Chinese Remainder Theorem

The Chinese remainder theorem helps us to solve a group of equations of the form:
$x = a_1 \bmod m_1$
$x = a_2 \bmod m_2$
$x = a_3 \bmod m_3$
...
$x = a_n \bmod m_n$
where all pairs of $m_1, m_2, m_3 \ldots m_n$ are coprime to each other.
Steps:

- Compute $X_k = (m_1.m_2.m_3 \ldots m_n)/(m_k)$ for each *k* from 1 to n.
- Let us denote the inverse of X under modulo m by X_m^{-1}. For each k from 1 to n, compute the inverse of each X_k under modulo m_k from the step above, the inverse modulo of X_k exists because X_k and $m_1 m_2 m_3 \ldots m_{k-1} m_{k+1} .. m_n$ are coprime to each other.
- The solution is given as $x = a_1 X_1 X_{1(m1)}^{-1} + a_2 X_2 X_{2(m2)}^{-1} + \ldots . + a_n X_n X_{n(mn)}^{-1}$.

In this solution, for each k = 1,2,3,...,n -> $a_k X_k X_{k(mk)}^{-1} \bmod m_k = a_k$ as $X_k X_{k(mk)}^{-1} \bmod m_k = 1$, since all the other terms in the expression are divisible by m_k, hence they have no effect on the remainder.

For Example: Given the group of equations:
x = 2 mod 5
x = 3 mod 7
x = 1 mod 3
Computing $X_1 = (5.7.3)/(5) = 21$, $X_2 = (5.7.3)/(7) = 15$, $X_3 = (5.7.3)/(3) = 35$
$X_{1(m1)}^{-1} = 1$, $X_{2(m2)}^{-1} = 1$, $X_{3(m3)}^{-1} = 2$
x = 2.21.1 + 3.15.1 + 1.35.2 = 157

Once we have found a solution x that satisfies the group of equations, we can create infinitely many solutions of the form - $x + m_1 m_2 m_3 \ldots m_n$.