**Bharathidasan University**
Tiruchirappalli - 620 024
Tamil Nadu, India

**Programme: M.Sc., Mathematics**

Course Title :Theory of Numbers
COurse Code : 21M04CC

# Divisibility

**Dr. V. Piramanantham**
Professor
Department of Mathematics

Divisibility:

$a \neq 0,\ b \in \mathbb{Z}$

If $\exists\ m \in \mathbb{Z}$ s.t. $b = ma$. we say that $a \mid b$.

(a divides b)

otherwise we say that $a \nmid b$.

Properties of Division

① If $a \mid b$ and $b \mid c$, then $a \mid c$.

② If $a \mid b$ & $a \mid c$, then $a \mid bx + cy$, $\forall x, y \in \mathbb{Z}$

③ If $a \mid b$, then $-|b| \leq a \leq |b|$.

④ If $a > 0$ & $b > 0$, then $a \leq b$.
(+ve divisor is always smaller than dividend)

⑤ If $a \mid b$ and $b \mid a$, then $a = \pm b$.

proof: $a \mid b \Rightarrow \exists\, m_1 \in \mathbb{Z}$ s.t. $b = m_1 a$ — ①

$b \mid a \Rightarrow \exists\, m_2 \in \mathbb{Z}$ s.t. $a = m_2 b$ — ②

Substituting ② in ① $\Rightarrow$ $b = m_1 (m_2 b)$

$b = (m_1 m_2) b$

since $b \neq 0$, $m_1 m_2 = 1$

Since the only numbers having multiplicative inverse are $+1$ and $-1$.

$$m_1 = \pm 1 \ \& \ m_2 = \pm 1$$

From ② $\Rightarrow$ $a = \pm b$

Corollary of ⑤

⑤' If $a > 0, b > 0$, $a \mid b$ and $b \mid a$, then $a = b$.

⑥ If $m \neq 0$, then $a \mid b \Leftrightarrow ma \mid mb$.

Assume that $a \mid b$

$\exists\, n \in \mathbb{Z}$ s.t. $b = na$

$\Rightarrow \quad mb = m(na)$
$\qquad\qquad = n(ma)$

$\Rightarrow ma \mid mb$

conversely assume that $ma \mid mb$

$\exists\, k \in \mathbb{Z}$ s.t. $mb = k(ma)$

$mb = m(ka)$

since $m \neq 0$, $b = ka$

$\Rightarrow a \mid b$. //

## Division Algorithm

Statement: If $a$ and $b$ are any two integers with $a > 0$, then there exist unique integers $q$ and $r$ such that

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

Here $q$ is called quotient & $r$ is called remainder on the division of $b$ by $a$.

Proof:

Consider $A = \{ b + ka \mid k \in \mathbb{Z} \text{ and } b + ka \geq 0 \}$

clearly $A$ is a nonempty subset of $\mathbb{Z}$ because $k \geq -\frac{b}{a}$; ($\mathbb{Z}$ is unbdd).

By well-ordering principle, there exists a smallest element in $A$.

Let $r$ be the smallest number in $A$.

$\exists\ q \in \mathbb{Z}$ such that $b - qa = r$

$\Rightarrow b = qa + r$ — (*)

$k = -q$

$b + ka = r$

$r = b - qa$

By the definition of $A$,

$r \geqslant 0$

$0 \leq r < a$

$r < a$

we prove that $r < a$.

suppose that $r \geq a$.

$\Rightarrow b - qa \geq a$

$\Rightarrow b - qa - a \geq 0$

$\Rightarrow b - (q+1)a \geq 0 \Rightarrow b - (q+1)a \in A$

$k = -(q+1)$

But $b - (q+1)a < b - qa = r$

$\Rightarrow \Leftarrow$ to the choice of $r$.

$\therefore r < a$

So far, we have proved that $\underline{\exists\ q\ \&\ r}$ such that

$$\underline{b = qa + r \ \&\ 0 \le r < a}$$

<u>Uniqueness of $q$ & $r$</u>:

Suppose that there exist another integers $q'$ and $r'$ such that

$$b = q'a + r' \text{ and } 0 \le r' < a.$$

<u>claim</u>: $r = r'$ and $q = q'$.

