Congruence.

Definition: Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n, symbolized by $a \equiv b \pmod{n}$ if n divides the difference $a - b$

i.e. if $n \mid a-b \Rightarrow a-b = nk$ for some integer k.

eg. $5 \equiv 9 \pmod{2}$ since $2 \mid (5-9) = -4$

$3 \equiv -5 \pmod{4}$ since $4 \mid (3-(-5)) = 8$

Note: If $m \nmid (a-b)$ then we say a is incongruent to b mod m and we write $a \not\equiv b \pmod{m}$

eg. $5 \not\equiv 4 \pmod{2}$

Property: $a \equiv b \pmod{m}$ iff a and b have the same remainder on division by m.

Pf: Let $a \equiv b \pmod{m}$.

To show that a and b have the same remainder on division by m.

Now, $a \equiv b \pmod{m} \Rightarrow m \mid (a-b)$ — (1)

Let $a = mq_1 + r$, $0 \le r < m$, $q_1 \in \mathbb{Z}$.

i.e. r is the remainder when a is divided by m.

Scanned with CamScanner

(1) $\Rightarrow m \mid (a-b) \Rightarrow a-b = ms, s \in \mathbb{Z}$

$\Rightarrow mq_1 + r - b = ms$

$\Rightarrow b = m(q_1 - s) + r$

$\Rightarrow b = mq_2 + r, \; q_2 = q_1 - s \in \mathbb{Z}$

$\therefore$ r is the remainder when b is divided by m.

Conversely let a and b have the same remainder on division by m.

Let $a = mq + r, \; 0 \le r < m, q \in \mathbb{Z}$

and $b = mq' + r, \; 0 \le r < m, q' \in \mathbb{Z}$

Now, $a - b = m(q - q')$

$\Rightarrow m \mid (a-b), \; \because q - q' \in \mathbb{Z}$.

$\Rightarrow a \equiv b \pmod{m}$ #

Prop. 2. Let $a \in \mathbb{Z}, m \in \mathbb{N}$. If $a = mq + r$, $0 \le r < m$, then $a \equiv r \pmod{m}$.

Pf. Let $a = mq + r$

$\Rightarrow a - r = mq \Rightarrow m \mid (a - r)$

$\Rightarrow a \equiv r \pmod{m}$.

Scanned with CamScanner

$\Rightarrow b - a = mk', \quad k' \in \mathbb{Z}$

$\Rightarrow m \mid (b-a)$

$\Rightarrow b \equiv a \pmod{m}$.

(iii) Let $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$.

$\therefore n \mid (a-b)$ and $n \mid (b-c)$

$\Rightarrow a - b = nk_1$ and $b - c = nk_2$

for some integers k_1, k_2

Now

$$a - c = (a-b) + (b-c)$$
$$= nk_1 + nk_2 = n(k_1 + k_2)$$
$$= nk, \quad k = k_1 + k_2 \in \mathbb{Z}$$

$\Rightarrow a - c = nk$

$\Rightarrow n \mid (a-c)$

$\Rightarrow a \equiv c \pmod{n}$

(iv) Let $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$

$\Rightarrow n \mid (a-b)$ and $n \mid c-d$

$\Rightarrow a - b = nk_1, \quad c - d = nk_2$

for some integers k_1, k_2

Now,

$$(a+c) - (b+d) = (a-b) + (c-d)$$
$$= nk_1 + nk_2$$

Scanned with CamScanner

$\Rightarrow (a+c)-(b+d) = n(k_1+k_2)$

$= nk, \quad k = k_1+k_2 \in \mathbb{Z}$

$\Rightarrow (a+c)-(b+d) = nk$

$\Rightarrow n \mid (a+c)-(b+d)$

$\Rightarrow a+c \equiv b+d \pmod n$.

Also,

$ac = (b+nk_1).(d+nk_2)$

$= bd + (bk_2+dk_1+nk_1k_2)n$

$\Rightarrow ac-bd = n(bk_2+dk_1+nk_1k_2) \quad -(1)$

$\because b, d, n, k_1, k_2 \in \mathbb{Z}$ & so $bk_2+dk_1+nk_1k_2$ is an integer and let it be k'.

$\therefore (1) \Rightarrow ac-bd = nk', \quad k' \in \mathbb{Z}$

$\Rightarrow n \mid ac-bd$

$\Rightarrow ac \equiv bd \pmod n$ #

(v) Let $a \equiv b \pmod n$.

We know by property (i), for any integer c

$c \equiv c \pmod n$.

$\therefore$ applying property (iv) we get

$a+c \equiv b+c \pmod n$ &

and $ac \equiv bc \pmod n$.

Scanned with CamScanner

(VI) Let $a \equiv b \pmod{n}$. To show $a^k \equiv b^k \pmod{n}$, for any positive integer k. We will prove it by using principle of mathematical induction.

For $k = 1$, the given statement is true. ~~$a^1 \equiv b^1 \pmod{n}$~~

Let us assume that the result is true for fixed k.

$\therefore a^k \equiv b^k \pmod{n}$.

Now, $a \equiv b \pmod{n}$ and $a^k \equiv b^k \pmod{n}$

So by property (IV) we get

$$a \cdot a^k \equiv b \cdot b^k \pmod{n}$$

$$\Rightarrow a^{k+1} \equiv b^{k+1} \pmod{n}$$

$\therefore$ the result is true for $k+1$.

Hence the result is true for all k.

ff

Scanned with CamScanner