4.4

Chinese Remainder Theorem:

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than 1 and $a_1, a_2, \ldots, a_n$ be arbitrary integers. Then the system:

$x \equiv a_1 \mod m_1$
$x \equiv a_2 \mod m_2$
$\vdots$
$x \equiv a_n \mod m_n$

has a unique solution modulo $m = m_1 m_2 \ldots m_n$

$M_k = \frac{m}{m_k}$ for $k = 1, 2, \ldots, n$

Y_k is an inverse of $M_k \mod m_k$, such that

$M_k Y_k \equiv 1 \mod m_k$

$x \equiv (a_1 M_1 Y_1 + a_2 M_2 Y_2 + \ldots + a_n M_n Y_n) \mod m$

ex:

Solve the system of congruences

$x \equiv 2 \mod 3$
$x \equiv 3 \mod 5$ ←
$x \equiv 2 \mod 7$

To check answer
If you take the answer, in this case 23, then divide it by the modulus, You will get the same remainder as in each equation of the problem,

23 divided by 3, gives 2 as the remainder.
23 divided by 5, gives 3 as the remainder.

solution:

$a_1 = 2$ $m_1 = 3$

$a_2 = 3$ $m_2 = 5$

$a_3 = 2$ $m_3 = 7$

23 divided by 7, gives 2 as the remainder.

$m = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105$

$M_1 = \frac{m}{m_1} = \frac{105}{3} = 35$

$M_2 = \frac{m}{m_2} = \frac{105}{5} = 21$

$M_3 = \frac{m}{m_3} = \frac{105}{7} = 15$

$M_1 Y_1 \equiv 1 \bmod m_1$

$35 Y_1 \equiv 1 \bmod 3 \leftarrow$ 35 times what and then divided by 3 gives 1 as the remainder?

$35 \cdot 2 \equiv 1 \bmod 3$

$Y_1 = 2$

$M_2 Y_2 \equiv 1 \bmod m_2$

$21 Y_2 \equiv 1 \bmod 5$

$21 \cdot 1 \equiv 1 \bmod 5$

$Y_2 = 1$

$M_3 Y_3 \equiv 1 \bmod m_3$

$15 Y_3 \equiv 1 \bmod 7$

$15 \cdot 1 \equiv 1 \bmod 7$

$Y_3 = 1$

$x \equiv (a_1 M_1 Y_1 + a_2 M_2 Y_2 + \ldots + a_n M_n Y_n) \bmod m$

$x \equiv (2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1) \bmod 105$

$\equiv 233 \bmod 105$

$\equiv 23 \bmod 105$