Suppose that $r \neq r'$. Then either $r < r'$ or $r > r'$.

If $r < r'$.

$$\Rightarrow 0 < r' - r < a \quad \text{— (A)}$$

$$r' - r = b - q'a - (b - qa)$$

$$= (q - q')a$$

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

$$\Rightarrow a \mid r' - r$$

$a > 0$, $r' - r > 0$. By property (4), $a \leq r' - r$. — (B)

which is a contradiction to our assumption.

$$\therefore r \nless r'$$

IIIly we can prove that $r' \nless r$.

$$\therefore r = r'.$$

$$b = qa + \cancel{r} = q'a + \cancel{r'}$$

$$\Rightarrow \quad qa = q'a \qquad \text{because } r = r'$$

$$\Rightarrow \quad (q - q')a = 0$$

Since $a > 0$, $\quad q - q' = 0 \Rightarrow q = q'$

$\therefore (q, r)$ is unique.

Hence the result.

If $a$ & $b \in \mathbb{Z}$ with $a > 0$, then $\exists$ $q$ & $r \in \mathbb{Z}$ such that

$$\underline{b = qa + r}, \quad 0 \le r < a.$$

**Problem** (Division algorithm)

$b = 96, \quad a = 13 \qquad q = 7 \quad r = 5$

$b = -38 \quad a = 7 \qquad q = -6 \quad r = 4$

$b = -21 \quad a = 7 \qquad q = 3 \quad r = 0$

$$-100 = (-8)\,13 + 14$$

$\boxed{100 = 7 \cdot 13 + 9} \longrightarrow r' = 9 \qquad 0 \le r' < 13$

$-100 = q \cdot 13 + r, \quad 0 \le r < 13 \qquad -13 < -r' \le 0$

$0 < 13 - r' \le 13$

$-100 = -7 \cdot 13 - 9 \qquad r = \{ r', \quad r' = 0$

$-100 = q \cdot 13 + r, \quad 0 \leq r < 13$ $\quad 0 < \underbrace{13 - r'}\leq 13$

$\underset{\sim}{-100} = -7 \cdot 13 - 9$

$= -\underbrace{7 \cdot 13 - 13} + 13 - 9$

$= (-8) \cdot 13 + 4$

$\boxed{q = -8, \quad r = 4}$

$r = \begin{cases} r', & r' = 0 \\ 13 - r' & 0 < r' < 13 \end{cases}$

$b \in \mathbb{Z}, \quad \underset{\sim}{a > 0} \quad \exists!\, q, r \in \mathbb{Z}$ s.t.

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

## Modified Division Algorithm:

Let $a, b \in \mathbb{Z}$ such that $a \neq 0$. Then there exist unique integers $q$ and $r$ such that

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

EXERCISE

Find $q$ & $r$ such that $35 = q \cdot (-6) + r$ & $0 \leq r < 6$.

Common Divisors:

$b = 18$, $\{1, 2, 3, 6, 9, 18\}$

Result:

$a \mid b \iff -a \mid b \iff a \mid -b \iff -a \mid -b$.

$a$ is divisor of $b \iff -a$ is a divisor of $b$.

We concentrate only on +ve divisors

$b = 0$ All the nonzero integers divide $b$

$b = 24$ $\{1, 2, 3, 4, 6, 8, 12, 24\}$

1 & b are the trivially divisors of b.

b & c

b → list all the divisors of b

c → " " of c

Definition Let b & c be given integers.

A non zero integer a is called a common divisor of b and c if

1 is a common divisor of any two numbers.

Definition: Let $b_1, b_2, \dots, b_n$ be given numbers. A nonzero number $a$ is called a common divisor of $b_1, b_2, \dots, b_n$ if

$$a \mid b_i \ , \ i = 1, 2, \dots n$$

If $b \neq 0$, then there are only finitely many divisors of $b$.

If any one of $b$ & $c$ is non zero, then there are finitely many common divisors

In particular, There are finite number of common divisors of $b$ & $c$.

Definition (Greatest Common Divisor)

Let $b$ & $c$ be given integers, not both zero, Then the largest among the +ve common divisor of $b$ & $c$ is known as the greatest common divisor (gcd) of $b$ & $c$

The gcd of $b$ & $c$ is denoted by

$$(b, c).$$

**Definition** Let $a_1, a_2, \ldots, a_n$ be given integers, not all zero. Then the gcd of $a_1, a_2, \ldots, a_n$ is the largest among the +ve common divisors of $a_1, a_2, \ldots, a_n$.

