Divisibility :-

An integer $a \neq 0$, is said to be divide an integer b if there exists an integer k such that $b = ak$ & it is denoted by a/b.

Ex:- ① $2/8 \Rightarrow 8 = 2(4)$

② $3/24 \Rightarrow 24 = 3(8)$

Note:- ① If 'a' does not divides 'b' is denoted by $a \nmid b$.

② If $a/b \Rightarrow a/-b$

③ If $-a/b \Rightarrow -a/-b$

Properties of divisibility :-

① If a/b, then P.T a/bx, where 'x' is an integer.

Pf:- Given $a/b \Rightarrow b = ak_1 \quad \forall : k_1 \in Z$

x^{ly} B.S 'x'

$bx = ak_1x \quad (\because k_1x = k \in Z)$

$bx = ak$

$\Rightarrow a/bx$

② If a/b & b/c then P.T a/c.

Soln:- If $a/b \Rightarrow b = ak_1 \quad \forall : k_1 \in Z$

& $b/c \Rightarrow c = bk_2 \quad \forall : k_2 \in Z$

$\Rightarrow c = (ak_1)k_2$

$\Rightarrow c = ak$ where $k = k_1k_2$

$\Rightarrow a/c \quad \forall : k \in Z$.

③ If a/b & a/c then P.T ⓘ a/bc ⓘⓘ $a/(b+c)$ ⓘⓘⓘ $a/(b-c)$

Soln:- Given $a/b \Rightarrow b = k_1 a \rightarrow ①$ $\forall : k_1 \in Z$

$a/c \Rightarrow c = k_2 a \rightarrow ②$ $\forall : k_2 \in Z$

ⓘ $① \times ② \Rightarrow bc = ak_1 ak_2$

$bc = ak$ $\quad \because k = \cancel{k_1 k_2} k_1 a k_2$

$\Rightarrow a/bc$

ⓘⓘ $① + ② \Rightarrow b + c = k_1 a + k_2 a$

$= a(k_1 + k_2)$

$b + c = ak$ $\quad \because k = k_1 + k_2$

$\Rightarrow a/(b+c)$

ⓘⓘⓘ $① - ② \Rightarrow b - c = k_1 a - k_2 a$

$= a(k_1 - k_2)$

$b - c = ak$ $\quad \because k = k_1 - k_2$

$\Rightarrow a/(b-c)$

④ If a/b & b/a then P.T $a = \pm b$.

Soln: Given $a/b \Rightarrow b = ak_1 \rightarrow ①$ $\forall : k_1 \in Z$

$b/a \Rightarrow a = bk_2 \rightarrow ②$ $\forall : k_2 \in Z$

$a = (ak_1)k_2$

$\div a$

$1 = k_1 k_2$

$\Rightarrow k_1 = k_2 = 1$ & $k_1 = k_2 = -1$

when, $\left.\begin{array}{l} k_1 = 1 \Rightarrow a = b \\ k_2 = -1 \Rightarrow a = -b \end{array}\right\} \Rightarrow a = \pm b.$

⑤ If a/b & a/c for any integer m & n then show that $a/(bm+cn)$

Soln:- Given $a/b \Rightarrow a/bm \Rightarrow bm = ak_1 \rightarrow ①$ $\forall : k_1 \in Z$

$a/c \Rightarrow a/cn \Rightarrow cn = ak_2 \rightarrow ②$ $\forall : k_2 \in$

$① + ② \Rightarrow bm + cn = ak_1 + ak_2$

$bm + cn = a(k_1 + k_2)$

$bm + cn = ak$ where $k = k_1 + k_2 \in Z$.

$\Rightarrow a/(bm+cn)$

⑥ If ac/bc & $c \neq 0$ then P.T a/b.

Soln:- Given $ac/bc \Rightarrow bc = ack_1$ $(\because k_1 \in Z)$

$\div c$

$\Rightarrow b = ak_1$

$\Rightarrow a/b$.

⑦ If $a = b + c$ & 'd' is the divisor of any two integers of a, b, c, Then P.T 'd' divides the third

Soln: Let $d/a \Rightarrow a = dk_1$

& $d/b \Rightarrow b = dk_2$

Given $a = b + c$

$c = a - b$

$① - ② \Rightarrow a - b = dk_1 - dk_2$

$c = d(k_1 - k_2)$

$c = dk$ $\because k = k_1 - k_2$

$\Rightarrow d/c$

Thm-8:- If $c = ax + by$ and d/a but $d \nmid c$ then $d \nmid b$

Pf:- we have, $d/a \Rightarrow \exists$ an integer q_1 such that

$$a = dq_1$$

$$\therefore c = ax + by$$

$$c = dq_1x + by$$

suppose, $d/b \Rightarrow \exists$ an integer q_2 such that $b = dq_2$

$$c = dq_1x + dq_2y$$

$$c = d(q_1x + q_2y)$$

$$\Rightarrow d/c$$

Conversely, $d \nmid c \Rightarrow d \nmid b$.

Th-9:- If integer 'b' divides a positive integer 'a' then 'b' is not numerically greater than 'a'.

Pf:- we have $b/a \Rightarrow \exists$ an integer 'q' (with $|q| \geq 1$) such that $a = bq$

Hence, $a = |a| = |bq|$

$$a = |b| \cdot |q|$$

$$a \geq |b|$$

Division Algorithm :-

Thm-1 :- For given integers a & $b>0$ there exist unique integers q & r such that $a=bq+r$, $0\le r<b$. The integers q & r are called the quotient and the remainder respectively.

Pf :- Consider, the infinite sequence of multiples of 'b' given below.

$$\ldots -b, 0, b, \ldots, bq, \ldots$$

obviously, either 'a' must be equal to one of the multiples of 'b' say bq. it must lie between two consecutive multiples say bq and $b(q+1)$.

Thus, we have, $bq \le a \le b(q+1)$ $\forall : q$.

$$0 \le a-bq < b$$

$$\text{let } a-bq = r$$

Then, we have, $a = bq + (a-bq)$

$$a = bq + r$$

$$0 \le r < b$$

This completes existance part of the theorem.

