Th$\underline{m}$/ THE CHINESE REMAINDER THEOREM:
Let $m_1, m_2, .., m_r$ be pairwise relatively prime positive integers. Then the system of congruences

$$x \equiv a_1 \pmod{m_1},\ x \equiv a_2 \pmod{m_2}, .., x \equiv a_r \pmod{m_r}$$

has a unique sol$\underline{n}$ modulo $M = m_1 m_2 \dots m_r$.

Proof: 1$\underline{st}$ construct a sol$\underline{n}$ of the system. Let $M_k = \frac{M}{m_k}$ where $M = m_1 m_2 \cdots m_r$. Note, $\gcd(M_k, m_k) = 1$ thus $[M_k]^{-1}$ exists mod m_k. That is, $\exists y_k$ such that $y_k M_k \equiv 1 \bmod m_k$.
Let,

$$\boxed{x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_r M_r y_r} \leftarrow \text{How to construct the sol}^{\underline{n}}.$$

observe, $M_j \equiv 0 \bmod m_i$ for $i \neq j$ hence,

$$x \equiv a_i M_i y_i \quad \text{for} \quad y_i M_i \equiv 1 \bmod m_i$$
(other terms dropped to zero)

$$\equiv a_i. \quad \text{as } y_i M_i \equiv 1.$$

Next, suppose x_0, x_1 both be sol$\underline{n}$'s to the system of congruences. Then $x_0 \equiv x_1 \equiv a_k \pmod{m_k}$ for $k \in \mathbb{N}_r$
Hence, $m_k \mid (x_0 - x_1)$. By Th$\underline{m}$(4.8) ~~(which is in my Episode I)~~
~~we find M_k | linear comb. over $\mathbb{Z}$ $\Rightarrow x_0 = x$ mod~~
we find $\underbrace{m_1 m_2 \cdots m_r}_{M.} \mid (x_0 - x_1)$ $\therefore$ $M \mid (x_0 - x_1)$ $\therefore x_0 \equiv x_1 \bmod M$.

Example:
$x \equiv 2 \pmod 3$, $m_1 = 3$
$x \equiv 7 \pmod{11}$, $m_2 = 11$
$M = 33$, $M_1 = \frac{33}{3} = 11$, $M_2 = \frac{33}{11} = 3$

$y_1 M_1 \equiv 1 \bmod 3 \hookrightarrow 11 y_1 \equiv 1 \pmod 3$ $\therefore$ $[y_1] = [11]^{-1} = [2]^{-1} = [2]$
$y_2 M_2 \equiv 1 \bmod 11 \rightarrow [y_2] = \underbrace{[3]^{-1}}_{\text{mod 11 classes}} = [4]$ we find $y_1 = 2$, $y_2 = 4$
$\therefore x = 2(11)(2) + 7(3)(4)$
Thus, $\boxed{x = 128}$

Ex ① $x \equiv 2 \mod 3$
② $x \equiv 7 \mod 11$ } solve via substitution method.

$x = 2 + 3t$ for some $t \in \mathbb{Z}$

Hence, subst. into ②,

$$2 + 3t \equiv 7 \pmod{11}$$

$$\Rightarrow 3t \equiv 5 \mod 11$$

$$\Rightarrow 4 \cdot 3t \equiv 20 \mod 11 \qquad (4 \cdot 3 = 12 \equiv 1 \mod 11)$$

$$\Rightarrow \underline{t \equiv 9 \mod 11}.$$

Thus, $x = 2 + 3(9) = \boxed{29}$ (notice $128 \equiv 29 \mod 33$) same answer as last attempt.

Ex $\boxed{\begin{array}{ll} x \equiv 1 & \mod 2 \\ x \equiv 2 & \mod 3 \\ x \equiv 3 & \mod 5 \end{array}}$ $\longrightarrow$ $x = 1 + 2t$ for some $t \in \mathbb{Z}$

(solved via substitution)

Hence, $1 + 2t \equiv 2 \mod 3$

$$\Rightarrow 2t \equiv 1 \mod 3$$

$$\Rightarrow 2 \cdot 2t \equiv 2 \mod 3$$

$$\Rightarrow t \equiv 2 \mod 3.$$

Thus $t = 2 + 3u$ for some $u \in \mathbb{Z}$. Now we have $x = 1 + 2t = 1 + 2(2 + 3u) = 5 + 6u$

Plugging into $x \equiv 3 \mod 5$

$$5 + 6u \equiv 3 \mod 5$$

$$6u \equiv -2 \equiv 3 \mod 5 \qquad \text{(duh, could } 8 \nearrow 0\text{)}$$

$$6 \cdot 6u \equiv 6 \cdot 3 \mod 5$$

$$36u \equiv 18 \mod 5$$

$$u \equiv 3 \mod 5$$

Thus, $u = 3 \hookrightarrow x = 5 + 6(3) = \underline{23}$ $\therefore \boxed{x \equiv 23 \mod 30}$

