumed to be prime, then

$$\phi(F_n) = F_n - 1 = 2^{2n}$$

and by induction we have

$2^{2^n} > 2^{n+1}$, whenever $n > 1$.

Thus the order of 2 modulo F_n is smaller than $\phi(F_n)$.

Therefore 2 cannot be a primitive root of F_n.

Example 5. Find the order of 5 $(mod\ 29)$.

Solution. Since $\phi(29) = 28$.

The divisors of 28 are 1, 2, 4, 7, 14, 28.

Since $O(5)\ (mod\ 29)$ is a divisor of $\phi(29)$,

therefore $O(5)\ (mod\ 29)$ is one of the number among 1, 2, 4, 7, 14 and 28.

$5^2 \equiv -4 \pmod{29}$

$5^4 \equiv 16 \pmod{29}$

$5^7 \equiv 5^4 \times 5^2 \times 5 \equiv 16 \times (-4) \times 5 \pmod{29}$ $[\because -20 \equiv 9 \pmod{29}]$

$\equiv 16 \times 9 \pmod{29}$ $[\because 144 \equiv -1 \pmod{29}]$

$\equiv -1 \pmod{29}$

$\Rightarrow \quad 5^{14} \equiv 1 \pmod{29}$

and hence $O(5)\ (mod\ 29) = 14$.

Example 6. *Find the order of* 16 (*mod* 17).

Solution. Since $16 = 2^4$

Firstly we find $O(2) \pmod{17}$

$$2^4 = 16 \equiv -1 \pmod{17}$$

$$\Rightarrow \quad 2^8 \equiv 1 \pmod{17}$$

Therefore $O(2) \pmod{17} = 8$

Hence the order of $2^4 \pmod{17}$

$$= \frac{8}{(4, 8)}$$

$$= \frac{8}{4} = 2$$

i.e order of 16 (*mod* 17) is 2.

Example 7. *Find the order of* 2 (*mod* 385).

Solution. Since $385 = 5 \cdot 7 \cdot 11$

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

$$\Rightarrow \quad 2^4 \equiv 1 \pmod{5}$$

$$\Rightarrow \quad O(2) \pmod{5} = 4$$

$$2^2 \equiv 4 \pmod{7}$$

$$\Rightarrow \quad 2^3 \equiv 1 \pmod{7}$$

$$\Rightarrow \quad O(2) \pmod{7} = 3$$

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

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

$$\Rightarrow \quad 2^5 \equiv -1 \pmod{11}$$

$$\Rightarrow \quad 2^{10} \equiv 1 \pmod{11}$$

Therefore $O(2) \pmod{11} = 10$

Hence $\quad O(2) \pmod{[5, 7, 11]} = [4, 3, 10]$

i.e order of 2 modulo 385 = 60.

Example 8. *Find the order of* 43 (*mod* 18).

Solution. $43 \equiv 7 \pmod{18}$

$$\Rightarrow \quad O(43) \pmod{18} = O(7) \pmod{18}$$

Since $\quad 7^2 = 49 \equiv -5 \pmod{18}$

$$\Rightarrow \quad 7^3 \equiv -35 \pmod{18}$$

$$\Rightarrow \quad 7^3 \equiv 1 \pmod{18}$$

$\Rightarrow$ order of 7 modulo 18 = 3

Hence order of 43 modulo 18 = 3.

Theorem 5. ***Let gcd*** $(a, n) = 1$ ***and let*** $a_1, a_2, \ldots\ldots, a_{\phi(n)}$ ***be the positive integers less than n and relatively prime to n. If a is a primitive root of n, then*** $a, a^2, \ldots\ldots, a^{\phi(n)}$ ***are congruent modulo n to*** $a_1, a_2, \ldots\ldots, a_{\phi(n)}$ ***in some order.***

Proof. Since a is relatively prime to n, the same holds for all the powers of a.

Hence each a^k is congruent modulo n to some one of the a_i.

Then $\phi(n)$ numbers in the set $\{a, a^2, \ldots\ldots, a^{\phi(n)}\}$ are incongruent by the corollary, "*If* a *has order* k *modulo* n, *then the integers* $a, a^2, \ldots\ldots, a^k$ *are incongruent modulo* n".

Thus, these powers must represent (not necessarily in order of appearance) the integers $a_1, a_2, \ldots\ldots, a_{\phi(n)}$.

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

Proof. Let a be a primitive root of n.

Then by the theorem, "*Let gcd* $(a, n) = 1$ *and let* $a_1, a_2, \ldots\ldots, a_{\phi(n)}$ *be the positive integers less than n and relatively prime to n. If a is a primitive root of n, then* $a, a^2, \ldots\ldots, a^{\phi(n)}$ *are congruent modulo n to* $a_1, a_2, \ldots\ldots, a_{\phi(n)}$ *in some order*", any other primitive root of n is found among the member of the set $\{a, a^2, \ldots\ldots, a^{\phi(n)}\}$.

But the number of powers a^k, $1 \le k \le \phi(n)$, that have order $\phi(n)$ = the number of integers k for which $gcd(k, \phi(n)) = 1$; there are $\phi(\phi(n))$ such integers.

Hence $\phi(\phi(n))$ are primitive roots of n.

Note

Now we illustrate the theorem 5.

Let us take $a = 2$ and $n = 9$.

Since $\phi(9) = 6$, the first six powers of 2 must be congruent modulo 9, in some order, to the positive integers less than 9 and relatively prime to it.

Thus 1, 2, 4, 5, 7, 8 are integers less than and relatively prime to 9.

Thus $\quad 2^1 \equiv 2 \pmod{9}$,

$2^2 \equiv 4 \pmod 9$,

$2^3 \equiv 8 \pmod 9$,

$2^4 \equiv 7 \pmod 9$,

$2^5 \equiv 5 \pmod 9$,

$2^6 \equiv 1 \pmod 9$

As we know that if n has a primitive root, then it has exactly $\phi(\phi(n))$ of them.

$\therefore$ there are exactly $\phi(\phi(9)) = \phi(6) = 2$ primitive roots of 9.

these being the integers 2 and 5.

PRIMITIVE ROOTS FOR PRIMES

Theorem 6. *State and prove Lagrange's theorem.*

Statement. ***If p is a prime and***

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots + a_1 x + a_0, a_n \not\equiv 0 \pmod p$$

is a polynomial of degree $n \geq 1$ with integral coefficients, then the congruence $f(x) \equiv 0 \pmod p$ has at most n incongruent solutions modulo p.

Or

State and prove Lagrange's theorem regarding incongruent solutions modulo p.

Proof. Let us prove the theorem by induction on n, the degree of $f(x)$.

If $n = 1$, then the polynomial is of the form

$$f(x) = a_1 x + a_0 .$$

Since $gcd(a_1, p) = 1$, then by the theorem, "*The linear congruence $ax \equiv b \pmod n$ has a solution if and only if $d \mid b$, where $d = gcd(a, n)$. If $d \mid b$, then it has d mutually incongruent solutions modulo n*", the congruence $a_1 x \equiv -a_0 \pmod p$ has a unique solution modulo p.

Thus, the theorem holds for $n = 1$.

Now let us assume that the theorem is true for polynomials of degree $k-1$ and let us consider the case in which $f(x)$ has degree k.

Either the congruence $f(x) \equiv 0 \pmod p$ has no solutions or it has at least one solution.

If $f(x) \equiv 0 \pmod p$ has no solutions then we are done.

Let a be the solution of this congruence.

If $f(x)$ is divided by $x - a$, then

$$f(x) = (x - a)\, q(x) + r, \qquad \ldots(1)$$

where $q(x)$ is a polynomial of degree $k-1$ with integral coefficients and r is an integer.

Putting $x = a$ in (1), we get

$$0 \equiv f(a) = (a - a)\, q(a) + r = r \pmod p$$

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

If b is another one of the incongruent solutions of

$$f(x) \equiv 0 \pmod p, \text{ then} \qquad \ldots(2)$$

$$0 \equiv f(b) \equiv (b - a)\, q(b) \pmod p$$

Since $b - a \not\equiv 0 \pmod p$,

then from (2), we have (dividing by $b - a$)

$$q(b) \equiv 0 \pmod p$$

In other words, any solution of $f(x) \equiv 0 \pmod p$ that is different from a must satisfy $q(x) \equiv 0 \pmod p$ that is different from a must satisfy $q(x) \equiv 0 \pmod p$.

By our induction assumption, the latter congruence can possess at most $k-1$ incongruent solutions.

Therefore $f(x) \equiv 0 \pmod p$ has no more than k incongruent solutions.

Hence the Proof.

Corollary. *If p is a prime number and $d \mid p-1$, then the congruence $x^d - 1 \equiv 0 \pmod p$ has exactly d solutions.*

Proof. Since $d \mid p - 1$,

therefore by definition of divisibility there exists an integer k such that

$$p - 1 = dk.$$

Then $x^{p-1} - 1 = (x^d - 1) f(x)$ where the polynomial

$f(x) = x^{d(k-1)} + x^{d(k-2)} + \ldots\ldots\ldots + x^d + 1$ has integral coefficients and is of degree

$$d(k-1) = dk - d = p - 1 - d.$$

By Lagrange's theorem, we know that the congruence $f(x) \equiv 0 \pmod p$ has at most $p - 1 - d$ solutions.

We also know from Fermat's theorem that $x^{p-1} - 1 \equiv 0 \pmod p$ has precisely $p - 1$ incongruent solutions namely the integers $1, 2, \ldots\ldots, p - 1$.

Now any solution $x \equiv a \pmod p$ of $x^{p-1} - 1 \equiv 0 \pmod p$ which is not a solution of $f(x) \equiv 0 \pmod p$ must satisfy

$$x^d - 1 \equiv 0 \pmod p.$$

Since $0 \equiv a^{p-1} - 1 = (a^d - 1) f(a) \pmod p$ with $p \nmid f(a)$ which gives that $p \mid a^d - 1$.

Thus $x^d - 1 \equiv 0 \pmod p$ must have at least

$p - 1 - (p - 1 - d) \equiv d$ solution.

This last congruence can possess no more than d solutions so by Lagrange's theorem it has exactly d solutions.

Theorem 7. ***Using the previous corollary prove Wilson's theorem.***

Proof. Given a prime p, let us define the polynomial $f(x)$ by

$$f(x) = (x-1)(x-2) \ldots\ldots (x-(p-1)) - (x^{p-1} - 1)$$
$$= a_{p-2} x^{p-2} + a_{p-3} x^{p-3} + \ldots\ldots + a_1 x + a_0$$

which is of degree $p - 2$.

Fermat's theorem implies that the $p - 1$ integer $1, 2, \ldots\ldots, p - 1$ are incongruent solutions of the congruence

$$f(x) \equiv 0 \pmod p$$

But this contradicts Lagrange's theorem, unless

$$a_{p-2} \equiv a_{p-3} \equiv \ldots\ldots \equiv a_1 \equiv a_0 \equiv 0 \pmod p$$

It follows that, for any choice of the integer x,

$$(x-1)(x-2) \ldots\ldots (x-(p-1)) - (x^{p-1} - 1) \equiv 0 \pmod p$$

Now putting $x = 0$ in the above congruence, we get

$$(-1)(-2) \ldots\ldots (-(p-1)) + 1 \equiv 0 \pmod p$$

Or $\quad (-1)^{p-1} (p-1)! + 1 \equiv 0 \pmod p$.

Either $p - 1$ is even or $p = 2$, in which case

$-1 \equiv 1 \pmod p$, at any rate, we get

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

which proves the Wilson's theorem.

Theorem 8. ***If p is a prime number and $d \mid p - 1$, then there are exactly $\phi(d)$ incongruent integers having order d modulo p.***

Proof. Let $d \mid p - 1$

and $\psi(d)$ denote the number of integers k, $1 \le k \le p - 1$,

that have order d modulo p.

Since each integer between 1 and $p - 1$ has order d for some $d \mid p - 1$,

$$p - 1 = \sum_{d \mid p-1} \psi(d) \quad \ldots(1)$$

Also by Gauss theorem, we have

$$p - 1 = \sum_{d \mid p-1} \phi(d) \quad \ldots(2)$$

Combining (1) and (2), we get

$$\sum_{d \mid p-1} \psi(d) = \sum_{d \mid p-1} \phi(d) \quad \ldots(3)$$

Now we are to show that

$\psi(d) \le \phi(d)$ for each divisor d of $p - 1$.

Given an arbitrary divisor d of $p - 1$, there are two possibilities:

Either $\psi(d) = 0$

Or $\quad \psi(d) > 0$.

If $\psi(d) = 0$, then clearly

$$\psi(d) \le \phi(d).$$

Let $\quad \psi(d) > 0$,

then there exists an integer a of order d.

Then the d integers $a, a^2, \ldots\ldots, a^d$ are incongruent modulo p and each of them satisfies the polynomial congruence

$$x^d - 1 \equiv 0 \pmod p \quad \ldots(4)$$

since, $(a^k)^d \equiv (a^d)^k \equiv 1 \pmod p$.

By the corollary to Lagrange's theorem, there can be no other solutions of equation (4).

It follows that any integer having order d modulo p must be congruent to one of $a, a^2, \ldots\ldots, a^d$.

But only $\phi(d)$ of the just mentioned powers have ordered, namely those a^k for which the exponent k has the property $\gcd(k, d) = 1$.

Hence in this case we have

$$\psi(d) = \phi(d),$$

and the number of integers having order d modulo $p = \phi(d)$.

Thus if p is a prime number and $d \mid p - 1$, then three are exactly $\phi(d)$ incongruent integers having order d modulo p.

Corollary. *If p is a prime, then there are exactly $\phi(p-1)$ incongruent primitive roots of p.*

Proof. Take $d = p-1$ in the proof of the previous theorem, we get the required result.

Note

If p is a prime of the form $4k+1$, then quadratic congruence $x^2 \equiv -1 \pmod{p}$ admits a solution.

Since $4 \mid p-1$, then by the above proved theorem there is an integer a having order 4 modulo p.

In other words

$$a^4 \equiv 1 \pmod{p}$$

Or $$a^4 - 1 \equiv 0 \pmod{p}$$

Or $$(a^2-1)(a^2+1) \equiv 0 \pmod{p}$$

Since p is a prime, it follows that either

$$a^2 - 1 \equiv 0 \pmod{p}$$

Or $$a^2 + 1 \equiv 0 \pmod{p}$$

If the first congruence holds, then a would have order less than or equal to 2, a contradiction.

Hence $a^2 + 1 \equiv 0 \pmod{p}$

which shows that the integer a is solution to the congruence $x^2 \equiv -1 \pmod{p}$.

Example 9. *Find the primitive roots of* 31.

Solution. In fact 2, 3 and 5 are the only primes less than 31.

Now $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 16,$

$2^5 \equiv 1 \pmod{31}$.

Hence 2 fails to be a primitive root of 31.

Again $3^1 \equiv 3, 3^2 \equiv 9, 3^3 \equiv 27,$

$3^4 \equiv 19, 3^5 \equiv 26, 3^6 \equiv 16, 3^7 \equiv 17,$

$3^8 \equiv 20, 3^9 \equiv 29, 3^{10} \equiv 25, 3^{11} \equiv 13,$

$3^{12} \equiv 8, 3^{13} \equiv 24, 3^{14} \equiv 10, 3^{15} \equiv 30,$

$3^{16} \equiv 28, 3^{17} \equiv 22, 3^{18} \equiv 4, 3^{19} \equiv 12,$

$3^{20} \equiv 5, 3^{21} \equiv 15, 3^{22} \equiv 14, 3^{23} \equiv 11,$

$3^{24} \equiv 2, 3^{25} \equiv 6, 3^{26} \equiv 18,$

$3^{27} \equiv 23, 3^{28} \equiv 7, 3^{29} \equiv 21, 3^{30} \equiv 1 \pmod{31}$

Thus shows $g = 3$ is a primitive root of 31.

A similar procedure will show that 5 is a primitive root of 31.

Since 1, 7, 11, 13, 17, 19, 23, 29 are relatively prime to 30 (*i.e* 31 – 1).

Hence 3, 17, 13, 24, 22, 12, 11 are also the primitive roots of 31.

Example 10. *Find the primitive roots of* 17.

Solution. We have

$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 16,$

$2^5 \equiv 15, 2^6 \equiv 13, 2^7 \equiv 9, 2^8 \equiv 1 \pmod{17}$.

Hence $g = 2$ is not a primitive root.