For uniqueness, let us assume the possibility of two different representations of 'a' as given below.

$$a = bq + r \rightarrow (1) \qquad 0 \le r < b$$

$$\& \; a = bq_1 + r_1 \rightarrow (2) \qquad 0 \le r_1 < b \quad \text{for } q, q_1, r \,\&\, r_1 \in \mathbb{Z}.$$

from (1) & (2)

$$bq + r = bq_1 + r_1$$

$$bq - bq_1 = r_1 - r$$

$$b(q-q_1) = r_1 - r$$

$$r_1 - r = b(q-q_1)$$

This shows that $b/(r_1-r)$. But this is not possible because both r & r_1 are positive integers less than 'b'.

Hence q & r must be unique.

This theorem is known as Division Algorithm.

Th-2:- For any two integers a & $b>0$ there exists integers q_1 & r_1 such that $a=bq_1+er_1$

$0 \le r_1 < \frac{b}{2}$, $e=+1$ or -1.

Pf:- By division Algorithm, we have

$$a=bq+r \quad , \quad 0 \le r < b \rightarrow (1)$$

Now we consider following cases.

case-1:- If $r<\frac{b}{2}$

let us take $q_1=q$, $r_1=r$ & $e=1$

from (1)

$$a=bq+er_1 \quad , \quad 0 \le r_1 < \frac{b}{2}$$

case-2:- If $r>\frac{b}{2}$ then $0<b-r$ & $e=-1$

then from (1)

$$a=b(q+1)-(b-r)$$

$$a=bq_1+er_1 \qquad 0 \le r_1 < \frac{b}{2}$$

case-3:- If $r=\frac{b}{2}$

If we take $q_1=q$, $r_1=r$ & $e=1$

$$a=bq_1+er_1 \qquad r_1=\frac{b}{2}$$

put $q_1=q+1$, $r_1=b-r$ & $e=-1$

$$a=b(q+1)-(b-r)$$

$$a=bq_1+er_1 \quad . \quad r_1=\frac{b}{2}.$$

Th-3:- Every integer is of the form.

i) $3q$ or $(3q \pm 1)$

ii) $4q$, $(4q \pm 1)$ or $(4q \pm 2)$

iii) $5q$, $(5q \pm 1)$ or $(5q \pm 2)$.

Soln:- Let 'a' be an integer.

i) Taking $b=3$ in theorem ②, we have

$$a = 3q_1 + er_1 \quad , \quad 0 \le r_1 \le \frac{3}{2} \, , \quad e = \pm 1$$

$\therefore r_1 = 0$ or 1

$\Rightarrow a = 3q$ or $(3q \pm 1)$

ii) Taking $b=4$ in theorem ②,

we have, $a = 4q_1 + er_1 \quad 0 \le r_1 \le \frac{4}{2} \, , \quad e = \pm 1$

$\therefore r_1 = 0, 1, 2$

$\Rightarrow a = 4q$, $(4q \pm 1)$ or $(4q \pm 2)$

iii) Taking $b=5$ in theorem ②

we have $a = 5q_1 + er_1 \quad 0 \le r_1 < \frac{5}{2} \, , \quad e = \pm 1$

$\therefore r_1 = 0, 1, 2$

$a = 5q, (5q \pm 1), (5q \pm 2)$

Th-4:- Every odd integer is of the form

i) $2q+1$ ii) $2q-1$ iii) $4q \pm 1$ iv) $\pm(4q+1)$.

Pf:- Since $2q$ is an even integer.

we have $(2q+1)$ & $(2q-1)$ are odd integers.

W.K.T every integer has one of the form $4q, (4q \pm 1)$

& $(4q \pm 2)$ are even integers.

$\therefore (4q \pm 1)$ are odd integers.

Now, $4q - 1 = -(-4q+1)$

$= -[4(-q)+1]$

$\therefore \pm(4q+1)$ is an odd integer.

Th-5:- The square of an odd integer is of the form $8q+1$.

Pf:- Let 'a' be an odd integer.

Then we have, $a = (4q_1+1)$ or $a = -(4q_1+1)$ for some integer q_1.

$$\text{Now, } a^2 = [\pm(4q_1+1)]^2$$
$$= 16q_1^2 + 1 + 8q_1$$
$$= 8(2q_1^2 + q_1) + 1$$
$$a^2 = 8q+1 \quad \text{where } q = 2q_1^2 + q_1 \text{ is an integer.}$$

$\Rightarrow$ Square of an odd integer is of the form $(8q+1)$.

Th-6:- One of every three consecutive integers is divisible by 3.

Pf:- Let $a, (a+1), (a+2)$ be any three consecutive integers.

Then 'a' is of the form $3q, (3q+1)$ or $(3q-1)$.

If $a=3q$, then it is divisible by 3.

If $a = 3q+1$
$$a+2 = 3q+1+2$$
$$= 3q+3$$
$$a+2 = 3(q+1)$$
$\therefore$ It is divisible by 3.

& $a+1 = 3q-1+1$

$a+1 = 3q$ is divisible by 3.

Thus, one of every three consecutive integers is divisible by 3.

Th-7:- The product of any three consecutive integers is divisible by $3!$.

Pf:- Let a, $a+1$ & $(a+2)$ be any three consecutive integers.

Now, we have to show that $a(a+1)(a+2)$ is divisible by $3!$.

We shall prove this result by mathematical induction.

For $a=1$.

we have, $a(a+1)(a+2) = 1.2.3$

which is obviously divisible by $3!$.

$\therefore$ The result is true for $a=1$.

Let the result is true for $a=k$.

i.e $k(k+1)(k+2)$ is divisible by $3!$.

Then for $a=k+1$.

we have. $a(a+1)(a+2) = (k+1)(k+2)(k+3)$

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

$\therefore$ The first term on the RHS of ① is divisible by $3!$ By our assumption.

