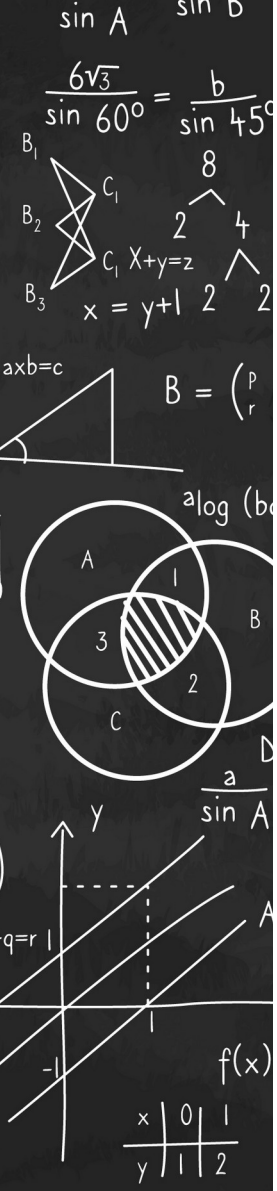


MATEMÁTICA DISCRETA 2

Aula 09

Congruência

Cristiane Loesch

Brasília
2025

Exercicio

Calcule $39 \oslash 38$ em Z_{351} .

Vamos pensar juntos?!

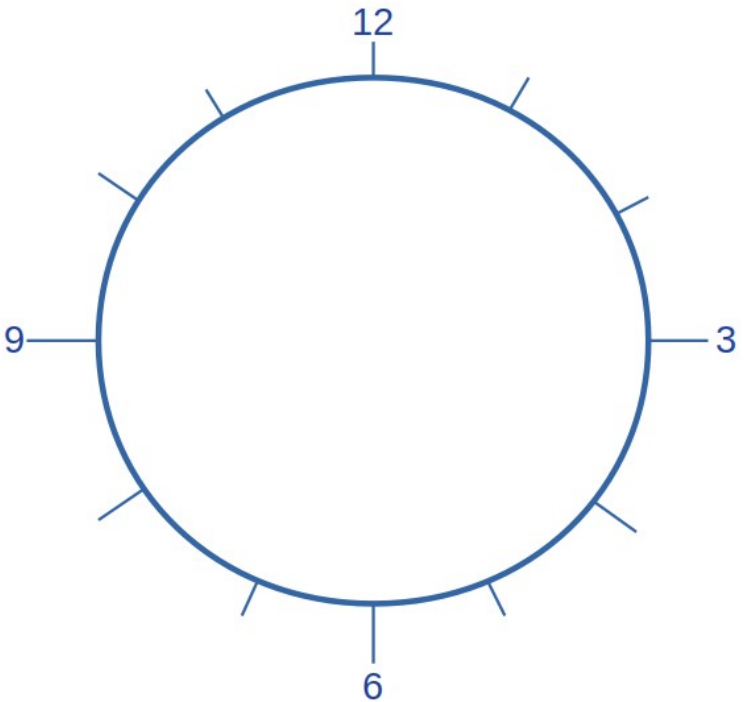
Em que situação $7+6=1$ faz sentido?

*FONTE: OBMEP

Vamos pensar juntos?!

Em que situação $7+6=1$ faz sentido?

Pensemos
num relógio!



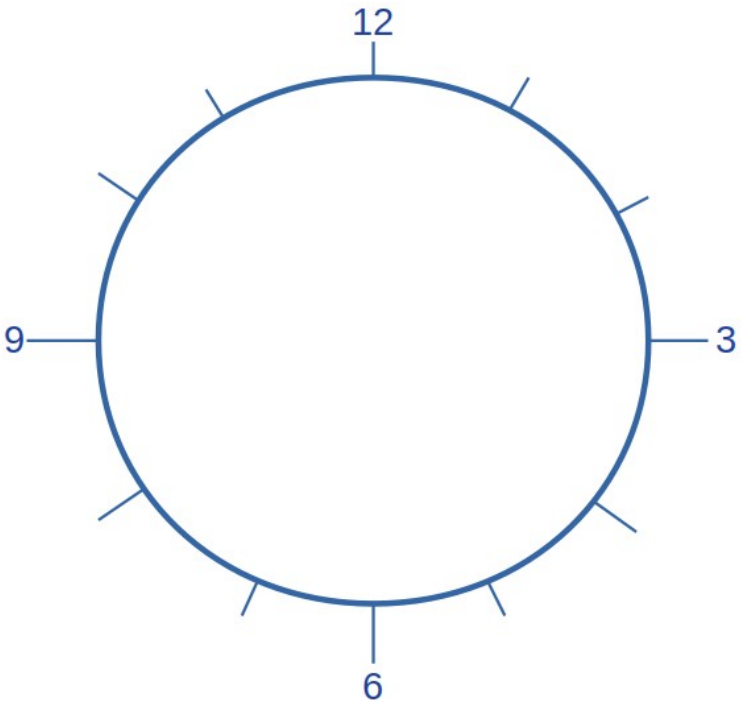
*FONTE: OBMEP

Vamos pensar juntos?!