Now $3^1 \equiv 3, 3^2 \equiv 9, 3^3 \equiv 10, 3^4 \equiv 13,$

$3^5 \equiv 5, 3^6 \equiv 15, 3^7 \equiv 11, 3^8 \equiv 16,$

$3^9 \equiv 14, 3^{10} \equiv 8, 3^{11} \equiv 7, 3^{12} \equiv 4,$

$3^{13} \equiv 12, 3^{14} \equiv 2, 3^{15} \equiv 6, 3^{16} \equiv 1 \pmod{17}$

Then $g = 3$ is a primitive root.

Note

The primes less than $\sqrt{17}$ will be considered to determine the primitive roots of 17.

Clearly 3 is required prime whose power up to $p-1$ *i.e* $17-1=16$ have produced the numbers 1,2,3,4,..... 16 in some order.

We observe that 1,3,5,7,9,11,13,15 are coprimes to 16, and also $3^1 \equiv 3, 3^3 \equiv 10, 3^5 \equiv 5, 3^7 \equiv 11, 3^9 \equiv 14, 3^{11} \equiv 7, 3^{13} \equiv 12$ and $3^{15} \equiv 6 \pmod{17}$.

Hence the primitive roots of 17 are :

3, 5, 6, 7, 10, 11, 12, 14.

Example 11. *Find the primitive roots of* 10.

Or

Find two primitive roots of 10.

Solution. We have

$$\phi(10) = \phi(2 \cdot 5)$$
$$= \phi(2)\,\phi(5)$$
$$= (2-1)(5-1)$$
$$= 4.$$

The possible co-prime to 10 are 3, 5, 7.
Thus, possible primitive roots may 3, 5 and 7.

Now $3^2 \equiv 9 \pmod{10}$

$3^3 \equiv 7 \pmod{10}$

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

Hence 3 is a primitive root of modulo 10.
Further,

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

$5^3 \equiv 5 \pmod{10}$

$\vdots \quad \vdots$

$5^n \equiv 5 \pmod{10}$

$\Rightarrow$ 5 is not a primitive root of modulo 10.
Finally,

$7^2 \equiv 9 \pmod{10}$

$7^3 \equiv 3 \pmod{10}$

$7^4 \equiv 1 \pmod{10}$

$\Rightarrow$ 7 is also a primitive root of modulo 10.
Hence 3 and 7 are two primitive roots of modulo 10.

Example 12. *Find the primitive root of* $p = 41$.

Solution. We have

$$p - 1 = 40 = 2^3 \cdot 5$$

$$\frac{p-1}{2} = 20.$$

By computation modulo 41, we have

$$3^2 = 9,\ 3^4 = 81 \equiv -1,\ 3^6 \equiv -9,\ 3^{16} \equiv 1,\ 3^{20} \equiv -1$$

$\Rightarrow$ 3 is not the solution of the congruence $x^{40/2} = x^{20} \equiv 1 \pmod{41}$.

As $\frac{p-1}{5} = 8$ and

$$2^2 = 4,\ 2^4 = 16,\ 2^8 = 256 = 1.$$

Clearly, 2 is not a solution of the congruence $x^{40/5} = x^8 \equiv 1 \pmod{41}$

Hence $3^5 \cdot 2^8 \equiv -3 \cdot 10 \equiv 11 \pmod{41}$ is a primitive root of 41.

Example 13. *Find the primitive roots of 15.*

Solution. We have

$$\begin{aligned}\phi(15) &= \phi(3 \cdot 5)\\ &= \phi(3)\,\phi(5)\\ &= (3-1)(5-1)\\ &= 2 \cdot 4\\ &= 8\\ &= 2^3\end{aligned}$$

$\Rightarrow$ 2 is the only prime divisor of $\phi(15)$.
The possible co-prime to 15 are 1, 2, 4, 7, 8, 11, 13, 14.
Thus possible primitive roots may be 2, 4, 7, 11, 13.

Now $2^4 \equiv 1 \pmod{15}$

$4^2 \equiv 1 \pmod{15}$

$7^{14} \equiv 1 \pmod{15}$

$11^2 \equiv 1 \pmod{15}$

$13^4 \equiv 1 \pmod{15}$

Hence there exists no primitive root of 15.

Example 14. *Show that 12 has no primitive root.*

Solution. We have

$$\begin{aligned}\phi(12) &= \phi(4 \cdot 3)\\ &= \phi(4)\,\phi(3)\\ &= 2 \cdot 2\\ 4 &= 2^2\end{aligned}$$

$\Rightarrow$ 2 is the only prime divisor of $\phi(12)$.
The possible co-prime to 12 are 1, 5, 7, 11.
Thus possible primitive roots may be 5, 7, 11.

Now $5^2 \equiv 1 \pmod{12}$

$7^2 \equiv 1 \pmod{12}$

$11^2 \equiv 1 \pmod{12}$

Hence there exists no primitive root of 12.

COMPOSITE NUMBERS HAVING PRIMITIVE ROOTS

Theorem 9. ***For any integer $k \geq 3$, prove that the integer 2^k has no primitive roots.***

Proof. If a is an odd integer, then for $k \geq 3$, we have

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

[$\because$ we know that if a is an odd integer then

$$a^{2^{n-2}} \equiv 1 \pmod{2^n} \ \forall\ n \geq 3]$$

If $k = 3$, then (1) becomes

$$a^2 \equiv 1 \pmod 8, \qquad \text{---(1)}$$

which is true as $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$.

For $k > 3$, let us proceed by induction on k.

Let us assume that the asserted congruence holds for the integer k;

i.e $a^{2^{k-2}} \equiv 1 \pmod{2^k}$

which is equivalent to the equation

$$a^{2^{k-2}} = 1 + b2^k,$$

where b is an integer.

Squaring both sides of (2), we get ---(2)

$$\begin{aligned} a^{2^{(k+1)-2}} &= a^{2^{k-1}} = (a^{2^{k-2}})^2 \\ &= 1 + 2(b2^k) + (b2^k)^2 \\ &= 1 + 2^{k+1}(b + b^2 2^{k-1}) \\ &\equiv 1 \pmod{2^{k+1}} \end{aligned}$$

so that the asserted congruence holds for $k+1$ and hence for all $k \geq 3$.

Now the integers that are relatively prime to 2^k are clearly the odd integers, so that

$$\phi(2^k) = 2^{k-1}.$$

Thus we have proved that if a is odd integer and $k \geq 3$,

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

and consequently there are no primitive roots of 2^k.

Theorem 10. ***If $gcd(m, n) = 1$, where $m > 2$ and $n > 2$, then the integer mn has no primitive roots.***

Proof. If possible, let a be a primitive root belonging to mn.

Then (i) a has exponent $\phi(mn)$ modulo mn and

(ii) $gcd(a, mn) = 1$.

(ii) $\Rightarrow gcd(a, m) = gcd(a, n) = 1$

Therefore by Euler's theorem, we have

$$a^{\phi(m)} \equiv 1 \pmod m,$$

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

Let $h = \dfrac{\phi(m)\,\phi(n)}{(\phi(m), \phi(n))}$

$= [\phi(m), \phi(n)]$

Now m and n are both greater than 2 ($\because \phi(m), \phi(n)$ are both even)

$\Rightarrow \quad (\phi(m), \phi(n)) \geq 2$

$\therefore \quad h \leq \dfrac{\phi(m)\,\phi(n)}{2} = \dfrac{\phi(mn)}{2} < \phi(mn)$ ....(1)

Also $a^h = (a^{\phi(m)})^{\frac{\phi(n)}{(\phi(m), \phi(n))}} \equiv 1 \pmod m$ ....(2)

and $a^h = (a^{\phi(n)})^{\frac{\phi(m)}{(\phi(m), \phi(n))}} \equiv 1 \pmod n$

As $gcd(m, n) = 1$,

(1) and (2) $\Rightarrow a^h \equiv 1 \pmod{mn}$

which contradicts the assumption that exponent of a is $\phi(mn)$ proving that there are no primitive roots $(mod\ mn)$.

Note

Some special cases of the above theorem are

The integer n fails to have a primitive root if either

(i) n is divisible by two odd primes or

(ii) n is of the form $n = 2^m p^k$, where p is an odd prime and $m \geq 2$.

Lemma 1

If p is an odd prime, then there exists a primitive root r of p such that

$$r^{p-1} \not\equiv 1 \pmod{p^2}.$$

Proof. Since we know that p has primitive roots, so let us choose any one say r.

If $r^{p-1} \not\equiv 1 \pmod{p^2}$, then we are done.

In the contrary case let us replace r by $r' = r + p$, which is also a primitive root of p.

Then using the bionomial theorem, we have

$$(r')^{p-1} \equiv (r+p)^{p-1}$$
$$\equiv r^{p-1} + (p-1)\,pr^{p-2} \pmod{p^2}$$

But it is assumed that $r^{p-1} \equiv 1 \pmod{p^2}$

Therefore $(r')^{p-1} \equiv 1 - pr^{p-2} \pmod{p^2}$

Since r is a primitive root of p, and

$gcd\,(r, p) = 1$,

$\therefore \quad p \nmid r^{p-2}$

which shows that $(r')^{p-1} \not\equiv 1 \pmod{p^2}$.

Hence the Proof.

Corollary. *If p is an odd prime, p^2 has a primitive root; infact, for a primitive root r of p, either r or $r + p$ (or both) is a primitive root of p^2.*

Proof. If r is a primitive root of p, then the order of r modulo p^2 is either $p-1$ or $p\,(p-1) = \phi\,(p^2)$.

Thus if r has order $p-1$ modulo p^2, then $r+p$ is a primitive root of p^2.

Note

3 is a primitive root of 7 and both 3 and 10 are primitive roots of 7^2.

Also 14 is a primitive root of 29 but not of 29^2.

Lemma 2

Let p be an odd prime and r be a primitive root of p with the property that $r^{p-1} \not\equiv 1 \pmod{p^2}$. Then for each positive integer $k \geq 2$,

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}.$$

Proof. We prove the lemma by induction on k.

By hypothesis, the result is true for $k = 2$.

Let us assume that the result is true for some $k \geq 2$.

We are to show that the result is true for $k+1$.

Since $gcd\,(r, p^{k-1}) = gcd\,(r, p^k) = 1$, then by Euler's theorem, we have

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

Hence, there exists an integer satisfying

$$r^{p^{k-2}(p-1)} \equiv 1 + a\,p^{k-1}, \qquad \ldots(1)$$

where $p \nmid a$ by our induction hypothesis.

Raising both sides of (1) to the p^{th} power, we get

$$r^{p^{k-1}(p-1)} = (1 + ap^{k-1})^p$$
$$\equiv 1 + ap^k \pmod{p^{k+1}}$$

Since the integer a is not divisible by p's we have

$$r^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}.$$

Thus the result is true for $k+1$.

Also it is true for $k = 2$.

Therefore, by induction the result is true.

Theorem 11. ***If p is an odd prime number and $k \geq 1$, then there exists a primitive root for p^k.***

Proof. By lemma 1 and lemma 2 let us choose a primitive root r of p for which

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}.$$

Thus any integer r satisfying the condition $r^{p-1} \not\equiv 1 \pmod{p^2}$ will serve our purpose.

In this way such an r will be primitive root for all powers of p.

Let n be the order of r modules p^k.

Then by the theorem, "*Let the integer a have order k modulo n. Then $a^k \equiv 1 \pmod{n}$ if and only if $k \mid h$*", n must divide

$$\phi\,(p^k) = p^{k-1}\,(p-1).$$

Since $r^n \equiv 1 \pmod{p^k}$

$\Rightarrow \quad r^n \equiv 1 \pmod{p}$

Again by the above quoted theorem,

$$p - 1 \mid n.$$

$\Rightarrow \quad n = p^m\,(p-1)$, where $0 \leq m \leq k-1$.

If $n \neq p^{k-1\,(p-1)}$, then

$p^{k-2\,(p-1)}$ will be divisible by n.

Then we get

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

which contradicts the choice of r.

Therefore, $n = p^{k-1}(p-1)$ and r is a primitive root for p^k.

Corollary. *There are primitive roots for $2p^k$, where p is an odd prime and $k \geq 1$.*

Proof. Let r be a primitive root for p^k.

Let us assume that r is an odd integer.

For if it is even, then

$r + p^k$ is odd

and it is also a primitive root for p^k.

Then $gcd(r, 2p^k) = 1$.

The order n of r modulo $2p^k$ must divide

$$\phi(2p^k) = \phi(2)\,\phi(p^k) = \phi(p^k).$$

But $r^n \equiv 1 \pmod{2p^k}$

$\Rightarrow$ $r^n \equiv 1 \pmod{p^k}$,

and therefore $\phi(p^k) \mid n$.

Thus combining these divisibility conditions, we get

$$n = \phi(2p^k)$$

which shows that r is a primitive root of $2p^k$.

Note

The prime 5 has $\phi(4) = 2$ primitive roots, namely, the integers 2 and 3.

Since $2^{5-1} \equiv 16 \not\equiv 1 \pmod{25}$

and $3^{5-1} \equiv 6 \not\equiv 1 \pmod{25}$,

These are also primitive roots for 52 and hence for all higher powers of 5.

The proof of the above corollary guarantees that 3 is a primitive root for all numbers of the form $2 \cdot 5^k$.

Theorem 12. ***An integer $n > 1$ has a primitive root if and only if $n = 2, 4, p^k$.***

Proof. To this end, we wish to show that the integers specified are the only integers with primitive roots.

Any integer $n > 1$ can be expressed in the form

(i) $n = 2^e$ $(e \geq 1)$

or in the form

(ii) $n = 2^e p_1^{e_1} p_2^{e_2} \ldots\ldots p_r^{e_r}$ $(e \geq 0,\ r \geq 1$ and each $e_i \geq 1)$,

where $p_1, \ldots\ldots, p_r$ are distinct odd primes.

Case 1 $\phi(e^2) = 2^{e-1}$.

We show, by induction, that if $gcd(a, 2^e) = 1$ and $e \geq 3$, then

$$a^{\frac{1}{2}\phi(2^e)} \equiv 1 \pmod{2^e} \qquad \ldots(1)$$

Since a is an odd integer k,

so $a = 1 + 2k$ for some integer k.

Thus $a^2 = 1 + 4k(k+1)$

$= 1 + 8k_1$, say, since either k or $k+1$ is even.

Hence $a^2 \equiv 1 \pmod{2^3}$.

The fact that $\frac{1}{2}\phi(2^3) = 2$ proves that (1) holds good with $e = 3$.

Now assume that (1) holds for an integer e.

Then $a^{\frac{1}{2}\phi(2^e)} = 1 + 2^e t_2$ for some integer t_2.

Hence $a^{\frac{1}{2}\phi(2^{e+1})} = a^{\phi(2^e)}$

$= (1 + 2^e t_2)^2$

$= 1 + 2^{e+1}(t_2 + t_2^2 2^{e-1})$

$\equiv 1 \pmod{2^{e+1}}$

Induction establishes that (1) hold true for each integer $e \geq 3$.

We have deduced from (1) that if $e \geq 3$, each integer prime to 2^e has as orde

$(mod\ 2^e)$ an integer $\leq \frac{1}{2}\phi(2^e)$.

Hence for $e \geq 3$, the integer 2^e has no primitive root.

If we write

$$\psi(2^e) = \begin{cases} \phi(2^e) & \text{for } e = 0, 1, 2 \\ \frac{1}{2}\phi(2^e) & \text{for } e \geq 3, \end{cases}$$

Then the result in case (1) can be states as follows :

If $(a, 2^e) = 1$, then $a^{\psi(2^e)} \equiv 1 \pmod{2^e}$

Case 2

The case provides :

$$\phi(n) = \phi(2^e)\, p_1^{e_1-1} \ldots\ldots p_r^{e_r-1} (p_1 - 1) \ldots\ldots (p_r - 1). \qquad \text{---(2)}$$

If $gcd(a, n) = 1$, then

$gcd(a, p_i) = 1$ for $i = 1, 2, \ldots\ldots, r$ and also $gcd(a, 2^e) = 1$.

Consequently

$a^{\phi(p_i^{e_i})} \equiv 1 \pmod{p_i^{e_i}}$ $(i = 1, 2, \ldots\ldots, r)$ and from (2),

$a^{\psi(2^e)} \equiv 1 \pmod{2^e}$

Now we write

$\psi(n) = \{\psi(2^e), \phi(p_1^{e_1}), \ldots\ldots, \phi(p_r^{e_r})\}$ as the least common multiple of

$\psi(2^e), \phi(p_1^{e_1}), \ldots\ldots,$ and $\phi(p_r^{e_r})$,

then

$a^{\psi(n)} \equiv 1 \pmod{p_i^{e_i}}$ $(i = 1, 2, \ldots\ldots, r)$ and $a^{\psi(n)} \equiv 1 \pmod{2^e}$.

