$a \equiv b \pmod{c}$

▸ Start

Start

$$a, b \in \mathbb{Z}\ ,\ c \in \mathbb{N}$$
$$a \equiv b \pmod{c}$$

$a \equiv b \pmod{c}$

Start

$a, b \in \mathbb{Z}\ ,\ c \in \mathbb{N}$

$a \equiv b \pmod{c}$: a and b are congruent modulo c

▸ Start

$a, b \in \mathbb{Z}\ ,\ c \in \mathbb{N}$

$a \equiv b \pmod{c}$: a and b are congruent modulo c

i.e.

Start

$a, b \in \mathbb{Z}$, $c \in \mathbb{N}$

$a \equiv b \pmod{c}$: a and b are congruent modulo c

i.e. $c \mid (a - b)$

Start

$$a, b \in \mathbb{Z}\ ,\ c \in \mathbb{N}$$

$$a \equiv b \pmod{c} \quad : \quad a \text{ and } b \text{ are congruent modulo } c$$

$$i.e.\ \ c \mid (a - b)$$

$$a\ ,\ a_1\ ,\ a_2\ ,\ b\ ,\ b_1\ ,\ b_2 \in \mathbb{Z}\ ,\ c\ , n \in \mathbb{N}$$

Start

$$a, b \in \mathbb{Z}\ ,\ c \in \mathbb{N}$$

$$a \equiv b \pmod{c} \quad : \quad a \text{ and } b \text{ are congruent modulo } c$$

$$i.e.\ \ c \mid (a - b)$$

$$a\ ,\ a_1\ ,\ a_2\ ,\ b\ ,\ b_1\ ,\ b_2 \in \mathbb{Z}\ ,\ c\ , n \in \mathbb{N}$$

- $a_1 \equiv b_1\ ,$

Start

$$a, b \in \mathbb{Z}\ ,\ c \in \mathbb{N}$$

$$a \equiv b \pmod{c} \quad : \quad a \text{ and } b \text{ are congruent modulo } c$$

$$i.e.\ \ c \mid (a - b)$$

$$a\ ,\ a_1\ ,\ a_2\ ,\ b\ ,\ b_1\ ,\ b_2 \in \mathbb{Z}\ ,\ c\ , n \in \mathbb{N}$$

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c}$

Start

$$a, b \in \mathbb{Z}\ ,\ c \in \mathbb{N}$$

$$a \equiv b \pmod{c} \quad : \quad a \text{ and } b \text{ are congruent modulo } c$$

$$i.e.\ \ c \mid (a-b)$$

$$a\ ,\ a_1\ ,\ a_2\ ,\ b\ ,\ b_1\ ,\ b_2 \in \mathbb{Z}\ ,\ c\ , n \in \mathbb{N}$$

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$

▸ Start

$$a, b \in \mathbb{Z} \ , \ c \in \mathbb{N}$$

$a \equiv b \pmod{c}$: a and b are congruent modulo c

i.e. $c \mid (a - b)$

$$a \ , \ a_1 \ , \ a_2 \ , \ b \ , \ b_1 \ , \ b_2 \in \mathbb{Z} \ , \ c \ , n \in \mathbb{N}$$

- $a_1 \equiv b_1 \ , \ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$

  $ex)1 \equiv 4 \ ,$

Start

$$a, b \in \mathbb{Z}\ ,\ c \in \mathbb{N}$$
$$a \equiv b \pmod{c} \quad : \quad a \text{ and } b \text{ are congruent modulo } c$$
$$i.e.\ \ c \mid (a-b)$$

$$a\ ,\ a_1\ ,\ a_2\ ,\ b\ ,\ b_1\ ,\ b_2 \in \mathbb{Z}\ ,\ c\ , n \in \mathbb{N}$$

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$
  $ex)1 \equiv 4\ ,\ 2 \equiv 11 \pmod{3}$