Em que situação $7+6=1$ faz sentido?

Pensemos num relógio!

Vamos pensar nas aulas de uma escola que iniciam as 7h e que os alunos tem 6 horas de aula.



*FONTE: OBMEP

Vamos pensar juntos?!

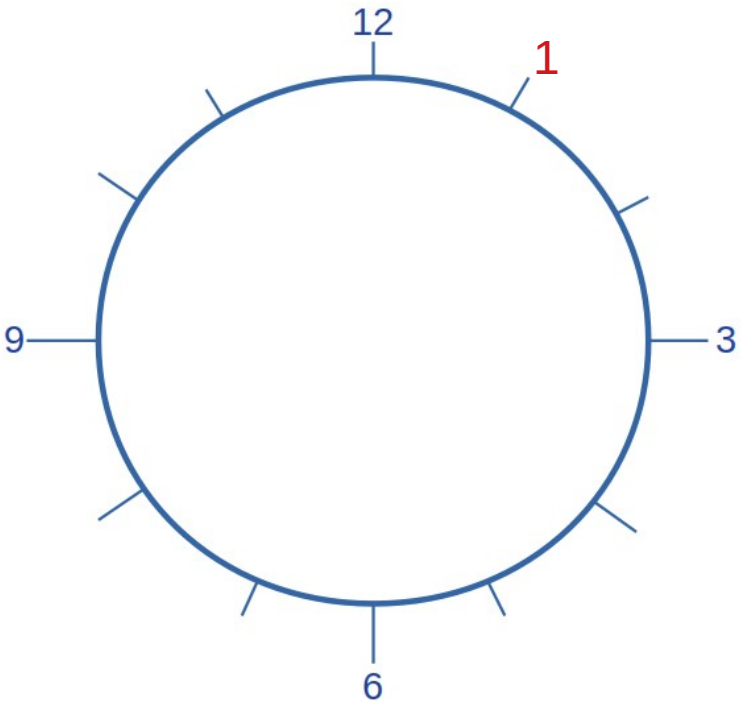
Em que situação $7+6=1$ faz sentido?

Pensemos
num relógio!

Vamos pensar
nas aulas de
uma escola que
iniciam as 7h e
que os alunos
tem 6 horas de
aula.

Aula terminam a 1h!

Possível solução!



*FONTE: OBMEP

Vamos pensar juntos?!

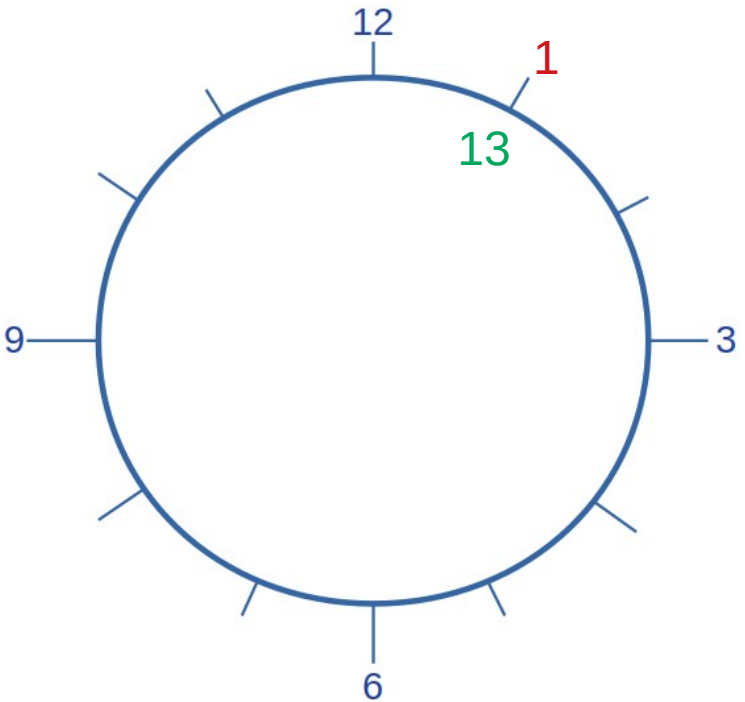
Em que situação $7+6=1$ faz sentido?

Pensemos num relógio!

Vamos pensar nas aulas de uma escola que iniciam as 7h e que os alunos tem 6 horas de aula.

Aula terminam a 1h!

Possível solução!



Alguns dizem 13h ao invés de 1h.

*FONTE: OBMEP

Vamos pensar juntos?!