Therefore $a^{\psi(n)} \equiv 1 \pmod{n}$.

Now $\psi(n) = \{\psi(2^e), p_1^{e_1-1}(p_1 - 1), \ldots\ldots, p_r^{e_r-1}(p_r - 1)\}$.

Integers $p_1 - 1, \ldots\ldots, p_r - 1$ are even, and they have atleast the factor 2 in common.

Thus for $r \geq 2$, it follows that $\psi(n) < \phi(n)$ and that n has no primitive root.

Also if $r = 1$ and $e \geq 2$, then $\psi(2^e)$ and $p_1 - 1$ have a common factor ≥ 2.

This again implies that

$\psi(n) < \phi(n)$ and that n has no primitive root.

Hence the Proof.

Example 15. Establish each of the statements below :

(i) If a has order bk modulo n then a^b has order k modulo n

(ii) If a has order 2k modulo the odd prime p, then $2^k \equiv -1 \pmod{p}$

Solution (i). We have $O(a) \pmod{n} = bk$

$$O(a^b) \pmod{n} = \frac{bk}{(b, bk)}$$

$$= \frac{bk}{b} = k$$

(ii) We have $O(a) \pmod{p} = 2k$

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

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

$\Rightarrow$ $p \mid (a^k - 1)(a^k + 1)$

$\Rightarrow$ $p \mid a^k - 1$ or $p \mid a^k + 1$

$\Rightarrow$ $a^k \equiv 1 \pmod{p}$ or

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

Since $O(a) \pmod{p} = 2k$,

therefore $2k$ is the least positive integer such that $a^{2k} \equiv 1 \pmod{p}$

$\therefore$ $a^k \not\equiv 1 \pmod{p}$

Hence $a^k \equiv 1 \pmod{p}$.

Example 16. Given that a has order 3 modulo p where p is an odd prime. Show that a + 1 must have order 6 modulo p.

Solution. Since $O(a) \pmod{p} = 3$

$\Rightarrow$ $a^3 \equiv 1 \pmod{p}$

$\Rightarrow$ $p \mid a^3 - 1$

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

$\Rightarrow$ $p \mid a - 1$ or $p \mid a^2 + a + 1$

Since $p \mid a - 1$

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

$\Rightarrow$ $O(a) \pmod{p} = 1$, $[\because O(a) \pmod{p} = 3]$

which is contradiction.

Therefore $p \mid a^2 + a + 1$

$\Rightarrow$ $a^2 + a + 1 \equiv 0 \pmod{p}$

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

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

$\Rightarrow$ $(a+1)^3 \equiv a(a+1) \pmod{p}$

i.e $(a+1)^3 \equiv a^2 + a \pmod{p}$ ...(1)

$\Rightarrow$ $(a+1)^3 \equiv -1 \pmod{p}$ by (1)

$\Rightarrow$ $(a+1)^6 \equiv 1 \pmod{p}$

$O(a+1) \pmod{p} = 6$.

Example 17. *If $O(a) \pmod{p} = k$ where p is prime number, then $O(a) \pmod{p^2} = k$ or kp.*

Solution. Let $O(a) \pmod{p^2} = h$

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

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

$\therefore$ $O(a) \pmod{p} \mid h \Rightarrow k \mid h$

$\Rightarrow$ $h = k\lambda$ for some integer λ

Since $O(a) \pmod{p} = k$

$\Rightarrow$ $a^k \equiv 1 \pmod{p}$ ...(1)

$\Rightarrow$ $a^k = 1 + tp$ for some integer t

$\Rightarrow$ $(a^k)^p = (1+tp)^p$

$\Rightarrow$ $a^{kp} = 1 +$ (terms containing p^2)

Taking $(mod\, p^2)$, we get

$a^{kp} \equiv 1 + 0 \pmod{p^2}$

i.e $a^{kp} \equiv 1 \pmod{p^2}$

$\therefore$ $O(a) \pmod{p^2} \mid kp$

$\Rightarrow$ $h \mid kp$

$\Rightarrow$ $k\lambda \mid kp$ by (1)

$\Rightarrow$ $\lambda \mid p$

$\Rightarrow$ $\lambda = 1$ or p

Therefore from (1), we have

$h = k$ or kp

i.e $O(a) \pmod{p^2} = k$ or kp

Example 18. *Show that 2 is primitive root of 11.*

Solution. We know that if $O(a) \pmod{n} = m$,

then $m \mid \phi(n)$.

Here $\phi(11) = 10$

Therefore divisors of $\phi(11)$ are 2, 5 and 10.

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

$\Rightarrow$ $2^5 \equiv 2^2 \cdot 2^3 \equiv 4 \times 8 \pmod{11}$

$\Rightarrow$ $2^5 \equiv -1 \pmod{11}$

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

Therefore 10 is the smallest positive integer such that

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

$\therefore$ $O(2) \pmod{11} = 10$

i.e $O(2) \pmod{11} = \phi(11)$

$\Rightarrow$ 2 is primitive root of 11.

Example 19. *Find the primitive root of 13.*

Solution. Here $p = 13$

$\therefore$ $p - 1 = 12 = 2^2 \cdot 3^1$

Consider $x^{2^2} - 1 \pmod{13}$ ....(1)

i.e $x^4 - 1 \pmod{13}$

and $x^{2^1} - 1 \pmod{13}$ ....(2)

i.e $x^2 - 1 \pmod{13}$

Since $x = 5$ is root of (1) which is not root of (2) so that $\beta_1 = 5$

Again consider $x^{3^1} - 1 \pmod{13}$

i.e $x^3 - 1 \pmod{13}$ ....(3)

and $x^{3^0} - 1 \pmod{13}$

i.e $x - 1 \pmod{13}$ ....(4)

Since $x = 3$ is a root of (3) which is not root of (4) so that $\beta_2 = 3$.

Therefore $\beta_1 \beta_2 = 5 \cdot 3$ is primitive root of 13

i.e 15 is primitive root of 13

$\Rightarrow$ 2 is primitive root of 13 [$\because 15 \equiv 2 \pmod{13}$]

Example 20. *Show that 5 is a primitive root of 18.*

Solution. We know that if a has order k modulo n then $k \mid \phi(n)$.

Here $\phi(18) = \phi(2 \cdot 3^2)$

$= \phi(2) \cdot \phi(3^2)$

$= 1 \cdot 3(3-1)$

$= 6$

Divisors of $\phi(18)$ are 2, 3 and 6

Now $5^2 \equiv 7 \pmod{18}$,

$5^3 \equiv -1 \pmod{18}$ and

$5^6 \equiv 1 \pmod{18}$

$\therefore$ $\phi(18) = 6$ is the smallest positive integer such that $5^6 \equiv 1 \pmod{18}$

$\Rightarrow$ 5 is a primitive root of 18.

Example 21. *Show that 5 is a primitive root of 23. Hence find all the primitive roots of 23.*

Solution. We know that if a has order k modulo n then $k \mid \phi(n)$.

Here $\phi(23) = 22$.

$\therefore$ Divisors of 22 are 1, 2, 11 or 22.

Now $5^1 \equiv 5 \pmod{23}$,

$5^2 \equiv 2 \pmod{23}$

$5^{11} = (5^2)^5 \cdot 5 \equiv 2^5 \cdot 5 \equiv 160 \equiv 22 \pmod{23}$

$\therefore$ 5 has order 22 modulo 23.

Hence 5 is a primitive root of 23.

Now order of 5^k modulo $23 = 22$

iff $\dfrac{22}{(k, 22)} = 22$

iff $(k, 22) = 1$

iff $k = 1, 3, 5, 7, 9, 13, 15, 17, 19, 21$

and $5^1 \equiv 5 \pmod{23}$,

$5^3 = 125 \equiv 10 \pmod{23}$,

$5^5 = 5^2 \cdot 5^3 \equiv 25 \cdot 10 \equiv 2 \cdot 10 \equiv 20 \pmod{23}$,

$5^7 = 5^2 \cdot 5^5 \equiv 2 \cdot 20 \equiv 17 \pmod{23}$,

$5^9 = 5^2 \cdot 5^7 \equiv 2 \cdot 17 \equiv 11 \pmod{23}$,

$5^{13} = (5^2)^2 \cdot 5^9 \equiv 4 \cdot 11 \equiv 21 \pmod{23}$,

$5^{15} = 5^2 \cdot 5^{13} \equiv 2 \cdot 21 \equiv 19 \pmod{23}$,

$5^{17} = 5^2 \cdot 5^{15} \equiv 2 \cdot 19 \equiv 15 \pmod{23}$,

$5^{19} = 5^2 \cdot 5^{17} \equiv 2 \cdot 15 \equiv 7 \pmod{23}$,

$5^{21} = 5^2 \cdot 5^{19} \equiv 2 \cdot 7 \equiv 14 \pmod{23}$.

Therefore primitive roots of 23 are 5, 7, 10, 11, 14, 15, 17, 19, 20 and 21.

Example 22. *Find all primitive roots of 9.*

Solution. The integers ≤ 9 which are relatively prime to 9 are 1, 2, 4, 5, 7, 8.

Since $9 \geq 3$, therefore, 1 cannot be a primitive root of 9.

Therefore possible integers for the primitive roots of 9 are 2, 4, 5, 7, 8.

Here $\phi(9) = 6$

and $2^2 \equiv 4 \pmod{9}$

$2^3 \equiv 8 \equiv -1 \pmod{9}$

$2^6 \equiv 1 \pmod{9}$

$\therefore$ 2 is a primitive root of 9.

Since $4^2 \equiv 7 \pmod{9}$

and $4^3 \equiv 1 \pmod{9}$

Therefore 4 is not primitive root of 9.

$5^2 \equiv 7 \pmod{9}$

$5^3 \equiv 8 \equiv -1 \pmod{9}$

$5^6 \equiv 1 \pmod{9}$

Therefore 5 is a primitive root of 9.

$7^2 \equiv 4 \pmod{9}$

$7^3 \equiv 1 \pmod{9}$

Therefore 7 is not a primitive root of 9.

$8^2 \equiv 1 \pmod 9$

$\therefore$ 8 is not primitive root of 9.

Example 23. *Find a primitive root of 7 and verify whether it is primitive root of 7^3.*

Solution. Let $p = 7$

$\therefore \quad p - 1 = 6 = 2^1 \cdot 3^1$

Consider $x^{2^1} - 1 \pmod 7$

i.e $x^2 - 1 \pmod 7$

and $x^{2^0} - 1 \pmod 7$ *i.e* $x - 1 \pmod 7$

Again consider

$x^{3^1} - 1 \pmod 7$ *i.e* $x^3 - 1 \pmod 7$ ...(1) ...(2)

and $x^{3^0} - 1 \pmod 7$

i.e $x - 1 \pmod 7$ ...(3)

Now $x = 2$ is root of (3) which is not root of (4) ...(4)

$\therefore -1 \cdot 2$ is a primitive root of 7

i.e -2 is primitive root of 7

$\Rightarrow$ 5 is primitive root of 7

Now $5^{7-1} = 5^6 = 5^3 \cdot 5^3 = 125 \times 125$ [$\because -2 \equiv 5 \pmod 7$]

$\equiv 27 \times 27 \pmod{7^2}$

$\not\equiv 1 \pmod{7^2}$

i.e $5^{7-1} \not\equiv 1 \pmod{7^2}$

$\therefore$ 5 is also primitive root of 7^3.

Example 24. *Prove that 3 is a primitive root of all integers of the form 7^k and $2 \cdot 7^k$.*

Or

Prove that 3 is a primitive root of all integers of the form 7^k, for any integer $k \geq 1$.

Solution. Here $\phi(7) = 6 = 2 \cdot 3$

Now $\frac{\phi(7)}{2} = \frac{6}{2} = 3$ and

$\frac{\phi(7)}{3} = \frac{6}{3} = 2$

A number a coprime to 7 is primitive root of 7 if $a^3 \not\equiv 1 \pmod 7$ and $a^2 \not\equiv 1 \pmod 7$

Letting $a = 2, 3$, we find

$2^3 \equiv 1 \pmod 7$ and $2^2 \not\equiv 1 \pmod 7$

so that 2 is not primitive root of 7.

$3^1 \not\equiv 1 \pmod 7$ and $3^2 \not\equiv 1 \pmod 7$

So that 3 is primitive root of 7

Therefore 3 is the smallest positive root of 7.

Now $3^{7-1} = 3^6 = 729 \not\equiv 1 \pmod{7^2}$

$\therefore$ *3 is also primitive root of $7^k \; \forall \; k \in N$.*

Since 3 is odd primitive root of 7^k,

therefore 3 is also primitive root of

$2 \cdot 7^k \; \forall \; k \in N$.

Example 25. *Find a primitive root of any integer of the form 17^k.*

Solution. Since 3 is a primitive root of 17 and

$3^{17-1} = 3^{16} = 3^8 \cdot 3^8$

$= 6561 \cdot 6561$

$\equiv 203 \cdot 203 \pmod{17^2}$

$\not\equiv 1 \pmod{17^2}$

Therefore 3 is a primitive root of $17^k \; \forall \; k \geq 1$.

THE THEORY OF INDICES

Definition. *Let r be a primitive root of n. If gcd $(a, n) = 1$, then the smallest positive inte*

k such that $a \equiv r^k \pmod n$ is called the ***index of a relative to r.***

In symbols we write as

$Ind_r\, a = k$ *if* $a \equiv r^k \pmod n$

Or simply ind $a = k$ whenever it is clear which primitive root is referred to.

e.g., the integer 2 is a primitive root of 5 and

$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 3, 2^4 \equiv 1 \pmod 5$

It follows that

$$Ind_2\, 1 = 4,\ Ind_2\, 2 = 1,\ Ind_2\, 3 = 3,\ Ind_2\, 4 = 2.$$

Theorem 13. ***If n has a primitive root r and let a denotes the index of a relative to r, then the following properties hold :***

(i) ind a = ind b iff $a \equiv b \pmod{n}$

(ii) ind (ab) = ind (a) + ind (b) $\pmod{\phi(n)}$

(iii) ind $a^k \equiv k \cdot$ ***ind a*** $\pmod{\phi(n)}$ ***for k***

(iv) ind $1 \equiv 0 \pmod{\phi(n)}$, ***ind*** $r \equiv 1 \pmod{\phi(n)}$

(v) ind $(-1) = \dfrac{\phi(n)}{2}$ ***for all*** $n > 2$.

Proof (i) By definition,

$$r^{ind\, a} \equiv a \pmod{n} \text{ and}$$

$$r^{ind\, b} \equiv b \pmod{n}$$

Let $ind\, a = ind\, b$

$$\Rightarrow \quad r^{ind\, a} \equiv r^{ind\, b} \pmod{n}$$

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

Conversely, let $a \equiv b \pmod{n}$

$$\Rightarrow \quad r^{ind\, a} \equiv r^{ind\, b} \pmod{n}$$

$$\Rightarrow \quad ind\, a \equiv ind\, b \pmod{n}$$

$$\Rightarrow \quad ind\, a = ind\, b$$

(ii) Let $ind\, a = r$ and $\qquad [\because 1 \le ind\, a,\ ind\, b \le n]$

$$ind\, b = s$$

Then $a \equiv c^r \pmod{n}$ and

$$b \equiv c^s \pmod{n}$$

Now $ab = c^r c^s \pmod{n}$

Or $ab = c^{r+s} \pmod{n}$

But, if $t = ind\, ab$, then

$$ab \equiv c^t \pmod{n}$$

$$\therefore \quad r + s = t \pmod{\phi(n)}$$

$$\Rightarrow \quad ind\,(ab) = ind\, a + ind\, b \pmod{\phi(n)}$$

(iii) Since $r^{ind\, a^k} \equiv a^k \pmod{n}$,

and by the laws of exponents

$$r^{k\, ind\, a} = (r^{ind\, a})^k$$

$$\equiv a^k \pmod{n}.$$

Hence $r^{ind\, a^k} \equiv r^{k\, ind\, a} \pmod{n}$.

which shows that

$$ind\, a^k \equiv k \cdot ind\, a \pmod{\phi(n)}.$$

(iv) The result is obvious.

e.g. 3 is a primitive root mod 5.

We give indices of 1, 2, 3, 4 (*mod* 5) relative to 3.

integer	1	2	3	4
Index	4	3	1	2

Or 0

The index 0 is not defined.