Ex

$$x \equiv 1 \mod 2 \longrightarrow M_1 = 15$$
$$x \equiv 2 \mod 3 \longrightarrow M_2 = 10 \quad \& \ M = 30$$
$$x \equiv 3 \mod 5 \longrightarrow M_3 = 6$$

$$\left.\begin{array}{l}\text{Find: } [15]_2^{-1} = [1]_2^{-1} = 1. = y_1 \\ \text{Find: } [10]_3^{-1} = [1]_3^{-1} = 1. = y_2 \\ \text{Find: } [6]_5^{-1} = [1]_5^{-1} = 1. = y_3\end{array}\right\} \text{funny.}$$

$$\begin{aligned} \therefore\ x &= a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \\ &= 1 \cdot 15 \cdot 1 + 2 \cdot 10 \cdot 1 + 3 \cdot 6 \cdot 1 \\ &= 15 + 20 + 18 \\ &= \boxed{53 \equiv 23 \mod 30} \end{aligned}$$

(I'll call this sol$^{\underline{n}}$, "by Chinese Rem. Th$^{\underline{m}}$")

Remark: The sol$^{\underline{n}}$ $\boxed{x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r \quad (*)}$ can perhaps be derived by r-fold substitution. The proof given was fine, but perhaps the origin of this formula is just brute-force. Then again, I'd be interested if you have a deeper intuition for (*).

Ex
$$x \equiv 2 \mod 11$$
$$x \equiv 3 \mod 12$$
$$x \equiv 4 \mod 13$$
$$x \equiv 5 \mod 17$$
$$x \equiv 6 \mod 19$$

I'll try ~~substitution~~ Chinese Rem T.

as $M_1 = 12\cdot 13\cdot 17\cdot 19 = 50,388$

$$[M_1]_{11}^{-1} = [12\cdot 13\cdot 17\cdot 19]_{11}^{-1} = [1\cdot 2\cdot 6\cdot 8]_{11}^{-1} = [8]_{11}^{-1} = [7]_{11}.$$

16, 24, 32, 40, 48, 56

$\therefore\ y_1 = 7.$

$$[M_2]_{12}^{-1} = [\underbrace{11\cdot 13\cdot 17\cdot 19}_{46,189}]_{12}^{-1} = [-1\cdot 1\cdot 5\cdot 7]_{12}^{-1} = [-35]_{12}^{-1} = [1]_{12}^{-1} = [1]_{12}\ \therefore\ y_2 = 1.$$

$$[M_3]_{13}^{-1} = [\underbrace{11\cdot 12\cdot 17\cdot 19}_{42,636}]_{13}^{-1} = [-2\cdot(-1)\cdot 4\cdot 6]_{13}^{-1} = [48]_{13}^{-1} = [9]_{13}^{-1} = [3]_{13}$$

~~$=[4]_{13}^{-1} = [7]_{13}$~~

$\therefore\ y_3 = 3$

Fine.

$(13, 9) = (a, b)$
$(9, 4) = (b, a-b)$
$(4, 1) = (a-b, b-2(a-b))$
$= (a-b, 3b-2a)$
$\therefore\ 1 = 3(9) - 2(13)$
$\therefore\ [9]_{13}^{-1} = [3]_{13}$

well, duh.

$(19, 7) = (a, b)$
$(7, 5) = (b, a-2b)$
$(5, 2) = (a-2b, b-a+2b)$
$(2, 1) = (3b-a, a-2b-2(3b-a))$
$1 = -8b+3a = -8(7)+3(19)$
$[7]_{19}^{-1} = [-8]_{19} = [11]_{19}$

$$[M_4]_{17}^{-1} = [\underbrace{11\cdot 12\cdot 13\cdot 19}_{32,604}]_{17}^{-1} = [-6\cdot(-5)\cdot(-4)\cdot 2]_{17}^{-1} = [30\cdot(8)]_{17}^{-1} = [-4\cdot(-8)]_{17}^{-1} = [32]_{17}^{-1} = [15]_{17}^{-1} = [8]_{17}$$

$\therefore\ y_4 = 8$

$(17, 15) = (a, b)$
$(15, 2) = (b, a-b)$
$(2, 1) = (a-b, b-7(a-b))$
$1 = -7a+8b$
$1 = -7\cdot 17 + 8\cdot 15$

$$[M_5]_{19}^{-1} = [\underbrace{11\cdot 12\cdot 13\cdot 17}_{29,172}]_{19}^{-1} = [8\cdot 7\cdot 6\cdot 2]_{19}^{-1} = [7]_{19}^{-1}$$

$[11]_{19}$ $\Downarrow$ $y_5 = 11$

~~$= [16\cdot 14]_{19}^{-1} = [-3\cdot -5]_{19}^{-1} = [15]_{19}^{-1} = [-5]_{19} = [14]_{19}$ $\therefore\ y_5 = 14$~~

