Chinese Remainder Theorem

1. Firstly expressed the problem as a system of congruence,

$$p \equiv b_i (\text{mod } n_i)$$

where, n_i are relatively prime numbers: n_1, n_2, n_3 and so on

b_i is the respective remainder for modulo n_i such that b_1 for n_1, b_2 for n_2 and so on.

p is the value of solution.

2. Calculate the value of N

$$N = n_1 * n_2 * \cdots * n_i$$

3. Calculate the value of $N_i = N/n_i$ such that $N_1 = N/n_1$, $N_2 = N/n_2$ and so on.
4. Calculate the multiplicative inverse for $y_i \equiv (N_i)^{-1}$ (mod n_i)

where y_i is the multiplicative inverse of N_i mod n_i.

5. The value of p is calculated as:

$$p \equiv (b_1N_1y_1 + b_2N_2y_2 + \ldots + b_rN_ry_r) \text{ mod } N$$

where, p is the solution of the problem.

EXAMPLE 6.30 Find the smallest multiple of 10 which has remainder 1 when divided by 3, remainder 6 when divided by 7 and remainder 6 when divided by 11.

Solution The factors of 10 are: 2 and 5.

Problem is now expressed as a system of congruence as:

$$p \equiv b_i (\text{mod } n_i)$$

where n = 2, 3, 5, 7 and 11 which are relatively prime and b = 0, 1, 0, 6 and 6 are the remainders for respective value of n.

$$p = 0 \text{ mod } 2$$
$$p = 1 \text{ mod } 3$$
$$p = 0 \text{ mod } 5$$
$$p = 6 \text{ mod } 7$$
$$p = 6 \text{ mod } 11$$

To solve for p we first calculate the value of N as:

$$N = n_1 * n_2 * \ldots * n_r$$
$$N = 2 * 3 * 5 * 7 * 11 = 2310$$

and find the value of $N_i = N/n_i$ as:

$$N_2 = 2310/2 = 1155$$
$$N_3 = 2310/3 = 770$$
$$N_5 = 2310/5 = 462$$
$$N_7 = 2310/7 = 330$$
$$N_{11} = 2310/11 = 210$$