Note Title 23-08-2021

MA-222

Lec-10

$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$. (mod n)

$\bar{a} + \bar{b} = \overline{a+b} \in \mathbb{Z}_n$.

More properties:

$\bar{0} \in \mathbb{Z}_n$ $\bar{0} \in \mathbb{Z}_m$

Construct $\mathbb{Z}_n$

Implement $+$ & $\cdot$ on $\mathbb{Z}_n$

Compute b s.t. $ab \equiv 1 \pmod{n}$.

i) if $a \equiv b \pmod{n}$ & $d \mid n$
then $a \equiv b \pmod{d}$

ii) if $a \equiv b \pmod{n}$ ~~& $r \in \mathbb{N}$~~.
then $ar \equiv br \pmod{nr}$ $\forall r \in \mathbb{N}$.

iii) $P(x)$ be a poly with integ coeff.
then $a \equiv b \pmod{n}$

$\Rightarrow P(a) \equiv P(b) \pmod{n}$

$ca \equiv cb \pmod{n}$

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

we l. : $a\cancel{\alpha} \equiv b\cancel{\alpha} \pmod{n}$

iff $\quad a \equiv b \left(\bmod \dfrac{n}{\underline{(n, \alpha)}}\right).$

In particular if $\underline{(n, \alpha) = 1}$.

then

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

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

$$\overline{a\alpha} = \overline{b\alpha}$$

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

eg. If $(a, n) = 1$ then $\exists$! b s.t.

$ab \equiv 1 \pmod{n}$. unique $\pmod{n}$.

$ax + ny = 1$

$(ax + ny) \equiv 1 \pmod{n}$

$ax \equiv 1 \pmod{n}$

$a = 4 \quad n = 5$

$4 \cdot (4) \equiv 1 \pmod{5}$

$9 \equiv 4 \pmod{5}$

vi)

$$\left.\begin{array}{l} a \equiv b \pmod{n_1} \\ a \equiv b \pmod{n_2}. \end{array}\right\} \text{then } a \equiv b \pmod{\operatorname{lcm}(n_1, n_2)}.$$

$$a \equiv b \pmod{n_i} \quad i = 1, \ldots, r.$$

then $a \equiv b \pmod{[n_1, \ldots, n_r]}$

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

$S_n = \{ \bar{a} \in \mathbb{Z}_n \mid (a,n) = 1 \}$.

$\bar{0} \notin S_n$

Ex $\bar{a}, \bar{b} \in S \Rightarrow \overline{ab} \in S$.

$\bar{1} \in S$

Since $(a,n)=1 \Rightarrow \exists\, b \in \mathbb{Z}_n$ s.t. $ab \equiv 1 \pmod n$

Que: $b \in S$?

$\sim$ on $\cancel{\mathbb{Z}}$ $\mathbb{R}$.

$a \sim b$ if $n \mid (a-b)$ for some $n \in \mathbb{N}$

$[0] = \mathbb{Z}$

$[\frac{1}{2}] =$

$[0.00001] = n.00001$

$\mathbb{R}/\sim = [0,1)$ or $[0,1]$

$\underline{|S_n| = \varphi(n)}$ Euler's phi-function.
totient

$\varphi(n)$ = no of +ve intg coprime to n
& less than n.

Linear congruences

$ax \equiv b \pmod{n}$

$\exists x \in \mathbb{Z}$ s.t. $n \mid ax - b$?

$\iff \exists x, y \in \mathbb{Z}$ s.t. $ax - b = ny$

$\iff ax + ny = b$

has a sol^n iff $\gcd(a, n) \mid b$.

Thm: $ax \equiv b \pmod{n}$ has a sol^n iff $d = (a, n) \mid b$.

If there is a sol^n, then there are exactly d incongruent sol^n's mod n.

(x_0, y_0)

$\left(x_0 + \frac{n}{d} t, \; y_0 + \frac{a}{d} t\right)$

$ax - ny = b$

$d = (a, n)$

Ex

Chinese remainder thm

$$\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ \vdots \\ a_r x \equiv b_r \pmod{n_r} \end{cases}$$

3rd century Sun Zi

Aryabhatta (6th cent)

Thm (CRT)

Let $n_1, \dots, n_r \in \mathbb{N}$ pairwise coprime

$a_1, \dots, a_r \in \mathbb{Z}$

Then the system of congruences

$$x \equiv a_1 \pmod{n_1} \longleftarrow \qquad n_1 k + a_1 \qquad k_1 \to$$

$$x \equiv a_2 \pmod{n_2} \qquad n_2 k_1 + a_2 \qquad k_2 \to$$

$$\vdots$$

$$x \equiv a_r \pmod{n_r}$$

has a soln. Further any two solns are congr mod N.

where $N = \prod n_i$.

$$x \equiv 0 \pmod{3}$$

$$x \equiv 2 \pmod{6}$$