Properties of Congruence Relations:
For \( a, b \in \mathbb{Z}^+ \), if \( a \equiv b \mod m \), then

- \( a^n \equiv b^n \mod m \) for \( n \in \mathbb{Z}^+ \)
- \( a + c \equiv b + c \mod m \) for \( c \in \mathbb{Z} \)
- \( ac \equiv bc \mod m \) for \( c \in \mathbb{Z} \)
- But we cannot cancel factors in general!

If we also have \( c \equiv d \mod m \), then

- \( a + c \equiv b + d \mod m \)
- \( ac \equiv bd \mod m \)

**Theorem:** The congruence \( ax \equiv c \mod m \) has a solution if and only if

\[
\gcd(a, m) \mid c.
\]

**Theorem:** If \( \gcd(b, m) = 1 \), then there always exists a solution to the congruence \( bx \equiv 1 \mod m \). We call \( x \) the multiplicative inverse of \( b \mod m \), and we denote it \( b^{-1} \).

**Fermat’s Little Theorem** If \( p \) is prime and \( \gcd(a, p) = 1 \), then

\[
a^{p-1} \equiv 1 \pmod{p}.
\]