▸ Start

$$a, b \in \mathbb{Z}\ ,\ c \in \mathbb{N}$$

$a \equiv b \pmod{c}$: a and b are congruent modulo c

i.e. $c \mid (a - b)$

$$a\ ,\ a_1\ ,\ a_2\ ,\ b\ ,\ b_1\ ,\ b_2 \in \mathbb{Z}\ ,\ c\ , n \in \mathbb{N}$$

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$

  $ex)1 \equiv 4\ ,\ 2 \equiv 11 \pmod{3} \Rightarrow 1 \pm 2 \equiv 4 \pm 11 \pmod{3}$

Start

$a, b \in \mathbb{Z}$, $c \in \mathbb{N}$

$a \equiv b \pmod{c}$: a and b are congruent modulo c

$i.e.\ \ c \mid (a-b)$

a , a_1 , a_2 , b , b_1 , $b_2 \in \mathbb{Z}$, c , $n \in \mathbb{N}$

- $a_1 \equiv b_1$, $a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$
  $ex)1 \equiv 4$, $2 \equiv 11 \pmod{3} \Rightarrow 1 \pm 2 \equiv 4 \pm 11 \pmod{3}$
- $a_1 \equiv b_1$,

Start

$$a, b \in \mathbb{Z}\ ,\ c \in \mathbb{N}$$

$$a \equiv b \pmod{c} \quad : \quad a \text{ and } b \text{ are congruent modulo } c$$

$$i.e.\ \ c \mid (a - b)$$

$$a\ ,\ a_1\ ,\ a_2\ ,\ b\ ,\ b_1\ ,\ b_2 \in \mathbb{Z}\ ,\ c\ , n \in \mathbb{N}$$

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$
  $ex)1 \equiv 4\ ,\ 2 \equiv 11 \pmod{3} \Rightarrow 1 \pm 2 \equiv 4 \pm 11 \pmod{3}$
- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c}$

▸ Start

$$a, b \in \mathbb{Z}\ ,\ c \in \mathbb{N}$$

$$a \equiv b \pmod{c} \quad : \quad a \text{ and } b \text{ are congruent modulo } c$$

$$i.e.\ \ c \mid (a - b)$$

$$a\ ,\ a_1\ ,\ a_2\ ,\ b\ ,\ b_1\ ,\ b_2 \in \mathbb{Z}\ ,\ c\ , n \in \mathbb{N}$$

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$

  $ex)1 \equiv 4\ ,\ 2 \equiv 11 \pmod{3} \Rightarrow 1 \pm 2 \equiv 4 \pm 11 \pmod{3}$
- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$

▸ Start

$$a, b \in \mathbb{Z}\ ,\ c \in \mathbb{N}$$

$$a \equiv b \pmod{c} \quad : \quad a \text{ and } b \text{ are congruent modulo } c$$

$$i.e.\ \ c \mid (a - b)$$

$$a\ ,\ a_1\ ,\ a_2\ ,\ b\ ,\ b_1\ ,\ b_2 \in \mathbb{Z}\ ,\ c\ , n \in \mathbb{N}$$

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$
  $ex) 1 \equiv 4\ ,\ 2 \equiv 11 \pmod{3} \Rightarrow 1 \pm 2 \equiv 4 \pm 11 \pmod{3}$
- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$
  $ex)\ 1 \equiv 4\ ,$

▸ Start

$$a, b \in \mathbb{Z}\ ,\ c \in \mathbb{N}$$

$$a \equiv b \pmod{c} \quad : \quad a \text{ and } b \text{ are congruent modulo } c$$

$$i.e.\ \ c \mid (a - b)$$

$$a\ ,\ a_1\ ,\ a_2\ ,\ b\ ,\ b_1\ ,\ b_2 \in \mathbb{Z}\ ,\ c\ , n \in \mathbb{N}$$

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$
  $ex)1 \equiv 4\ ,\ 2 \equiv 11 \pmod{3} \Rightarrow 1 \pm 2 \equiv 4 \pm 11 \pmod{3}$
- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$
  $ex)\ 1 \equiv 4\ ,\ 2 \equiv 11 \pmod{3}$

