Chinese Remainder Theorem :

According to the chinese Remainder Theorem, if one is aware of the remainders of the Euclidean division of an integer n by several integers, they can then be used to determine the unique remainder of n's divison by the product of these other integers, provided than the n and the divisors are pairwise coprime

Theorem :

If $m_1, m_2, \ldots, m_K$ are pairwise relatively prime positive integers, and if $a_1, a_2, \ldots, a_K$ are any integers, then the ~~solution~~ simultaneous congruences

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2} \ \ldots \ x \equiv a_K \pmod{m_K}$$

have a solution, and the solution is unique modulo m, where $m = m_1 m_2 \ldots m_K$

Chinese Remainder Theorem Proof:

Step 1: Compute the value $m = m_1 * m_2 * \ldots * m_K$

Step 2: For every $i = 1, 2, 3, \ldots, K$ compute

$$z_i = \frac{m}{m_i}$$

Step 3: For every $i = 1, 2, 3, \ldots, K$ compute

$$y_i = z_i^{-1} \pmod{m_i}$$

utilising Euclid's extended algorithm

Step 4: The integer $x = \sum_{i=1}^{K} a_i y_i z_i$ is a solution to the system of congruences and $x \bmod m$ is the unique solution modulo m

Now, lets check why x is the solution for every $i=1,2,\ldots,K$

$$x \equiv (a_1 y_1 z_1 + a_2 y_2 z_2 + \cdots + a_K y_K z_K) \pmod{m_i}$$
$$\equiv (a_i y_i z_i) \pmod{m_i}$$
$$\equiv a_i \pmod{m_i}$$

where the third line comes because of $y_i z_i \equiv 1 \pmod{m_i}$

Now assume that there are two solutions u and v to the given systems of congruences.

Then,

$$m_1 \mid (u-v),\ m_2 \mid (u-v), \ldots, m_K \mid (u-v)$$

Since $m_1, m_2, \ldots m_K$ are relatively co-primes.

So,

$$u \equiv v \bmod (m_1, m_2, \ldots, m_K)$$

Hence proved.

Example 1:

Solve the simultaneous congruences,

$$x \equiv 3 \pmod{5}$$
$$x \equiv 5 \pmod{7}$$

→

Since 5 and 7 are co-prime, the chinese remainder theorem tells us that there is an unique solution modulo m.

$$\therefore m = m_1 * m_2$$
$$= 5 * 7$$
$$= 35$$

We have from the simultaneous congruences,

$$K = 2 \quad m_1 = 5 \quad m_2 = 7$$
$$a_1 = 3 \quad a_2 = 5$$

Now,

We compute,

$$z_1 = \frac{m}{m_1} = \frac{m_1 * m_2}{m_1} = \frac{35}{5} = 7$$

$$z_2 = \frac{m}{m_2} = \frac{m_1 * m_2}{m_2} = \frac{35}{7} = 5$$

By Euclid's extended algorithm,

$$y_1 = z_1^{-1} \pmod{m_1} = 7^{-1} \pmod{5} = 3$$
$$y_2 = z_2^{-1} \pmod{m_2} = 5^{-1} \pmod{7} = 3$$

$$w_1 = y_1 z_1 \pmod{m} = 3 * 7 \pmod{35} = 21 \pmod{35}$$
$$w_2 = y_2 z_2 \pmod{m} = 3 * 5 \pmod{35} = 15 \pmod{35}$$

The Solution, which is unique modulo 35 is,

$$x \equiv a_1 w_1 + a_2 w_2 \pmod{35}$$

$$\equiv 3 * 21 + 5 * 15 \pmod{35}$$

$$\equiv 63 + 75 \pmod{35}$$

$$\equiv 138 \pmod{35}$$

$$\equiv 33 \pmod{35}$$

<u>Example 2</u>:

Solve the Simultaneous Congruences

$x \equiv 6 \pmod{11}$, $x \equiv 13 \pmod{16}$ $x \equiv 9 \pmod{21}$ $x \equiv 19 \pmod{25}$

→

Since 11, 16, 21 and 25 are pairwise relatively prime, the chinese remainder theorem tells us that there is a unique Solution modulo m where, $m = 11 * 16 * 21 * 25 = 92400$

We have from the Simultaneous Congruences.

$K = 4$ $m_1 = 11$ $m_2 = 16$ $m_3 = 21$ $m_4 = 25$

$a_1 = 6$ $a_2 = 13$ $a_3 = 9$ $a_4 = 19$

Now we compute,

$$z_1 = \frac{m}{m_1} = \frac{92400}{11} = 8400$$

$$z_2 = \frac{m}{m_2} = \frac{92400}{16} = 5775$$

$$z_3 = \frac{m}{m_3} = \frac{92400}{21} = 4400$$

$$z_4 = \frac{m}{m_4} = \frac{92400}{19} = 3696$$

By Euclidian's extended algorithm

$y_1 = z_1^{-1} \pmod{m_1} = 8400^{-1} \pmod{11} = 7^{-1} \pmod{11} = 8$

$y_2 = z_2^{-1} \pmod{m_2} = 5775 \pmod{16} = 15^{-1} \pmod{16} = 15$

$y_3 = z_3^{-1} \pmod{m_3} = 4400 \pmod{21} = 11^{-1} \pmod{21} = 2$

$y_4 = z_4^{-1} \pmod{m_4} = 3696 \pmod{25} = 21^{-1} \pmod{25} = 6$

Now,

$w_1 = y_1 z_1 \pmod{m} \equiv 8 * 8400 \pmod{92400} \equiv 67200 \pmod{92400}$

$w_2 = y_2 z_2 \pmod{m} \equiv 15 * 5775 \pmod{92400} \equiv 86625 \pmod{92400}$

$w_3 = y_3 z_3 \pmod{m} \equiv 2 * 4400 \pmod{92400} \equiv 8800 \pmod{92400}$

$w_4 = y_4 z_4 \pmod{m} \equiv 6 * 3696 \pmod{92400} \equiv 22176 \pmod{92400}$

The solution which is unique modulo 92400 is,

$x \equiv a_1 w_1 + a_2 w_2 + a_3 w_3 + a_4 w_4 \pmod{92400}$

$\equiv 6 * 67200 + 13 * 86625 + 9 * 8800 + 19 * 22176 \pmod{92400}$

$\equiv 2029869 \pmod{92400}$

$\equiv 89469 \pmod{92400}$