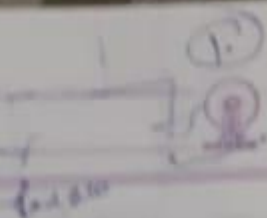


Divisibility Theory



Divisibility: An integer a is said to be divisible by an integer $b \neq 0$ if there exists an integer q such that $a = bq$ denoted by $b|a$

we can also say that a is a multiple of b

ex - 45 is divisible by 15 as 45 = 15 3.

Thus $15|45$.

If b divides a then $-b$ also divides a because $a = bq = (-b)(-q)$

we also have

- (i) $a|0$, $1|a$ and $a|a$
- (ii) $a|b$ and $c|d \Rightarrow ac|bd$
- (iii) $a|b$ and $b|c \Rightarrow a|c$ (Transitivity)
- (iv) $a|b$ and $b|a \Rightarrow a = \pm b$
- (v) $a|b$ and $a|c \Rightarrow a|bx + cy$ \forall integers x, y

Th 1 :- If $c = ax + by$ and $d|a$ but $d|c$ then $d|b$

Proof :- we have

$d|a \Rightarrow \exists$ an integer q_1 such that
 $a = dq_1$

Therefore $c = ax + by = dq_1x + by$

Since $d|c \Rightarrow \exists$ an integer q_2 such that

$$c = dq_2$$

$$\Rightarrow dq_2 = dq_1x + dq_2y$$

$$= d(q_1x + q_2y) \Rightarrow d|c$$

Thus $d|c \Rightarrow d|b$

Ex: The 2) - If integer b divides a positive integer a , then b is not numerically greater than a .

Proof: - we have

$$b|a \Rightarrow \exists \text{ an integer } q$$

$$\text{such that } a = bq$$

$$\text{also } a = |a| = |bq| = |b||q| \geq |b|$$

Ex: Division algorithm 1- for given integers a and $b > 0$, there exist unique integers q and r such that

The 1- $a = bq + r$; $0 \leq r < b$

q and r are called quotient and remainder
quotient \rightarrow remainder

Ex: Statement

The 2) - For any integer $a \geq b > 0$, $\exists r, v$ such that
Do itself: $a = bv + rv$,
 $0 \leq rv < b/2$, $v = \pm 1$ or -1

The 3) - Every integer n is of the form

- (i) $3v$ or $(3v \pm 1)$
- (ii) $4v$, $(4v \pm 1)$ or $(4v \pm 2)$
- (iii) $5v$, $(5v \pm 1)$ or $(5v \pm 2)$

(i) Let a be an integer
we know that $a = 3q + r$ — (1)

putting $b = 3$ in (1) above we get

$$a = 3q + r, \quad 0 \leq r < \frac{3}{3} = 1$$

it means $r = 0$ or 1 , hence

$$a = 3v \quad \text{or} \quad 3v \pm 1$$

Similarly (ii) & (iii)