▸ Start

$$a, b \in \mathbb{Z}\ ,\ c \in \mathbb{N}$$

$$a \equiv b \pmod{c} \quad : \quad a \text{ and } b \text{ are congruent modulo } c$$

$$i.e.\ \ c \mid (a - b)$$

$$a\ ,\ a_1\ ,\ a_2\ ,\ b\ ,\ b_1\ ,\ b_2 \in \mathbb{Z}\ ,\ c\ , n \in \mathbb{N}$$

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$
  $ex)1 \equiv 4\ ,\ 2 \equiv 11 \pmod{3} \Rightarrow 1 \pm 2 \equiv 4 \pm 11 \pmod{3}$
- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$
  $ex)\ 1 \equiv 4\ ,\ 2 \equiv 11 \pmod{3} \Rightarrow 1 \times 2 \equiv 4 \times 11 \pmod{3}$

▸ Start

$$a, b \in \mathbb{Z}\ ,\ c \in \mathbb{N}$$

$$a \equiv b \pmod{c} \quad : \quad a \text{ and } b \text{ are congruent modulo } c$$

$$i.e.\ \ c \mid (a - b)$$

$$a\ ,\ a_1\ ,\ a_2\ ,\ b\ ,\ b_1\ ,\ b_2 \in \mathbb{Z}\ ,\ c\ , n \in \mathbb{N}$$

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$
  $ex)1 \equiv 4\ ,\ 2 \equiv 11 \pmod{3} \Rightarrow 1 \pm 2 \equiv 4 \pm 11 \pmod{3}$
- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$
  $ex)\ 1 \equiv 4\ ,\ 2 \equiv 11 \pmod{3} \Rightarrow 1 \times 2 \equiv 4 \times 11 \pmod{3}$
- $a \equiv b \pmod{c}$

▸ Start

$$a, b \in \mathbb{Z}\ ,\ c \in \mathbb{N}$$

$a \equiv b \pmod{c}$: a and b are congruent modulo c
i.e. $c \mid (a - b)$

$$a\ ,\ a_1\ ,\ a_2\ ,\ b\ ,\ b_1\ ,\ b_2 \in \mathbb{Z}\ ,\ c\ , n \in \mathbb{N}$$

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$
  $ex)1 \equiv 4\ ,\ 2 \equiv 11 \pmod{3} \Rightarrow 1 \pm 2 \equiv 4 \pm 11 \pmod{3}$
- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$
  $ex)\ 1 \equiv 4\ ,\ 2 \equiv 11 \pmod{3} \Rightarrow 1 \times 2 \equiv 4 \times 11 \pmod{3}$
- $a \equiv b \pmod{c} \Rightarrow a^n \equiv b^n \pmod{c}$

▸ Start

$$a, b \in \mathbb{Z}\ ,\ c \in \mathbb{N}$$

$$a \equiv b \pmod{c} \quad : \quad a \text{ and } b \text{ are congruent modulo } c$$

$$i.e.\ \ c \mid (a - b)$$

$$a\ ,\ a_1\ ,\ a_2\ ,\ b\ ,\ b_1\ ,\ b_2 \in \mathbb{Z}\ ,\ c\ , n \in \mathbb{N}$$

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$
  $ex)1 \equiv 4\ ,\ 2 \equiv 11 \pmod{3} \Rightarrow 1 \pm 2 \equiv 4 \pm 11 \pmod{3}$
- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$
  $ex)\ 1 \equiv 4\ ,\ 2 \equiv 11 \pmod{3} \Rightarrow 1 \times 2 \equiv 4 \times 11 \pmod{3}$
- $a \equiv b \pmod{c} \Rightarrow a^n \equiv b^n \pmod{c}$
  $ex)\ 1 \equiv 4 \pmod{3}$