(v) Let $ind\,(-1) = i$

$$\Rightarrow \quad -1 \equiv r^i \pmod{n}$$

$$\Rightarrow \quad 1 \equiv r^{2i} \pmod{n}$$

Or $r^{2i} \equiv 1 \pmod{n}$ $\qquad [\because$ order of r and $n = \phi(n)]$

$$\Rightarrow \quad \phi(n) \mid 2i$$

$$\Rightarrow \quad 2i = k\,\phi(n) \text{ for some } k \in Z$$

Now $i \le \phi(n)$

$$\Rightarrow \quad 2i \le 2\,\phi(n)$$

$$\Rightarrow \quad k\,\phi(n) \le 2\,\phi(n)$$

$$\Rightarrow \quad k \le 2$$

$$\Rightarrow \quad k = 1 \text{ or } 2$$

If $k = 2$ then $i = \phi(n)$

$$\therefore \quad r^{\phi(n)} \equiv -1 \pmod{n}$$

which is not true as r is primitive root of n.

$\therefore \quad k = 1$

$\Rightarrow \quad 2i = \phi(n)$

$\Rightarrow \quad i = \frac{\phi(n)}{2}$

$\therefore \quad ind(-1) = \frac{\phi(n)}{2}$.

Example 26. *Construct the index table* (*mod* 11).

Solution. $\phi(11) = 10$ and 2 is the smallest primitive root of 11.

Now $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8,$

$2^4 \equiv 5, 2^5 \equiv 10, 2^6 \equiv 9, 2^7 \equiv 7,$

$2^8 \equiv 3, 2^9 \equiv 6, 2^{10} \equiv 1$

So the required table is arranged as follows :

Ind (*a*)	1	2	3	4	5	6	7	8	9	10
a	2	4	8	5	10	9	7	3	6	1

Example. *Construct the index table* (*mod* 17).

Solution 27. $\phi(17) = 16$ and 3 is the smallest primitive root of 17.

Now $3^1 \equiv 3, 3^2 \equiv 9, 3^3 \equiv 10, 3^4 \equiv 13,$

$3^5 \equiv 5, 3^6 \equiv 15, 3^7 \equiv 11, 3^8 \equiv 16,$

$3^9 \equiv 14, 3^{10} \equiv 8, 3^{11} \equiv 7,$

$3^{12} \equiv 4, 3^{13} \equiv 12, 3^{14} \equiv 2, 3^{15} \equiv 6, 3^{16} \equiv 1.$

So the required table is arranged as follows :

Ind (*a*)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
a	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Note

By using the properties of indices, we can solve the congruence $ax^n \equiv b \pmod{p}$ with the help of index table for prime p.

Example 28. *Solve the congruence* $7^x \equiv 5 \pmod{13}$ *using* 2 *as primitive root* (*mod* 13).

Solution. The given congruence is

$7^x \equiv 5 \pmod{13}$

Taking indices, we get

$Ind(7^x) \equiv Ind(5) \pmod{\phi(13)}$ ....(1)

$\Rightarrow \quad x\,Ind(7) \equiv Ind(5) \pmod{12}$

Now we construct the index table (*mod* 13) :

Ind	1	2	3	4	5	6	7	8	9	10	11	12
Number	2	4	8	3	6	12	11	9	5	10	7	1

Putting the values of indices, the congruence (1) becomes

$x \cdot 11 \equiv 6 \pmod{12}$

i.e $\quad 11x \equiv 6 \pmod{12}$

Now $\quad 11x \equiv 6 \pmod{12}$

Also $\quad 0 \equiv 60 \pmod{12}$

Adding

$11x \equiv 66 \pmod{12}$

$\Rightarrow \quad x \equiv 6 \pmod{12}$

Hence $x = 6$ is solution of the given congruence. $\Rightarrow \quad x \equiv 6 \pmod{12}$]

Example 29. *Solve the congruence* $11^x \equiv 28 \pmod{31}$ *using* 3 *as primitive root* (*mod* 31).

Solution. The given congruence is

$11^x \equiv 28 \pmod{31}$

Taking indices, we get

$Ind(11^x) \equiv Ind(28) \pmod{\phi(31)}$ ....(1)

$\Rightarrow \quad x\,Ind(11) \equiv Ind(28) \pmod{30}$

Now we construct the index table (*mod* 31) :

Ind	1	2	3	4	5	6	7	8	9	10	11	12
Number	3	9	27	19	26	16	17	20	29	25	13	8
Ind	13	14	15	16	17	18	19	20	21	22	23	24
Number	24	10	30	28	22	4	12	5	15	14	11	2

Putting the values of the indices, the congruence (1) becomes

$x \cdot 23 \equiv 16 \pmod{30}$

i.e $23x \equiv 16 \pmod{30}$

$\Rightarrow$ $x \equiv 2 \pmod{30}$

Hence $x = 2$ is solution of given congruence.

Example 30. *Solve the congruence* $2x^3 \equiv 23 \pmod{31}$ *using 3 as primitive root (mod 31).*

Solution. The given congruence is

$$2x^3 \equiv 23 \pmod{31}$$

Taking indices, we get

$$Ind\,(2x^3) \equiv Ind\,(23) \pmod{\phi\,(31)}$$

$\Rightarrow$ $Ind\,(2) + Ind\,(x^3) \equiv Ind\,(23) \pmod{30}$

Example 31. *Solve the congruence* $2x^3 \equiv 23 \pmod{31}$ *using 3 as primitive root (mod 31).*

Solution. The given congruence is

$$2x^3 \equiv 23 \pmod{31}$$

Taking indices, we get

$$Ind\,(2x)^3 \equiv Ind(23) \pmod{\phi\,(31)}$$

$\Rightarrow$ $Ind\,(2) + Ind\,(x^3) \equiv Ind\,(23) \pmod{30}$

$\Rightarrow$ $Ind\,(2) + 3\,Ind(x) \equiv Ind\,(23) \pmod{30}$

$\Rightarrow$ $Ind\,(2) + 3X \equiv Ind\,(23) \pmod{30}$

where $X = Ind\,(x)$ ....(1)

Now we construct the index table $(mod\,31)$:

Ind	1	2	3	4	5	6	7	8	9	10	11	12
Number	3	9	27	19	26	16	17	20	29	25	13	8
Ind	13	14	15	16	17	18	19	20	21	22	23	24
Number	30	28	22	24	10	4	12	5	15	14	11	2
Ind	25	26	27									
Number	6	18	23									

Putting the value of indices, the congruence (1) becomes

$$24 + 3X \equiv 27 \pmod{30}$$

$$3X \equiv 3 \pmod{30} \quad \ldots(2)$$

$\Rightarrow$ Since $(3, 30) = 3$ and $3 \mid 3$,

Therefore the congruence (2) is solvable and has three in congruent solution.

Now (2) implies $X \equiv 1 \pmod{10}$

$\Rightarrow$ $X = 1$ is solution of this congruence.

$X = 1$ is also solution of (2)

Therefore all incongruence solutions of (2) are

$$1,\ 1 + \frac{30}{3},\ 1 + \frac{2 \cdot 30}{3}$$

i.e all incongruent solutions of (2) are 1, 11, 21

i.e $X = 1, 11, 21$

$\Rightarrow$ $Ind\,(x) = 1, 11, 21$ (from the table)

$\Rightarrow$ $x = 3, 13, 15$

Hence 3, 13 and 15 are incongruent solutions of given congruence.

Example 32. *Solve the linear congruence* $7x \equiv 2 \pmod{9}$.

Solution. We know that 2 is a primitive root modulo 9.

Also, $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 7, 2^5 \equiv 5$ and $2^6 \equiv 1 \pmod{9}$.

Thus index of 7 is 4 and 2 is 1.

Now $7x \equiv 2 \pmod{9}$ is equivalent to

$$Ind\,7 + Ind\,x \equiv Ind\,2 \pmod{\phi\,(9)} \qquad (\because \phi\,(9) = 6)$$

Or $4 + Ind\,x \equiv 1 \pmod{6}$

Or $Ind\,x \equiv -3 \pmod{6}$

Hence $x \equiv 2^3 \pmod{9}$

Or $x \equiv 8 \pmod{9}$

Thus solution of $7x \equiv 2 \pmod{9}$ are of the form $9t + 8$ for $t = 0, \pm 1, \pm 2, \ldots\ldots$

Example 33. *Solve the congruence* $11x^3 \equiv 2 \pmod{23}$.

Solution. We know that 5 is a primitive root modulo 23.

Also, $5^1 \equiv 5, 5^2 \equiv 2, 5^3 \equiv 10, 5^4 \equiv 4, 5^5 \equiv 20, 5^6 \equiv 8, 5^7 \equiv 17,$
$5^8 \equiv 16, 5^9 \equiv 11, 5^{10} \equiv 9 \pmod{23}$, and

$11x^3 \equiv 2 \pmod{23}$ is equivalent to

$Ind\,11 + 3\,Ind\,x \equiv Ind\,2 \pmod{\phi(23)}$

Or $9 + 3\,Ind\,x \equiv 2 \pmod{22}$

Or $3\,ind\,x \equiv -7 \pmod{22}$

Or $3\,Ind\,x \equiv 15 \pmod{22}$

Or $Ind\,x = 5 \pmod{22}$

Hence $x \equiv 5^5 \pmod{23}$

Or $x \equiv 20 \pmod{23}$

Thus $x = 23t + 20, t = 0, \pm 1, \pm 2, \ldots$ are all solutions of the given congruence.

Example 34. *Is the congruence* $x^3 \equiv 4 \pmod{13}$ *solvable ?*

Solution. Given congruence is

$$x^3 \equiv 4 \pmod{13}$$

Now $d = gcd(3, \phi(13))$

$= gcd(3, 12)$

$= 3,$

and therefore $\frac{\phi(13)}{d} = \frac{12}{3} = 4$

Since $4^4 \equiv 9 \not\equiv 1 \pmod{13}$.

Thus by the theorem, "*Let n be an integer possessing a primitive root and let* $gcd(a, n) = 1$. *Then the congruence* $x^k \equiv a \pmod{n}$ *has a solution if and only if* $a^{\phi(n)/d} \equiv 1 \pmod{n}$

where $d = gcd(k, \phi(n))$", the congruence is not solvable.

Theorem 14. Let n be a positive integer possessing a primitive root and let $(a, n) = 1$.

Then the congruence $x^k \equiv a \pmod{n}$ ***has a solution if and only if*** $a^{\frac{\phi(n)}{d}} \equiv 1 \pmod{n}$ ***where***

$d, \phi(n))$ ***(if it has solution) there are exactly d solutions modulo n.***

of. We have

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

Taking indices, we get

$$Ind\left(a^{\frac{\phi(n)}{d}}\right) \equiv Ind(1) \pmod{\phi(n)}$$

$$\Rightarrow \frac{\phi(n)}{d} Ind\,(a) \equiv Ind\,(1) \pmod{\phi(n)}$$

$$\Rightarrow \frac{\phi(n)}{d} Ind\,(a) \equiv 0 \pmod{\phi(n)}\ [\because Ind\,(1) \equiv 0 \pmod{\phi(n)}]$$

which holds iff $d \mid Ind\,(a)$

i.e iff $x^k \equiv a \pmod{n}$ has solution.

Hence the congruence $x^k \equiv a \pmod{n}$ has solution iff

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

Example 35. Show that congruence $x^3 \equiv 3 \pmod{19}$ *has no solution while* $x^3 \equiv 11 \pmod{19}$ *has three incongruent solutions.* ....(1)

Solution. Consider the congruence

$$x^3 \equiv 3 \pmod{19}$$

Compare it with $x^k \equiv a \pmod{p}$, we get

$k = 3, a = 3, p = 19$ so that

$d = (k, p - 1) = (3, 18) = 3.$

Now the congruence (1) has solution iff

$$3^{\frac{19-1}{3}} \equiv 1 \pmod{19}$$

i.e $3^6 \equiv 1 \pmod{19}$

But $3^6 = 81 \times 9 \equiv 5 \times 9 \pmod{19}$

$\equiv 45 \pmod{19}$

$\equiv 7 \pmod{19}$

Therefore $3^6 \not\equiv 1 \pmod{19}$

Hence the given congruence has no solution.

Again consider the congruence

$$x^3 \equiv 11 \pmod{19}$$

Compare it with $x^k \equiv a \pmod{p}$, we get

$k = 3, a = 11, p = 19$ so that

$d = (k, p-1)$

$= (3, 18)$

$= 3$

Now the congruence (2) has solution iff

$$11^{\frac{19-1}{3}} \equiv 1 \pmod{19}$$

i.e iff $11^6 \equiv 1 \pmod{19}$

Now $11^6 = 121 \times 121 \times 121$

$\equiv 7 \times 7 \times 7 \pmod{19}$

$\equiv 49 \times 7 \pmod{19}$

$\equiv 11 \times 7 \pmod{19}$

$\equiv 77 \pmod{19}$

$\equiv 1 \pmod{19}$

i.e $11^6 \equiv 1 \pmod{19}$

Hence the congruence (2) is solvable and has exactly three incongruent solutions.

❑❑❑

8 CHAPTER
THE QUADRATIC RECIPROCITY LAW

DEFINITION

The quadratic reciprocity law deals with the solvability of quadratic congruence.

Let us consider the quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

where a, b, c are integers and p is prime such that $p \nmid a$ and $p \neq 2$.

Since $p \nmid a$ and p is an odd prime

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

Hence we can rewrite the congruence as

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}$$

Or $\quad (2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$

Let $\quad y = 2ax + b$ and

$$d = b^2 - 4ac$$

Hence $ax^2 + bx + c \equiv 0 \pmod{p}$ can be solved if and only if

$y^2 \equiv d \pmod{p}$ is solvable for y.

Definition. *Let p be an odd prime and gcd* $(a, p) = 1$.

If the quadratic congruence $x^2 \equiv a \pmod{p}$ *has a solution, then a is said to be a* ***quadratic residue*** *of p.*

Otherwise, a is called a ***quadratic nonresidue*** *of p.*

e.g. Let $p = 3$

In fact, $1^2 \equiv 1 \pmod{3}$

$2^2 \equiv 1 \pmod{3}$.

Then 1 is a quadratic residue of 3, where as 2 is a non-quadratic residue of 3.

EULER'S CRITERION

Theorem 1. *Let p be an odd prime and gcd $(a, p) = 1$. Then a is a quadratic residue of p if and only if $a^{(p-1)/2} \equiv 1 \pmod p$.*

Proof. Suppose that a is a quadratic residue $(mod\ p)$.

Then $x^2 \equiv a \pmod p$ has a solution say x_1.

$\Rightarrow \quad x_1^2 \equiv a \pmod p$

$\Rightarrow \quad gcd\ (x_1, p) = 1$

Therefore by Fermat's theorem

$$x_1^{p-1} \equiv 1 \pmod p \qquad \ldots(1)$$

Hence $a^{(p-1)/2} \equiv (x_1^2)^{(p-1)/2}$

$$\equiv x_1^{p-1} \pmod p \qquad \ldots(2)$$

$$\equiv 1 \pmod p \qquad [\text{by (1)}]$$

Conversely, let $a^{(p-1)/2} \equiv 1 \pmod p$. [by (2)]

If r is a primitive root $(mod\ p)$, then $1, r, r^2, \ldots\ldots, r^{p-2}$ form a reduced residue system $(mod\ p)$;

and $a \equiv r^k \pmod p$ for some integer k, $1 \le k \le p-2$.

Now, $\quad 1 \equiv a^{\frac{p-1}{2}} \equiv (r^k)^{\frac{p-1}{2}}$

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

Since, r is a primitive root $(mod\ p)$, r has exponent $p-1$ $(mod\ p)$

$\Rightarrow \quad p - 1 \mid \dfrac{k\,(p-1)}{2}$

$\Rightarrow \quad k$ must be an even integer, say $k = 2t$.

$\therefore \quad a \equiv r^{2t} \pmod p$.

$\Rightarrow \quad r^t$ is a solution of $x^2 \equiv a \pmod p$.

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

Corollary. *Let p be an odd prime and gcd $(a, p) = 1$. Then a is a quadratic residue or nonresidue of p according to whether*

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

Or $\quad a^{(p-1)/2} \equiv -1 \pmod p$.

Proof. By Fermat's theorem,

we have $\quad a^{p-1} \equiv 1 \pmod p$

$\Rightarrow \quad 0 \equiv a^{p-1} - 1 \equiv (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \pmod p$

If a is a quadratic residue $(mod\ p)$,

then by Euler's criterion

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

and is a quadratic non-residue

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

Note

To find quadratic residues $(mod\ p)$, we should find the integers

$$1^2, 2^2, \ldots\ldots, k^2, \ldots\ldots, \left(\frac{p-1}{2}\right)^2 \pmod p.$$

Example 1. *Examine whether $+3$ and -3 are quadratic residues or non-residues of 37.*

Solution. Here $\frac{1}{2}(p-1) = \frac{1}{2}(37-1) = 18$ and hence

$$(\pm 3)^{18} = 9^9 \equiv (27)^6 = (-10)^6 \equiv 1000^2$$

$$\equiv 1 \pmod{37}$$

Therefore by Euler's criterion :

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

which asserts that $+3$ and -3 are quadratic residues of 37.