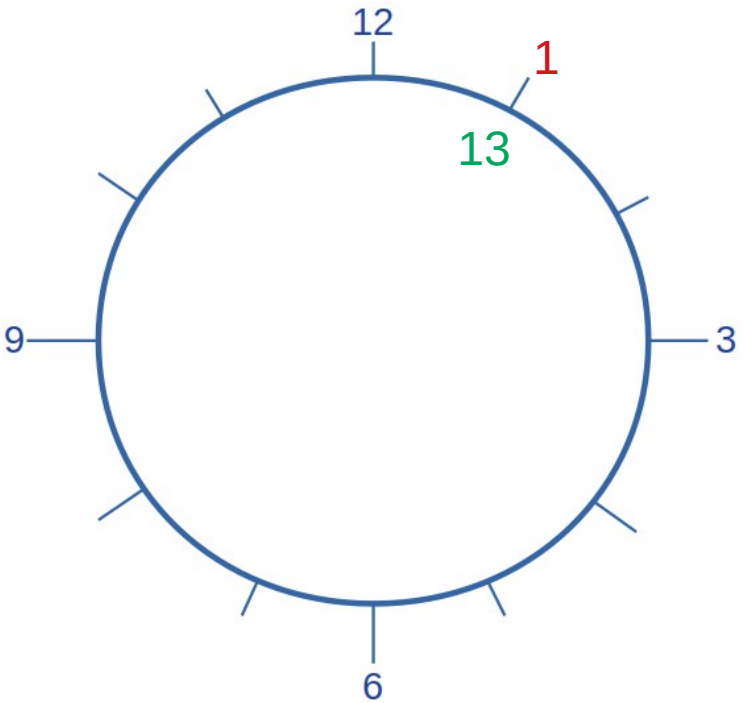
Em que situação $7+6=1$ faz sentido?

Pensemos num relógio!

Vamos pensar nas aulas de uma escola que iniciam as 7h e que os alunos tem 6 horas de aula.

Aula terminam a 1h!

Possível solução!



Alguns dizem 13h ao invés de 1h.

Matematicamente, pode-se dizer que:

$$13 \equiv 1 \, mod \, 12$$

*FONTE: OBMEP

Vamos pensar juntos?!

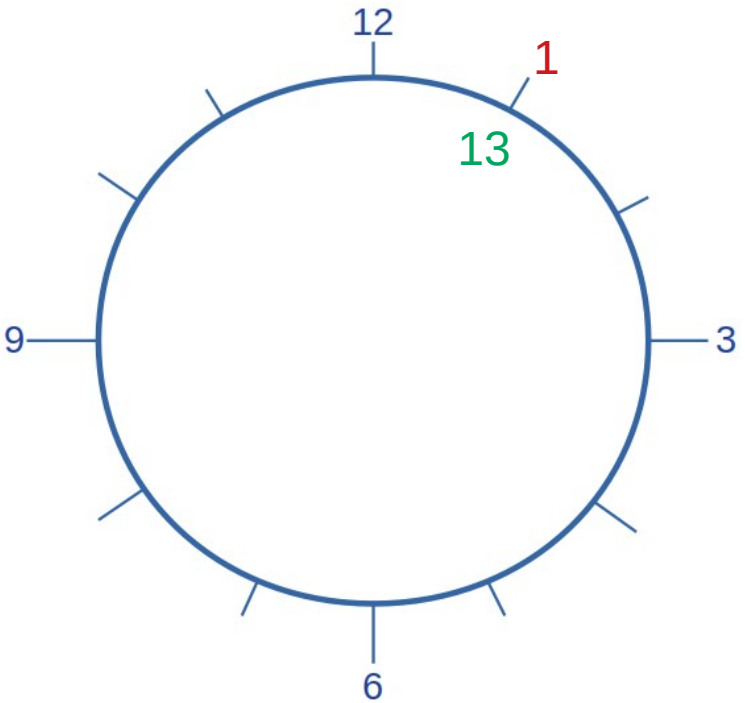
Em que situação $7+6=1$ faz sentido?

Pensemos num relógio!

Vamos pensar nas aulas de uma escola que iniciam as 7h e que os alunos tem 6 horas de aula.

Aula terminam a 1h!

Possível solução!



Alguns dizem 13h ao invés de 1h.

Matematicamente, pode-se dizer que:

$$13 \equiv 1 \, mod \, 12$$

Informa o número de partes que se divide o relógio

*FONTE: OBMEP

Vamos pensar juntos?!