▸ Start

$$a, b \in \mathbb{Z}\ ,\ c \in \mathbb{N}$$

$$a \equiv b \pmod{c} \quad : \quad a \text{ and } b \text{ are congruent modulo } c$$

$$i.e.\ \ c \mid (a - b)$$

$$a\ ,\ a_1\ ,\ a_2\ ,\ b\ ,\ b_1\ ,\ b_2 \in \mathbb{Z}\ ,\ c\ , n \in \mathbb{N}$$

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$
  $ex)1 \equiv 4\ ,\ 2 \equiv 11 \pmod{3} \Rightarrow 1 \pm 2 \equiv 4 \pm 11 \pmod{3}$
- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$
  $ex)\ 1 \equiv 4\ ,\ 2 \equiv 11 \pmod{3} \Rightarrow 1 \times 2 \equiv 4 \times 11 \pmod{3}$
- $a \equiv b \pmod{c} \Rightarrow a^n \equiv b^n \pmod{c}$
  $ex)\ 1 \equiv 4 \pmod{3} \Rightarrow 1^n \equiv 4^n \pmod{3}$

First

$$a, b \in \mathbb{Z}\ ,\ c \in \mathbb{N}$$

$$a \equiv b \pmod{c} \quad : \quad a \text{ and } b \text{ are congruent modulo } c$$

$$i.e.\ \ c \mid (a-b)$$

$$a\ ,\ a_1\ ,\ a_2\ ,\ b\ ,\ b_1\ ,\ b_2 \in \mathbb{Z}\ ,\ c\ , n \in \mathbb{N}$$

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$ proof
  $ex) 1 \equiv 4\ ,\ 2 \equiv 11 \pmod{3} \Rightarrow 1 \pm 2 \equiv 4 \pm 11 \pmod{3}$
- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$ proof
  $ex)\ 1 \equiv 4\ ,\ 2 \equiv 11 \pmod{3} \Rightarrow 1 \times 2 \equiv 4 \times 11 \pmod{3}$
- $a \equiv b \pmod{c} \Rightarrow a^n \equiv b^n \pmod{c}$ proof
  $ex)\ 1 \equiv 4 \pmod{3} \Rightarrow 1^n \equiv 4^n \pmod{3}$

▸ Start

- $a_1 \equiv b_1$, $a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$

Start

- $a_1 \equiv b_1 \ , \ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$

$c \mid (a_1 - b_1)$

Start

- $a_1 \equiv b_1$, $a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$

  $c \mid (a_1 - b_1)$, $c \mid (a_2 - b_2)$

Start

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$

  $c \mid (a_1 - b_1)\ ,\ c \mid (a_2 - b_2)$
  $c \mid \{(a_1 - b_1) \pm (a_2 - b_2)\}$

$a \equiv b \pmod{c}$

Start

- $a_1 \equiv b_1$, $a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$

$$c \mid (a_1 - b_1) \ , \ c \mid (a_2 - b_2)$$
$$c \mid \{(a_1 - b_1) \pm (a_2 - b_2)\}$$
$$c \mid \{(a_1 \pm a_2) - (b_1 \pm b_2)\}$$

$a \equiv b \pmod{c}$

Start

- $a_1 \equiv b_1$, $a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$

  $c \mid (a_1 - b_1)$, $c \mid (a_2 - b_2)$
  $c \mid \{(a_1 - b_1) \pm (a_2 - b_2)\}$
  $c \mid \{(a_1 \pm a_2) - (b_1 \pm b_2)\}$
  $\therefore a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{c}$

Start

- $a_1 \equiv b_1$, $a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$

$a \equiv b \pmod{c}$

▸ Start

- $a_1 \equiv b_1$, $a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$

  $c \mid (a_1 - b_1)$

▸ Start

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$

  $c \mid (a_1 - b_1)\ ,\ c \mid (a_2 - b_2)$

Start

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$

  $c \mid (a_1 - b_1)\ ,\ c \mid (a_2 - b_2)$
  $a_1 - b_1 = ck_1$

Start

- $a_1 \equiv b_1$, $a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$

  $c \mid (a_1 - b_1)$, $c \mid (a_2 - b_2)$
  $a_1 - b_1 = ck_1$, $a_2 - b_2 = ck_2$

