Name: Anish Kulkarni
Roll Number: 43227

Page No.
Date: / /

Assignment 2

Aim: Develop a program in C++ or Java based on number theory such as Chinese Remainder Theorom or Extended Euclidean Algorithm.

Objective: To study

1. Chinese Remainder Theorom
2. Set of residues
3. Relatively prime numbers.
4. Modular multiplicative inverse.

Theory:

Relatively prime numbers:

Two integers are relatively prime if common factor is 1.

eg - 18 and 35

Set of residues:

Set of non negative integers less than n.

$Z_n = \{0, 1, 2, 3, \cdots, (n-1)\}$

Chinese Remainder Theorom:

It states that there always exists a x that satisfies given congrunc congruenc

Steps:

1. Find $N = m_1 \cdot m_2 \cdots m_k$ (Common modulus).
2. Find $N_i = \frac{N}{m_i} \quad \forall k$.
3. Find multiplicative inverse of $N_1, N_2, \cdots N_k$ using moduli $m_1, m_2, \cdots, m_k$
4. The solution to simultaneous equations is

$x = (a_1 N_1 N_1^{-1} + a_2 N_2 N_2^{-1} + \cdots + a_k N_k N_k^{-1}) \bmod N$

Page No.
Date: / /

Example:

$x = 2 \bmod 3$

$x = 4 \bmod 5$

$x = 5 \bmod 7$.

Find x.

$N = 3 \times 5 \times 7 = 105$

b_i	$N_i = N/m_i$
2	35
4	21
5	15

$N_1 = 105/3$

$N_2 = 105/5$

$N_3 = 105/7$

Calculating multiplicative inverses

$35x_1 = 1 \bmod 3$

$35x_1 \pmod 3 = 1$

$2x_1 \pmod 3 = 1$

$\therefore x_1 = 2$

$21x_2 \pmod 5 = 1$

$x_2 \pmod 5 = 1$

$x_2 = 6$.

$15x_3 \pmod 7 = 1$

$x_3 \pmod 7 = 1$

$x_3 = 8$

b_i	N_i	x_i	$b_i N_i x_i$
2	35	2	140
4	21	6	504
5	15	8	600
			1244

$1244 \% N = 1244 \% 105 = 89 \quad \therefore x = 89$

Conclusion:

Successfully studied, understood and implemented Chinese Remainder Theorem.