It is denoted by $(a_1, a_2, \ldots, a_n)$

**Example** $b = 24$, $c = 18$

$b = 24 \rightarrow 1, 2, 3, 4, 6, 8, 12, 24$

$2, 3, 6, 9, 18$

I can write $\frac{b}{a}$ if $a \mid b$.

$m = \frac{b}{a}$ $\quad \exists\, m \in \mathbb{Z}$ s.t. $b = ma$

either $a \neq 0$ or $b \neq 0$ or both

$(a,b)$ is defined

$$\boxed{b = \frac{b}{a} \cdot a}$$

$\cancel{\frac{15}{7}}$

$a \mid b$

$\cancel{x} = \frac{28}{7}$

ordinary $\to \sin^2\theta + \cos^2\theta = 1$

Legend $\to 1 = \sin^2\theta + \cos^2\theta$

$(a,b)$

If $a = b = 0$, gcd not defined

Properties of gcd:

## Properties of gcd:

① For any +ve integer m,

$$(ma, mb) = m(a, b).$$

**Proof** $g = (ma, mb)$

$d = (a, b)$

Prove that $g = md$

$$\begin{cases} g \geq md & \text{— ①} \\ g \leq md & \text{— ②} \end{cases}$$

$$\begin{array}{r|l} 2 & 24,\ 18 \\ \hline 3 & 12,\ 9 \\ \hline 1 & 4,\ 3 \\ \hline 1 & \cancel{4},\ 3 \end{array}$$

$(4, 3) = 1$

$3 \cdot (4, 3) = 3$

$\Rightarrow (12, 9) = 3$

$\Rightarrow 2(12, 9) = 6$

① $md \le g$, $g = (ma, mb)$

d is a common divisor of a & b $\Rightarrow$ $d \mid a$ & $d \mid b$

$\Rightarrow md \mid ma$ & $md \mid mb$

$\Rightarrow md$ is a common divisor of $ma$ & $mb$

But $g = (ma, mb)$, $md \le g$ — ①

$n \mid g$

$\Rightarrow \frac{g}{m}$ is integer

② $g \leq md$

$g = (ma, mb) \Rightarrow g \mid ma$ & $g \mid mb$

$\Rightarrow \frac{g}{m} \mid a$ & $\frac{g}{m} \mid b$

$\Rightarrow \frac{g}{m}$ is a common divisor of $a$ & $b$

But $d = (a, b)$

$$\frac{g}{m} \leq d$$

$$g \leq md \quad \text{——} \quad ②$$

$$g = md$$

$$(ma, mb) = m(a, b).$$

<u>corollary</u>: If $d \mid a$ & $d \mid b$ & $d > 0$, then

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

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

**Proof** $m > 0$, $(ma, mb) = m(a, b)$

$m = d$, $a \Rightarrow a/d$ $b \Leftarrow b/d$

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

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

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

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

If $g=(a,b)$ , $\left(\frac{a}{g}, \frac{b}{g}\right) = \frac{\cancel{(a,b)}}{\cancel{g}} = 1$

$$\therefore \left(\frac{a}{g}, \frac{b}{g}\right) = 1$$

$7 \mid 42 \Rightarrow \frac{42}{7} = \underline{\underline{6}}$

$\underline{42 = 6 \cdot 7} \Rightarrow 6 \cdot 7$ is decomposition of $42$

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

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

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

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

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

$\Rightarrow (a,b)$ is divisible by $d$

$$\frac{(a,b)}{d} \in \mathbb{Z}$$

$\Rightarrow (a,b)$ is divisible by $d$

$$\frac{(a,b)}{d} \in \mathbb{Z}$$

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

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

$$c = 1 \cdot c$$

$$c = ab$$

$$\frac{c}{a} = b$$

$$\frac{c}{b} = a$$

$$d = g = (a,b)$$

$$\left(\frac{a}{g}, \frac{b}{g}\right) = \frac{\cancel{(a,b)}}{\cancel{g}} = 1$$