

Assignment No. 2

Aim:

Develop on 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.

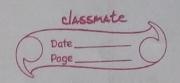
Two distinct primes and are always relatively prime. Relative primality is not transitive.

Example.

 $18 = 2 \times 3 \times 3$

 $35 = 7 \times 5$

So, 18 & 35 are relative prime



	•	Set	OF	Residues	
--	---	-----	----	----------	--

It is set of nonnegative integers less than n. $Zn = \{0, 1, 2, \dots (n-1)\}$

· Chinese Remainder Theorem:

Let m1, m2, ... mk be pair wise relatively prime positive integers. That is, gcd (mi, mj) = 1.

· Steps in CRT

- 1. Find M = m1 x m2 x ... mk. This is common modulus.
- 2. Find MI = M/MI, ... Mk = M/mk
- 3. Find Multiplicative inverse of M1, M2, MK.
- 4. Solution to simultaneous equation is,

Z = (a1x M1 x Mi' + + ak x Mk x Mk') mod M

· Example:

Find a of following equations.

 $x \equiv 2 \mod 3$

 $X \equiv 3 \mod 5$

 $x \equiv 2 \mod 7$

Answet:

- 1. M = 3x5x7 = 105
- $2. M_1 = 105/3 = 35$

 $M_2 = 105/5 = 21$

 $M_3 = 105/7 = 15$

3. Inverse,

Mi = 2 d sm (m 10 +1)

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

- 4. $\chi = (2x35x2 + 3x21x1 + 2x15x1) \mod 105$ = 23 mod 105
- 5. X = 23. X M X M = M NAT

Conclusion:

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