The second term on the RHS of ① is also divisible by $3!$ because $(k+1)(k+2)$ is divisible by $2! = 2$

Thus. $a(a+1)(a+2)$ is divisible by $3!$ for $a=k+1$

i.e the result is true for $a=k+1$

Hence by mathematical induction the product of any three consecutive integers is divisible by $3!$

Hence the proof.

Greatest common divisor :- (GCD)

or Highest common factor :- (HCF).

consider the integers 18 & 24.

The positive divisors of 18 are 1, 2, 3, 6, 9, 18

The positive divisors of 24 are, 1, 2, 3, 4, 6, 8, 12, 24.

∴ The common divisors of 18 & 24 are 1, 2, 3, 6

$\Rightarrow$ 6 is the GCD of 18 & 24.

The GCD 6 satisfies the following properties.

i) 6 is the common divisor of 18 & 24.

ii) Every common divisor of 18 & 24 divides 6,

i.e $1/6$, $2/6$, $3/6$ & $6/6$

Thus the GCD of two integers is defined as follows.

Defn:- The GCD of two integers a & b is a unique positive integer d such that

i) d is the common divisor of both a & b i.e d/a & d/b

ii) every common divisor of a & b divides 'd'

i.e x/a & $x/b \Rightarrow x/d$.

The GCD of two numbers a & b is written as (a, b). i.e $d = (a, b)$

Ex's:- $(12, 18) = 6$, $(3, 12) = 3$. $(10, 10) = 10$

$(6, 1) = 1$, $(1, 7) = 1$. $(9, 14) = 1$.

Basic properties:-

① The GCD of two numbers (where atleast one of them is not zero) is always positive & unique.

② $(a, b) = (b, a)$

③ $(a, b) = (a, -b) = (-a, b) = (-a, -b)$ Ex: $(8, -12) = 4$

④ If 'a' is any integer, then $(a, 1) = 1$

<u>Ex:-</u> $(6, 1) = 1$, $(-3, 1) = 1$, $(0, 1) = 1$

⑤ If 'a' is a non-zero integer then

i) $(a, 0) = a$ if 'a' is +ve

ii) $(a, 0) = -a$ if 'a' is -ve

Ex: $(8, 0) = 8$, $(-8, 0) = -(-8) = 8$.

⑥ $(0, 0)$ does not exist.

⑦ If $(a, b) = d$ and 'm' is any positive integer then $(ma, mb) = md$

⑧ If $(a, b) = d$ then $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

<u>Euclidean Algorithm:-</u>

The GCD of two integers a & b can be determined by a process known as Euclidean Algorithm.

Let a & b both are positive and $a > b$. Then there exist integers q_1 & r_1 such that

$$a = bq_1 + r_1 \quad , \quad 0 \le r_1 < b \rightarrow ① \quad [\because \text{By division algorithm}]$$

Again there exist two integers q_2 & r_2 such that

$$b = r_1 q_2 + r_2 \quad , \quad 0 \le r_2 < r_1 \rightarrow ②$$

Continuing this process, we get

$$r_1 = r_2 q_3 + r_3 \quad , \quad 0 \le r_3 < r_2$$

$$\vdots$$

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

where $q_n \ge 2$

$\Rightarrow a > b > r_1 > r_2 \ldots$

Thus, these numbers form a decreasing sequence of non-negative integers. $\Rightarrow r_n = 0$ for some integer 'n'

The set of equations ① to ④ is called Euclidean Algorithm for GCD (a, b)

$\therefore$ The GCD of a & b will be r_{n-1}.

<u>Theorem-1</u>:- Let 'a' & 'b' be positive integers such that $a>b$ and let $r_n=0$ in Euclid's algorithm. Then r_{n-1} is the GCD of 'a' & 'b'.

<u>Pf</u>:- By Euclidean Algorithm, we have

$$r_{n-2} = r_{n-1} q_n + r_n$$

$$r_n = 0$$

$$\Rightarrow r_{n-2} = r_{n-1} q_n + 0 \longrightarrow ①$$

$$\Rightarrow r_{n-1} / r_{n-2}$$

Again, we have $r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}$

$$= r_{n-1} q_n q_{n-1} + r_{n-1} \quad \text{using ①.}$$

$$r_{n-3} = r_{n-1}[q_n q_{n-1} + 1]$$

$$\Rightarrow r_{n-1} / r_{n-3} \longrightarrow ②$$

Thus, r_{n-1} satisfies condition ① of GCD.

Further, let c divides a & b. Since $a = bq_1 + r_1$

$\Rightarrow c$ divides b and r_1

& also $b = r_1 q_2 + r_2$

$\Rightarrow c$ divides r_1 & r_2

continuing this process, we finally have that 'c' divides r_{n-1}.

This shows that r_{n-1} satisfies condition ② of GCD.

Hence $GCD(a, b) = r_{n-1}$.

Minimal Algorithm (Absolutely least Remainder Algorithm) :—

Let a & b both are positive and $a > b$.
Then there exist integers Q_1 & R_1 such that

$$a = bQ_1 + e_1 R_1 \quad , \quad 0 < R_1 \leq \frac{b}{2} . \rightarrow ①$$

Again there exist integers Q_2 & R_2 such that

$$b = R_1 Q_2 + e_2 R_2 \quad . \quad 0 < R_2 \leq \frac{R_1}{2} \rightarrow ②$$

continuing like this

$$R_1 = R_2 Q_3 + e_3 R_3 \quad , \quad 0 < R_3 \leq \frac{R_2}{2} \rightarrow ③$$

$$\vdots$$

$$R_{n-3} = R_{n-2} Q_{n-1} + e_{n-1} R_{n-1} \; , \; 0 < R_{n-1} \leq \frac{R_{n-2}}{2} \; -(n-1)$$

$$R_{n-2} = R_{n-1} Q_n + e_n R_n \; , \quad R_n = 0$$

where $e_1 . e_2 . e_3 . \dots . e_n$ all are $+1$ or -1.
Since $a > b > R_1 > R_2 > \dots\dots > R_n$ form a decreasing sequence of non-negative integers.