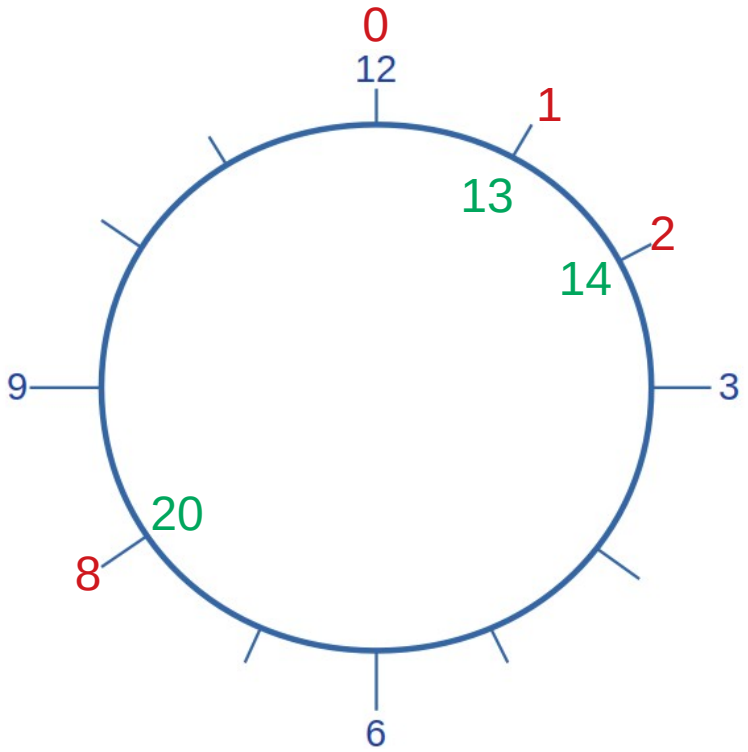
Em que situação $7+6=1$ faz sentido?

Pensemos num relógio!

Vamos pensar nas aulas de uma escola que iniciam as 7h e que os alunos tem 6 horas de aula.

Aula terminam a 1h!

Possível solução!



Alguns dizem 13h ao invés de 1h.

Matematicamente, pode-se dizer que:

$$13 \equiv 1 \, mod \, 12$$

Informa o número de partes que se divide o relógio

Logo,

$$14 \equiv 2 \, mod \, 12$$
$$20 \equiv 8 \, mod \, 12$$

*FONTE: OBMEP

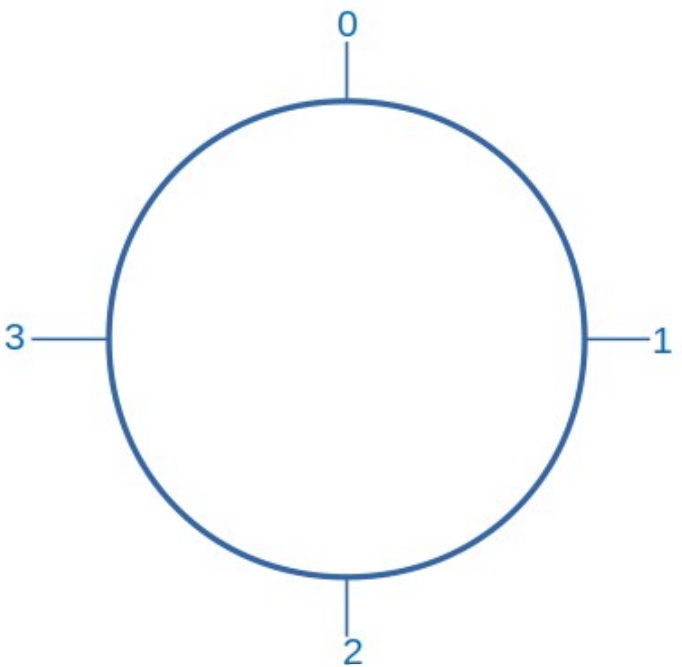
Vamos pensar juntos?!

E se dividirmos em 4 partes?

*FONTE: OBMEP

Vamos pensar juntos?!

E se dividirmos em 4 partes?

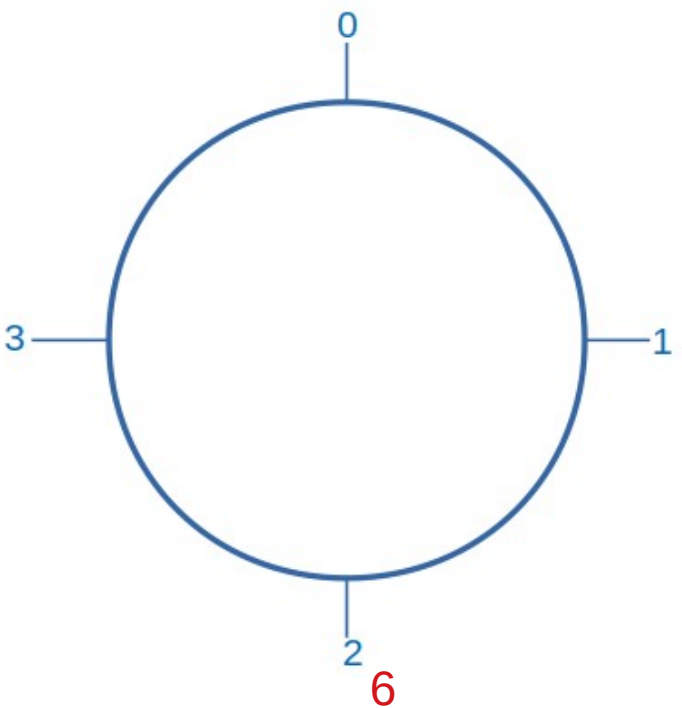


*FONTE: OBMEP

Vamos pensar juntos?!

