THE CHINESE REMAINDER THEOREM

The Chinese Remainder Theorem says it is possible to reconstruct integers in certain range from their residues modulo a set of pair wise relatively prime moduli.

$x \equiv a_1 \bmod n_1$, $x \equiv a_2 \bmod n_2$, $x \equiv a_k \bmod n_k$

If $n_1, n_2, .., n_k$ are positive integers that are pairwise co-prime and $a_1, a_2, \ldots, a_k$ are any integers, then CRT is used to find the values of x that solves the following congruence simultaneously.

Value of $x = (a_1 m_1 y_1 + a_2 m_2 y_2 + \ldots + a_k m_k y_k) \bmod M$

Where $M = n_1 n_2 n_3 .. n_k$

$m_i = M / n_i$

$m_i y_i = 1 \bmod n_i$

Problem 1

$x \equiv 1 \bmod 5$

$x \equiv 2 \bmod 6$

$x \equiv 3 \bmod 7$

$a_1 = 1$

$a_2 = 2$

$a_3 = 3$

$n_1 = 5$

$n_2 = 6$

$n_3=7$

$M=n_1n_2n_3$

$M=5*6*7=210$

$m_i=M/n_i$

$m1=210/5=42$

$m2=210/6=35$

$m3=210/7=30$

$m_iy_i=1 \bmod n_i$

$42y_1=1 \bmod 5$

$y_1=3 \bmod 5$

$35y_2= 1 \bmod 6$

$y_2=5 \bmod 6$

$30y_3=1 \bmod 7$

$y_3=4 \bmod 7$

$x=(a_1m_1y_1+a_2m_2y_2+ a_3m_3y_3) \bmod M$

$=((1*42*3)+(2*35*5)+(3*30*4)) \bmod 210$

$=836 \bmod 210$

$=206$

Problem 2

A bag has contained number of pens if you take out 3 pens at a time 2 pens are left. If you take out 4 pens at a time 1 pen is left and if you take out 5 pens at a time 3 pens are left in the bag. What is the number of pens in the bag.

$x \equiv 2 \bmod 3$

$x \equiv 1 \bmod 4$

$x \equiv 3 \bmod 5$

$a_1=2$

$a_2=1$

$a_3=3$

$n_1=3$

$n_2=4$

$n_3=5$

$M=n_1n_2n_3$

$M=3*4*5=60$

$m_i=M/n_i$

$m1=60/3=20$

m2=60/4=15

m3=60/5=12

$m_i y_i = 1 \bmod n_i$

$20y_1 = 1 \bmod 3$

$y_1 = 2 \bmod 3$

$15y_2 = 1 \bmod 4$

$y_2 = 3 \bmod 4$

$12y_3 = 1 \bmod 5$

$y_3 = 3 \bmod 5$

$x = (a_1 m_1 y_1 + a_2 m_2 y_2 + a_3 m_3 y_3) \bmod M$

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

$= 233 \bmod 60$

$= 53$