▸ Start

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$

$$c \mid (a_1 - b_1)\ ,\ c \mid (a_2 - b_2)$$
$$a_1 - b_1 = ck_1\ ,\ a_2 - b_2 = ck_2$$
$$a_1 = b_1 + ck_1$$

$a \equiv b \pmod{c}$

▸ Start

- $a_1 \equiv b_1 \ , \ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$

$$c \mid (a_1 - b_1) \ , \ c \mid (a_2 - b_2)$$
$$a_1 - b_1 = ck_1 \ , \ a_2 - b_2 = ck_2$$
$$a_1 = b_1 + ck_1 \ , \ a_2 = b_2 + ck_2$$

Start

- $a_1 \equiv b_1 \ , \ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$

$$c \mid (a_1 - b_1) \ , \ c \mid (a_2 - b_2)$$
$$a_1 - b_1 = ck_1 \ , \ a_2 - b_2 = ck_2$$
$$a_1 = b_1 + ck_1 \ , \ a_2 = b_2 + ck_2$$
$$a_1 \times a_2 = (b_1 + ck_1) \times (b_2 + ck_2)$$

Start

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$

$$c \mid (a_1 - b_1)\ ,\ c \mid (a_2 - b_2)$$
$$a_1 - b_1 = ck_1\ ,\ a_2 - b_2 = ck_2$$
$$a_1 = b_1 + ck_1\ ,\ a_2 = b_2 + ck_2$$
$$a_1 \times a_2 = (b_1 + ck_1) \times (b_2 + ck_2)$$
$$a_1 \times a_2 = b_1 \times b_2 + b_1 \times ck_2 + ck_1 \times b_2 + ck_1 \times ck_2$$

Start

- $a_1 \equiv b_1$, $a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$

$$
\begin{aligned}
& c \mid (a_1 - b_1) \ , \ c \mid (a_2 - b_2) \\
& a_1 - b_1 = ck_1 \ , \ a_2 - b_2 = ck_2 \\
& a_1 = b_1 + ck_1 \ , \ a_2 = b_2 + ck_2 \\
& a_1 \times a_2 = (b_1 + ck_1) \times (b_2 + ck_2) \\
& a_1 \times a_2 = b_1 \times b_2 + b_1 \times ck_2 + ck_1 \times b_2 + ck_1 \times ck_2 \\
& a_1 \times a_2 = b_1 \times b_2 + c(b_1 k_2 + k_1 b_2 + ck_1 k_2)
\end{aligned}
$$

$a \equiv b \pmod{c}$

▸ Start

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$

  $$c \mid (a_1 - b_1)\ ,\ c \mid (a_2 - b_2)$$
  $$a_1 - b_1 = ck_1\ ,\ a_2 - b_2 = ck_2$$
  $$a_1 = b_1 + ck_1\ ,\ a_2 = b_2 + ck_2$$
  $$a_1 \times a_2 = (b_1 + ck_1) \times (b_2 + ck_2)$$
  $$a_1 \times a_2 = b_1 \times b_2 + b_1 \times ck_2 + ck_1 \times b_2 + ck_1 \times ck_2$$
  $$a_1 \times a_2 = b_1 \times b_2 + c(b_1k_2 + k_1b_2 + ck_1k_2)$$
  $$\text{Let } k_3 = b_1k_2 + k_1b_2 + ck_1k_2$$

Start

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$

$$
\begin{aligned}
& c \mid (a_1 - b_1)\ ,\ c \mid (a_2 - b_2) \\
& a_1 - b_1 = ck_1\ ,\ a_2 - b_2 = ck_2 \\
& a_1 = b_1 + ck_1\ ,\ a_2 = b_2 + ck_2 \\
& a_1 \times a_2 = (b_1 + ck_1) \times (b_2 + ck_2) \\
& a_1 \times a_2 = b_1 \times b_2 + b_1 \times ck_2 + ck_1 \times b_2 + ck_1 \times ck_2 \\
& a_1 \times a_2 = b_1 \times b_2 + c(b_1k_2 + k_1b_2 + ck_1k_2) \\
& \text{Let } k_3 = b_1k_2 + k_1b_2 + ck_1k_2 \\
& a_1 \times a_2 = b_1 \times b_2 + ck_3
\end{aligned}
$$

