Divisibility in Integers

Dr. Amol Sonawane

Assistant Professor
Department of Mathematics
Government College of Arts and Science
Aurangabad

Divisibility

Definition:

Let a and b be integers with $a \neq 0$.
The integer a *divides* the integer b, if there exists an integer q such that $b = aq$.
Also, we say that b is divisible by a.
It is denoted by $a \mid b$.

E.g.

1. $2 \mid 6$ ($\because 6 = 2 \cdot 3$)
2. $3 \mid -12$ ($\because -12 = 3 \cdot (-4)$)
3. $-5 \mid 10$ ($\because 10 = (-5) \cdot (-2)$)
4. $-7 \mid -14$ ($\because -14 = (-7) \cdot 2$)

Note: If there does not exist an integer q such that $b = aq$, then we say that a does not divide b.
E.g. $2 \nmid 3$

Note: Let a be an integer. Then

1. $a \mid 0$ $(\because 0 = a \cdot 0)$

Note: Let a and b be integers with $a \neq 0$. Then

1. $a \mid b \implies a \mid -b$.
   Proof. Suppose $a \mid b$.
   Then $b = aq$ for some $q \in \mathbb{Z}$.
   We can write $-b = a(-q)$.
   By definition of divisibility, $a \mid -b$.
2. $a \mid b \implies -a \mid b$.
3. $a \mid b \implies -a \mid -b$.

If $a \mid b$ and $b \mid c$, then prove that $a \mid c$.

Proof. $a \mid b \implies b = aq$ for some $q \in \mathbb{Z}$.
Similarly, $b \mid c \implies c = br$ for some $r \in \mathbb{Z}$.
We can write, $c = (aq)r = a(qr)$.
$\implies c = as$, where $s = qr \in \mathbb{Z}$.
Hence $a \mid c$.

If $a \mid b$ and $a \mid c$, then prove that $a \mid (b + c)$.

Proof. $a \mid b \implies b = aq$ for some $q \in \mathbb{Z}$.
Similarly, $a \mid c \implies c = ar$ for some $r \in \mathbb{Z}$.
We can write, $b + c = aq + ar = a(q + r)$.
$\implies b + c = as$, where $s = q + r \in \mathbb{Z}$.
Hence $a \mid (b + c)$.

Exercise: Prove that

- If $a \mid b$ and $a \mid c$, then $a \mid (b - c)$.
- If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any $x, y \in \mathbb{Z}$.
- If $a \mid b$ and $c \mid d$, then $ac \mid bd$.

Thank You!