E se dividirmos em 4 partes?

$6 \equiv 2 \, mod \, 4$



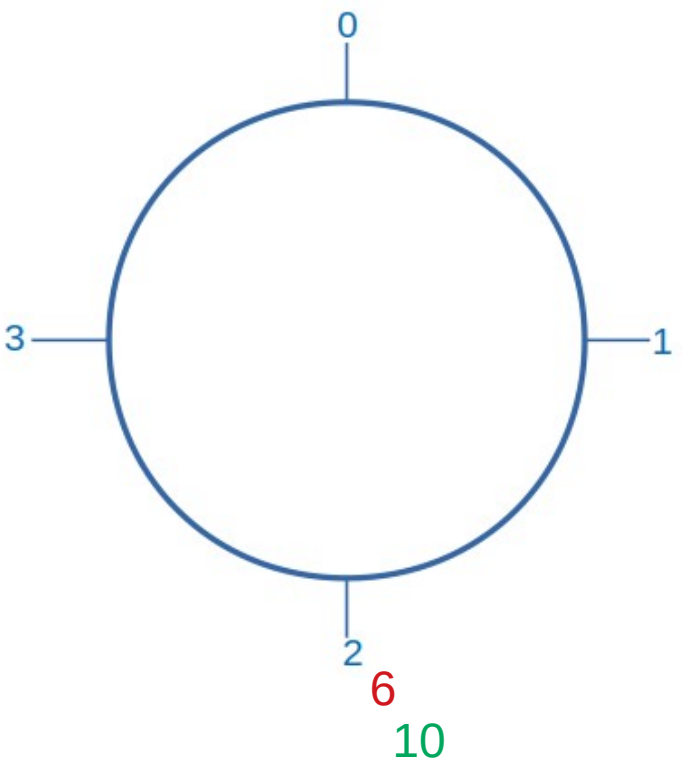
*FONTE: OBMEP

Vamos pensar juntos?!

E se dividirmos em 4 partes?

$6 \equiv 2 \, mod \, 4$

$10 \equiv 2 \, mod \, 4$



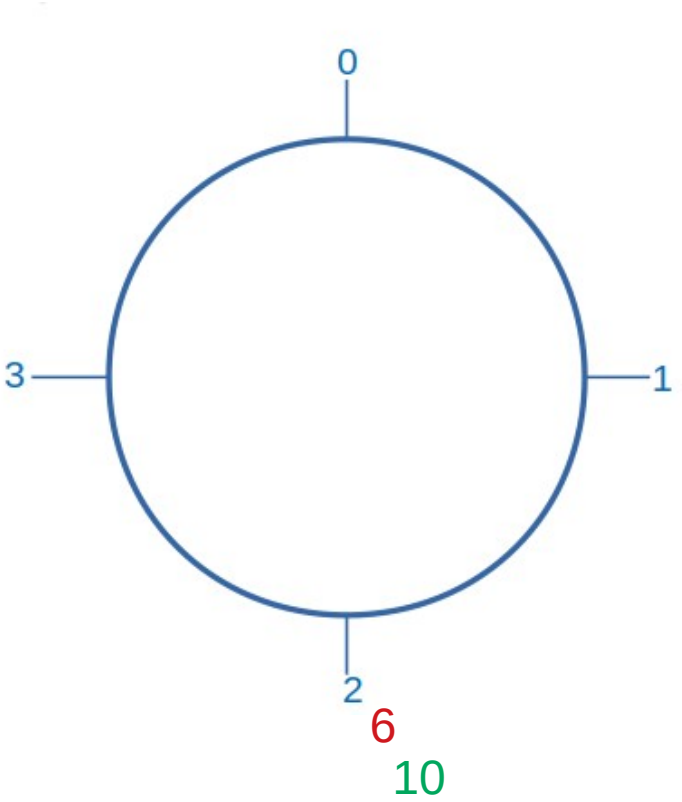
*FONTE: OBMEP

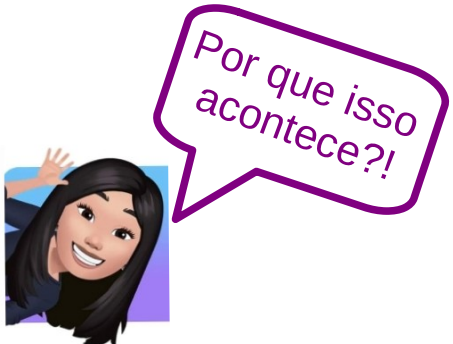
Vamos pensar juntos?!