$\Rightarrow$ It follows that $R_n = 0$ for some integer 'n'.

The process ends at this stage.
The GCD of a & b will be R_{n-1} as in Euclid's Algorithm.

Th-2 :- If 'a' and 'b' are any two integers not both zero then GCD(a, b) exists and is unique.

Pf :- Existance : obviously the GCD(a, b) is not affected by the signs of a & b.

$\therefore$ we assume that both a & b are positive and $a \geq b$.

By division algorithm

$$a = bq_1 + r_1 \quad , \quad 0 \leq r_1 < b \longrightarrow (1)$$

If $r_1 = 0$ then b/a & GCD$(a, b) = b$.

$\Rightarrow$ GCD(a, b) exists.

If $r_1 \neq 0$, then By division Algorithm we have, $b = r_1 q_2 + r_2 \quad , \quad 0 \leq r_2 < r_1 \longrightarrow (2)$

If $r_2 = 0$ then r_1/b & therefore from (1).

$$a = (r_1 q_2) q_1 + r_1$$

$$a = r_1 [q_1 q_2 + 1]$$

$$\Rightarrow r_1/a$$

Let s/a, $s/b \Rightarrow s/(a - bq_1)$

$\Rightarrow s/r_1$ from (1).

$\therefore$ GCD$(a, b) = r_1 \Rightarrow$ GCD(a, b) exists.

If $r_2 \neq 0$ we repeat the process

This process terminates in finite steps n.

In this way we will arrive at zero remainder after n^{th} step, we have sequence of integers r_i such that

$$0 \leq r_n < r_{n-1} < \dots < r_2 < r_1 < b,$$

$$r_{n-2} = r_{n-1} q_n + r_n \ , \ n \geq 3 \ \& \ r_{n-1} = q_{n+1} r_n$$

Thus r_n/r_{n-1}, r_n/r_{n-2}, ... r_n/b and r_n/a.

Now, if s is a common divisor of a & b then s/a & s/b

$\Rightarrow s/a-bq$

$\Rightarrow s/r_1$

$\Rightarrow s/r_2$

$\vdots$

$\Rightarrow s/r_n$

Thus, $GCD(a,b)=r_n \Rightarrow GCD(a,b)$ exists.

uniqueness:- If d_1 & d_2 are two GCDs of a & b then by defn of GCD we have $d_1 \geq d_2$ & $d_2 \geq d_1 \Rightarrow d_1=d_2$

This shows that $GCD(a,b)$ is unique.

Theorem-3:- If 'a' & 'b' are any two integers not both zero then there exists integers x & y such that $GCD(a,b)=ax+by$.

Pf:- Let $GCD(a,b)$ be 'd' &

let $S=\{ax_1+by_1 : ax_1+by_1>0,\ x_1, y_1 \text{ are integers}\}$.

since at least one of a or b is non-zero either $|a|$ or $|b| \in S$

Thus, 'S' is non-empty.

By well-ordering principle 'S' has a least element $d=ax_0+by_0$.

By defn $d \leq |a|, |b|$

By division Algorithm, we have.

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

$$r=|a|-dq$$

$$= \pm a - q(ax_0+by_0)$$

$$r = a(\pm 1 - x_0 q) + b(-y_0 q)$$

This is of the form $ax+by$.

If $r>0$, $\Rightarrow$ r is a member of 'S'
which is a contradiction
'd' is the least integer in 'S'.

consequently. $|a| = dq$
$\Rightarrow d/|a|$
$\Rightarrow d/a$

$1^{||y}$ we shall show that d/b.

Thus, 'd' is a common divisor of 'a' & 'b'.

Now, if 'c' is an arbitrary positive common divisor of a & b.
i.e c/a & c/b
then $c/(ax+by) = c/d$

Hence, d is the greatest common divisor of 'a' & 'b'
i.e $d = GCD(a,b) = ax+by$.

<u>Corollary</u>:- If a, b are any two given integers, not both zero, then the set
$S_1 = \{ax+by : x, y \text{ are integers}\}$ consists of multiple of $d = GCD(a,b)$.

<u>Pf</u>:- Since d/a and d/b
$\Rightarrow d/(ax+by) \quad \forall : x, y \in Z$.

Thus every member of S_1 is a multiple of 'd'.

Let $d = ax_0 + by_0$. where x_0, y_0 are suitable integers.

Now, $nd = n(ax_0+by_0)$
$nd = a(nx_0) + b(ny_0) \in S_1$
$nd \in S_1$ [$\because$ nd is a linear combn of a & b]

Theorem-4 :- If a, b are any two integers, not both zero and 'k' is any integer then $(ka, kb) = |k| (a, b)$.

Pf :- Let $\cancel{d}$ $d=(a,b)$ & $d_1=(ka,kb)$, where 'k' is +ve.

Since, $d=(a,b)$ $\exists$ integers x & y such that

$$d = ax+by.$$

$$\therefore\ dk = x(ka) + y(kb)$$

$$dk = d_1 r$$

$$\Rightarrow d_1/dk \longrightarrow ①$$

& also, $d/a, d/b \Rightarrow dk/ka$ and dk/kb.

This shows that dk is a common multiple of ka & kb.

$$dk/d_1 \longrightarrow ②$$

From ① & ②

$$d_1 = dk$$

$$(ka, kb) = k(a,b)$$

Hence the proof.

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

Pf :- Since $d = GCD(a,b)$

we have, d/a and d/b

$\therefore$ a/d and b/d both are integers.

& also $d = (a,b)$

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

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

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

Hence the proof.

