Chinese remainder Theorem:

Ex: In the first Century Sun-Tsu asked: A certain number is unknown. when divided by 3 the remainder is 2, when divided by 5 the remainder is 3 & when divided by 7 the remainder is 2. What is the number?

This is asking us to solve:

$$x \equiv 2 \bmod 3$$
$$x \equiv 3 \bmod 5$$
$$x \equiv 2 \bmod 7.$$

The Chinese Remainder Theorem states this has a unique solution:

Theorem:
Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime integers & $a_1, a_2, \ldots, a_n$ arbitrary integers. Then has a unique solution modulo $m = m_1 \cdot m_2 \cdots m_n$.

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

The proof is constructive, & provides the solution:

i.e. First $\forall k = 1, 2, \ldots, n$ define $M_k = \frac{m}{m_k}$ that is M_k = all m_i multiplied except m_k. Since $\gcd(m_i, m_k) = 1$ then $\gcd(m_k, M_k) = 1$. Thus $\exists\, y_k$

s.t. $y_k \equiv M_k^{-1} \bmod m_k$.

Then $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n \pmod m$.

Then by construction:

$$x \bmod m_i = 0 + 0 + \cdots + a_2 M_i y_i + 0 + \cdots + 0$$
$$\equiv a_2 \cdot 1 \bmod m_i$$
$$= a_2 \checkmark$$

$\square$

This is very formulaic. Lets think about why its true with the above example.

<u>Ex</u>: Solve $x \equiv 2 \mod 3$

$x \equiv 3 \mod 5$

$x \equiv 2 \mod 7.$

Our solution will have the form

$x = 2 \cdot \_ \cdot \_ + 3 \cdot \_ \cdot \_ + 2 \cdot \_ \_$

We want $3 \cdot \_ \cdot \_$ & $2 \cdot \_ \cdot \_ = 0$ when mod 3

$\Rightarrow$ need a 3 in each

$x = 2 \cdot \_ \cdot \_ + 3 \cdot 3 \cdot \_ \cdot \_ + 2 \cdot 3 \cdot \_ \cdot \_$

want $2 \cdot \_ \cdot \_$ & $2 \cdot 3 \cdot \_ \cdot \_ = 0$ when mod 5

$\Rightarrow$ need a 5

$x = 2 \cdot 5 \cdot \_ \cdot \_ + 3 \cdot 3 \cdot \_ \cdot \_ + 2 \cdot 3 \cdot 5 \cdot \_$

want $2 \cdot 5 \cdot \_ \_$ & $3 \cdot 3 \cdot \_ \cdot \_ = 0$ when mod 7

$\Rightarrow$ need a 7

$x = 2 \cdot 5 \cdot 7 \cdot \_ + 3 \cdot 3 \cdot 7 \cdot \_ + 2 \cdot 3 \cdot 5 \cdot \_$

need $2 \cdot 5 \cdot 7 \cdot \_ = 2$ when mod 3

$\Rightarrow$ need $35^{-1} \mod 3$ $\quad 35 \mod 3 \equiv 2$ $\quad 2^{-1} \mod 3 = 2$

need $3 \cdot 3 \cdot 7 \cdot \_ = 3$ when mod 5

$\Rightarrow$ need $21^{-1} \mod 5$ $\quad 21 \mod 5 = 1$ $\quad 1^{-1} \mod 5 = 1$

need $2 \cdot 3 \cdot 5 \cdot \_ = 2$ when mod 7

$\Rightarrow$ need $15^{-1} \mod 7$ $\quad 15 \mod 7 = 1$ $\quad 1^{-1} \mod 7 = 1$

So $x = 2 \cdot 5 \cdot 7 \cdot 2 + 3 \cdot 3 \cdot 7 \cdot 1 + 2 \cdot 3 \cdot 5 \cdot 1 = 233 \equiv 23 \mod 105$

Check $23 \mod 3 \equiv 2$ ✓ $23 \mod 5 \equiv 3$ ✓ $23 \mod 7 = 2$ ✓

Ex: Solve $x \equiv 1 \bmod 5$
$x \equiv 2 \bmod 6$
$x \equiv 3 \bmod 7$

$x = 1 \cdot 6 \cdot 7 \cdot \_ + 2 \cdot 5 \cdot 7 \cdot \_ + 3 \cdot 5 \cdot 6 \cdot \_$

$42^{-1} \bmod 5 \equiv ?$

$42 \bmod 5 \equiv 2 \quad 2^{-1} \bmod 5 \equiv 3$

$35^{-1} \bmod 6 = ?$

$35 \bmod 6 = 5 \quad 5^{-1} \bmod 6 \equiv 5$

$30^{-1} \bmod 7 = ?$

$30 \bmod 7 \equiv 2 \quad 2^{-1} \bmod 7 = 4$

$x = 1 \cdot 6 \cdot 7 \cdot 3 + 2 \cdot 5 \cdot 7 \cdot 5 + 3 \cdot 5 \cdot 6 \cdot 4$

$= 836$

$\equiv 206 \bmod 210$

Check: $206 \bmod 5 \equiv 1$ ✓
$206 \bmod 6 \equiv 2$ ✓
$206 \bmod 7 \equiv 3$ ✓