E se dividirmos em 4 partes?

$6 \equiv 2 \, mod \, 4$

$10 \equiv 2 \, mod \, 4$





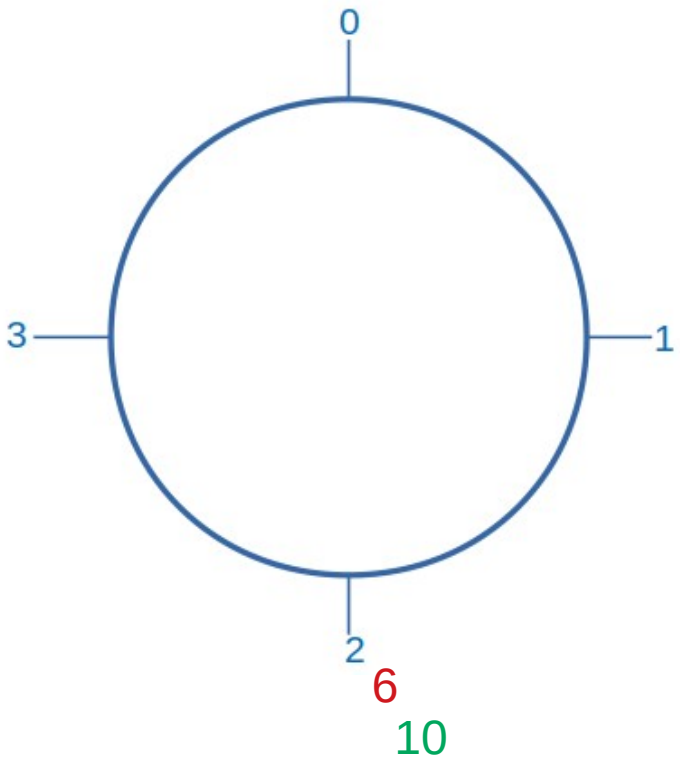
*FONTE: OBMEP

Vamos pensar juntos?!

E se dividirmos em 4 partes?

$6 \equiv 2 \, mod \, 4$

$10 \equiv 2 \, mod \, 4$



Por que isso acontece?!

Isto acontece por conta dos restos. O número 2 é o resto das divisões euclidianas de 2, 6 e 10 por 4. Logo eles fazem parte da mesma classe de equivalência. Vamos verificar?!

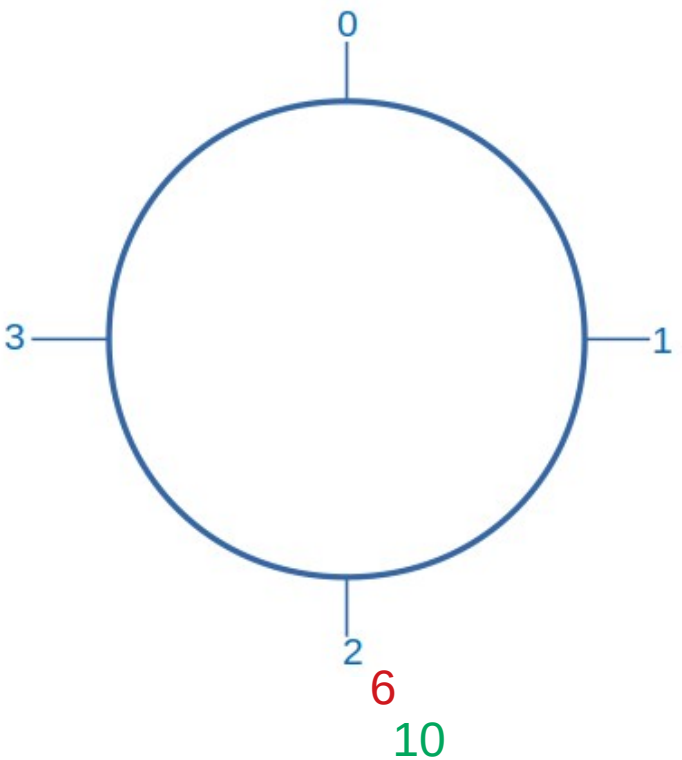
*FONTE: OBMEP

Vamos pensar juntos?!

E se dividirmos em 4 partes?