① Find the GCD of 81 & 237. Express it in the form of $81x + 237y$

<u>Soln</u> :-

$81 \overline{)\,237\,}(2$
$\underline{162}$
75

$75 = 237 - 2[81]$

$75 \overline{)\,81\,}(1$
$\underline{75}$
6

$6 = 81 - 1[75]$

$6 \overline{)\,75\,}(12$
$\underline{72}$
3

$3 = 75 - 12[6]$

$3 \overline{)\,6\,}(2$
$\underline{6}$
0

$\therefore$ GCD of 81 & 237 is 3

$$
\begin{aligned}
3 &= 75 - 12[6] \\
&= 237 - 2[81] - 12\{81 - 1[75]\} \\
&= 237 - 2[81] - 12[81] + 12[75] \\
&= 237 - 14[81] + 12\{237 - 2[81]\} \\
&= 237 - 14[81] + 12[237] - 24[81] \\
&= 13[237] - 38[81]
\end{aligned}
$$

$$3 = -38[81] + 13[237]$$

$\therefore x = -38$ & $y = 13$

② Find the GCD of $(55, 210)$ & express it in the form of $55x + 210y$ and show that expression is not unique.

Soln

$$55)\,210\,(3$$
$$\underline{165}$$
$$45$$

$45 = 210 - 3[55]$

$$45)\,55\,(1$$
$$\underline{45}$$
$$10$$

$10 = 55 - 1[45]$

$$10)\,45\,(4$$
$$\underline{40}$$
$$5$$

$5 = 45 - 4[10]$

$$5)\,10\,(2$$
$$\underline{10}$$
$$00$$

$\therefore$ GCD of $(55, 210)$ is 5.

$$5 = 45 - 4[10]$$
$$= 210 - 3[55] - 4\{55 - 1[45]\}$$
$$= 210 - 3[55] - 4[55] + 4[45]$$
$$= 210 - 7[55] + 4\{210 - 3[55]\}$$
$$= 210 - 7[55] + 4[210] - 12[55]$$
$$= 5[210] - 19[55]$$
$$5 = -19[55] + 5[210] \longrightarrow ①$$
$$x = -19 \quad \& \quad y = 5$$
$$5 = -19[55] + 5[210] + [55]210 - [55]210$$
$$= 55[210 - 19] + 210[5 - 55]$$
$$5 = 55(191) + 210(-50) \longrightarrow ②$$
$$x = 191 \quad \& \quad y = -50$$

From ① & ②

This expression is not unique.

Prime numbers:- (P)

An integer $p>1$ which has no divisor except one and the number itself is called a prime number.

or

An integer $p>1$, is called a prime number if it is not divisible by any other number except ± 1 and $\pm p$.

Ex:- 2, 3, 5, 7, 11, 13 ......

Composite number:-

Composite number is an integer which is not a prime number.

or

An integer $a>1$, is called a composite number if it has a divisor other than ± 1 or $\pm a$.

Ex:- 4, 6, 8, 9, 10 .....

Note:-

* '0' & '1' are neither prime nor composite.
* '2' is the only even prime.
* If 'p' is a prime number then '-p' is also a prime number.

Relatively prime numbers:- (Co-prime) or (Twin-prime)

Two numbers a & b are said to be relatively prime if and only if the GCD of a & b is 1. i.e $GCD(a,b)=1$.

Ex:- $(8,15)=1$, $(2018, 2019)=1$

Note:-

1) Every composite number can be expressed as the product of the prime factors and this product is unique.

Ex:- $45 = 3 \times 3 \times 5 = 3^2 \times 5^1$

2) Let 'N' is a composite number.

$$N = P_1^{\alpha_1} P_2^{\alpha_2} P_3^{\alpha_3} \dots \dots P_n^{\alpha_n}$$

where $P_1 . P_2 . P_3 \dots$ are all prime numbers.

& $\alpha_1 . \alpha_2 . \alpha_3 \dots$ are +ve integers.

This is known as canonical representation of 'N'.

3) Formula to find the number of +ve divisor of a number 'N'.

$$T(N) = (1+\alpha_1)(1+\alpha_2)(1+\alpha_3) \dots \dots (1+\alpha_n)$$

4) Formula to find the sum of the +ve divisor of a number (N).

$$S(N) = \left(\frac{P_1^{1+\alpha_1} - 1}{P_1 - 1}\right)\left(\frac{P_2^{1+\alpha_2} - 1}{P_2 - 1}\right)\left(\frac{P_3^{1+\alpha_3} - 1}{P_3 - 1}\right) \dots \dots \left(\frac{P_n^{1+\alpha_n} - 1}{P_n - 1}\right)$$

① Find the number of +ve divisors and their sum of a number 303.

Soln $3 \,\underline{|\, 303}$
$ 101$

$$303 = 3^1 \times 101^1$$

$P_1 = 3 \qquad \alpha_1 = 1$

$P_2 = 101 \qquad \alpha_2 = 1$

$\therefore$ The no of +ve divisors.

$$T(303) = (1+\alpha_1)(1+\alpha_2)$$
$$= (1+1)(1+1)$$
$$T(303) = 4$$

The sum of the +ve divisor

$$S(N) = \left(\frac{P_1^{1+\alpha_1} - 1}{P_1 - 1}\right)\left(\frac{P_2^{1+\alpha_2} - 1}{P_2 - 1}\right)$$

$$= \left(\frac{3^2 - 1}{3-1}\right)\left(\frac{101^2 - 1}{101 - 1}\right)$$

$$S(N) = 408$$

② Find the number and sum of all positive divisors of 960.

③ Find the number and sum of all positive divisors of 48, 136 and 526.

④ Express 560 as the product of prime factors.

Soln

$$560 = 2 \times 280$$
$$= 2 \times 2 \times 140$$
$$= 2 \times 2 \times 2 \times 70$$
$$= 2^3 \times 2 \times 35$$
$$560 = 2^4 \times 5 \times 7$$

⑤ Express 144 as the product of prime factors.

⑥ Show that $\sqrt{2}$ is not a rational number.

