Assignment No. 2

Aim :

Develop an program in C++ or Java based on number theory such as Chinese Remainder or Extended Euclidian algorithm.

Objective :

To study,

- Chinese Remainder theorem
- Set of Residues
- Relatively prime numbers
- What is modulo multiplicative inverse

Theorey :

- Relative Prime Numbers :

Two integers are termed relative prime if the only common factor between them is 1.
i.e. GCD(m,n) = 1.

Any integer can be broken down into certain multiples of prime number this is called prime factorization.

Two distinct primes and are always relatively prime. Relative primality is not transitive.
Example.

18 = 2 x 3 x 3

35 = 7 x 5

So, 18 & 35 are relative prime.

- Set of Residues :

It is set of nonnegative integers less than n.

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

- Chinese Remainder Theorem :

Let $m_1, m_2, \dots m_k$ be pair wise relatively prime positive integers. That is, $\gcd(m_i, m_j) = 1$.

- Steps in CRT

1. Find $M = m_1 \times m_2 \times \dots m_k$. This is common modulus.

2. Find $M_1 = M/m_1, \dots M_k = M/m_k$.

3. Find Multiplicative inverse of $M_1, M_2, \dots M_k$.

4. Solution to simultaneous equation is,

$$x = (a_1 \times M_1 \times M_1^{-1} + \dots + a_k \times M_k \times M_k^{-1}) \bmod M$$

- Example :

Find x of following equations,

$x \equiv 2 \bmod 3$

$x \equiv 3 \bmod 5$

$x \equiv 2 \bmod 7$

Answer :

1. $M = 3 \times 5 \times 7 = 105$
2. $M_1 = 105/3 = 35$
   $M_2 = 105/5 = 21$
   $M_3 = 105/7 = 15$
3. Inverse,
   $M_1^{-1} = 2$
   $M_2^{-1} = 1$
   $M_3^{-1} = 1$
4. $x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$
   $= 23 \bmod 105$
5. $x = 23$.

Conclusion :

Hence, we have successfully implemented CRT using C++ and also learned about relative prime numbers, residues & multiplicative inverse of numbers.