# Modulo Congruence

## Definition

Let $n \in Z^+$. To say that $a$ is equivalent to $b$ modulo $n$, denoted $a \equiv_n b$ or $a \equiv b \pmod{n}$, means:

$$n \mid (b - a)$$

## Theorem

Let $n \in Z^+$:

$$a \equiv b \pmod{n} \iff \exists\, k \in \mathbb{Z}, b = a + kn$$

Proof

$$\begin{aligned} a \equiv b \pmod{c} \quad &\iff \quad n \mid (b - a) \\ &\iff \quad \exists\, k \in \mathbb{Z}, b - a = kn \\ &\iff \quad b = a + kn \end{aligned}$$

## Theorem

Modulo congruence is an equivalence relation on $\mathbb{Z}$.

Proof

Assume $n \in \mathbb{Z}^+$.

1). Assume $a \in \mathbb{Z}$.
$a - a = 0$
$n \mid 0$
$n \mid (a - a)$
$a \equiv a \pmod{n}$
$a \sim a$
Therefore, modulo congruence is reflexive.

2). Assume $a \sim b$.
$a \equiv b \pmod{n}$
$n \mid (b - a)$
$\exists\, k \in \mathbb{Z}, b - a = kn$
$a - b = (-k)n$
$-k \in \mathbb{Z}$
$n \mid (a - b)$
$b \equiv a \pmod{n}$
$b \sim a$
Therefore, modulo congruence is symmetric.

3). Assume $a \sim b$ and $b \sim c$.
$a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$
$n \mid (b-a)$ and $n \mid (c-b)$
$\exists\, h \in \mathbb{Z}, (b-a) = hn$
$\exists\, k \in \mathbb{Z}, (c-b) = kn$
$(b-a)+(c-b) = hn + kn$
$c - a = (h+k)n$
$h + k \in \mathbb{Z}$
$n \mid (c-a)$
$a \equiv c \pmod{n}$
$a \sim c$
Therefore, modulo congruence is transitive.

The $n$ equivalence classes: $\overline{0}, \overline{1}, \ldots, \overline{n-1}$, are called the *residue* classes modulo $n$.

**Example**

Let $n = 15$

$\overline{a} = \{a + kn \mid k \in \mathbb{Z}\}$

$\overline{0} = \{0, 15, -15, 30, -30, \ldots\}$
$\overline{1} = \{1, 16, -14, 31, -29, \ldots\}$
$\vdots$
$\overline{14} = \{14, 29, -1, 44, -16, \ldots\}$

Per the division algorithm, the residue class modulo $n$ for $m \in \mathbb{Z}$ is the remainder $r$:

$$\begin{aligned}
&m = nq + r, \qquad 0 \le r < n \\
&m - r = nq \\
&r - m = (-q)n \\
&n \mid (r - m) \\
&m \equiv r \pmod{n}
\end{aligned}$$

To find the residue class $\overline{r}$ modulo $n$ for a given $m \in \mathbb{Z}$:

$$r = m - \left\lfloor \frac{m}{n} \right\rfloor \cdot n$$

**Example**

Let $n = 15$

$\frac{1796}{15} \approx 119.73$
$r = 1796 - 119 \cdot 15 = 11$
$1796 \equiv 11 \pmod{15}$
$1796 \in \overline{11}$

$\frac{-1796}{15} \approx -119.73$
$r = -1796 + 120 \cdot 15 = 4$
$-1796 \equiv 4 \pmod{15}$
$-1796 \in \overline{4}$