Example 2. *Prove that 3 is a quadratic residue of 13, but has a quadratic non-residue of 7.*

Solution. Here $3^{(13-1)/2} = 3^6 \equiv (27)^2 \pmod{13}$

$$\equiv 1 \pmod{13}$$

Hence 3 is a quadratic residue.

But $3^{(7-1)/2} = 3^3 \equiv 27 \pmod 7 \equiv -1 \pmod 7$

which shows that 3 is a quadratic non-residue of 7.

Example 3. *Find the quadratic residues (mod 17).*

Solution. All quadratic residues (*mod p*) are integers $1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2 \pmod{17}$

i.e 1, 4, 9, 7, 8, 2, 15, 13 (*mod* 17)

Or 1, 2, 4, 7, 8, 9, 13, 15 (*mod* 17).

LEGENDRE SYMBOL AND ITS PROPERTIES

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

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

Note

(1) Another standard notation for the Legendre symbol is (a/p) or $(a \mid p)$.

(2) Since $x^2 \equiv 2 \pmod{17}$ has a solution 2 is a quadratic residue (*mod* 17).

Hence $\left(\frac{2}{17}\right) = 1$.

Also $x^2 \equiv 3 \pmod{13}$ has a solution

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

But $x^2 \equiv 2 \pmod{13}$ has no solution

$\Rightarrow \quad \left(\frac{2}{13}\right) = -1.$

(3) $1 + \left(\frac{a}{p}\right)$ is a number of solutions modulo p to the equation $x^2 \equiv a \pmod{p}$ for any a.

(4) Euler's criterion can be states as :

If p is an odd prime and a is an integer coprime to p

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

Theorem 2. *Let p be an odd prime and let a and b be integers that are relatively prime to p. Then the following hold :*

(i) *If* $a \equiv b \pmod{p}$, *then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

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

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

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

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

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

Proof.

(i) If $a \equiv b \pmod{p}$, then $x^2 \equiv a \pmod{p}$ and $x^2 \equiv b \pmod{p}$ simultaneously have solutions or no solutions

i.e. if one of $x^2 \equiv a \pmod{p}$ or $x^2 \equiv b \pmod{p}$ has a solution, the other will also have the solution.

Thus if a (or b) is a quadratic residue (*mod p*) or a quadratic non-residue (*mod p*) so will b (or a) be.

In other words

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

(ii) By definition

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

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

$= a^{p-1} \equiv 1 \pmod{p}$ by Fermat's theorem.

Note

In particular $\left(\frac{1}{p}\right)=1$.

(iii) By Fermat's theorem, we have

$(a^{(p-1)/2}-1)(a^{(p-1)/2}+1)\equiv a^{p-1}-1\equiv 0 \pmod p$, and hence

$a^{(p-1)/2}\equiv \pm 1 \pmod p$.

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

(iv) By Euler's criterion

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

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

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

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

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

Since Legendre symbol takes values –1, 0 or 1 only, we have

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

(v) By definition

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

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

$$=a^{p-1}$$

$\equiv 1 \pmod p$ in view of Fermat's theorem.

In particular, $\left(\frac{1}{p}\right)=1$.

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

Since we know that

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

Taking $a=-1$, we have

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

Since the quantities $\left(-\frac{1}{p}\right)$ and $(-1)^{\frac{p-1}{2}}$ are either 1 or –1, the resulting congruence.

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

implies that

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

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

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

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

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

Corollary. *If p is an odd prime, then*

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

Proof. The congruence

$x^2 \equiv -1 \pmod p$ has a solution iff

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

If p is of the form $4n+1$, then $(-1)^{\frac{p-1}{2}} = (-1)^{2n} = ((-1)^2)^n = 1$.

If p is of the form $4n+3$, then

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

Hence $\left(-\frac{1}{p}\right)=\begin{cases} 1 & \text{if } p\equiv 1 \pmod 4 \\ -1 & \text{if } p\equiv 3 \pmod 4. \end{cases}$

Theorem 3. ***There are infinitely many primes of the form*** $4k+1$.

Proof. Let us suppose that there are only a finite number of primes of the form $4k+1$, say $p_1, p_2, \ldots\ldots, p_n$.

Let us define

$$N = (2p_1 p_2 \ldots\ldots p_n)^2 + 1.$$

Clearly N is an integer of the form $4k+1$ and is coprime to each of $p_1, p_2, \ldots\ldots, p_n$.

By fundamental theorem of arithmetic N has a prime factor p.

Since p cannot be one of $p_1, p_2, \ldots\ldots, p_n$ so it must be a prime of the form $4m+3$ as all odd primes are either of the form $4k+1$ or $4k+3$

$\Rightarrow$ $(2p_1 p_2 \ldots\ldots p_n)^2 \equiv -1 \pmod p$

$\therefore$ $2p_1 p_2 \ldots\ldots p_n$ is a solution of $x^2 \equiv -1 \pmod p$

$\Rightarrow$ -1 is a quadratic residue $(\mathrm{mod}\, p)$.

But then it contradicts the corollary, "If p is an odd prime, then

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

since p is of the form $4m+3$.

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

orem 3. If p is an odd prime, then $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)=0$.

nce, there are precisely $\left(\frac{p-1}{2}\right)$ ***quadratic residues and*** $\frac{p-1}{2}$ ***quadratic non-residues***

p.

roof. Let r be a primitive root of p.

We know that, modulo p, the powers $r, r^2, \ldots\ldots, r^{p-1}$ are just a permutation of the integers $1, 2, \ldots\ldots, p-1$.

Thus, for any a lying between 1 and $p-1$, there exist a unique positive integer $k\,(1 \le k \le p-1)$, such that $a \equiv r^k \pmod p$.

By Euler's criterion, we have

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

$$= (r^{(p-1)/2})^k$$

$$\equiv (-1)^k \pmod p,$$

since r is a primitive root of p, $r^{\frac{p-1}{2}} \equiv -1 \pmod p$.

But $\left(\frac{a}{p}\right)$ and $(-1)^k$ are equal to either 1 or -1, so the equality holds in equation (1),

Now adding the Legendre's symbols, we get

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

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

which proves the theorem.

Example 4. $x^2 \equiv -a^2 \pmod p$ *has a solution if and only if*

$p \equiv 1 \pmod 4$.

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

$$= \left(-\frac{1}{p}\right)\left(\frac{a}{p}\right)^2$$
$$= \left(-\frac{1}{p}\right)$$
$$= (-1)^{\frac{p-1}{2}} \pmod p$$ by Euler's criterion.

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

$\Leftrightarrow$ $p = 4k+1$; result follows by Euler's criterion.

Example 5. *Show that* $\left(\frac{3}{7}\right)\left(\frac{2}{7}\right) = \left(\frac{6}{7}\right)$

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

Let $a = 3, p = 7$.

Then $3^{\frac{(7-1)}{2}} \equiv \frac{3}{7}$

i.e $3^3 \equiv \left(\frac{3}{7}\right) \equiv -1$ if $3\ N\ 7$.

Let $a = 2, p = 7$.

Then $2^3 \equiv \left(\frac{2}{7}\right)$

i.e $2^3 \equiv \left(\frac{2}{7}\right) \equiv 1$ if $2\ R\ 7$.

If $a = 6, p = 7$, then

$$\left(\frac{6}{7}\right) = 6^2 \ (mod\ 7) \equiv -1 \text{ if } 6\ N\ 7.$$

Hence $\left(\frac{6}{7}\right) = \left(\frac{3}{7}\right)\left(\frac{2}{7}\right)$.

The result also follows from

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

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

$(ab, p) = 1.$

GAUSS LEMMA

Theorem 4. State and prove Gauss lemma

Statement. *Let p be an odd prime and let gcd* $(a, p) = 1$. *If n denotes the number of integers that leave negative least residues in the set* $S = \left\{a, 2a, 3a, \ldots\ldots, \left(\frac{p-1}{2}\right)a\right\}$, *then* $\left(\frac{a}{p}\right) = (-1)^n$.

Proof. Since $gcd\ (a, p) = 1$, each of integers in the set S are coprime to p and no two are congruent to each other $(mod\ p)$.

Let $r_1, r_2, \ldots\ldots, r_m$ be those remainders obtained upon dividing by p such that $0 < r_i < \frac{p}{2}$.

Let $s_1, s_2, \ldots\ldots, s_n$ be those remainders such that $p > s_i > \frac{p}{2}$.

Then $m + n = \frac{(p-1)}{2}$, and the integers

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

To prove that these integers are all distinct, it is sufficient to show that no $p - s_i$ is equal to any r_j. Let us assume that $p - s_i = r_j$ for some choice of i and j.

Then there exists integers h and k, with $1 \le h, k \le \frac{(p-1)}{2}$, satisfying

$s_i \equiv ha\ (mod\ p)$

and $r_j \equiv ka\ (mod\ p)$.

Hence $(h + k)\ a \equiv s_i + r_j = p \equiv 0\ (mod\ p)$

which implies that

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

But there does not exist such congruence because $1 < h + k \le p - 1$.

Thus $\frac{(p-1)}{2}$ numbers

$r_1, \ldots\ldots, r_m, p - s_1, \ldots\ldots, p - s_n$ are simply the integers $1, 2, \ldots\ldots, \frac{(p-1)}{2}$, not necessarily in the same order.

Thus, their product is $\frac{[(p-1)]}{2}!$,

$$\left(\frac{p-1}{2}\right)! = r_1 \ldots\ldots r_m (p - s_1) \ldots\ldots (p - s_n)$$

$$\equiv r_1 \ldots\ldots r_m (-s_1) \ldots\ldots (-s_n) \pmod{p}$$

$$\equiv (-1)^n r_1 r_2 \ldots\ldots r_m s_1 \ldots\ldots s_n \pmod{p}$$

But we know that $r_1, r_2, \ldots\ldots, r_m, s_1, \ldots\ldots, s_n$ are congruent modulo p to a, $2a, \ldots\ldots, \left[\frac{(p-1)}{2}\right]a$, in some order, so that

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

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

But $\left(\frac{p-1}{2}\right)!$ is relatively prime to p, so cancelling $\left(\frac{p-1}{2}\right)!$ from both sides, we get

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

Multiplying both sides by $(-1)^n$, we get

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

Or $a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$ using Euler's criterion, we have

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

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

Hence the Proof.

Theorem 5. If p is an odd prime, then

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

Or

If p is an odd prime, find $\left(\frac{2}{p}\right)$.

Proof. By Gauss lemma

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

where n is the number of integers in set

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

having negative least residue $(mod\ p)$.

Clearly these are the even integers that lie in the interval

$$\left[\frac{p+1}{2}, p-1\right].$$

Further p being an odd prime, p must be either of the form

$$8k+1, 8k+3, 8k+5 \text{ or } 8k+7.$$

By direct calculations,

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

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

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

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

Hence, $\left(\frac{2}{p}\right) = \begin{cases} 1 \text{ if } p = \pm 1 \pmod 8 \\ -1 \text{ if } p = \pm 3 \pmod 8 \end{cases}$

Now $(-1)^{\frac{p^2-1}{8}} = \begin{cases} (-1)^{\frac{64k^2+16k+1-1}{8}} & \text{if } p = 8k+1 \\ (-1)^{\frac{64k^2+48k+9-1}{8}} & \text{if } p = 8k+3 \\ (-1)^{\frac{64k^2+80k+25-1}{8}} & \text{if } p = 8k+5 \\ (-1)^{\frac{64k^2+112k+49-1}{8}} & \text{if } p = 8k+7 \end{cases}$

$$= \begin{cases} +1 \text{ if } p \equiv 1 \pmod 8 \\ -1 \text{ if } p \equiv 3 \pmod 8 \\ -1 \text{ if } p \equiv 5 \pmod 8 \\ +1 \text{ if } p \equiv 7 \pmod 8 \end{cases}$$

$$= \begin{cases} 1 \text{ if } p = \pm 1 \pmod 8 \\ -1 \text{ if } p = \pm 3 \pmod 8 \end{cases}$$

Theorem 6. ***There are infinitely many primes of the form*** $8k-1$.

Proof. Suppose that there are only a finite number of primes of the form $8k-1$ say $p_1, p_2, \ldots\ldots, p_n$.

Let us define

$$N = (4p_1 p_2 \ldots\ldots p_n)^2 - 2.$$

Clearly N is an integer of the form $2(8n-1)$ and therefore has an odd prime divisor p say. Hence

$$N \equiv 0 \pmod p$$

$\Rightarrow$ $x^2 \equiv 2 \pmod p$ has a solution $4p_1 p_2 \ldots\ldots p_n \pmod p$.

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

By the theorem, "Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = \begin{cases} 1 \text{ if } p \equiv \pm 1 \pmod 8 \\ -1 \text{ if } p \equiv \pm 3 \pmod 8 \end{cases}$$

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

p must be of the form $8n+1$ or $8n-1$.

p cannot be of the form $8n-1$ since p and $2, p_1, p_2, \ldots\ldots, p_n$ are coprime.

Hence p must be of the form $8k+1$ which implies that all prime divisors of N are of the form $8n+1$ for some integer n.

Thus N (as a product of such primes) must be of the form $8t+1$ for some integer t; a contradiction.

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

QUADRATIC RECIPROCITY

Theorem 7. State and prove Gauss Quadratic reciprocity law.

Statement. If p and q are distinct odd primes, then

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

Proof. Let S_1 denote the set of all pairs (x, y) such that x and y are integers and

$$1 \le x \le \left(\frac{p-1}{2}\right), 1 \le y \le (p-q)\,x.$$

Let S_2 denote the set of pairs (x, y) such that $1 \le y \le \frac{(q-1)}{2}$,

$$1 \le x < (p-q)\,y.$$

Now consider any (u, v) such that

$$1 \le u \le \frac{(p-1)}{2}, 1 \le v \le \frac{(q-1)}{2}.$$

If $v > \left(\frac{q}{p}\right)u$ then (u, v) is in S_1 and if $u > \left(\frac{p}{q}\right)v$, then (u, v) is in S_2.

Furthermore $v > \left(\frac{q}{p}\right)u$, is impossible, since it would imply $\frac{p}{q}$ with $1 \le u < p$.

Therefore, each of the $\left\{\left(\frac{p-1}{2}\right)\right\}\left\{\left(\frac{q-1}{2}\right)\right\}$ pairs (u, v) is in either S_1 or in S_2 but not in both.

In the other direction if (x, y) is in S_1 then $1 \le x \le \frac{(p-1)}{2}$ and

$$1 \le y < \left(\frac{q}{p}\right)x \le \left(\frac{q}{p}\right)\left(\frac{p-1}{2}\right) = \left\{\frac{(p-1)}{p}\right\}\left\{\frac{q}{2}\right\} < \frac{q}{2}$$

Since q is odd and y is an integer this implies that $1 \le y \le \frac{(q-1)}{2}$, and hence (x, y) is of the form (u, v).

Similarly (x, y) is in S_2 implies that (x, y) is of the form (u, v).

This shows that S_1 and S_2 together, contain exactly

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

For each x such that

$1 \le x \le \frac{(p-1)}{2}$ the pair (x, y) is in S_1 just for

$$y = 1, 2, \ldots\ldots\ldots\ldots, \left[\frac{qx}{p}\right].$$

There are $\left[\frac{qx}{p}\right]$ of these y's and hence the number of pairs in

$$S_1 \text{ is } \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right]$$

Similarly S_2 consists of $\sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right]$ pairs.

So we have

$$\sum_{j=1}^{\frac{(p-1)}{2}} \left[\frac{qj}{p}\right] + \left[\frac{pj}{q}\right] = \frac{p-1}{2} \cdot \frac{q-1}{2};$$

and hence

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

Hence the Proof.

***Theorem 8.** Let p be an odd prime 3. Then*

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 6 \\ -1 & \text{if } p \equiv 5 \pmod 6 \end{cases}$$

i.e. -3 is a quadratic residue mod $p \Leftrightarrow p = 1 \pmod 6$.

Proof. By Gauss lemma,

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

where n is the number of integers in the set

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

that have negative least residue $(mod\ p)$.