Soln: suppose if possible $\sqrt{2}$ is a rational number

then $\sqrt{2} = \frac{p}{q}$ $\forall : p, q \in \mathbb{Z}$ & $(p.q) = 1$

$\Rightarrow$ Now. $\sqrt{2} = \frac{p}{q}$

$$2 = \frac{p^2}{q^2} \Rightarrow p^2 = 2q^2 = 2q.q$$
$$\Rightarrow q/p^2$$

If $q > 1$. By fundamental theorem of arithmatic $\exists$ at least one prime P_1 such that $P_1/q \Rightarrow P_1/p^2$
$$\Rightarrow P_1/p$$

$\therefore (p.q) = P_1$

But $(p.q) = 1 \Rightarrow P_1 = q = 1$

Now. $q = 1 \Rightarrow p = \sqrt{2} \Rightarrow$ which is not possible because p is a +ve integer. Hence $\sqrt{2}$ is not a rational no.

(7) Show that every prime of the form $3m+1$ is necessarily of the form $6k+1$.

Soln:- Let $n = 3m+1$ be a prime, where 'm' is a positive integer.

Now, 'm' may be even or odd.

i.e $m = 2k$ or $2k+1$

If $m = 2k \Rightarrow n = 3m+1 = 3 \times 2k + 1 = 6k+1$

If $m = 2k+1 \Rightarrow n = 3(2k+1)+1 = 6k+3+1 = 6k+4$
$= 2[3k+2]$

which is not possible as $2(3k+2)$ is not a prime.

Hence, prime 'n' is of the form $3m+1$ will also be of the form $6k+1$.

(8) If a & b are two odd integers then show that a^2+b^2 cannot be a perfect square.

Soln. Let $a = 2k_1+1$ & $b = 2k_2+1$ be two odd integers.

Then $a^2+b^2 = (2k_1+1)^2 + (2k_2+1)^2$

$= 4k_1^2 + 4k_1 + 1 + 4k_2^2 + 4k_2 + 1$

$a^2+b^2 = 2[2k_1^2 + 2k_2^2 + 2k_1 + 2k_2 + 1]$

Thus, a^2+b^2 is not a pefect square

Properties of prime numbers:-

Th-1:- PT the smallest divisor (other than 1) of a composite number is a prime.

or The smallest positive divisor (>1) of any number 'a' is always a prime number.

Pf:- Let $p>1$ be the smallest divisor of an integer 'a'.

$\therefore p/a$

where 'p' is either preme or composite number.

case-1:- If 'p' is a prime number then there is nothing to prove. Thus the property is proved.

case-2:- If 'p' is a composite number then there exists a divisor $d<p$.

such that d/p

Also d/p & $p/a \Rightarrow d/a$

which is a contradiction, our assumption 'p' composite is wrong.

Hence 'p' is a prime number.

Th-2:- If 'p' is a prime and 'a' is any integer Then either $(a,p)=1$ or 'a' is a multiple of 'p'.

Pf:- Since 'p' is a prime, it has two divisors 1 & p.

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

If $(a,p)=1$ then the theorem is proved.

& if $(a,p)=p$ then obviously 'a' is a multiple of 'p'.

Th-3:- If 'p' is a prime and p/ab then either p/a or p/b.

Pf:- Given 'p' is a prime number & p/ab.

If p/a then there is nothing to prove.

$\therefore$ If $p \nmid a$ to p.T p/b

$\therefore p \nmid a$ & 'p' is a prime.

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

$\Rightarrow 1 = px + ay. \quad \forall : x.y \in Z$.

x^{ly} B.S by 'b'.

$b = pbx + aby \rightarrow (1)$.

Given p/ab

w.k.T. $p/p \Rightarrow p/pbx$. & p/aby

$\Rightarrow p/(pbx+aby)$

$\Rightarrow p/[b(px+ay)]$

$\Rightarrow p/b$.

Hence the proof.

Th-4:- If 'p' is a prime and $p/a_1a_2a_3 \ldots a_n$ then p/a_k where $1 \leq k \leq n$.

Pf:- Let if possible 'p' does not divide any of the numbers $a_1 . a_2 . a_3 \ldots a_n$.

Then 'p' is relatively prime to each of these numbers.

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

$\therefore a_1 . a_2 . a_3 \ldots a_n$ is not a multiple of 'p'.

which contradicts the fact that 'p' divides atleast one of the numbers $a_1 . a_2 \ldots a_n$

i.e p/a_k. $1 \leq k \leq n$.

Corollary:— If $p.q_1.q_2....q_n$ are all primes and $p/q_1q_2....q_n$ then $p=q_k$ where $1\le k\le n$.

Pf:— By the above theorem p/q_k $\forall: k$ with $1\le k\le n$.

But q_k is divisible by 1 or q_k as q_k is a prime.

Since $p>1$. we have. $p=q_k$.

Th-5:— P.T there are infinitely many primes

or P.T the number of prime numbers is infinite.

Pf:— Let the numbers of prime be finite.

$P_1.P_2.P_3....P_n$ are the primes in which P_n is the largest primes.

Consider. $N=P_1.P_2.P_3...P_n+1$

when we divide 'N' be each P_i's leave the remainder one.

$\therefore$ 'N' is not divisible by each one of the P_i's.

$\therefore$ 'N' can not be a composite ($\because$ Every composite number as have a prime divisor)

$\therefore$ N is a prime number

As $N>P_n$ & $N\neq 0, 1$

Thus, our assumption is wrong.

Hence the no of primes are infinite.

Th-6:— If a & c are relatively prime & a/bc then P.T a/b.

or If a/bc and $(a,c)=1$ then P.T a/b.

Pf:— Given GCD of $(a.c)=1 \Rightarrow 1=ax+cy$ [where x & y are integers]

x^{ly} B.S by 'b'

$b=abx+bc.y$

W.K.T $a/a \Rightarrow a/abx$
Given $a/bc \Rightarrow a/bcy$ $\Big\} \Rightarrow a/(abx+bcy)$

$\Rightarrow a/b(ax+cy)$

$\Rightarrow a/b\cdot 1$

$\Rightarrow a/b$.

