How to solve

\[ ax = b \mod N \]
1. If \( \gcd(a, N) = 1 \)

\[ \exists! x \equiv b \mod N \]

\[ \therefore ax = b \mod N \]

\[ \Rightarrow a^{-1}ax = a^{-1}b \mod N \]

\[ \Rightarrow x = a^{-1}b \mod N \]
② If $g = \gcd(a, N) \neq 1$ and $g \mid b$, there are $g$ solutions!

How to find these $g$ solutions?

Let $a' = \frac{a}{g}$, $b' = \frac{b}{g}$, $N' = \frac{N}{g}$

Solve $a'x = b' \mod N'$ as in $\Box$
Let $x'$ is the unique solution (mod $N'$).

Those $g$ solutions are

$$x = x' + iN'$$

$$i = 0, 1, \ldots, g-1$$
③ If \( g = \gcd(a, N) \neq 1 \) and \( g \neq b \), there is NO solution!
Eg for \( \mathbb{Z} \):

\[ 21 \cdot x \equiv 12 \mod 36 \]

Sol: \( g = 3 = \gcd (21, 36) \)

Solve \( 7 \cdot x \equiv 4 \mod 12 \)

\[ x = 7^{-1} \cdot 4 = 7 \cdot 4 = 28 = 4 \mod 12 \]
there are 3 solutions \((\text{mod } 36)\)

\[ x = 4 + i \cdot 12 \quad \text{for } i = 0, 1, 2 \]

\[ \therefore x = 4, 16, 28 \quad \text{mod } 36 \]