Such integers are multiples of -3 modulo p that lie in the interval

$$\left(\frac{p}{2}, p\right).$$

Further, since

$$-3t \equiv p - 3t \ (mod\ p)$$

Or $\quad -3t \equiv 2p - 3t \ (mod\ p)$;

therefore, if $p - 3t$ or $2p - 3t \in \left(\frac{p}{2}, p\right)$ for some integer t, then

$$0 < t < \frac{p}{6} \text{ or}$$

$$\frac{p}{3} < t < \frac{p}{2}.$$

If there is an integer t such that

$$\frac{p}{6} < t < \frac{p}{3}; \text{ then}$$

$$0 < p - 3t < \frac{p}{2},$$

so that $p - 3t$ does not leave negative residue $(mod\ p)$.

Thus if $p = 6k + 1$ for some integer k, there are k integers in $\left(0, \frac{p}{6}\right)$ and k integers in $\left(\frac{p}{3}, \frac{p}{2}\right)$ that leave negative least residue $(mod\ p)$ implying $n = 2k$.

If $p = 6k + 5$ for some integer k then there are k integers in $\left(0, \frac{p}{6}\right)$ and $k+1$ integers in $\left(\frac{p}{3}, \frac{p}{2}\right)$ that leave negative least residue $(mod\ p)$ so that $n = 2k + 1$.

Hence $\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \ (mod\ 6) \\ -1 & \text{if } p \equiv 5 \ (mod\ 6) \end{cases}$

Example 6. *Evaluate* $\left(\frac{59}{131}\right)$.

Solution. Since $59 \equiv 3 \ (mod\ 4)$ and

$$131 \equiv 3 \ (mod\ 4)$$

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

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

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

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

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

$$= -(-1) = 1.$$

Note

Deductions

(1) If one of p, q is of the form $4n + 1$, then

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

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

(2) If both p and q are of the form $4n - 1$, then

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

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

(3) If both p and q are of the form $4n + 3$, then

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

Example 7. *Decide whether 67 is a quadratic residue of 89.*

Solution. $\left(\frac{67}{89}\right) = \left(-\frac{22}{89}\right)$

$$= \left(-\frac{1}{89}\right)\left(\frac{2}{89}\right)\left(\frac{11}{89}\right)$$

$$= \left(-\frac{1}{89}\right)\left(\frac{2}{89}\right)\left(\frac{89}{11}\right)$$

$$= \left(-\frac{1}{89}\right)\left(\frac{2}{89}\right)\left(\frac{1}{11}\right),$$

since $\left(\frac{11}{89}\right)\left(\frac{89}{11}\right) = 1$ by quadratic reciprocity law we have

$$\left(-\frac{1}{89}\right) = (-1)^{(89-1)/2} = +1 \qquad \left[\because \left(-\frac{1}{p}\right) = (-1)^{(p-1)/2}\right]$$

Also we know that

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

$$\therefore \quad \left(\frac{2}{89}\right) = (-1)^{(89^2-1)/8} = +1$$

and $\left(\frac{1}{11}\right) = +1.$

Hence $\left(\frac{67}{89}\right) = +1.$

Therefore, 67 is a quadratic residue of 89.
or in other words

$x^2 \equiv 67 \pmod{89}$ has a solution.

Example 8. *Find the value of* $\left(-\frac{42}{61}\right)$.

Solution. $\left(-\frac{42}{61}\right)=\left(\frac{19}{61}\right)$

$$=\left(\frac{61}{19}\right)$$

$$=\left(\frac{4}{19}\right)$$

$$=\left(\frac{2}{19}\right)\left(\frac{2}{19}\right)$$

$$=((-1)^{(19^2-1)/8})^2$$

$$=((-1)^{(20\cdot 18)/8})^2$$

$$=(-1)^2$$

$$=+1.$$

Example 9. *Evaluate* $\left(\frac{31}{103}\right)$.

Solution. Using reciprocity law, we have

$$\left(\frac{31}{103}\right)=-\left(\frac{103}{31}\right)$$

$$=-\left(\frac{10}{31}\right)$$

$$=-\left(\frac{2}{31}\right)\left(\frac{5}{31}\right)$$

$$=-\left(\frac{31}{5}\right)$$

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

$$=-1.$$

since $\left(\frac{2}{31}\right)=(-1)^{(31^2-1)/8}$

$=+1$ and $\left(\frac{1}{5}\right)=1$.

Example 10. *Is the congruence* $x^2 \equiv 5 \pmod{227}$ *solvable ?*

Solution. We have

$$\left(\frac{5}{227}\right)=\left(\frac{227}{5}\right)$$

$$=\left(\frac{2}{5}\right)$$

$$=(-1)^{(5^2-1)/8}$$

$$=(-1)^3$$

$$=-1.$$

Hence the given congruence is not solvable.

Example 11. *Is the congruence* $x^2 \equiv 5 \pmod{229}$ *solvable ?*

Solution. Here

$$\left(\frac{5}{229}\right)=\left(\frac{229}{5}\right)$$

$$=\left(\frac{4}{5}\right)$$

$$=\left(\frac{2}{5}\right)^2$$

$$=((-1)^{(5^2-1)/8})^2$$

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

Hence the given congruence is solvable.

Example 12. *Verify that the congruence* $x^2 \equiv -7 \pmod{1019}$ *is solvable.*

Solution. Here

$$\left(-\frac{7}{1019}\right) = \left(-\frac{1}{1019}\right)\left(\frac{7}{1019}\right)$$

But $\left(-\frac{1}{1019}\right) = (+1)$

Also $\left(\frac{7}{1019}\right) = \left(\frac{1019}{7}\right)$

$$= \left(\frac{4}{7}\right)$$
$$= \left(\frac{2}{7}\right)\left(\frac{2}{7}\right)$$
$$= ((-1)^{(7^2-1/8)})^2$$
$$= ((-1)^6)^2$$
$$= +1.$$

$\therefore$ $\left(-\frac{7}{1019}\right) = \left(-\frac{1}{1019}\right)\left(\frac{7}{1019}\right)$

$$= (+1)\,(+1)$$
$$= +1.$$

Hence the given congruence is solvable.

Example 13. *For an odd prime p, show that*

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

Solution. Now

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

$$= (-1)^{\frac{p-1}{2}}\,(-1)^{\frac{p^2-1}{8}}$$
$$= (-1)^{\frac{p^2+4p-5}{8}}$$
$$= \begin{cases} 1 \text{ if } p \equiv 1 \pmod 8 \\ 1 \text{ if } p \equiv 3 \pmod 8 \\ -1 \text{ if } p \equiv 5 \pmod 8 \\ -1 \text{ if } p \equiv 7 \pmod 8 \end{cases}$$

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

Example 14. *Solve the congruence* $x^2 \equiv 91 \pmod{3^3}$.

Solution. Let us determine $\left(\frac{91}{3}\right)$.

$$\left(\frac{91}{3}\right) = \left(\frac{1}{3}\right) = 1$$

$\Rightarrow$ $x^2 \equiv 91 \pmod{3^3}$ has a solution.

Since any solution of

$x^2 \equiv 91 \pmod{3^3}$ is also a solution of $x^2 \equiv 91 \pmod 3$,

So we first solve

$$x^2 \equiv 91 \pmod 3$$

Now $x^2 \equiv 91 \pmod 3$

$\Rightarrow$ $x^2 \equiv 1 \pmod 3$

Clearly 1 (even 2) is a solution of $x^2 \equiv 1 \pmod 3$

With $x_0 = 1$, $x_0 y \equiv 1 \pmod 3$

also has a solution $y_0 \equiv 1 \pmod 3$.

Since $x_0^2 = 1 = 91 + 3(-30)$,

therefore $x_0 = 1 - (-30) \cdot 1 \cdot \frac{3+1}{2} \cdot 3$

$= 181$ is a solution of $x^2 \equiv 91 \pmod{3^2}$.

To find the solution of $x^2 \equiv 91 \pmod{3^3}$, repeating the above procedure again.

Let us first solve

$$181\, y \equiv 1 \pmod 3$$

Or $$y \equiv 1 \pmod 3$$

Clearly $y_1 = 1$ can be taken as a solution of $y \equiv 1 \pmod 3$.

Then by taking

$$x_1^2 = 181^2 = 91 + 3^2(-3430),$$

$$y_1 = 1,$$

$$x_2 = 181 - (-3430) \cdot 1 \cdot \frac{3+1}{2} \cdot 3^2$$

$$= 61921$$

is the solution of required congruence.

Example 15. *Prove that the quadratic congruence* $x^2 \equiv 9 \pmod{120}$ *is solvable.*

Solution. The given congruence is equivalent to the following simultaneous system of quadraticcongruences:

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

$$x^2 \equiv 9 \pmod 3$$

and $$x^2 \equiv 9 \pmod 5$$

since $9 \equiv 1 \pmod 8$,

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

has a solution;

$$x^2 \equiv 0 \pmod 3$$

admits 0 (zero) as its only solution and finally

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

$\Rightarrow x^2 \equiv 9 \pmod 5$ also has a solution.

Hence the given congruence has a solution.

Theorem 9. *If p is an odd prime and gcd $(a, p) = 1$, then the congruence*

$$x^2 \equiv a \pmod{p^n},\ n \geq 1$$

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

Proof. Suppose that $x^2 \equiv 9 \pmod{p^n}$ has a solution x_0.

Then $$x_0^2 \equiv a \pmod{p^n}$$

Or $$p^n \mid x_0^2 - a$$

Or $$p \mid x_0^2 - a,$$ so that

$$x^2 \equiv a \pmod p$$ has a solution.

Hence, by Euler's criterion, $\left(\frac{a}{p}\right) = 1$.

Again suppose that $\left(\frac{a}{p}\right) = 1$,

which by Euler's criterion implies that

$$x^2 \equiv a \pmod p$$ has a solution.

We are to prove that $x^2 \equiv a \pmod{p^n}$,

$n \geq 1$ has a solution.

Clearly for $n = 1$, the statement is true.

Let us assume that

$$x^2 \equiv a \pmod{p^n},\ n \geq 1$$ has a solution.

We show that $x^2 \equiv a \pmod{p^{n+1}}$ also admits a solution.

Let x_0 be the solution of $x^2 \equiv a \pmod{p^n}$.

Then $x_0^2 \equiv a + t\,p^n$ for some integer t.

Clearly $(x_0, p) = 1$.

Thus the linear congruence

$$x_0\, y \equiv 1 \pmod p$$

has a unique solution y_0.

Therefore $x_0 y_0 = 1 + sp$ for some integer s.

Let us define

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

Then, $x_1^2 = x_0^2 - 2tx_0 y_0 \frac{p+1}{2} p^n + t^2 y_0^2 \left(\frac{p+1}{2}\right)^2 \cdot p^{2n}$

$$= a + tp^n - 2t(1+sp) \cdot \frac{p+1}{2} p^n + t^2 y_0^2 \left(\frac{p+1}{2}\right)^2 \cdot p^{2n}$$

$$= a + tp^n - tp^n + p^{n+1} \cdot (\text{some integer})$$

$$\equiv a \pmod{p^{n+1}};$$

Consequently x_1 is a solution of $x^2 \equiv a \pmod{p^{n+1}}$.

Hence by principle of induction

$$x^2 \equiv a \pmod{p^n}$$

has a solution for each $n \geq 1$.

Theorem 10. ***Let a be an odd integer then***

(i) $x^2 \equiv a \pmod 2$ ***always admit a solution.***

(ii) $x^2 \equiv a \pmod 4$ ***has a solution if and only if*** $a \equiv 1 \pmod 4$

(iii) $x^2 \equiv a \pmod{2^n}$, $n \geq 3$ ***has a solution of any only if*** $a \equiv 1 \pmod 8$.

Proof.

(i) Since $a \equiv 1 \pmod 2$,

1 is the solution of $x^2 \equiv a \pmod 2$.

(ii) Since a is odd,

$a \equiv 1$ or $3 \pmod 4$

Also $b^2 = 0$ or $1 \pmod 4$ for each integer k.

In order that

$x^2 \equiv a \pmod 4$ have a solution b, a must be congruent to $1 \pmod 4$.

Conversely, if $a \equiv 1 \pmod 4$, then 1 or 3 both satisfy

$x^2 \equiv 1 \pmod 4$.

(iii) If $a \equiv 1 \pmod 8$, then we must show

$x^2 \equiv a \pmod{2^n}$ has a solution for each $n \geq 3$.

Suppose $n = 3$.

We has the congruence

$x^2 \equiv 1 \pmod 8$.

Clearly 1, 3, 5, 7 all satisfy it.

Again suppose $x^2 \equiv 1 \pmod{2^n}$ has a solution for $n \geq 3$ say x_0.

Then $x_0^2 = 1 + t2^n$ for some integer t.

Also the linear congruence

$x_0 y \equiv 1 \pmod 2$ has a unique solution y_0, so that $x_0 y_0 \equiv 1 + 2s$, for some integer s.

Clearly $x_1 = x_0 - 2^{n-1} t y_0$ is the solution of

$x^2 \equiv 1 \pmod{2^{n+1}}$; for,

$$x_1^2 = x_0^2 - 2^n t y_0 x_0 + 2^{2n-2} t^2 y_0^2$$

$$= 1 + 2^n t - 2^n t(1+2s) + 2^{n+1} 2^{n-3} t^2 y_0^2$$

$$\equiv 1 \pmod{e^{n+1}}.$$

Conversely, if $x^2 \equiv a \pmod{2^n}$ has a solution for each $n \geq 3$, say x_0, then $x_0^2 \equiv a \pmod{2^n}$.

In particular $x_0^2 \equiv a \pmod 8$.

Since a is odd x_0 must be odd.

Thus $x_0 \equiv 1, 3, 5, 7 \pmod 8$

Or $a \equiv x_0^2 \equiv 1 \pmod 8$.

Example 16. *Find* $\left(\frac{168}{11}\right)$.

Solution. Here, we have

$$168 = 2^3 \cdot 3 \cdot 7$$

Therefore,

$$\left(\frac{168}{11}\right)=\left(\frac{2^3\cdot 3\cdot 7}{11}\right)$$

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

$$=(-1)^3\,(1)\,(-1)$$

$$=1$$

($\because$ 2 and 7 are quadratic non-residue of 11 and 3 is a quadratic residue of 11).

Example 17. *Evaluate* $\left(-\frac{23}{59}\right)$.

Solution. We have

$$\left(-\frac{23}{59}\right)=\left(\frac{-1\times 23}{59}\right)$$

$$=\left(-\frac{1}{59}\right)\left(\frac{23}{59}\right)$$

$$=-1\left(\frac{23}{59}\right)$$

$$=\left(-\frac{23}{59}\right)$$

$$=-1 \qquad (\because \text{ 23 is a quadratic residue of 59})$$

Example 18. *Evaluate* $\left(\frac{219}{383}\right)$, 383 *being a prime.*

Solution. We have

$$\left(\frac{219}{383}\right)=\left(\frac{3}{383}\right)\left(\frac{73}{383}\right)$$

Now $\left(\frac{3}{383}\right)=(1)^{\frac{383-1}{2}\cdot\frac{3-1}{2}}\left(\frac{383}{3}\right)$

$$=-\left(\frac{383}{3}\right)$$

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

$$\left(\frac{73}{383}\right)=(-1)^{\frac{383-1}{2}\cdot\frac{73-1}{2}}\left(\frac{383}{73}\right)$$

$$=\left(\frac{383}{73}\right)$$

$$=\left(\frac{18}{73}\right)$$

$$=\left(\frac{3^2}{73}\right)\left(\frac{2}{73}\right)$$

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

$$=1$$

Hence, $\left(\frac{219}{383}\right)=1$, *i.e* 219 is a quadratic residue of 383.

Example 19. *Show that* $\left(\frac{43}{23}\right)=-\left(\frac{23}{43}\right)$.

Solution. Since 23 and 43 both are odd primes.

Also $23=4\times 5+3$

$43=4\times 10+3$

are of the form $4m+3$.

Therefore

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

Example 20. *Find n of Gauss Lemma for* $\left(\frac{5}{19}\right)$.

Solution. We have $a=5, b=19$.

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

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

with respect to modulo 19, the number of the set S becomes

5, 10, 15, 1, 6, 11, 16, 2, 7

Since there are four numbers greater than $\frac{p}{2}=\frac{19}{2}$

Hence $n=4$.

Example 21. *Evaluate Jacobi symbol* $\left(\frac{22}{105}\right)$.

Solution. Here, we have

$$\left(\frac{22}{105}\right)=\left(\frac{22}{3\times5\times7}\right)$$

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

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

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

$$=-1.$$

Example 22. *Evaluate the Jacobi Symbol* $\left(\frac{32}{15}\right)$.