Th-7:- If there exist integers x & y such that $ax+by=1$, then $(a,b)=1$.

Pf:- Let $(a,b)=d$ i.e GCD of a & b is d.

$\Rightarrow d/a$ & d/b

$\Rightarrow d/ax$ & d/by

$\Rightarrow d/ax+by$

$\Rightarrow d/1$

$\Rightarrow d=1$

$\therefore (a,b)=1$.

Th-8:- If $(a,b)=1$ & $(a,c)=1$ then P.T $(a,bc)=1$.

Pf:- Given $(a,b)=1 \Rightarrow 1=ax+by \rightarrow ①$ $\forall: x,y \in Z$

$(a,c)=1 \Rightarrow 1=ax_1+cy_1 \rightarrow ②$ $\forall: x_1,y_1 \in Z$.

$\times^{ly}$ ① & ②

$1=(ax+by)(ax_1+cy_1)$

$1=a^2xx_1+acxy_1+abx_1y+bcyy_1$

$1=a(axx_1+cxy_1+byx_1)+bc(yy_1)$

$1=aX+bcY$ $\because X=axx_1+cxy_1+byx_1 \in Z$

$\Rightarrow (a,bc)=1$ & $Y=yy_1 \in Z$.

Th-9:- The smallest +ve divisor (>1) of a composite number 'a' does not exceed $\sqrt{a}$.

Pf:- Given $b/a \Rightarrow a = bk$ $(\because k \in Z)$

$$\Rightarrow 1 < b \leq k$$

$$\Rightarrow b \leq k$$

$\times^{ly}$ B.S 'b'

$$b^2 \leq bk$$

$$b^2 \leq a$$

$$b \leq \sqrt{a}$$

Thus, the smallest divisor greater than one of a number 'a' does not exceed $\sqrt{a}$.

The linear diophantine equation :—

An equation of the form

$$ax+by+c=0 \rightarrow ①$$

with $a\neq 0$, $b\neq 0$ and 'c' integer, is called a linear diophantine equation in two unknowns x & y.

A pair ~~&~~ x_0, y_0 of integers is called a soln of ①.

$$ax_0+by_0+c=0$$

Ex:- $2x+3y=12$ is a linear diophantine eqn
$x=3$ & $y=2$ is the solution of this equation
we may write this solution as $(3,2)$

But $8x+17y=7$ has ~~x~~ no solution.

Th-1:- If $(a,b)=d$ then the equation $ax+by=c$ has a solution (integral soln) iff d/c.

Pf:- suppose $d/c \Rightarrow c=rd$ where 'r' is an integer.
Since $(a,b)=d$ $\exists$ an integers x_1 & y_1 such that

$$ax_1+by_1=d.$$

x^{ly} B.S by $\frac{c}{d}$

$$\frac{c}{d}ax_1+\frac{c}{d}by_1=\frac{c}{d}d=c$$

$$\Rightarrow c=a\left(\frac{c}{d}x_1\right)+b\left(\frac{c}{d}y_1\right)=ax+by$$

$\Rightarrow$ Thus. $\left(\frac{c}{d}x_1\right)$ & $\left(\frac{c}{d}y_1\right)$ satisfy the eqn $ax+by=c$
Hence linear diophantine eqn has a solution.
Conversely, The eqn $ax+by=c$ has a solution say (x_0,y_0)

Then $ax_0+by_0=c$
But ax_0+by_0 must be a multiple of 'd'.
i.e $ax_0+by_0=rd$. where $r\in Z$

$$c=rd$$

$$\Rightarrow d/c$$

Hence the Proof.

Th-2:- If (x_0, y_0) is one solution of $ax+by=c$ & $(a,b)=d$ then $x_1 = x_0 - \frac{b}{d}t$, $y_1 = y_0 + \frac{a}{d}t$ is the general solution.

Pf:- Let $ax+by=c \rightarrow ①$ & $(a,b)=d$

Since (x_0, y_0) is a solution of eqn ①.

$\therefore ax_0 + by_0 = c \rightarrow ②$

Let (x_1, y_1) be a general solution of eqn ①

$ax_1 + by_1 = c \rightarrow ③$

$③ - ② \Rightarrow a(x_1 - x_0) + b(y_1 - y_0) = 0$

$\Rightarrow a(x_1 - x_0) = -b(y_1 - y_0) \rightarrow ④$

Since $(a,b)=d$, $\exists$ integers r_1 & r_2 such that $a = r_1 d$ & $b = r_2 d$

eqn ④ becomes

$r_1 d(x_1 - x_0) = -r_2 d(y_1 - y_0)$

$r_1(x_1 - x_0) = -r_2(y_1 - y_0) \rightarrow ⑤$

$\Rightarrow r_1 / -r_2(y_1 - y_0)$

$\Rightarrow r_1 / (y_1 - y_0)$

$\therefore y_1 = y_0 + t r_1 \quad \forall : t \in Z$

$y_1 = y_0 + \frac{a}{d}t$

eqn ⑤ becomes

$r_1(x_1 - x_0) = -r_2 r_1 t$

$x_1 - x_0 = -r_2 t$

$x_1 = x_0 - r_2 t$

$x_1 = x_0 - \frac{b}{d}t$

Thus, $x_1 = x_0 - \frac{b}{d}t$ and $y_1 = y_0 + \frac{a}{d}t$ is the general solution of eqn ①. $ax+by=c$.

Hence the proof.

carollary-1:- If (x_0, y_0) is one solution of $ax+by=c$, $(a,b)=d$ then $x_1 = x_0 + \frac{b}{d}t$, $y_1 = y_0 - \frac{a}{d}t$ is the general solution of $ax+by=c$.

Pf:- Replacing t by $-t$ in the Th-2. we get required result.

carollary-2:- If (x_0, y_0) is one solution of $ax+by=c$, $(a,b)=1$, then $x_1 = x_0 + bt$, $y_1 = y_0 - at$ is the general solution of the eqn $ax+by=c$.

