# Unit-I

## MSF

## Greatest Common divi
&
## Prime Factorization

## Division Algorithm $\boxed{\text{or}}$ Euclidian Algorithm

Let $a, b \neq 0 \in \mathbb{Z}$. Then $\exists$ two integers

$\boxed{q, r} \Rightarrow \boxed{a = bq + r.}$

b>0
↓ අවශ්‍ය
නැත.

where $0 \leq r < |b|$

$$b \overline{)\, a \,(} q$$
$$\underline{x}$$
$$r$$

**Example:- i) $a = 14$, $b = -3$**

$$-3 \overline{)\,14\,(} -4$$
$$\underline{12}$$
$$2$$

$2 \Rightarrow$ remainder එක 0 ත් b අතර
වෙන්න ඕනෙ.

$0 \longrightarrow b$
remainder එක හෝ zero
වෙන්න ඕනෙ.

$$14 = (-3)(-4) + 2$$

$$a = bq + r$$

$\boxed{\text{where } 0 \leq r < |b|}$

$$0 \leq 2 < |-3|$$

Example-2 :- 133

$$b = 21 \overset{a}{\overline{)\,133\,}}(6 = q$$
$$\underline{126}$$
$$7 = r$$

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

$133 = 21 \times 6 + 7$

&

$0 \le 7 < 21$

So remainder = 7 which lies b/w 0 to 21.

Example- -50

$a = bq + r$

$-50 = 8(-7) + 6$

$0 \le 6 < 8$

Here remainder = 6 which lies b/w 0 to 8.

$$b = 8 \overset{a}{\overline{)\,-50\,}}(-7 = q$$
$$\underline{-42}$$
$$8 = r$$

V.V.Imp

Division Algorithm or

Euclidian Algorithm or

Division Algorithm

State & Prove Euclidian Algorithm?

or

State & Prove Euclidian's Lemma?

or

State & Prove Division Algorithm?

Scanned with CamScanner

Division Algorithm:— (or) State & Prove Euclidian Algorithm:— Division Algorithm?

Statement:—

→ There are several procedures for finding gcd of two positive integers.

→ An efficient method for finding the greatest common divisor of two integers based on the quotient & remainder technique is called the Euclidean Algorithm.

(or)

To develop a systematic method (or) algorithm, To find the greatest common divisor of two positive integers. This

## Statement:

Let a, b are two integers $\boxed{(b>0)}$

$\exists$ two Unique numbers q, r : $a = bq + r$ &

$\boxed{0 \le r < b.}$

(or)

$0 \le r < |b|$

where q = quotient

r = remainder.

$\boxed{a = bq + r}$ → Euclidean algorithm formula

a → divisor

b → dividend

q → quotient

r → remainder.

proof By data $\boxed{a = bq + r}$ — (1)

$0 \leq r < b$.

Consider, Set of multiple of b are

$0, \pm b, \pm 2b, \pm 3b \ldots\ldots$

Now, we are going to prove $\boxed{3}$ diffirent cases.

a is multiple of b

a is not multiple of b

$\Rightarrow r = 0$

Case-1: ~~Let us~~ Consider $\boxed{\text{Set if}}$ multiple of b :-

a is multiple of b. When it happens. a|b. pakka.

ie perfect divides. Happens only remainder $=0$.

b)a(q

(r) = 0

$$\boxed{a = bq}$$

$(\because r = 0)$ from - 1

Case-2:- If a is not multiple

If a is not multiple of b. Happens ca, ...

a lies b/w two Consequent numbers.

In mathematically.

$$\boxed{\begin{aligned} bq < a < b(q+1) \\ bq < a < bq+b \end{aligned}}$$

Now $\boxed{bq}$ is substracting in above equation.

$$\cancel{bq}-\cancel{bq} < a-bq < \cancel{bq}+b-\cancel{bq}$$

$$0 < a-bq < b$$

w.k.t
$a = bq + r$
$a - bq = r$

fudn-①

$$\boxed{0 < r < b}$$

ie

Prime: — positive integer ... If the only ... are $\boxed{P \ \& \ 1}$ ... $\boxed{n > 1}$ is not prim ... $\boxed{\text{Composite}}$ ...

$0 \leq r < b$

$\cancel{=}$ is not equal to Zero. We get only

$\boxed{0 < r < b}$

Case-3:- Uniqueness:-

7:-

$2)\,7\,(3$
$\quad 6$
$\quad \overline{1}$

$\Rightarrow 7 = 2 \times 3 + 1.$

if I have written

Every problem for any integer. q & r are

Uniqueness.

Consider another two integers.

$q_1$ & $r_1$.

From our (1) -equation $a = bq + r$ —— (1)

$a = bq_1 + r_1$ —— (2)

From (1) & (2) $\Longrightarrow$

$$bq + r = bq_1 + r_1$$

$$bq - bq_1 = r_1 - r$$

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

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

$$b(q_1 - q) = r - r_1 \quad (3)$$

From divisibility Definition

$$b \mid r - r_1 \quad (\text{b divides } r - r_1 \text{. So})$$

Let $r - r_1 = 0$ or $r = r_1$. Then eq (3) becomes.

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

i.e $b = 0$ & $q_1 - q = 0$

but $b=0$ is not possible.