~~$(19, 15) = (a, b)$~~
~~$(15, 4) = (b, a-b)$~~
~~$(4, 3) = (a-b, b-3a+3b)$~~
~~$(3, 1) = (4b-3a, a-b-(4b-3a))$~~
~~$1 = 4a-5b$~~
~~$1 = 4(19) - 5(15)$~~

$x = 4,585,143 \equiv \boxed{150,999}$

$$\therefore\ x = 2(50388)(7) + 3(46,189)(1) + 4(42,636)(3) + 5(32,604)(8) + 6(29,172)(11) = \cancel{5110239}$$

$$\boxed{x \equiv \cancel{121,827} \mod 554268}$$

Concerning non-coprime moduli

Claim: The system of congruences

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

Has sol$^{\underline{n}}$ iff $(m_1, m_2) \mid (a_1 - a_2)$. Moreover, when $\exists$ sol$^{\underline{n}}$, it is unique modulo $[m_1, m_2]$.

Proof: $\S$ $\gcd(m_1, m_2) \mid (a_1 - a_2)$. If $x \equiv a_1 \bmod m_1$ then $x = a_1 + m_1 t$ for some $t \in \mathbb{Z}$. Hence,

$m_1 t + a_1 \equiv a_2 \bmod m_2 \Rightarrow m_1 t \equiv (a_2 - a_1) \bmod m_2$

Note, $m_1 t \equiv (a_2 - a_1) \bmod m_2$ has sol$^{\underline{n}}$ when,

Th$^{\underline{m}}$/ $ax \equiv b \bmod n$ has sol$^{\underline{n}}$ iff $\gcd(a,n) \mid b$ $\quad a = m_1,\ n = m_2,\ b = a_2 - a_1$

$\underline{\gcd(m_1, m_2) \mid (a_2 - a_1)}^{*}$. As this $(*)$ was given we find sol$^{\underline{n}}$'s $t = t_0 + \dfrac{ns}{\gcd(m_1, m_2)} = t_0 + \dfrac{m_2 s}{\gcd(m_1, m_2)}$ for $s \in \mathbb{Z}$.

If x_0, x_1 both solve the system $\Rightarrow \exists\, s_0, s_1 \in \mathbb{Z}$ s.t.

$$x_0 = a_1 + m_1\left(t_0 + \frac{m_2 s_0}{\gcd(m_1, m_2)}\right)$$ likewise for x_1 with $s_0 \mapsto s_1$

Hence, as the a_1's cancel, and t_0's cancel,

$$x_1 - x_0 = m_1\left[\frac{m_2(s_1 - s_0)}{\gcd(m_1, m_2)}\right] = \frac{m_1 m_2 (s_1 - s_0)}{\gcd(m_1, m_2)}$$

Therefore, using $\operatorname{lcm}(m_1, m_2)\gcd(m_1, m_2) = m_1 m_2$ we find

$x_1 - x_0 = (s_1 - s_0)\operatorname{lcm}(m_1, m_2) \therefore x_1 \equiv x_0 \bmod \operatorname{lcm}(m_1, m_2)$. //

(it remains to show $\gcd(m_1, m_2) \nmid (a_1 - a_2) \Rightarrow$ no sol$^{\underline{n}}$'s
I leave that to the reader.)

Ex $\boxed{\begin{array}{ll} x \equiv 4 & \text{mod } 6 \\ x \equiv 13 & \text{mod } 15 \end{array}}$

Notice $\gcd(6,15) = 3 \neq 1$ thus this is not the coprime case, but, we may attempt the subst. sol^{n} just the same.

$$x \equiv 4 \mod 6 \Rightarrow x = 4 + 6t \text{ for some } t \in \mathbb{Z}$$

$$x \equiv 13 \mod 15 \Rightarrow 4 + 6t \equiv 13 \mod 15$$

$$\Rightarrow 6t \equiv 9 \mod 15$$

Recall: $ax \equiv b \mod (n)$ has sol^{n} iff $\gcd(a, n) \mid b$

$a = 6$
$b = 9$
$n = 15$
$\gcd(6,15) = 3 \mid 9.$

Continuing, $6t \equiv 9 \pmod{15}$

$$3 \cdot 2t \equiv 3 \cdot 3 \pmod{15}$$

$$2t \equiv 3 \mod 15$$

$$8 \cdot 2t \equiv 3 \cdot 8 = 24 \equiv 9 \pmod{15}$$

$$\underline{t \equiv 9 \mod 15}. \Rightarrow x = 4 + 6(9) = 58$$

$$\text{lcm}(6,15) = 30 \rightarrow \boxed{x \equiv 58 \equiv 28 \mod 30}$$

Ex $\boxed{\begin{array}{ll} x \equiv 7 & \text{mod } 10 \\ x \equiv 4 & \text{mod } 15 \end{array}}$

$$x = 7 + 10t \Rightarrow 7 + 10t \equiv 4 \mod 15$$

$$\Rightarrow 10t \equiv -3 \mod 15 \quad \gcd(10,15) = 5 \nmid -3$$

$\Rightarrow$ $\underline{\nexists \text{ a sol}^{n} \text{ to this system.}}$