DATE __/__/__
PAGE NO _____

# Assignment - 02

 43304

* **Aim →** Develop a program in C++ or Java based on CRT

* **Objective →** To study :- 1. Chinese Remainder Theorem
2. Set of residues
3. Modulo multiplicative number
4. Relatively prime numbers

* **Theory →**

A. **Relatively Prime Numbers :**

Two integers are termed relative prime if GCD is 1.
Two distinct prime numbers are always relatively prime
Relative primity is not Transitive

Example -

$18 = 2 \times 3 \times 3$

$35 = 5 \times 7$

∴ 18 and 35 are relative primes

B. **Set of Residues :**

It is a set of non-negative integers less than n.

$Z_n = \{0, 1, 2 \dots (n-1)\}$

C. **Chinese Remainder Theorem :**

Let $M_1, M_2, \dots M_K$ be pair wise relatively prime +ve integers, i.e, $\gcd(M_i, M_j) = 1$

* **Steps in CRT -**

1. Find $M = M_1 \times M_2 \times \dots M_K$. This is common modulus
2. Find $M_1 = M/M_1$, $M_2 = M/M_2$, $\dots$ $M_K = M/M_K$
3. Find the multiplicative inverse of $M_1, M_2, \dots M_K$ using the corresponding modulis ($M_1, M_2 \dots M_K$)
4. The solution of the simultaneous eq$^n$ is

$$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \dots a_K \times M_K \times M_K^{-1}) \text{ Mod } M$$

- Example -

$x \equiv 2 \mod 3$

$x \equiv 3 \mod 5$

$x \equiv 2 \mod 7$

1. $M = \frac{3 \times 5 \times 7}{\cancel{2 \times 3 \times 5}} = 105$
2. $M_1 = 105/3 = 35$ , $M_2 = 105/5 = 21$ , $M_3 = 105/7 = 15$
3. The inverses are , $M_1^{-1} = 2$ , $M_2^{-1} = 1$ , $M_3^{-1} = 1$
4. $x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \mod 105$

$\rightarrow x = 23 \mod 105$

5. $\boxed{x = 23}$

* Conclusion → Thus in this assignment , we learnt about CRT and implemented it in C++.