Date / /
Page No.

ASSIGNMENT ▼

Aim: Develop a program C++ or Java based on number theory such as Chinese Remainder Theorem.

Theory:

Relatively Prime Numbers:

Two integers are termed as relatively prime if the only common factor between them is 1.
i.e Greatest Common Divisor $(m, n) = 1$

Two distinct primes and are always relatively prime.

Example:

$18 = 2 \times 3 \times 3$

$35 = 7 \times 5$

so 18 and 35 are relatively prime.

Set of residues

Zr is a set of non negattive integers less than n

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

Chineser Remaindr theorom (CRT)

Let $m1, m2, m3, \dots mK$ be pair wise relatively prime postive integers. that is,

$\gcd(m_i, m_j) = 1$ for $1 \leq i < j \leq k$

Steps in CRT:

1. Find $M = m1 \times m2 \times \dots \times mk$. This is the common modulves
2. Find $M1 = M/m1$, $M2 = M/m2 \dots$ $Mk = M/mk$
3. Find the multiplicative inverse of $M1, M2, M3 \dots Mk$ using corresponding moduli

   $(m1, m2, \dots mk)$. Call the inverses $M1^{-1}, M2^{-1}, \dots Mk^{-1}$

4. The solution to the simultaneous equations is

$$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \dots a_k \times M_k \times M_k^{-1}) \bmod M$$

Conclusion: Chinese remaindr theoron for 3 numbers was implemented successfully in C++ and Java.