Chineese Remainder Theorum.

for $a = \{a_1, a_2 \ldots a_n\}$ & $M = \{m_1, m_2 \ldots m_n\}$

find x such that

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_3 \pmod{m_3}$$

$m_1, m_2 \ldots m_n$ are pairwise coprime : $\forall i \forall j \, (i \neq j \rightarrow \gcd(m_1, m_2) = 1)$

we can say as a result that $x \equiv a \pmod{m}$

$m = m_1 \times m_2 \times m_3 \ldots m_n$

Finding a: consider only: $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$

from Bezout : $n_1 m_1 + n_2 m_2 = 1$

Extended Euclid.

Euclid ended when $b = 0$, $a = g$

so easily $g \cdot 1 + 0 \cdot 0 = 1$

let $(x, y) = (1, 0)$ for $(g, 0)$

finding (x_1, y_1) for $(b, a \bmod b)$

$$b \cdot x_1 + \underbrace{(a \bmod b)}_{a - \lfloor \frac{a}{b} \rfloor b \ (*)} y_1 = g \quad ①$$

& $$ax + by = g \quad ②$$

$$bx_1 + (a - \lfloor \tfrac{a}{b} \rfloor b) y_1 = g \quad \text{from ① \& (*)}$$

$$g = ay_1 + b(x_1 - y_1 \lfloor \tfrac{a}{b} \rfloor)$$
$$= ax + by \quad ②$$

so $x = y_1$, $y = x_1 - y_1 \lfloor \frac{a}{b} \rfloor$

So one can say that:

to find $gcd(a, b, \&x, \&y)$

call

$gcd(b, a \bmod b, x1, y1)$

then assign $x = y1$

$y = x1 - y_1 \lfloor \frac{a}{b} \rfloor$

---

get back to $n_1m_1 + n_2m_2 = 1$

$gcd(m_1, m_2, n_1, n_2)$

$\downarrow$

$gcd(m_2, m_1 \bmod m_2, n_1', n_2')$

$n_1 = n_2'$

$n_2 = n_1' - n_2' \lfloor \frac{m_1}{m_2} \rfloor$

Define a solution:

$$a = a_1 n_2 m_2 + a_2 n_1 m_1 \mod m_1 m_2$$

General solution:

$$a = \sum_{i=1}^{k} a_i M_i N_i \quad (\bmod \prod_{i=1}^{k} m_i)$$

where $M_i = \prod_{i \neq j} m_j$ & $N_i := M_i^{-1} \bmod m_i$

so basically it is the summation of

$$a_i \times \underbrace{\left(\frac{\prod_{j=1}^{k} m_j}{m_i} \right)}_{M_i} \times \left(M_i^{-1} \bmod m_i \right)$$

What if m_i $\forall i$
are not coprime.

$$\begin{cases} a \equiv 1 \pmod 4 \\ a \equiv 2 \pmod 6 \end{cases} \Rightarrow \text{this has no solution}$$

$$a \equiv a_i \pmod{m_i}$$
$$\Downarrow$$
$$a \equiv a_i \pmod{p_j^{n_j}}$$

$$\left.\begin{cases} a \equiv 1 \pmod 4 \\ a \equiv 2 \pmod 6 \end{cases}\right\} \to \begin{cases} a \equiv 1 \pmod 4 \\ a \equiv 2 \equiv 0 \pmod 2 \\ a \equiv 2 \pmod 3 \end{cases}$$

but $a \equiv 1 \pmod 4 \to a \equiv 1 \pmod 2$

PF of 6

contradiction
with $a \equiv 0 \pmod 2$