PAGE NO.:
DATE:

Chinese Remainder Theorem

CRT is used to solve a set of congruent eq^{n}s with one variable but different modulo, which are relatively prime

you will be given

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$\vdots \quad \vdots$

$x \equiv a_k \pmod{m_k}$

→ Above eq^{n}s have a unique soln if modulo are relatively prime

you have to go step by step procedure and find x

step1: $m = m_1 \times m_2 \times \cdots \times m_k$

step2: $m_1 = m / m_1$

$m_2 = m / m_2$

$\vdots$

$m_k = m / m_k$

step3: Find inverse

$m_1^{-1} \bmod m_1$

$m_2^{-1} \bmod m_2$

$\vdots$

$m_k^{-1} \bmod m_k$

step4: $x = (a_1 * m_1 * m_1^{-1} + a_2 * m_2 * m_2^{-1} + \cdots a_k * m_k * m_k^{-1}) \bmod m$

Example

$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$

$23 \bmod 3 = 2$
$23 \bmod 5 = 3$
$23 \bmod 7 = 2$

$a_1 = 2, \quad a_2 = 3, \quad a_3 = 2$

$m_1 = 3, \quad m_2 = 5, \quad m_3 = 7$

$m = m_1 \times m_2 \times m_3 = 3 \times 5 \times 7 = 105$

$m_1 = m/m_1 = 105/3 = 35$

$m_2 = m/m_2 = 105/5 = 21$

$m_3 = m/m_3 = 105/7 = 15$

$\star \quad m_1^{-1} \bmod m_1$

$\Rightarrow 35^{-1} \bmod 3 = 2 \Rightarrow 2^{-1} \bmod 3 = 2$

q	s_1	s_2	s	t_1	t_2	t
0	3	35	3	0	1	0
11	35	3	2	1	0	1
1	3	2	1	0	1	-1
2	2	1	0	1	-1	3
	1	0		-1	3	

$-1 + 3 = 2$

23

Verify $35 \times 2 = 70$

$3 \overline{)70}$ — 6, 10, 9, (1)

✱ $m_2^{-1} \bmod m_2$ $\quad 5 \overline{)21}$ — 20, 1 (4)

$\Rightarrow 21^{-1} \bmod 5 = 1 \Rightarrow 1^{-1} \bmod 5 = 1$

q	s_1	s_2	s	t_1	t_2	t
0	5	21	5	0	1	0
4	21	5	1	1	0	1
5	5	1	0	0	1	-5
	1	0		1	-5	

Verify $1 \times 21 = 21$

$5 \overline{)21}$ — 20, 1 (4)

✱ $m_3^{-1} \bmod m_3$

$\Rightarrow 15^{-1} \bmod 7 = 1 \Rightarrow 1^{-1} \bmod 7 = 1$

q	s_1	s_2	s	t_1	t_2	t
0	7	15	7	0	1	0
2	15	7	1	1	0	1
7	7	1	0	0	1	-7
	1	0		1	-7	

Verify $15 \times 1 = 15$

$7 \overline{)15}$ — 14, 1 (2)

DATE:

$$x = (a_1 * m_1 * m_1^{-1} + a_2 * m_2 * m_2^{-1} + a_3 * m_3 * m_3^{-1}) \bmod m$$

$$= (2 * 35 * 2 + 3 * 21 * 1 + 2 * 15 * 1) \bmod 105$$

$$= (140 + 63 + 30) \bmod 105$$

$$= 233 \bmod 105$$

$$\boxed{x = 23}$$

$$105 \overline{)\,233\,(\,2} \quad 210 \quad 23$$