MA-222

Note Title 24-08-2021

Lec - 11

Thm: (CRT)

$n_1, n_2, \ldots, n_r \in \mathbb{N}$ pairwise coprime.

$a_1, \ldots, a_r \in \mathbb{Z}$.

$\bar{x} = \bar{a}_1$ in $\mathbb{Z}_{n_1}$

$\bar{x} = \bar{a}_2$ in $\mathbb{Z}_{n_2}$

$\bar{x} = \bar{a}_r$ in $\mathbb{Z}_{n_r}$

$\Leftrightarrow$

$x \equiv a_1 \pmod{n_1}$

$\vdots$

$x \equiv a_r \pmod{n_r}$

$\bar{a}_i \in \mathbb{Z}_{n_i}$

$x_1 \equiv x_2 \pmod{N}$

$N = \prod n_i$

CRT (Set theoretic version)

$N = \prod n_i$ Then there exists a bijection bet^n

$$\mathbb{Z}_N \longleftrightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}.$$

$$(\bar{x}) \longmapsto (\bar{x}, \bar{x}, \ldots, \bar{x})$$

Pf:

$N = \prod n_i$ $\qquad N_i = \frac{N}{n_i}$

$(N_i, n_i) = 1$

Find $x_i, y_i \in \mathbb{Z}$ s.t.

$a_1, \dots, a_r$.
$x_1, \dots, x_r$.

$$x_i N_i + y_i n_i = 1.$$

$$\tilde{x} = x_1 N_1 a_1 + x_2 N_2 a_2 + \cdots + x_r N_r a_r$$

$$\tilde{x} \equiv x_1 N_1 a_1 \pmod{n_1} \equiv a_1 \pmod{n_1}.$$

$$x_i N_i + y_i n_i \equiv 1 \pmod{n_i}$$

$$x_i N_i \equiv 1 \pmod{n_i}$$

$$\tilde{x} \equiv a_i \pmod{n_i} \quad \forall i = 1, \ldots, r.$$

$$\tilde{x} \equiv x_i N_i a_i \pmod{n_i}.$$

$$\equiv \left[x_i N_i \pmod{n_i}\right]\left[a_i \pmod{n_i}\right].$$

$$\equiv 1 \cdot a_i \pmod{n_i}.$$

$a \equiv b \pmod{n}$

$a \equiv d \pmod{n}$

Then $a \equiv bd \pmod{n}$

$bd = b \cdot d$

x_1, x_2 be two solns to the system.

$$x_1 \equiv a_i \pmod{n_i} \quad \forall i$$

$$x_2 \equiv a_i \pmod{n_i} \quad \forall i$$

$$x_1 - x_2 \equiv 0 \pmod{n_i} \quad \forall i \Rightarrow n_i \mid x_1 - x_2.$$

$$\Rightarrow \prod_{i=0}^{N} n_i \mid x_1 - x_2$$

$$\Rightarrow \underline{x_1 \equiv x_2 \pmod{N}}.$$

□

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

$S = \{ a \in \mathbb{Z} \mid (a,n) = 1 \}$ & for each $b \in \mathbb{Z}$ $\exists!$ a in this set s.t. $b \equiv a \pmod{n}$

Reduced residue system.

$\mathbb{Z}_6^* = \{1, 5\}$, $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$.

CRS

Complete residue system

$\mathbb{Z}_n$

$|\mathbb{Z}_n^*| = \varphi(n)$

CRS mod 6 $\{0, 1, 2, 3, 4, 5\}$

$\{6, -5, 8, 21, -20, 5\}$

$\forall n \in \mathbb{Z} \longrightarrow \exists!\ a \in$ s.t. $a \equiv n \pmod 6$

RRS mod 6 $= \{1, 5\}$

$= \{-5, 5\}$.

Arithmetic Functions.

Tom Apostol
Analytic No. th.

$f : \mathbb{N} \to \mathbb{R}$ or $f : \mathbb{N} \to \mathbb{C}$

· $f : \mathbb{N} \to \mathbb{N}$ ✓

Examples: ① $Id : \mathbb{N} \to \mathbb{N}$.

② Euler's phi $\varphi(n)$ = no of integ $< n$ & coprime to n.

③ $\pi(n) = \sum_{\substack{p < n \\ p : \text{prime}}} 1$

$\varphi(n) = \sum_{\substack{m=1 \\ (m,n)=1}}^{n} 1$

③ No of divisors of n.

$$\tau(n) = \sum_{d|n} 1$$

$\tau(6) = 4$

1, 2, 3, 6

$\tau(12) = 6$.

1, 2, 3, 4, 6, 12

④ Sum of divisors of n.

$$\sigma(n) = \sum_{d|n} d$$

$\sigma(6) = \_\_\_$

$\sigma(12) = \_\_\_$

Multiplicative function (Additive)

f is said to be multiplicative if

$$f(mn) = f(m) \cdot f(n) \quad \forall \ (m,n) = 1$$

[additive $\longrightarrow$ $f(mn) = f(m) + f(n) \quad \forall (m,n)=1$

[Totally multi. if $f(mn) = f(m) \cdot f(n) \quad \forall\ m,n \in \mathbb{N}$.

Totally additive $\forall\ m,n \in \mathbb{N}$.

Thm: φ is multiplicative.

Write $n = \prod_{i=1}^{\delta} p_i^{\alpha_i}$

then $\varphi(n) = \prod_{i=1}^{\delta} \varphi(p_i^{\alpha_i})$

$$= \prod \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1} \right)$$

$$= n \cdot \prod \left(1 - \frac{1}{p_i} \right)$$

Defn: **Convolution** of arithmetic fns.

$$(f * g)(n) = \sum_{d \mid n} f(d)\, g\left(\frac{n}{d}\right)$$

↖ summation over all positive divisors of n.

Cf. f, g

$$(f * g)(x) = \int_{-\infty}^{\infty} f(t)\, g(x-t)\, dt$$

$$\delta(n) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{otherwise} \end{cases}$$

Compute

Ex

$$(f * \delta)(n) = ?$$

$$(\delta * f)(n) = ?$$

Remark: δ is multiplicative

$$U(n) = 1 \quad \forall\, n \in \mathbb{N}.$$

$$(f * U)(n) = \sum_{d \mid n} f(d)\, U\left(\frac{n}{d}\right)$$

$$= \sum_{d \mid n} f(d)$$

$$f \rightsquigarrow \sum_{d \mid n} f(d) = (Df)(n)$$

Remarks: U is multiplicative.

Ex: $U * U = ?$

Thm: f, g : mult. Then $f * g$ is multiplicative.

Further $f * g = g * f$. ⟵

$(f * g) * h = f * (g * h)$. ⟵

Thm: $\sum_{d \mid n} \varphi(d) = ?$ (Ex.)

try few examples & then try to prove!

Def: Möbius function

$$\mu(n) = \begin{cases} (-1)^r & \text{if } n = p_1 \cdots p_r \text{ and } p_i\text{'s are distinct} \\ 0 & \text{if } p^2 \mid n \text{ for some prime } p. \end{cases}$$

Thm:

$$\mu * U = \delta$$

For any mult. f, $f = \mu * Df$.

Thm: $$\varphi(n) = \sum_{d \mid n} \mu(d)\, \varphi\left(\frac{n}{d}\right)$$

In gen $$f(n) = \sum_{d \mid n} \mu(d)\, f\left(\frac{n}{d}\right)$$

Möbius inversion formula.

Ex $\sum_{d \mid n} \mu(d) = ?$ //