<u>Chinese Reminder Theorem</u>

Let $m_1, m_2, \ldots. m_n$ be pairwise relatively prime positive integers and a1, a2, …. a_n arbitrary integers. Then the system

$x = a_1 \bmod(m_1)$

$x = a_2 \bmod(m_2)$

$x = a_3 \bmod(m_3)$

.

.

$x = a_n \bmod(m_n)$

has a unique solution modulo $m = m_1 m_2 \ldots m_n$. (That is , there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

<u>Proof</u>: First let $M_k = \frac{m}{m_k}$ for k = 1 , 2 , . . . , n .

That is, M_k is the product of the moduli except for m_k. Because m_i and m_k have no common factors greater than 1 when $i \neq k$, it follows that $\gcd(m_k , M_k) = 1$. Consequently, by Theorem 3, we know that there is an integer y_k an inverse of M_k modulo m_k such that,

$$M_k y_k = 1(\bmod m_k)$$

To construct a simultaneous solution, form the sum

$$X = a_1M_1y_1 + a_2M_2y_2 + \ldots + a_nM_ny_n$$

We will now show that x is a simultaneous solution. First, note that because $M_j \equiv 0 \pmod{m_k}$ whenever $j \neq k$, all terms except the kth term in this sum are congruent to 0 modulo m_k. Because $M_ky_k \equiv 1 \pmod{m_k}$ we see that,

$$x \equiv a_kM_ky_k \equiv a_k \pmod{m_k}$$

for k = 1 , 2, . . . , n. We have shown that x is a simultaneous solution to the n congruences.