MA-222

Note Title 20-08-2021

Lec-9

Congruences

Fixed $n \in \mathbb{N}$. $n \geq 2$

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

$a \equiv b \pmod{n}$ if $n \mid a-b$.

$n \mid a-a$

$n \mid a-b \Rightarrow n \mid b-a$

Ex $n \mid a-b$ & $n \mid b-c \Rightarrow n \mid a-c$?

$a \equiv a \pmod{n}$

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

$a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$

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

Define $\sim_n$ on $\mathbb{Z}$ (for a fixed n)

$a \sim b$ if $a \equiv b \pmod{n}$.

$\sim$ is a equi. rel^n on $\mathbb{Z}$.

Th^{m} $a \equiv b \pmod{n}$ iff both a & b leave the same remainder when div by n.

Pf: Ex

$$[a] = \{ b \in \mathbb{Z} \mid a \sim b \}.$$

$$= \{ b \in \mathbb{Z} \mid a \equiv b \pmod{n} \}.$$

$$= \{ b \in \mathbb{Z} \mid a \text{ \& } b \text{ leave same rem. when div by } n \}$$

$n = 5$.

$\overline{1} = [1] = \{ 5k+1 \mid k \in \mathbb{Z} \}$. $\quad \overline{0} = [0] = \{ 5k \mid k \in \mathbb{Z} \}$.

$\overline{3} = [3] = \{ -2, 3, 8, -7, \ldots \}$.

Denote $\overline{a}$ for $[a]_{\text{mod } n}$. / residue mod n.

Defn: Given a, n $\exists! q, r$ s.t.

$$a = nq + r \qquad 0 \le r < n.$$

Possible remainders are

$$S = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$$

$a \in \mathbb{Z}$

Given $a \in \mathbb{Z}$ $\exists! \overline{r} \in S$ s.t. $a \equiv r \pmod n$ $\forall r' \in \overline{r}$.

Defn: $S = \{\overline{0}, \ldots, \overline{n-1}\}$ is called as smallest positive residue system mod n.

Defn: Complete residue system mod n (CRS).

A set $\{a_1, \ldots, a_n\}$ is called CRS mod n if for every integer $a \in \mathbb{Z}$ $\exists$ exactly one a_i s.t.

$$a \equiv a_i \pmod{n}.$$

$\{0, 1, 2, 3, 4\}$

$\{5, -4, -2, -1, -3\}$

$\{-5, -1, -2, -3, -4\}$

$\{-2, -1, 0, 1, 2\}$

$y = 0$

$y = -5$

Properties of congruences

$\mathbb{Z}_n = \underline{CRS}$

$= \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$

$= \{0, 1, \ldots, n-1\}$

$\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$= \{\bar{0}, \overline{-1}, \overline{-2}, \overline{-3}, \overline{-4}\}$

$\rightarrow \underline{\mathbb{Z}_p}$

$+ \quad \cdot$

On $\mathbb{Z}_n$ define $+$: addition mod n
& $\cdot$: multiplication mod n.

Properties:

i) $\overline{a+b} = \overline{a} + \overline{b}$ & $\overline{ab} = \overline{a} \cdot \overline{b}$

ii) $\forall a, b \in \mathbb{Z}$, $\overline{a+b} \in \mathbb{Z}_n$ & $\overline{ab} \in \mathbb{Z}_n$. Closure property

iii) $a \equiv b \pmod n$ $\overline{a} = \overline{b}$
& $c \equiv d \pmod n$ $(\overline{c} = \overline{d})$
$\Rightarrow \overline{a+c} = \overline{b+d}$
i.e. $a + c \equiv b + d \pmod n$

$ac \equiv bd \pmod n$ $\overline{ac} = \overline{bd}$.

Def. $a \equiv b \pmod n$ then

$a^r \equiv b^r \pmod n \quad \forall \ r \geq 1$

$r \geq 0$

$a^0 \equiv 1 \pmod n$

Que: What if $r < 0$?

$a^r \overset{?}{\equiv} b^r \pmod n$?

a not in $\mathbb{Z}_n$

Cancellation laws.

$\forall c \in \mathbb{Z}$ $\quad a + c \equiv b + c \pmod{n} \Rightarrow a \equiv b \pmod{n}$.

If $(n, c) = 1$ then $ac \equiv bc \pmod{n} \overset{?}{\Rightarrow} a \equiv b \pmod{n}$.

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

$$\Rightarrow n \mid a - b \Rightarrow a \equiv b \pmod{n}$$

$$\overline{a+c} = \overline{b+c}$$

$$\Leftrightarrow \overline{a} = \overline{b} \quad \forall c \in \mathbb{Z}_n$$

$$\overline{a \cdot c} = \overline{b \cdot c}$$

$$\Rightarrow \overline{a} = \overline{b} \text{ if } (c, n) = 1.$$

$ac \equiv bc \pmod{n}$

$\Rightarrow n \mid ac - bc$

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

If $(c, n) = 1$ then

$n \mid a - b$.

$a \equiv b \pmod{n}$.

$6 \mid 3 \cdot 4$

$6 \mid 5 \cdot 12$

$\Rightarrow 6 \mid 12$

What abt the converse!

If $(c, n) = 1$ then $\bar{a} \cdot \bar{c} = \bar{b} \cdot \bar{c}$

$\Rightarrow \bar{a} = \bar{b}$

$\bar{a} + \bar{0} = \bar{a} \quad \forall \bar{a} \in \mathbb{Z}_n$

$\bar{a} \cdot \bar{1} = \bar{a} \quad \forall \bar{a} \in \mathbb{Z}_n$

$(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$

$(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$

$(\bar{a} + \bar{b}) \cdot \bar{c} = \bar{a} \cdot \bar{c} + \bar{b} \cdot \bar{c}$