Solution. We have

$$\left(\frac{32}{15}\right)=\left(\frac{32}{3\times5}\right)$$

$$=\left(\frac{32}{3}\right)\left(\frac{32}{5}\right)$$

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

$$=(-1)^{\frac{3+1}{4}}\times(-1)^{\frac{5+1}{4}}$$

$$=(-1)^1\times(-1)^1$$

$$=1.$$

Example 23. *Evaluate* $\left(\frac{429}{363}\right)$, *563 being prime.*

Solution. We have

$$\left(\frac{429}{563}\right)=(-1)^{\frac{429-1}{2}\cdot\frac{563-1}{2}}\left(\frac{563}{429}\right)$$

$$=\left(\frac{563}{429}\right)$$

$$=\left(\frac{134}{429}\right)$$

$$=\left(\frac{2}{429}\right)\left(\frac{67}{429}\right)$$

$$=(-1)^{\frac{429^2-1}{2}}\left(\frac{67}{429}\right)$$

$$=-\left(\frac{67}{429}\right)$$

$$=-(-1)^{\frac{67-1}{2}\cdot\frac{429-1}{2}}\left(\frac{429}{67}\right)$$

$$=-\left(\frac{429}{67}\right)$$

$$=-\left(\frac{27}{67}\right)$$

$$=(-1)^{\frac{27-1}{2}\cdot\frac{67-1}{2}}\left(\frac{67}{27}\right)$$

$$=\left(\frac{67}{27}\right)$$

$$= \left(\frac{13}{27}\right)$$

$$= (-1)^{\frac{27-1}{2}\cdot\frac{13-1}{2}} \left(\frac{27}{13}\right)$$

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

$$= 1.$$

Example 24. *Show that* 3 *is quadratic residue of* 23 *but non-residue of* 31.

Solution. 3 is quadratic residue of 23 iff

$$3^{\frac{23-1}{2}} \equiv 1 \ (mod\, 23)$$

i.e iff $3^{11} \equiv 1 \ (mod\ 23)$

Now $3^{11} \equiv (3 \times 3 \times 3)^3 \cdot 9 \ (mod\ 23)$

$$\equiv (4)^3 \cdot 9 \ (mod\ 23)$$

$$\equiv 64 \cdot 9 \ (mod\ 23)$$

$$\equiv (-5) \cdot 9 \ (mod\ 23)$$

$$\equiv -45 \ (mod\ 23)$$

$$\equiv 1 \ (mod\ 23)$$

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

$\Rightarrow$ 3 is quadratic residue of 23.

Now 3 is quadratic non-residue of 31 iff

$$3^{\frac{31-1}{2}} \equiv -1 \ (mod\, 31)$$

i.e iff $3^{15} \equiv -1 \ (mod\ 31)$

$$3^{15} \equiv (3 \times 3 \times 3)^5$$

$$\equiv (27^5) \ (mod\ 31)$$

$$= (-4)^5 \ (mod\ 31)$$

$$\equiv (-4)^3 (-4)^2 \ (mod\ 31)$$

$$\equiv -64 \cdot 16 \ (mod\ 31)$$

$$\equiv -2 \cdot 16 \ (mod\ 31)$$

$$\equiv -32 \ (mod\ 31)$$

$$\equiv -1 \ (mod\ 31)$$

i.e $3^{15} \equiv -1 \ (mod\ 31)$

$\Rightarrow$ 3 is quadratic non-residue of 31.

Example 25. *Show that* 3 *is a quadratic residue of* 23.

Solution. 3 is quadratic residue of 23 iff

$$3^{\frac{23-1}{2}} \equiv 1 \ (mod\, 23)$$

i.e iff $3^{11} \equiv 1 \ (mod\ 23)$

Now $3^{11} \equiv (3 \times 3 \times 3)^3 \cdot 9 \ (mod\ 23)$

$$\equiv (4)^3 \cdot 9 \ (mod\ 23)$$

$$\equiv 64 \cdot 9 \ (mod\ 23)$$

$$\equiv (-5) \cdot 9 \ (mod\ 23)$$

$$\equiv -45 \ (mod\ 23)$$

$$\equiv 1 \ (mod\ 23)$$

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

$\Rightarrow$ 3 is quadratic reside of 23.

Example 26. *Knowing that* 2 *is primitive root of* 19, *find all the quadratic residue of* 19.

Solution. $\phi(19) = 18$.

Since 2 is primitive root of 19, therefore all quadratic residues of 19 are

$$2^2, 2^4, 2^6, 2^8, 2^{10}, 2^{12}, 2^{14}, 2^{16}, 2^{18}.$$

But $2^2 \equiv 4 \ (mod\ 19)$,

$2^4 \equiv 16 \ (mod\ 19)$,

$2^6 \equiv 64 \equiv 7 \ (mod\ 19)$,

$2^8 \equiv 28 \equiv 9 \ (mod\ 19)$,

$2^{10} \equiv 17 \ (mod\ 19)$,

$2^{12} \equiv 68 \equiv 11 \ (mod\ 19)$,

$2^{14} \equiv 44 \equiv 6 \ (mod\ 19)$,

$2^{16} \equiv 24 \equiv 5 \ (mod\ 19)$,

$2^{18} \equiv 20 \equiv 1 \ (mod\ 19)$

Therefore all quadratic residues of 19 are

4, 16, 7, 9, 17, 11, 6, 5, 1

i.e all quadratic residues of 19 are 1, 4, 5, 6, 7, 9, 11, 16, 17.

Example 27. *Prove that* -1 *is quadratic residue of prime number of the form* $4k+1$ *and quadratic non-residue of prime number of the form* $4k+3$.

Solution. Let p be any odd prime, then $(-1, p) = 1$.

By Euler's criterion, -1 is quadratic residue of p iff

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

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

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

i.e iff $\frac{p-1}{2} =$ even number $= 2k$ (say)

i.e iff $p = 4k+1$

Hence -1 is quadratic residue of prime numbers of the form $4k+1$ and -1 is quadratic non-residue of prime numbers of the form $4k+3$.

Example 28. *Show that if* p *is prime number and* a, b *are two integers such that* $(ab, p) = 1$ *and if* $x^2 \equiv a \pmod{p}$ *and* $x^2 \equiv b \pmod{p}$ *are not solvable then* $x^2 \equiv ab \pmod{p}$ *is solvable.*

Solution. $(ab, p) = 1 \Rightarrow (a, p) = 1$ and $(b, p) = 1$

Since $x^2 \equiv a \pmod{p}$ and

$x^2 \equiv b \pmod{p}$

are not solvable,

therefore a and b are quadratic non-residues of p

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

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

$\Rightarrow ab$ is quadratic residue of p

$\Rightarrow x^2 \equiv ab \pmod{p}$ is solvable.

Example 29. *Determine which primes can divide each of* n^2+1, n^2+2, n^2+3 *for some value of* n.

Solution. (i) Let $p \mid n^2+1$ be any prime.

If $p = 2$, then $n =$ odd integer so that

$2 \mid n^2+1$

If p is odd prime, then

$p \mid n^2+1$

$\Rightarrow \quad n^2+1 \equiv 0 \pmod{p}$

$\Rightarrow \quad n^2 \equiv -1 \pmod{p}$

$\Rightarrow \quad x = n$ is solution of $x^2 \equiv -1 \pmod{p}$

$\Rightarrow \quad x^2 \equiv -1$ is solvable

$\Rightarrow \quad -1$ is quadratic residue of p

$\Rightarrow \quad p \equiv 1 \pmod{4}$

Hence the required primes are $p = 2, p \equiv 1 \pmod{4}$

(ii) Let $p \mid n^2+2$ be any prime.

If $p = 2$, then $n =$ even integer so that

$2 \mid n^2+2$.

If p is odd prime, then

$p \mid n^2+2$

$\Rightarrow \quad x^2 \equiv -2 \pmod{p}$

$\Rightarrow \quad x = n$ is solution of $x^2 \equiv -2 \pmod{p}$

$\Rightarrow \quad x^2 \equiv -2 \pmod{p}$ is solvable

$\Rightarrow \quad -2$ is quadratic residue of p

$\Rightarrow \quad p \equiv 1$ or $3 \pmod{8}$

Hence the required primes are $p = 2$, $p \equiv 1$ or $3 \pmod{8}$.

(iii) Let $p \mid n^2+3$ be any prime.

If $p = 2$, then $n =$ odd integer so that

$2 \mid n^2+3$.

If p is od prime, then $p \mid n^2+3$

$\Rightarrow$ $n^2 \equiv -3 \pmod{p}$

$\Rightarrow$ $x = n$ is solution of $x^2 \equiv -3 \pmod{p}$

$\Rightarrow$ $x^2 \equiv -3 \pmod{p}$ is solvable.

$\Rightarrow$ -3 is quadratic residue of p

$\Rightarrow$ $p \equiv 1 \pmod{6}$

Hence the required primes are

$p = 2, p \equiv 1 \pmod{6}$.

Example 30. *Verify that the prime divisors $p \neq 3$ of the integer $n^2 - n + 1$ are of the form $6k + 1$.*

Solution. If $p \mid n^2 - n + 1$, then

$n^2 - n + 1 \equiv 0 \pmod{p}$

$\Rightarrow$ $4n^2 - 4n + 4 \equiv 0 \pmod{p}$

$\Rightarrow$ $(2n-1)^2 \equiv -3 \pmod{p}$

$\Rightarrow$ $x = 2n - 1$ is solution of

$x^2 \equiv -3 \pmod{p}$

$\Rightarrow$ -3 is quadratic residue of p

$\Rightarrow$ $p \equiv 1 \pmod{6}$

i.e. p is of the form $6k + 1$.

Example 31. *Verify that the prime divisors p of the integer $2n(n+1)$ are of the form $p \equiv 1 \pmod{4}$.*

Solution. If $p \mid 2n(n+1) + 1$, then

$2n^2 + 2n + 1 \equiv 0 \pmod{p}$

$\Rightarrow$ $4n^2 + 4n + 2 \equiv 0 \pmod{p}$

$\Rightarrow$ $(2n+1)^2 \equiv -1 \pmod{p}$

$\Rightarrow$ $x = 2n + 1$ is solution of

$x^2 \equiv -1 \pmod{p}$

$\Rightarrow$ $x^2 \equiv -1 \pmod{p}$ is solvable

$\Rightarrow$ -1 is quadratic residue of p

$\Rightarrow$ $p \equiv 1 \pmod{4}$.

Example 32. Verify that the prime divisors $p \neq 5$ of integer $n^2 + n - 1$ are of the form $10k + 1$ or $10k + 9$.

Solution. If $p \mid n^2 + n - 1$, then $n^2 + n - 1 \equiv 0 \pmod{p}$

$\Rightarrow$ $4n^2 + 4n - 4 \equiv 0 \pmod{p}$

$\Rightarrow$ $4n^2 + 4n + 1 \equiv 5 \pmod{p}$

$\Rightarrow$ $(2n+1)^2 \equiv 5 \pmod{p}$

$\Rightarrow$ $x = 2n + 1$ is solution of

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

$\Rightarrow$ $x^2 \equiv 5 \pmod{p}$ is solvable

$\Rightarrow$ 5 is quadratic residue of p

$\Rightarrow$ $p = 10k + 1$ or $p = 10k + 9$.

Example 33. *Verify the prime divisors p of the integer $3n(n+1) + 1$ are of the form $p \equiv 1 \pmod{6}$.*

Solution. If $p \mid 3n(n+1) + 1$, then

$3n^2 + 3n + 1 \equiv 0 \pmod{p}$

$\Rightarrow$ $36n^2 + 36n + 12 \equiv 0 \pmod{p}$

$\Rightarrow$ $36n^2 + 36n + 9 \equiv -3 \pmod{p}$

$\Rightarrow$ $(6n+3)^2 \equiv -3 \pmod{p}$

$\Rightarrow$ $x = 6n + 3$ is solution of

$x^2 \equiv -3 \pmod{p}$

$\Rightarrow$ $x^2 \equiv -3 \pmod{p}$ is solvable

$\Rightarrow$ -3 is quadratic residue of p

$\Rightarrow$ $p \equiv 1 \pmod{6}$.

Example 34. *If p and q are odd primes satisfying $p = q + 4a$ for some a then show that $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.*

Solution. Since $\left(\frac{4a}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{a}{p}\right)$

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

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

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

$$= 1 \cdot \left(\frac{a}{p}\right) \qquad [\because 2 \text{ is a quadratic residue of } p \text{ so } \left(\frac{2}{p}\right) = 1]$$

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

i.e. $\left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right)$

$$= \left(-\frac{q}{p}\right) \qquad [\because 4a = p - q \Rightarrow 4a \equiv -q \pmod{p}]$$

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

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

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

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

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

$$= \left(\frac{p}{q}\right)(-1)^{\frac{q-1+4a}{2}\cdot\frac{q+1}{2}} \qquad (\because p = q + 4a \Rightarrow p - 1 = q - 1 + 4a)$$

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

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

$$= \left(\frac{p}{q}\right)(-1)^{\frac{q^2-1}{4}}(-1)^{2a\cdot\frac{q+1}{2}}$$

$$= \left(\frac{p}{q}\right)(-1)^{\frac{q^2-1}{4}}$$

$$= \left(\frac{p}{q}\right)(-1)^{\frac{q^2-1}{4}}$$

$$= \left(\frac{4a}{q}\right)(-1)^{\frac{q^2-1}{4}} \qquad [\because p \equiv 4a \pmod{q}]$$

$$= \left(\frac{4a}{q}\right)\cdot 1$$

$[\because q = \text{odd} = 2k+1 \Rightarrow q^2 = 4k^2 + 4k + 1 \Rightarrow \frac{q^2-1}{4} = k^2 + k = k(k+1) = \text{even}]$

$[\because p \equiv 4a \pmod{q}]$

$$= \left(\frac{4a}{q}\right)$$

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

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

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

i.e. $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

Example 35. *Show that* $x^2 \equiv -a^2 \pmod{p}$ *has a solution iff* $p \equiv 1 \pmod{4}$.

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

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

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

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

$=(-1)^{\frac{p-1}{2}}$ (by property of Legendre symbol)

$=1$ iff $p\equiv 1\ (mod\ 4)$

$\Rightarrow x^2\equiv -a^2\ (mod\ p)$ has a solution iff $p\equiv 1\ (mod\ 4)$.

Example 36. *If* $p\equiv 7\ (mod\ 8)$, *show that* $p\mid 2^{\frac{p-1}{2}}-1$ *and hence show that* 2^n-1 *are composite for* $n=11, 23$.

Solution. Now $p\equiv 7\ (mod\ 8)$

$\Rightarrow \quad p\equiv -1\ (mod\ 8)$

$\Rightarrow \quad p=8k-1$ type

$\Rightarrow$ 2 is quadratic residue of p

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

By the property of Legendre symbol, we have

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

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

$\Rightarrow \quad p\mid 2^{\frac{p-1}{2}}-1.$

Deduction

When $n=11$.

To prove that $2^{11}-1$ *is composite number.*

Comparing $2^{11}-1$ *with* $2^{\frac{p-1}{2}}-1$, *we get*

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

$\Rightarrow \quad p=23$

Since, $23\equiv 7\ (mod\ 8)$,

therefore by above result,

$23\mid 2^{11}-1$

$\Rightarrow \quad 2^{11}-1$

is composite number.

When $n=23$.

To prove $2^{23}-1$ *is composite number.*

Comparing $2^{23}-1$ *with* $2^{\frac{p-1}{2}}-1$, *we get*

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

$\Rightarrow \quad p=47$

Since $47\equiv 7\ (mod\ 8)$,

therefore by above result,

$47\mid 2^{23}-1$

$\Rightarrow \quad 2^{23}-1$ *is composite number.*

Example 37. *Prove that if* p *and* q *are distinct primes of the form* $4k+3$ *and if* $x^2=p\ (mod\ q)$ *has no solution, then* $x^2=q\ (mod\ p)$ *has two solutions.*

Solution. Since $x^2\equiv p\ (mod\ q)$ has no solution. ...(1)

$\therefore$ p is quadratic non-residue of q.

$\Rightarrow \quad \left(\frac{p}{q}\right)=-1$

Again, since p and q are distinct odd primes of the form $4k+3$.

Therefore by reciprocity law,

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

$$\Rightarrow \quad \left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right)=-(-1) \text{ by (1)}$$

$\Rightarrow$ q is quadratic residue of p

$\Rightarrow$ $x^2 \equiv q \pmod{p}$ is solvable.