$6 \equiv 2 \, mod \, 4$

$10 \equiv 2 \, mod \, 4$



Método clássico:

$$\begin{array}{r|l} 6 & 4 \\ \cline{2-2} -4 & 1 \\ \cline{1-1} 2 & \end{array}$$

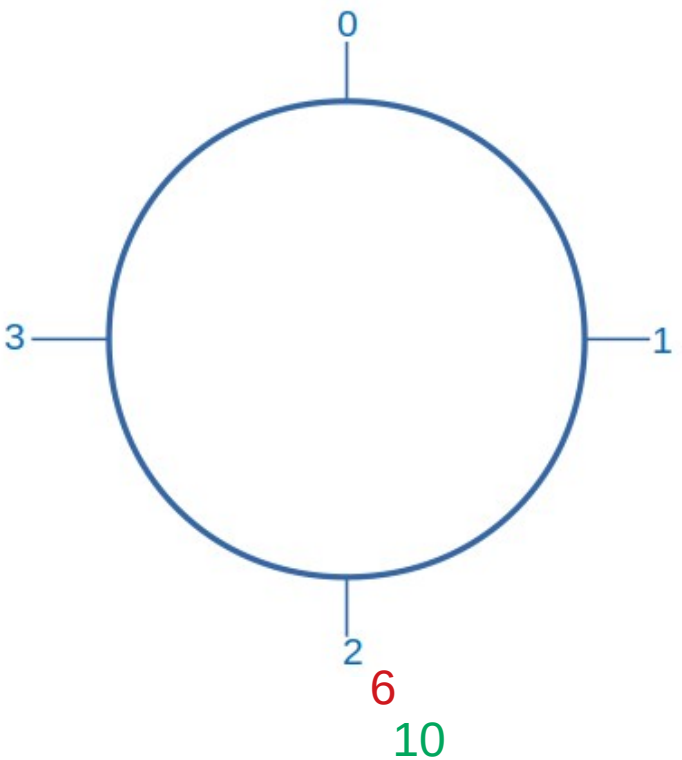
*FONTE: OBMEP

Vamos pensar juntos?!

E se dividirmos em 4 partes?

$6 \equiv 2 \, mod \, 4$

$10 \equiv 2 \, mod \, 4$



Método clássico:

$$\begin{array}{r|l} 6 & 4 \\ \cline{2-2} -4 & 1 \\ \cline{1-1} 2 & \end{array}$$

$$\begin{array}{r|l} 10 & 4 \\ \cline{2-2} -8 & 2 \\ \cline{1-1} 2 & \end{array}$$

*FONTE: OBMEP

Vamos pensar juntos?!

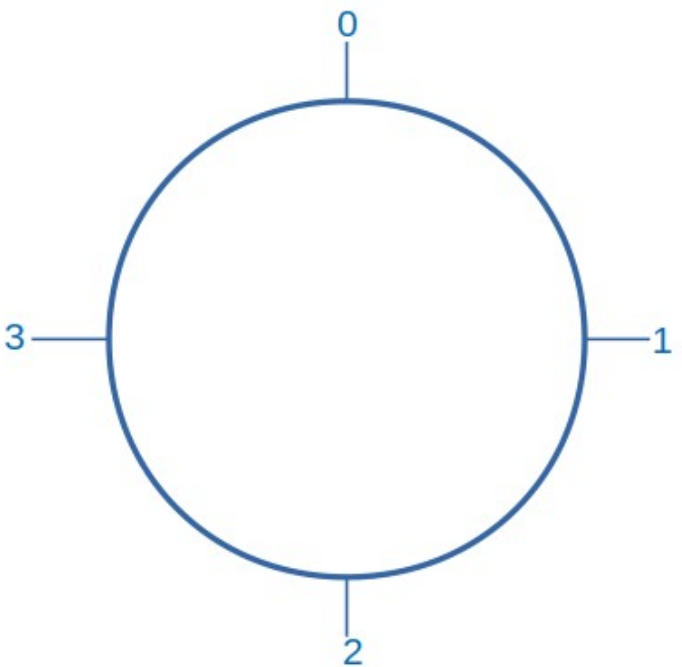
E se dividirmos em 4 partes?

$6 \equiv 2 \, mod \, 4$

$10 \equiv 2 \, mod \, 4$

Neste exemplo existem
4 classes de equivalência:
0, 1, 2, 3.

0 → resto 0
1 → resto 1
2 → resto 2
3 → resto 3



Método clássico:

$$\begin{array}{r|l} 6 & 4 \\ \cline{2-2} -4 & 1 \\ \cline{1-1} 2 & \end{array}$$

$$\begin{array}{r|l} 10 & 4 \\ \cline{2-2} -8 & 2 \\ \cline{1-1} 2 & \end{array}$$

*FONTE: OBMEP

Vamos pensar juntos?!

