Rollno 43320

Date ___/___/_____

Saathi

Assignment 2

Aim: develop 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
4. Modular multiplications inverse

Theory: Relative prime numbers

Two integers are relatively prime if the common factor between them is 1.

i.e. g.c.d. = 1

examples : 18 and 35

set of residues

25 is a set of non-negative integers less than n

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

Roll no : 3320

Date __/__/____

Saathi

* Chinese remainder theorem (CRT)

CRT states that there always exists a x that satisfies the given congruence

$x = rem[0] \pmod{num[0]}$
$x = rem[1] \pmod{num[1]}$
:

where num[0], num[1] must be coprime to each other.

Steps in CRT

1. Find $N = m_1 \times m_2 \times \ldots m_k$ common modules
2. Find $N_i = \frac{N}{m_i}$ for all k
3. find the multiplicative inverse of N_1, N_2
4. The solution to the simultaneous equation is

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

Example

Given modular equations are

$x = 2 \bmod 3$ $\quad x = 5 \bmod 7$
$x = 4 \bmod 5$

Page No.

Roll no 43320

Date __/__/____

Saathi

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

bi	Ni
2	35
4	21
5	15

$N_1 = 105/3$
$N_2 = 105/5$
$N_3 = 105/7$

Calculating multiplicative inverse

$35 x_1 = 1 \bmod 3$

OR

$35 x_1 \pmod 3 = 1$
$2 x_1 \pmod 3 = 1$
$\therefore x_1 = 2$

$21 x_2 \pmod 5 = 1$

$x_2 \pmod 5 = 1$
$x_2 = 6$

$15 x_3 \pmod 7 = 1$
$x_3 \pmod 7 = 1$
$x_3 = 8$

bi	Ni	xi
2	35	2
4	21	6
5	15	8

bi Ni xi
140
504
600
1244

$1244 \% N = (1244 \% 105) = 89$

$\boxed{x = 89}$

Page No.

Date ___/___/___

Conclusion

Thus, we studied the chinese remainder theorem.