Because in the statement. $b>0$ only division algorithm possible. So,

Only possibility $\boxed{q_1 - q = 0}$

$$\boxed{q_1 = q}$$

# Common divisor:—

If $a, b \in \mathbb{Z}$. Then an integer ($d$) is said to be a Common divisor of $a, b$ if

$$\boxed{d \mid a \ \& \ d \mid b}$$

Example:— ① $3 \mid 6$ & $3 \mid 9 \Rightarrow \boxed{3}$ is Common divisor of 6, 9

Factors of 3 = 1, 3

Factors of 6 = 1, 3, 6

Factors of 9 = 1, 3, 6, 9

② $-4 \mid 8$ & $-4 \mid 12 \Rightarrow$ $-4$ is Common divisor of 8, 12

~~Factors of $-4$ =~~

③ $a = 6$, $b = 8 \Rightarrow$ Common divisor of $\boxed{\pm 1, \pm 2}$

Factors of 6 = 1, 2, 3, 6

Factors of 8 = 1, 2, 4, 8

Common = 1, 2

Integers = $\pm 1, \pm 2$

④ $a = 7$, $b = 5 \Rightarrow$ Common divisor of $\boxed{d = \pm 1}$

Factors of 7 : 1, 7

Factors of 5 : 1, 5

Common $\boxed{1}$.

Integral = $\pm 1$

Scanned with CamScanner

# Greatest Common divisor :- $\boxed{GCD}$.

The greatest Common divisors of two integers (a,b) is the largest integer that divides both the integers. **Representation:-**

GCD or gcd of a,b is denoted by (a,b).

$\boxed{\text{gcd of } (a,b) = \text{Number.}}$

**Ex:- GCD of (3,6):-**

Factors of 3 :- $\boxed{1, 3}$
Factors of 6 :- $\boxed{1, 3}$, 2, 6

Common factors $\boxed{1,3}$.

Common factors of (3,6) = 1,3.

↓

1,3 greatest number is 3

Greatest Common factor of (3,6) = $\boxed{3}$.

$\boxed{\therefore \text{GCD of } (3, 6) = 3}$

Scanned with CamScanner

② GCD of (20, 16) :—

Factors of 20 :— $\boxed{1, 2, 4}$, 5, 10, 20

Factors of 16 :— $\boxed{1, 2, 4}$, 8, 16

Common factors 1, 2, 4

Common factors = 1, 2, 4

↓

what is largest value =

greatest number is $\boxed{4}$.

ie big Value = 4

Greatest number = 4.

$$\boxed{\therefore \text{GCD of } (20, 16) = 4}$$

## IM

Let $a, b \in \mathbb{Z}$

① $d|a$ & $d|b$ $\Rightarrow$ $\boxed{d}$ is common divisor of a, b

+

② $c|a$ & $c|b$ $\boxed{(c \in \mathbb{Z})}$ $\Rightarrow$ $\boxed{c < d}$ (d is gcd)

**Representation:**— gcd of a, b is denoted by (a, b)

Exaples of gcd: How find G. given Nos. using Normal Method?

1. $(6,8) = 2$ Ans
2. $(7,5) = 1$ Ans
3. $(24,-32) = 8$ Ans

   C.d:

   $\pm 1, \pm 2, \pm 4, \pm 8$

4. $(16,48) = 16$ Ans

   C.d:

   $\pm 1, \pm 2, \pm 4, \pm 8, \pm 16$

# GCD @ Problems by General Method

(or)

## Greatest Common Divisors - problems

① Find the greatest common divisor of the numbers 12 & 14?

Factors of 12 :- 1, 2, 3, 4, 12

Factors of 14 :- 1, 2, 7, 14

Common factors 1, 2

Common factors = 1, 2

GCD = 2

$\boxed{\therefore \text{GCD of } (12, 14) = 2}$

② Find the greatest Common divisor 8 & 12 ?..

Factors of 8 :- $\boxed{1, 2}$, $\boxed{4}$, 8

Factors of 12 :- $\boxed{1, 2}$, 3, 4, 6, 12

} 1, 2, 4

Common factors = 1, 2, 4

GCD = 4

$\boxed{\therefore \text{GCD of } (8, 12) = 4}$

Find GCD of (2, 10)? Ans: 2

Factors of 2 :- $\boxed{1, 2}$

Factors of 10 :- $\boxed{1, 2}$, 5, 10

Common factors = 1, 2

Common factors = 1, 2

GCD = 2

$$\boxed{\therefore \text{GCD of } (2, 10) = 2}$$

(4) Find gcd (18, 24)? Ans: 6

Factors of 18 :- 1, 2, 3, 6, 9, 18

Factors of 24 :- 1, 2, 3, 6, 12, 24

1, 2, 3, 6

Common factors :- 1, 2, 3, 6

GCD = 6

$\boxed{\text{GCD of } (18, 24) = 6}$

gcd(325, 858)? HCF

Factors of 325 :- 1, 5, 13, 325

Factors of 858 :- 1, 2, 3, 11, 13, 858

Common factors = 1, 13

GCD = 13

$\boxed{\text{GCD of } (325, 858) = 13}$

5 | 325
5 | 65
13 | 13
1

2 | 858
3 | 429
13 | 143
11