Th: The congruence $ax \equiv b \pmod{n}$ has a solution $\Leftrightarrow \gcd(a,n) \mid b$

proof: $\Rightarrow$ suppose x_0 solves our congurance

$\Rightarrow ax_0 \equiv b \pmod{n}$

$\Rightarrow ax_0 - b = mn \quad m \in \mathbb{Z}$

$\Rightarrow ax_0 - nm = b$

let $d = \gcd(a,n)$ since $d \mid a, d \mid n$

$\Rightarrow d \mid b$ —

$\Leftarrow$ suppose $\gcd(a,n) \mid b$, $d \mid b$

$\Rightarrow b = dk \quad k \in \mathbb{Z}$

using bezout identity

$d = sa + tn$

$\Rightarrow b = (sk)a + (tk)n$

let $s_1 = sk$, $t_1 = tk$

$\Rightarrow b = s_1 a + t_1 n$

$\Rightarrow s_1 a = b + t_1 n \Rightarrow nt_1 = s_1 a - b$

$\Rightarrow n \mid s_1 a - b \Rightarrow ax_1 \equiv b \pmod{n}$ //

Th: $\exists d = \gcd(a,n)$ incongruent solutions to these equations.

proof: let x_0 be a solution to $ax \equiv b \pmod{n}$

consider $x_m = x_0 + m\left(\frac{n}{d}\right)$ $\quad d = \gcd(n,a)$

$0 \le m \le d-1$

$m = 0, 1, \dots, d-1$

First, we need to show that they are solutions. Then we show that they are incongruent

$$ax_m = ax_0 + n\left(\frac{a}{d}\right)_{\in \mathbb{Z}} \equiv_n 0 \quad \text{since } d \mid a$$

$$= ax_0 \equiv_n b. \checkmark$$

Now, we show that they are incongruent solutions.

Suppose $x_i \equiv x_j \pmod n$ with $i \neq j$

$$x_0 + i\left(\frac{n}{d}\right) \equiv_n x_0 + j\left(\frac{n}{d}\right)$$

$$i\left(\frac{n}{d}\right) \equiv_n j\left(\frac{n}{d}\right) \Rightarrow (i-j)\left(\frac{n}{d}\right) = nl$$

$$\Rightarrow \frac{i-j}{d} \in \mathbb{Z}$$

$i, j \in [0, d-1] \Rightarrow i - j < d$

$\Rightarrow i - j = 0 \Rightarrow i = j$. a contradiction

Example: solve $12x \equiv 8 \pmod{20}$

$\gcd(12, 20) = 4$ since $4 \mid 8 \Rightarrow \exists$ a solution

There are 4 different solutions.

$(12x_0 + 20y_0 = 4) \times 2$, $x_0 = 2$, $y_0 = -1$

$12(4) - 2(20) = 8$

x

$\equiv \{4, 9, 14, 19\}$ ← 4 distinct solutions

Ex2: $10x \equiv 3 \pmod{15}$

$\gcd(15, 10) = 5$, $5 \nmid 3 \Rightarrow$ ~~$\nexists$~~ Solution

Ex : $143x \equiv 44 \pmod{231}$

$\gcd(231, 143) = \gcd(143, 88) = \gcd(88, 55)$
$= \gcd(55, 33) = 11$

$11 \mid 44$ ✓

$143(-8) + 231(5) = 11$ $\times 4$

$143(-32) + 231(20) = 44$

$\Rightarrow x = -32 \equiv 199$

$\{199, 210, \ldots 309\}$ $\{199 + 21m\}$

Find $9x \equiv 5 \pmod{85}$

$987x \equiv 610 \pmod{1597}$

$9 = 1 \cdot 5 + 4$

$5 = 1 \cdot 4 + 1$

$\gcd(9, 5) = 1$ ✓