SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College of Engineering

Somaiya TRUST

CHINESE REMAINDER THEOREM

What is chinese remainder theorem?

The Chinese Remainder Theorem is a mathematical theorem that describes a method for solving a system of linear congruences. It is named after the ancient Chinese mathematicians who first discovered and used the theorem.

Statement of theorem:

Let N1, N2, ..., Nk be positive integers that are pairwise relatively prime, and let a1, a2, ..., ak be any integers. Then the system of linear congruences:

$$x \equiv a1 \pmod{N1}$$
$$x \equiv a2 \pmod{N2} \ldots$$
$$x \equiv ak \pmod{Nk}$$

*has a unique solution modulo N = N1 * N2 * ... * Nk.*

Example:

Suppose we have the following system of congruences:

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{4}$$
$$x \equiv 1 \pmod{5}$$

We want to find a solution for x that satisfies all three congruences simultaneously.

- First, we check if the moduli (3, 4, and 5) are pairwise coprime, meaning that their greatest common divisors are all 1. It is true in this case.
- Next, we compute the product of all the moduli:
  $n = 3 * 4 * 5 = 60$
  This value will be used as the modulus in the final solution.
- Now, we can use the Chinese Remainder Theorem algorithm to compute the solution. The algorithm involves the following steps:

1. Compute the values of the "partial remainders"(n_k) for each congruence.

For the first congruence ($x \equiv 2 \pmod 3$): $n_1 = 60 / 3 = 20$
For the second congruence ($x \equiv 3 \pmod 4$): $n_2 = 60 / 4 = 15$
For the third congruence ($x \equiv 1 \pmod 5$): $n_3 = 60 / 5 = 12$

2. Compute the multiplicative inverse of each partial remainder modulo its corresponding modulus.

For $n_1 = 20 \pmod 3$: $20^{(-1)} \equiv 2 \pmod 3$
For $n_2 = 15 \pmod 4$: $15^{(-1)} \equiv 3 \pmod 4$
For $n_3 = 12 \pmod 5$: $12^{(-1)} \equiv 3 \pmod 5$

3. Compute the solution x by taking the sum of the products of the original congruences, the corresponding partial remainders, and the corresponding multiplicative inverses modulo the modulus.

$$x \equiv (2 * 20 * 2 + 3 * 15 * 3 + 1 * 12 * 3) \pmod{60}$$
$$x \equiv 80 + 135 + 36 \pmod{60}$$
$$x \equiv 251 \pmod{60}$$

So, the solution $x \equiv 251 \pmod{60}$ satisfies all three congruences simultaneously.

Properties and applications:

- **Existence and Uniqueness of Solutions:** The CRT guarantees that a solution exists and is unique, provided that the moduli are pairwise coprime.
- **Efficient Computation:** The CRT provides an efficient algorithm for computing the solution.
- **Applications in Cryptography:** The CRT has applications in cryptography, since it is used in some algorithms for encrypting and decrypting messages, such as the RSA algorithm.
- **Error Detection and Correction:** The CRT can be used for error detection and correction in computer systems, such as in error-correcting codes and digital communication systems.

Batch - A2
Arya Nair - 16010421063
Bhavya Nanda - 16010421064
Tanvi Natu - 16010421065