PAGE NO.
DATE / /

Assignment - 02

Roll NO :- 43236

Aim :- Develope a program in C++ or Java based on number theory such as Chinese remainder

objective :- To study
1) Chinese remainder theorem
2) set of residues
3) Relatively prime numbers

Theory :-

Relative Prime Numbers :-

Two integers are relatively prime if the only common factor between these is 1 i.e. gcd = 1.

eg

18 & 35 →

Set of residues :- Zn is a set of non-negative numbers less than n.

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

Chinese remainder theorem :-

CRT states that there always exists x that satisfies the given congruences

x = rem[0] (mod num[0])
x = rem[1] (mod num[1])

where num[0], num[1] must be co-prime to each.

steps in CRT:-

1) Find $N = m_1 \times m_2 \times m_3 \cdots \times m_n$ common modulus
2) find $N_i = \frac{N}{(m_i)}$ for all i's
3) find $a(i) = \frac{N_i}{m_i}$ for all (k)
4) The solution to the simultaneous congruence equation is $n = (a_1 \times N_1 \times N_1^{-1} + a_2 \times N_2 \times N_2^{-1} + a_k N_k \times N_k^{-1}) \pmod{N}$

Example :-

given modular equations are
$x = 2 \pmod 3$ $x = 3 \pmod 5$
$x = 4 \pmod 7$

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

b_i	N_i	
2	35	$N_1 = 105/3$
4	21	$N_2 = 105/5$
5	15	$N_3 = 105/7$

Calculating multiplicative inverse :-

$35 x_1 = 1 \bmod 3$, $21 (x_2 \pmod 5) = 1$

or

$35 (x_1) \pmod 3 = 1$ $\qquad$ $x_2 \pmod 5 \rightarrow$

$2x_1 \pmod 3 = 1$ $\qquad$ $x_2 = 6$

$\therefore x_1 = 2$

$15 x_3 \pmod 7 = 1$

$x_3 \pmod 7 = 1$

$x_3 = 8$

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

$1244 \bmod N$

$= (1244 \bmod 105) = 89$

$x = 89$

Conclusion :-

Thus we studied the chinese remainder theorem.