We know that if x_0 is solution of $x^2 \equiv q \pmod{p}$, then $p - x_0$ is also solution of this congruence.

Hence $x^2 \equiv q \pmod{p}$ has two solutions.

Example 38. *Show that 7 and 18 are the only incongruent solutions of* $x^2 \equiv -1 \pmod{25}$.

Or

Solve the congruence $x^2 \equiv -1 \pmod{5}$.

Solution. Consider the congruence

$$x^2 \equiv -1 \pmod{5} \qquad \ldots(1)$$

Since $\left(-\frac{1}{5}\right)=(-1)^{\frac{5-1}{2}}=1$,

therefore (1) has a solution.

Clearly, $x_0 = 2$ is a solution of (1)

Now $x_0^2 = 4(-1) + (1)\,5$ so that $b = 1$.

Therefore $2x_0 y \equiv -b \pmod{p}$ becomes

$$4y \equiv -1 \pmod{5}$$

which is satisfied by $y_0 = 1$

$$\therefore \quad x_1 = x_0 + 5y_0$$
$$= 2 + 5 \cdot 1 = 7$$

is a solution of congruence

$$x^2 \equiv -1 \pmod{5^2}$$

Also as $-7 \equiv 18 \pmod{25}$, therefore 18 is the other solution.

Hence 7 and 18 are the only incongruent solutions of

$$x^2 \equiv -1 \pmod{25}.$$

❑❑❑

APPENDIX

UNIVERSITY PAPERS (H.P.U.)

Paper-303 : ANALYTIC NUMBER THEORY

JUNE, 2021

(HELD IN SEPT., 2021)

Time : 3 Hrs. M. Marks : 80

Note : Attempt five questions in all, selecting at least one question but not more than two questions from any section.

SECTION-I

1. (a) Prove that no integer in the sequence 11, 111, 1111, 11111, ... is a perfect square. (6)

(b) If a/bc, with $gcd(a,b)=1$, prove that a/c. (5)

(c) For positive integers a, b and $n \geq 1$, if $gcd(a,b)=1$, prove that $gcd(a^n, b^n)=1$. (5)

2. (a) Prove that the linear Diophantine equation $ax+by=c$ has a solution if and only d/c, where $d=gcd(a,b)$. (6)

(b) If $n>1$ is an integer not of the form $6k+3$ prove that n^2+2^n is composite. (5)

(c) Prove that the number of primes of the form $4n+3$ is infinite. (5)

3. (a) If a is an odd integer, prove that $a^{2^n} \equiv 1 \pmod{2^{n+2}}$ for any $n \geq 1$. (5)

(b) Prove that no integer whose digits add up to 15 can be a square of a cube. (5)

(c) Prove that the linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if d/b, where $d=gcd(a,n)$. (6)

SECTION-II

4. (a) If 7 does not divide a, prove that either a^3+1 or a^3-1 is divisible by 7. (4)

(b) If p is prime, prove that $\lfloor p-1 \equiv -1 \pmod{p}$. (7)

(c) Prove that $4(\lfloor 29) + \lfloor 5$ is divisible by 31.

5. (a) The functions τ and σ are both multiplicative functions. (5)

(b) If F is a multiplicative function and $F(n) = \sum_{d|n} f(d)$, (3+3)

prove that f is also multiplicative.

(c) If N is a positive integer, prove that (5)

$$T(N) = \sum_{n=1}^{N} \left([N/n] - \left[\frac{N-1}{n} \right] \right).$$

6. (a) Prove that $\phi(3n) = 3\phi(n)$ if and only if 3/n. (4) (5)

(b) If n is a positive integer and $gcd(a,n) = 1$, prove that $a^{\phi(n)} \equiv 1 (\text{mod } n)$. (5)

(c) If $n = pq = 274279$ and $\phi(n) = 272376$, find the primes p and q. (7)

SECTION-III

7. (a) If the integer a has order k modulo n and $b > 0$, prove that a^b has order $k/gcd(b,k)$ modulo n. (6)

(b) Prove that there are infinitely many primes of the form $2kp + 1$, where p is an odd prime. (5)

(c) Determine all the primitive roots of 23, expressing each as a power of some and of the roots. (5)

8. (a) If p is a prime number and d/p − 1, prove that there are exactly $\phi(d)$ incongruent integers having order d modulo p. (6)

(b) If $gcd(m,n) = 1$, where $m > 2, n > 2$ prove that the integer mn has no primitive roots. (6)

(c) Find the remainder when $3^{24} \cdot 5^{13}$ is divided by 17. (5)

9. (a) Show that 3 is a quadratic residue of 23, but a non-residue of 31. (4)

(b) If p and q are distinct odd primes, prove that $(p/q)(q/p) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$. (8)

(c) Show that 7 and 18 are the only incongruent solutions of $x^2 \equiv -1 (\text{mod } 5^2)$. (4)

NOV. / DEC., 2021

(HELD IN MARCH, 2022)

Time : 3 Hrs. M. Marks : 80

Note: Attempt five questions in all, selecting at least one question from each section but not more than two questions from any section.

SECTION-I

1. (a) Show that the expression $\frac{a(a^2+2)}{3}$ is an integer for all $a \geq 1$. (6)

(b) Given integers a and b, not both of which are zero. Show that there exist integers x and y such that $gcd(a,b) = ax + by$. (5)

(c) For positive integers a and b prove that $gcd(a,b) l\ cm\ (a,b) = ab$. (5)

2. (a) Prove that the number $\sqrt{2}$ is a rational number. (6)

(b) If P_n is the nth prime number, then prove that $P_n \leq 2^{2^{n-1}}$. (5)

(c) If P^2 and $P^2 + 8$ are both primes, then prove that $P^3 + 4$ is also a prime. (5)

3. (a) (i) Find the remainder when 2^{50} is divided by 7. (6)

(ii) What is the remainder when the sum $1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5$ is divided by 4 ? (5)

(b) Find the last two digits of 9^{9^9}. (5)

(c) Find the solution of $3x + 4y \equiv 5 (\text{mod } 13)$, $2x + 5y \equiv 7 (\text{mod } 13)$. (6)

SECTION-II

4. (a) If p is an odd prime then prove that $1^p + 2^p + \cdots (p-1)^p \equiv 0 (\text{mod } p)$. (5)

(b) If n be a composite square free integer, say, $n = p_1 p_2 \cdots p_r$. If $p_i - 1 | n - 1$ for $l = 1,2,3 \ldots r$, then show that n is an absolute pseudoprime. (5)

(c) If p is a prime, prove that for any integer $a, p | a^p + (p-1)p!$ and $p | (p-1)! a^p + a$? (6)

5. (a) If f is a multiplicative function and F is defined by $F(n) = \sum_{d|n} f(d)$, then prove that F is also a multiplicative function. (6)

(b) For a positive integer r, the product of any r consecutive positive integers is divisible $r!$. (5)

(c) Find the years in the decade 2000 to 2009 when November 29 is on Sunday. (5)

6. (a) In a length ciphertext message sent using a linear cipher $C = aP + b(\text{mod } 26)$, the most frequently occurring letter is Q and the second most frequent is J. Break the cipher by determining the values a and b. (6)

(b) For each positive integer $n \geq 1$, prove that $n = \sum_{d/n} \varphi(d)$. The sum being extended over all positive divisor of n. (5)

(c) For $n > 2$, prove that $\varphi(n)$ is an even integer. (5)

SECTION-III

7. (a) Define primitive root ? If $F_n = 2^{2^n} + 1$, $n > 1$, is a prime number, then show that 2 is not a primitive root of F_n. (6)

(b) Verify that 2 is primitive root mod 19 but not of mod 17. (5)

(c) Let r be a primitive root of the odd prime p. Prove that if $P \equiv 3(\text{mod } 4)$, then r has order $\frac{p-1}{2}$ modulo p. (5)

8. (a) State and prove the Euler's theorem. (6)

(b) Show that the congruence $x^3 \equiv 3(\text{mod } 19)$ has no solution whereas $x^3 \equiv 11(\text{mod } 13)$ has three incongruent solutions. (5)

(c) State and proof the Euler's criterion. (5)

9. (a) Knowing that 2 is a primitive root of 19, find all the quadratic residue of 19. (6)

(b) Prove that there are infinitely many primes of the form $8k - 1$. (5)

(c) If p and q are distinct odd primes, then prove that

$$(p/q)(q/p) = \begin{cases} 1 & : \text{if } p \equiv 1(\text{mod}) \text{ or } q \equiv 1(\text{mod } 4) \\ -1 & : \text{if } p \equiv q \equiv 3(\text{mod } 4) \end{cases}$$ (5)

Total No. of Questions – 9] [Total Pages : 4
(2112)

5546

M.A./M.Sc. Examination

MATHEMATICS

(Analytical Number Theory)

Paper–M-303

(Semester–III)

Time : Three Hours] [Maximum Marks : 80

The candidates shall limit their answers precisely within the answer-book (40 pages) issued to them and no supplementary/ continuation sheet will be issued.

Note : Attempt *five* questions in all, selecting at least *one* question from each section but not more than *two* questions from any section.

SECTION–I

1. (a) Given integers a and b, with $b > 0$, prove that there exist unique integer's q and r such that $a = qb + r^2$, $a \leq r < b$. (6)

(b) If $gcd(a, b) = d$, prove that $gcd\ (a/d, b/d) = 1$. (4)

(c) Prove that the diaphragmatic equation $ax + by = c$ has a solution if and only if d/c, where $d = gcd\ (a, b)$. (6)

2. (a) Prove that every positive integer $n > 1$ can be expressed as a product of prime. (5)

(b) If p_n is the nth prime, prove that $p_n \leq 2^{2^{n-1}}$. (6)

(c) Find the values of n for which $\lfloor n \rfloor + \lfloor n+1 \rfloor + \lfloor n+2 \rfloor$ is a perfect square. (5)

3. (a) Prove that for arbitrary integers a, b, $a \equiv b \pmod{n}$ if and only if a and b prove the same non-negative remainder when divided by n. (5)

(b) Prove that the integer $53^{303} + 103^{53}$ is divisible by 39. (5)

(c) Prove that congruence $ax \equiv b \pmod{n}$ has a solution if and only if d/b where $d = gcd\ (a, n)$. If d/b, prove that the congruence has d mutually in congruent solutions modulo n. (6)

SECTION–II

4. (a) If p is a prime which does not divide a, prove that $a^{p-1} \equiv 1 \pmod{p}$. (5)

(b) When p is an odd prime, prove that the quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$. (7)

(c) Verify that $4 \lfloor 29 + \lfloor 5$ divisible by 31. (4)

5. (a) Let $n = p_1^{k_1}, p_2^{k_2} \ldots\ldots p_r^{k_r}$ be the prime factorization of $n > 1$. Prove that the positive divisors of n are those integers $d = p_1^{a_1}, p_2^{a_2} \ldots\ldots, p_r^{a_r}$, where $a \leq a_i \leq k_i$, $i = 0, 1 \ldots\ldots r$. Also prove that

$$\tau(n) = (k_1 + 1)\ (k_2 + 1) \ldots\ldots (k_r + 1).$$ (6)

(b) Let F and f be two number theoretic functions related by $F(n) = \sum_{d/n} f(d)$. Prove that

$$f(n) = \sum_{d/n} u(d)\ F\left[\frac{n}{d}\right]$$

Also prove that forming positive integer N,

$$\sum_{n=1}^{N} F(n) = \sum_{k=1}^{N} f(k)\left[\frac{N}{k}\right]$$ (5+5)

6. (a) If p is a prime and $k > 0$, prove that

$$\phi(p^k) = p^k\left(1 - \frac{1}{p}\right).$$ (5)

(b) If $\phi(n) \mid n - 1$, prove that n is a square free integer. (6)

(c) Prove that for $n > 1$, the sum of the positive integers less than n and relatively prime to n is $\frac{1}{2} n\,\phi(n)$. (5)

SECTION-III

7. (a) If the integer a has order be modulo n and $h > 0$, prove that a^h has order $k/gcd\ (h, k)$ modulo n. (6)

(b) If $F_n = 2^{2^n} + 1$, $n > 1$, is a prime, prove that 2 is not a primitive root of F_n. (5)

(c) Obtain all the primitive roots of 41. (5)

8. (a) If n has a porimitive root r and int a denotes the index of a relative to r, prove that

int $a^k = k$ and $a \pmod{\phi(n)}$ for $k > a$. (6)

(b) Prove that 3 is a quadratic residue of 23, but is a non-residue of 31. (5)

(c) If $p = 2^k + 1$ is prime verify that every quadratic non-residue of p is a primitive root of p. (5)

9. (a) Describe if the congruence $x^2 \equiv -46 \pmod{17}$ is soluble. (4)

(b) If p is an odd prime, prove that

$$(2/p) = \begin{cases} 1 \text{ if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \\ -1 \text{ if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8 \end{cases} \quad (5)$$

(c) Solve the congruence $x^2 \equiv 146 \pmod{1357}$. (7)

M.A./M.Sc. Examination

MATHEMATICS

(Analytical Number Theory)

Paper–M-303

(Semester–III)

Time : Three Hours] [Maximum Marks : 80

The candidates shall limit their answers precisely within the answer-book (40 pages) issued to them and no supplementary/ continuation sheet will be issued.

Note : Attempt *five* questions in all, selecting at least *one* question from each section but not more than *two* questions from any section.

SECTION–I

1. (a) Given any integer a and b, not both of which are zero, prove that there exist integers x and y such that $\gcd(a, b) = ax + by$. 6

(b) Show that the expression $\frac{a(a^2+2)}{3}$ is an integer. 5

(c) If p is a prime number and $p \mid ab$, then show that $p \mid a$ or $p \mid b$. 5

2. (a) If $k > 0$, then prove that gcd $(ka, kb) = k$ gcd (a, b). 6

(b) Prove that there is an infinite number of primes. 5

(c) Show that 41 divides $2^{20} - 1$. 5

3. (a) Prove that the conjecture that every even integer greater than 2 is the sum of two primes is equivalent to the statement that every integer greater than 5 is the sum of three primes. 6

(b) State and prove the Chinese Remainder Theorem. 5

(c) Prove that the system of linear congruences

$$ax + by \equiv r \pmod{n}, \quad cx + dy = s \pmod{n}$$

has a unique solution modulo n whenever gcd $(ad - bc, n) = 1$. 5

SECTION–II

4. (a) Let p be a prime number and suppose $p \mid a$, then prove that $a^{p-1} \equiv 1 \pmod{p}$. 6

(b) Define the absolute pseudoprime. Let n be a composite square-free integer, say, $n = p_1 p_2 \ldots p_r$, where p_i are distinct primes. If $p_i - 1 \mid n - 1$ for $i = 1, 2, 3 \ldots r$, then prove that n is an absolute pseudoprime. 5

(c) If f is a multiplicative function and F is defined by $F(n) = \Sigma_{d|n} f(d)$, then prove that F is also a multiplicative function. 5

5. (a) If $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ is the prime factorization of $n > 1$, then prove that the number of positive divisors of n equal to $(k_1 + 1)(k_2 + 1) \ldots (k_r + 1)$. 6

(b) If p is prime, then prove that $(p - 1)! \equiv -1 \pmod{p}$. 5

(c) Determine the day of the week on which you were born. 5

6. (a) If p is a prime then prove that $\phi(p^k) = p^k - p^{k-1}$. 6

(b) Prove that if the integer n has r distinct odd prime factors then $2^r \mid \phi(n)$. 5

(c) State and prove the Euler's theorem. 5

SECTION–III

7. (a) Show that if $F_n = 2^{2^n} + 1$, $n > 1$ is a prime, then 2 is not a primitive root of F_n. 6

(b) If p is an odd prime, then the only incongruent solution of $x^2 \equiv 1 \pmod{p}$ are 1 and $p - 1$ solution. 5

(c) If p is an odd prime, then prove that there exists a primate root r of p such that $r^{p-1} \not\equiv 1 \pmod{p^2}$. 5

8. (a) Let p be an odd prime and gcd $(a, p) = 1$. Then prove that a is a quadratic residue of p if and only if

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p.$$ 6

(b) Test whether the congruence $x^2 \equiv -46 \pmod{17}$ is solvable or not. 5

(c) Let r be a primitive root of integer n, prove that r^k is a primitive root of n if and only if gcd $(k, \phi(n)) = 1$. 5

9. (a) Test whether the congruence equation $x^2 = 196 \pmod{1537}$ is solvable or not. 6

(b) If the integer a has order k modulo n, and $h > 0$, then show that a^h has order $\frac{k}{\gcd(h, k)}$ modulo n. 5

(c) If p is an odd prime then prove that

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