▸ Start

- $a_1 \equiv b_1 \ , \ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$

$$c \mid (a_1 - b_1) \ , \ c \mid (a_2 - b_2)$$
$$a_1 - b_1 = ck_1 \ , \ a_2 - b_2 = ck_2$$
$$a_1 = b_1 + ck_1 \ , \ a_2 = b_2 + ck_2$$
$$a_1 \times a_2 = (b_1 + ck_1) \times (b_2 + ck_2)$$
$$a_1 \times a_2 = b_1 \times b_2 + b_1 \times ck_2 + ck_1 \times b_2 + ck_1 \times ck_2$$
$$a_1 \times a_2 = b_1 \times b_2 + c(b_1 k_2 + k_1 b_2 + ck_1 k_2)$$
Let $k_3 = b_1 k_2 + k_1 b_2 + ck_1 k_2$
$$a_1 \times a_2 = b_1 \times b_2 + ck_3$$
$$a_1 \times a_2 - b_1 \times b_2 = ck_3$$

Start

- $a_1 \equiv b_1$, $a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$

$$c \mid (a_1 - b_1) \text{ , } c \mid (a_2 - b_2)$$
$$a_1 - b_1 = ck_1 \text{ , } a_2 - b_2 = ck_2$$
$$a_1 = b_1 + ck_1 \text{ , } a_2 = b_2 + ck_2$$
$$a_1 \times a_2 = (b_1 + ck_1) \times (b_2 + ck_2)$$
$$a_1 \times a_2 = b_1 \times b_2 + b_1 \times ck_2 + ck_1 \times b_2 + ck_1 \times ck_2$$
$$a_1 \times a_2 = b_1 \times b_2 + c(b_1 k_2 + k_1 b_2 + ck_1 k_2)$$
$$\text{Let } k_3 = b_1 k_2 + k_1 b_2 + ck_1 k_2$$
$$a_1 \times a_2 = b_1 \times b_2 + ck_3$$
$$a_1 \times a_2 - b_1 \times b_2 = ck_3$$
$$c \mid (a_1 \times a_2 - b_1 \times b_2)$$

Start

- $a_1 \equiv b_1\ ,\ a_2 \equiv b_2 \pmod{c} \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}$

$$
\begin{aligned}
& c \mid (a_1 - b_1)\ ,\ c \mid (a_2 - b_2) \\
& a_1 - b_1 = ck_1\ ,\ a_2 - b_2 = ck_2 \\
& a_1 = b_1 + ck_1\ ,\ a_2 = b_2 + ck_2 \\
& a_1 \times a_2 = (b_1 + ck_1) \times (b_2 + ck_2) \\
& a_1 \times a_2 = b_1 \times b_2 + b_1 \times ck_2 + ck_1 \times b_2 + ck_1 \times ck_2 \\
& a_1 \times a_2 = b_1 \times b_2 + c(b_1k_2 + k_1b_2 + ck_1k_2) \\
& \text{Let } k_3 = b_1k_2 + k_1b_2 + ck_1k_2 \\
& a_1 \times a_2 = b_1 \times b_2 + ck_3 \\
& a_1 \times a_2 - b_1 \times b_2 = ck_3 \\
& c \mid (a_1 \times a_2 - b_1 \times b_2) \\
& \therefore a_1 \times a_2 \equiv b_1 \times b_2 \pmod{c}
\end{aligned}
$$

$a \equiv b \pmod{c}$

Start

- $a \equiv b \pmod{c} \Rightarrow a^n \equiv b^n \pmod{c}$

Start

- $a \equiv b \pmod{c} \Rightarrow a^n \equiv b^n \pmod{c}$

  i) The statement is true for $n = 1$.

