THE CHINESE REMAINDER THM.

Ex: Determine whether the following pair of congruences has a solution or not.

$$x \equiv 6 \pmod{9}$$
$$x \equiv 4 \pmod{11}$$

Sol: $x = 15$

Thm: Let m and n be two +ve integers s.t $\gcd(m, n) = 1$. For any integers a and b, the following pair has a unique solution modulo $m \times n$.

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

<u>Proof</u>: Since $x \equiv a \pmod{m}$

we have $x = a + my$ for some $y \in Z$

Since $x \equiv b \pmod{n}$

we have ~~$x = b + nz$~~ for some $z \in Z$

~~$x = b + mz$~~ $x = b + nz$

$a + my = b + nz$

$$\boxed{my - nz = b - a} \quad \text{——— } ①$$

Finding a solution to the pair of congruences boils down to finding y and z that satisfies eq ①

Since $\gcd(m, n) = 1$, $\exists\, i, j \in Z$ s.t

$mi + nj = 1$

$$\boxed{mi(b-a) + nj(b-a) = b-a} \text{ — } ②$$

Comparing ① & ② $y = i(b-a)$

$z = j(a-b)$

Uniqueness of the Solution

Given $x \equiv a \pmod{m}$
$x \equiv b \pmod{n}$

Suppose c and c' both satisfy the above pair.

Then we have $c \equiv c' \pmod{m}$
$c \equiv c' \pmod{n}$

$\Rightarrow \quad m \mid (c-c') \quad \wedge \quad n \mid (c-c')$

Since $\gcd(m,n)=1$, $\quad m \cdot n \mid (c-c')$

$\Rightarrow \quad c \equiv c' \pmod{m \cdot n}$

EXTENSION TO MORE THAN TWO CONGRUENCES.

Thm: For $r \geq 2$, let $m_1, m_2, \ldots, m_r$ be nonzero integers that are pairwise relatively prime.

That is, $\gcd(m_i, m_j) = 1$ for $i \neq j$.

Then for any integers $a_1, a_2, \ldots, a_r$ the system of Congruences

$$x \equiv a_1 \bmod m_1$$
$$x \equiv a_2 \bmod m_2$$
$$\vdots$$
$$x \equiv a_r \bmod m_r$$

has a solution, which is Unique modulo $m_1 \cdot m_2 \cdot m_3 \cdots m_r$

Ex: $x \equiv 1 \pmod{3}$

$x \equiv 2 \pmod{5}$

$x \equiv 2 \pmod{7}$

find x.

<u>Thm</u>: If $\gcd(m,n)=1$, then

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

<u>Proof</u> $U_m = \{ a \bmod m \mid \gcd(a,m)=1 \}$

$$U_n = \{ b \bmod n \mid \gcd(b,n)=1 \}$$

$$U_{m \cdot n} = \{ c \bmod m \cdot n \mid \gcd(c, m \cdot n)=1 \}$$

$$f : U_{m \cdot n} \longrightarrow U_m \times U_n$$

$$f(c \bmod m \cdot n) = (c \bmod m \,,\, c \bmod n)$$

Prove that f is a Bijection