DATE

(II) Chienese Remainder Theorem :-

Chienese Remainder Theorem States that there always exists an 'x' that satisfies the given congruence.

Chienese Remainder Theorem :-

$x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
$x = a_3 \pmod{m_3}$

if we want to find the value of x then the condition is → GCD of m_1, m_2, m_3 they all should be co-prime to each other.

$$\gcd(m_1, m_2) = \gcd(m_2, m_3) = \gcd(m_3, m_1) = 1$$

∴ i.e., all coprime.

$$x = (M_1 X_1 a_1 + M_2 X_2 a_2 + M_3 X_3 a_3 + \cdots M_n X_n a_n) \bmod M$$

$$M = m_1 * m_2 * m_3 \ldots m_n$$

$$M_i = \frac{M}{m_i}$$

eg., $M_1 = \frac{M}{m_1} = \frac{\cancel{m_1} m_2 m_3}{\cancel{m_1}} = m_2 m_3$

$$\boxed{M_1 = m_2 m_3}$$

sim $\boxed{M_2 = m_1 m_3}$

$$\boxed{M_3 = m_1 m_2}$$

To calculate X_i

$$M_i X_i \equiv 1 \mod m_i$$

e.g., $M_1 X_1 \equiv 1 \mod m_1$

General form :-

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

1) Find out common modulus M,

$$M = m_1 \times m_2 \times m_3 \times \ldots m_n$$

2) Find : $M_1 = \dfrac{M}{m_1}$ $\quad M_2 = \dfrac{M}{m_2}$

3) Find out inverse $M_1^{-1}, M_2^{-1}, \ldots M_n^{-1}$

With respect to $m_1, m_2, m_3 \ldots m_n$

4) $x = \Big((a_1 * M_1 * M_1^{-1}) +$
$(a_2 * M_2 * M_2^{-1}) + \ldots$
$(a_n * M_n * M_n^{-1}) \Big) \bmod M$

$x \equiv 4 \pmod{11}$ $\quad m_1 = 11 \quad a_1 = 4$

$x \equiv 5 \pmod{7}$ $\quad m_2 = 7 \quad a_2 = 5$

$x \equiv 6 \pmod{13}$ $\quad m_3 = 13 \quad a_3 = 6$

common Modulus $M =$

① $\longrightarrow$ $M = m_1 * m_2 * m_3$

$= 11 * 7 * 13$

$\boxed{M = 1001}$

② $\longrightarrow$ $M_1 = \frac{M}{m_1}$ $\quad M_2 = \frac{M}{m_2}$ $\quad M_3 = \frac{M}{m_3}$

$= \frac{1001}{11}$ $\quad = \frac{1001}{7}$ $\quad = \frac{1001}{13}$

$= 91$ $\quad = 143$ $\quad = 77$

$M_1 = 91$ $\quad \boxed{M_2 = 143}$ $\quad \boxed{M_3 = 77}$

③ $\longrightarrow$

$M^{-1} = 91^{-1} \bmod m_1$

Ecludian theorem

$= 91^{-1} \pmod{11}$

$(x * 91) \bmod 11 = 1$

4

17
23 2
5 1
5 4 1
5 9 1
5

PAGE NO.:
DATE

$M_1^{-1} = 91^{-1} \pmod{11} \Rightarrow 4$

$M_2^{-1} = 143^{-1} \pmod{7} \Rightarrow 5$

$M_3^{-1} = 77^{-1} \pmod{13} \Rightarrow 12$

(4) $\longrightarrow$ $x = \left((4 * 91 * 4) + (5 * 143 * 5) + (6 * 77 * 12) \right) \bmod 1001$

$\boxed{x = 565}$

we have got $\boxed{565}$

565 mod 11 $\Rightarrow$ 4
565 mod 7 $\Rightarrow$ 5
565 mod 13 $\Rightarrow$ 6.

143 mod 7

$91^{-1} \times 91 = 1 \bmod 4$

$1 \times 91 = 91 \bmod 4$

4×91