Start

- $a \equiv b \pmod{c} \Rightarrow a^n \equiv b^n \pmod{c}$

  i) The statement is true for $n = 1$.

  $a \equiv b \pmod{c}$

▸ Start

- $a \equiv b \pmod{c} \Rightarrow a^n \equiv b^n \pmod{c}$

  i) The statement is true for $n = 1$.

  $a \equiv b \pmod{c}$

  ii) Assume the statement is true for $n = k$.

Start

- $a \equiv b \pmod{c} \Rightarrow a^n \equiv b^n \pmod{c}$

  i) The statement is true for $n = 1$.
  $a \equiv b \pmod{c}$
  ii) Assume the statement is true for $n = k$.
  $a \equiv b\ ,\ a^k \equiv b^k (\bmod\ c)$

Start

- $a \equiv b \pmod{c} \Rightarrow a^n \equiv b^n \pmod{c}$

i) The statement is true for $n = 1$.

$a \equiv b \pmod{c}$

ii) Assume the statement is true for $n = k$.

$a \equiv b\ ,\ a^k \equiv b^k \pmod{c}$

$a \times a^k \equiv b \times b^k \pmod{c}$

Start

- $a \equiv b \pmod{c} \Rightarrow a^n \equiv b^n \pmod{c}$

  i) The statement is true for $n = 1$.

  $a \equiv b \pmod{c}$

  ii) Assume the statement is true for $n = k$.

  $a \equiv b\ ,\ a^k \equiv b^k \pmod{c}$

  $a \times a^k \equiv b \times b^k \pmod{c}$

  $a^{k+1} \equiv b^{k+1} \pmod{c}$

Start

- $a \equiv b \pmod{c} \Rightarrow a^n \equiv b^n \pmod{c}$

  i) The statement is true for $n = 1$.
  $a \equiv b \pmod{c}$
  ii) Assume the statement is true for $n = k$.
  $a \equiv b\ ,\ a^k \equiv b^k \pmod{c}$
  $a \times a^k \equiv b \times b^k \pmod{c}$
  $a^{k+1} \equiv b^{k+1} \pmod{c}$
  The statement is true for $n = k + 1$.

▸ Start

- $a \equiv b \pmod{c} \Rightarrow a^n \equiv b^n \pmod{c}$

  i) The statement is true for $n = 1$.

  $a \equiv b \pmod{c}$

  ii) Assume the statement is true for $n = k$.

  $a \equiv b \ , \ a^k \equiv b^k \pmod{c}$

  $a \times a^k \equiv b \times b^k \pmod{c}$

  $a^{k+1} \equiv b^{k+1} \pmod{c}$

  The statement is true for $n = k + 1$.

  by i), ii)

Start

- $a \equiv b \pmod{c} \Rightarrow a^n \equiv b^n \pmod{c}$

  i) The statement is true for $n = 1$.

  $a \equiv b \pmod{c}$

  ii) Assume the statement is true for $n = k$.

  $a \equiv b\ ,\ a^k \equiv b^k (\text{mod } c)$

  $a \times a^k \equiv b \times b^k (\text{mod } c)$

  $a^{k+1} \equiv b^{k+1} (\text{mod } c)$

  The statement is true for $n = k + 1$.

  by i), ii) (Mathematical Induction)

▸ Start

- $a \equiv b \pmod{c} \Rightarrow a^n \equiv b^n \pmod{c}$

i) The statement is true for $n = 1$.

$a \equiv b \pmod{c}$

ii) Assume the statement is true for $n = k$.

$a \equiv b \ , \ a^k \equiv b^k (\text{mod } c)$

$a \times a^k \equiv b \times b^k (\text{mod } c)$

$a^{k+1} \equiv b^{k+1} (\text{mod } c)$

The statement is true for $n = k + 1$.

by i), ii) (Mathematical Induction)

$\therefore a \equiv b \pmod{c} \Rightarrow a^n \equiv b^n \pmod{c}$