ASSIGNMENT - 2

AIM: To develop a CN or Java program to Chinese Remainder Theorem & Extended Euclidean theorem.

THEORY:

- RELATIVE PRIME NUMBERS:

- 2 integers are termed relatively prime if the only common factor b/w them is 1.

- Any integer can be broken down into certain multiples of prime nos. This is called prime factorization.

- When 2 integers are prime factorized the only common no. is 1, then 2 integers are relative primes.

- 2 distinct prime nos. are always relatively prime

- Relative primality is not transitive.

ex: $18 = 2 \times 3 \times 3$

$35 = 7 \times 5$

$\therefore$ 18 & 35 are relative primes.

- Set of residues:

It is a set of non-negative integers less than

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

- CHINESE REMAINDER THEOREM:

Let $m_1, m_2, m_3, \ldots, m_n$ be pairwise prime positive integers, i.e., $\gcd(m_i, m_j) = 1$

Steps for CRT:

1. Find $m = m_1 * m_2 * \ldots * m_n$
   This is common modulus
2. Find $M_1 = m / m_1$, $M_2 = m / m_2$
3. Find multiplicative inverse of $M_1, M_2, \ldots, M_n$

ex: $x_1 = 2 \mod 3$
$x_2 = 3 \mod 5$
$x_3 = 2 \mod 7$

$M = x_1 * x_2 * x_3 = 3 \times 5 \times 7 = 105$
$M_1 = 105 / 3 = 35$
$M_2 = 105 / 5 = 21$
$M_3 = 105 / 7 = 15$

$M_1^{-1} = 2$ $M_2^{-1} = 1$ $M_3^{-1} = 1$

$u = [(2 \times 35 \times 2) + (3 \times 21 \times 1) + (2 \times 15 \times 1)] \bmod 105$

$u = 23 \mod 105$
$= 23$

Input: Values of a_i & m_i

Output: Unique values of x

CONCLUSION :

Hence the CAT has been learnt & imple