Recap $\begin{cases} ax+by \equiv r \\ cx+dy \equiv s \end{cases}$ over $\mathbb{Z}_n$

$\gcd(ad-bc, n) = 1$

x is uniquely decided.

Same arguments for y for its unique possibility as a soln.

Chinese remainder Thm:

Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$.

Thm: If $m_1, m_2, \ldots, m_n$ are such that $(m_i, m_j) = 1$ (i.e. m_i & m_j are coprime) for $1 \leq i \neq j \leq n$, then the congruences ~~eqns~~ $x \equiv a_i \mod m_i$ $1 \leq i \leq n$, then there is a unique $0 \leq y \leq m-1$, where $m = m_1 m_2 \cdots m_n$ s.t. $y \equiv a_i \mod m_i$.

$[\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}]$

Ring theoretically:

$$\begin{aligned} \mathbb{Z} &\longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n} \\ t &\longmapsto (t \bmod m_1, t \bmod m_2, \ldots, t \bmod m_n) \\ & \qquad (a_1, a_2, \ldots, a_{m_n}) \end{aligned}$$

is surjective

In fact,

$$\begin{aligned} \mathbb{Z}_{m_1 m_2 \cdots m_n} &\longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n} \\ t \bmod m_1 \cdots m_n &\longmapsto (t \bmod m_1, t \bmod m_2, \ldots, t \bmod m_n) \end{aligned}$$

is an isomorphism of rings.

Proof: We have to construct $y \in \mathbb{Z}$ s.t. $y \equiv a_i \mod m_i$

Let $M_i = \dfrac{m}{m_i}$ $\left(= m_1 m_2 \cdots \widehat{m_i} \cdots m_n\right)$

$(1 \leq i \leq n)$

Since $(M_i, m_i) = 1$

$y_i M_i + z_i m_i = 1$ for some $y_i, z_i \in \mathbb{Z}$ $1 \le i \le n$

so, $\underline{y_i M_i \equiv 1 \mod m_i}$, & for $i \neq j$, $\underline{M_j \equiv 0 \mod m_i}$

~~Define~~ $y = \sum_{i=1}^{n} a_i y_i M_i$

$$y \equiv a_i \underline{y_i M_i} \mod m_i$$
$$\equiv \underline{a_i \mod m_i}$$

E.g.) Find a common $x \in \mathbb{Z}$ s.t.

$\underline{x \equiv 1 \mod 3, \quad x \equiv 2 \mod 5 \quad \& \ x \equiv 4 \mod 7}$

$m_1 = 3,\ a_1 = 1,\quad m_2 = 5,\ a_2 = 2,\quad m_3 = 7,\ a_3 = 4$

$y_1 = M_1^{-1} = \left(\frac{3 \times 5 \times 7}{3}\right)^{-1} = (35)^{-1} \mod 3$
$= 2^{-1} \mod 3 = 2 \mod 3$

$\left(M = 105 = 3 \times 5 \times 7\right.$

$y_2 = M_2^{-1} = 21^{-1} \mod 5 = 1 \mod 5$

$y_3 = M_3^{-1} = 15^{-1} \mod 7 = 1 \mod 7.$

$y = a_1 y_1 M_1 + a_2 y_2 M_2 + a_3 y_3 M_3 = \underline{1 \times 2 \times 35 + 2 \times 1 \times 21 + 4 \times 1 \times 15}$

$= \underline{67 \mod \underline{105}}$

$\phi(n) = |U(\mathbb{Z}_n)|$ = the number non negative integers $< n$ & coprime to n.

E.g. $\underline{\phi(1) = 1}$, $\phi(2) = 1$, $\phi(3) = 2$

Thm: $\boxed{\phi(mn) = \phi(m)\phi(n) \quad \text{if } (m,n) = 1}$

$\cancel{\phi(m)}$

By chinese remainder theorem, i.e.

$$\cancel{\frac{\mathbb{Z}}{mn} \cong \frac{\mathbb{Z}}{m} \times \frac{\mathbb{Z}}{n}}$$

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$$

isomorphism of groups

$$U(\mathbb{Z}_{mn}) \cong U(\mathbb{Z}_m \times \mathbb{Z}_n) = U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$$

In particular $|U(\mathbb{Z}_{mn})| = |U(\mathbb{Z}_m)| \times |U(\mathbb{Z}_n)|$.

If $ab = 1$ then $f(ab) = f(1) = 1$

$\Rightarrow f(a)f(b) = 1.$

$$|U(\mathbb{Z}_{mn})| = \phi(mn)$$

$$|U(\mathbb{Z}_m)| = \phi(m)$$

$$|U(\mathbb{Z}_n)| = \phi(n)$$

$$\phi(mn) = \phi(m)\phi(n)$$

Observation $a \in U(\mathbb{Z}_m)$

b a zero divisor of $\mathbb{Z}_n$

$= \mathbb{Z}_n \setminus U(\mathbb{Z}_n)$

so that $\exists c$ s.t. $bc = 0$

$(a, b)(0, c) = (0, 0)$

On the other hand

if $a \in U(\mathbb{Z}_m)$ & $b \in U(\mathbb{Z}_n)$

then $\exists$ $a' \in U(\mathbb{Z}_m)$ & $b' \in U(\mathbb{Z}_n)$

s.t. $aa' = 1$ & $bb' = 1$

So $(a, b)(a', b') = (aa', bb') = (1, 1)$

Propn: Let $a, c \in \mathbb{Z}^+$. If $b^a \equiv 1 \mod m$ & $b^c \equiv 1 \mod m$ then $b^d \equiv 1 \mod m$ where

$d = \gcd(a, c)$.

Proof: Let $s, t \in \mathbb{Z}$ s.t. $d = as + ct$

Then $(b^a)^s \equiv 1 \mod m$. $\left(((b^a)^{-1})^{-s} = (b^a)^s \right)$

$(b^c)^t \equiv 1 \mod m$

So $b^d \equiv b^{as+nt} \equiv (b^a)^s \, (b^n)^t \equiv 1 \times 1 \equiv 1 \mod m.$

Prop 7.2 Let p be a prime s.t. $p \mid b^n - 1$.

Then $p \mid b^d - 1$ for some smaller d (than n), or $p \equiv 1 \mod n$

And if $p > 2$ & n is odd then $p \equiv 1 \mod 2n$.

Proof: Set $d = \gcd(n, p-1)$.

Case 1 $d < n$. Then $d \mid n$.

Since $p \mid b^n - 1$ so that $b^n \equiv 1 \mod p$

& we know $b^{p-1} \equiv 1 \mod p$ (Fermat's little thm)

Since $d = \gcd(n, p-1)$

$b^d \equiv 1 \mod p$

Case 2 $d = n$. Then $n \mid p-1$ so that $p \equiv 1 \mod n$.

& if $p > 2$ & n is odd

$p \equiv 1 \mod 2n$.