43308

Assignment 2

Aim: Develop program in C++ or java on Chinese Remainder Theorem.

Theory

I Relative prime number

Two number called as relative only if they have GCD of 1.

Eg gcd (18, 35) = 1

II Chinese Remainder Theorem (CRT) Algorithm

a) Given

$x \equiv a_1 \bmod m_1$

$x \equiv a_2 \bmod m_2$

$\vdots$

$x \equiv a_k \bmod m_k$

b) Find $m = m_1 \times m_2 \ldots m_k$ this is common modulus

43308

c) Find $M_1 = M / m_1$
$M_2 = M / m_2$
$M_R = M / m_R$

d) Find the multiplicative universe of $m_1 M_2 M_K$ using a and corresponding module

$(m_1, m_2, \ldots m_R)$ call the ~~inter~~ inverse M^{-1}, M^{-2}, M_R

e) The solution to the Sumit kong equation is

$x = (a_1 \times M_1 \times M^{-1}.) + (a_2 \times M_2 \times M_2$
$+ (a_R \times M_R * M_R^{-1}))$ need M^2

Example

$x \equiv 2 \bmod 3$
$x \equiv 3 \bmod 4$
$x \equiv 1 \bmod 5$

$M = M_1 \times M_2 \times M_3$
$= 3 \times 4 \times 5$
$= 60$

43308

$m_1 = \frac{60}{3} = 20$

$m_2 = \frac{60}{4} = 15$

$m_3 = \frac{60}{5} = 12$

Multiplicative inverse

$20 x_1 = 1 \pmod 3$

$2x_1 = 1 \bmod 3$

$x_1 = 2$

$15 x_2 \pmod 4$

$3x_2 \pmod 4$

$x_2 = 3$

$12 x_3 \equiv (\bmod 5) 1$

$2 x_3 \pmod 5 = 1$

$x = (20 \times 2 * 2 + 15 \times 3 \times 3 + 12 \times 3 \times 1) \bmod 60$

$x = (80 + 135 + 36) \bmod 36$

$x = 1$

conclusion

we implemented the chinese remainder theorem to calculate value of x