Pf put $d=1$ in Th-2. we get the required result.

carollary-3:- If (x_0, y_0) is one solution of $ax+by=c$, $(a,b)=1$ Then $x_1 = x_0 + bt$, $y_1 = y_0 - at$ is the general solution of the equation $ax+by=1$.

Pf:- Replace t by $-t$ in the result of carollary (2) we get the required result.

Th-3:- If $ax+by=c$, $(a,b)=1$, b is numerically smaller of the two co-efficients a & b and a_1 & c_1 are the minimal remainders of a and c respectively w.r.t $|b|$. Then $ax+by=c$ can be written in the form $a_1x + |b| x_1 = c_1$ in which $|a_1| \le \frac{|b|}{2}$ & $|c_1| \le \frac{|b|}{2}$

Pf:- Since a_1 & c_1 are minimal remainders of a & c w.r.t $|b|$.

we have, $a = |b| q_1 + a_1$, $0 < |a_1| \le \frac{|b|}{2}$

$c = |b| q_2 + c_1$, $0 < |c_1| \le \frac{|b|}{2}$

Thus, $ax+by=c$ can be written as

$$(|b|\,q_1 + a_1)x + by = |b|\,q_2 + c_1$$

$$a_1 x + |b|\left(q_1 x + \frac{b}{|b|}y - q_2\right) = c_1$$

put $x_1 = q_1 x + \frac{b}{|b|}y - q_2$ the above equation reduces

to $a_1 x + |b|\,x_1 = c_1$.

Hence the proof.

Problems:-

① Find the general solution of $170x - 455y = 625$

soln To find GCD of 170 & 455

$$170\overline{)455}(2 \qquad 455 - 340 = 115$$

$115 = 455 - 2[170]$

$$115\overline{)170}(1 \qquad 170 - 115 = 55$$

$55 = 170 - 1[115]$

$$55\overline{)115}(2 \qquad 115 - 110 = 5$$

$5 = 115 - 2[55]$

$$5\overline{)55}(11 \qquad 55 - 55 = 0$$

$\therefore$ GCD of 170 & 455 is 5.

Now, $5 | 625 \Rightarrow 170x - 455y = 625$ has a solution.

At $x = 1$ & $y = -1$ is a particular soln of the given eqn

$$\therefore x_1 = x_0 - \frac{b}{d}t$$

$$x_1 = 1 - \left(\frac{-455}{5}\right)t \Rightarrow x_1 = 1 + 91t \quad \forall\, t \in Z$$

$$\& \; y_1 = y_0 + \frac{a}{d}t$$

$$y_1 = -1 + \left(\frac{170}{5}\right)t \Rightarrow y_1 = -1 + 34t \quad \forall\, t \in Z$$

② Find the general solution of $70x + 112y = 168$

Fundamental theorem of Arithmatic :—

Statement :- Every ~~integer~~ positive integer $n>1$ can be expressed as the product of prime factors uniquely.

Pf :- Let $n>1$ be an integer.

If 'n' is a prime number then there is nothing to prove.

If 'n' is a composite number then there exists a prime p_1 such that $n = p_1 n_1$ $\forall : n_1 \in \mathbb{Z}$.

If n_1 is a prime then 'n' is expressed as product of prime factors.

If n_1 is a composite number then there exists a prime 'p_2' such that

$$n = p_1 n_1 = p_1 p_2 n_2 \quad \forall : n_2 \in \mathbb{Z}$$

If n_2 is a prime then 'n' is expressed as the product of prime factors.

If n_2 is a composite then we continue the process

$$n > n_1 > n_2 > \dots\dots$$

the process cannot continue infinitely.

After finite number of steps we get

$$n = p_1 p_2 p_3 \dots p_k \text{ . where all } p_i\text{'s are primes.}$$

Uniqueness :- Suppose it possible 'n' can be represented as a product of primes in two ways such as

$$n = p_1 p_2 p_3 \dots p_r = q_1 q_2 q_3 \dots q_s \text{ , } r<s \rightarrow ①$$

where p_i & q_i are primes in the increasing order.

i.e $p_1 \le p_2 \le p_3 \le \dots \le p_r$

& $q_1 \le q_2 \le q_3 \le \dots \le q_s$

Since $p_1 / q_1 q_2 \ldots q_s$ $\exists$ some q_k such that p_1 / q_k.

But p_1 & q_k are both primes

$\therefore p_1 = q_k$

we rearrange q_i's such that $p_1 = q_1$

Now cancelling p_1 & q_1 in ①, we get

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

continue the process till all p_i's are exhausted. (say)

$$1 = q_{r+1} q_{r+2} \ldots q_s$$

But it is not possible as q_i's are primes

$\therefore$ r cannot be less than 's'

$||^{ly}$ we can show that 's' cannot be less than 'r'.

Hence $r = s$

$\therefore p_i = q_i \quad \forall i$

Thus, the representation is unique.

<u>Corollary</u>:- Any positive integer $n > 1$ can be written uniquely in a canonical form

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_r^{\alpha_r}$$

, where α_i is a positive integer, $i = 1, 2, \ldots r$ and each p_i is a prime such that $p_1 < p_2 < p_3 < \ldots < p_r$

<u>Pf</u>:- By fundamental theorem of arithmatic

we have, $n = p_1 \cdot p_2 \cdot p_3 \ldots p_s$

Here $p_1 \cdot p_2 \cdot p_3 \ldots p_s$ may be repeated

combining repeating factors can be written as

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

, where $p_1 < p_2 < \ldots < p_r$ & $\alpha_i \geq 1$

uniqueness can be proved in the proof of fundamental theorem of algebra.

Theorem-2: If 'n' is not divisible by any prime $\le \sqrt{n}$ then 'n' is a prime.

Pf:- Suppose it possible 'n' is not a prime.
thus 'n' is a composite number.
It can be written as
$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_r^{\alpha_r}$$
But $p_1, p_2 > \sqrt{n}$
$\therefore$ which is not possible
Hence 'n' is a prime number.