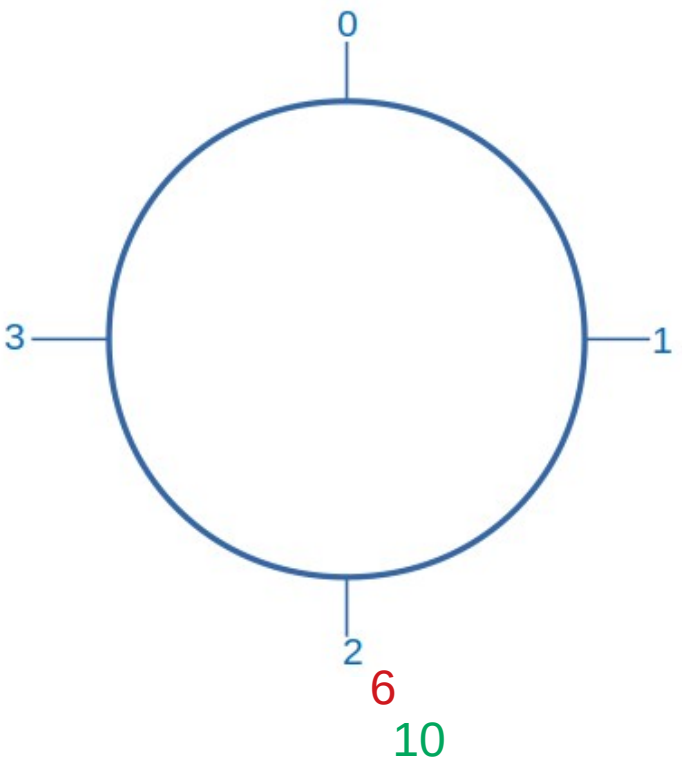
E se dividirmos em 4 partes?

$6 \equiv 2 \, mod \, 4$

$10 \equiv 2 \, mod \, 4$

Neste exemplo existem
4 classes de equivalência:
0, 1, 2, 3.

0 → resto 0
1 → resto 1
2 → resto 2
3 → resto 3



Assim, 6 e 10 pertencem à mesma classe de equivalência, pois deixam o mesmo resto na divisão por 4.

*FONTE: OBMEP

Vamos pensar juntos?!

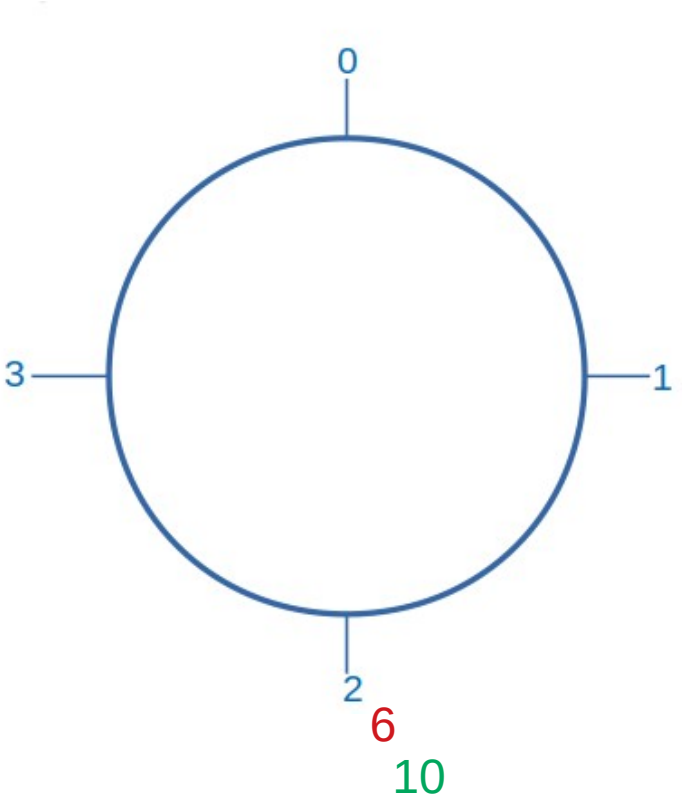
E se dividirmos em 4 partes?

$6 \equiv 2 \, mod \, 4$

$10 \equiv 2 \, mod \, 4$

Neste exemplo existem
4 classes de equivalência:
0, 1, 2, 3.

0 → resto 0
1 → resto 1
2 → resto 2
3 → resto 3



Assim, 6 e 10 pertencem à mesma classe de equivalência, pois deixam o mesmo resto na divisão por 4.

Logo,
6 , 10 e 2 são
congruentes mod 4

*FONTE: OBMEP

Congruência módulo n

DEFINIÇÃO: Seja $n \in \mathbb{Z}$, $n>1$. Diz-se que dois números $a, b \in \mathbb{Z}$ são congruentes módulo n, se os restos se sua divisão euclidiana por n são iguais.

$$a \equiv b \pmod{n}$$

ou

$$a \equiv b \mod n$$

Obs: $n>1$ pois $7 \equiv 0 \mod 1$

Congruência módulo n

DEFINIÇÃO: Seja $n \in \mathbb{Z}$, $n>1$. Diz-se que dois números $a, b \in \mathbb{Z}$ são congruentes módulo n, se os restos se sua divisão euclidiana por n são iguais.

$$a \equiv b \pmod{n}$$

ou

$$a \equiv b \mod n$$

Obs: existem autores que utilizam a notação $a \equiv b [n]$. Não a utilizaremos aqui.

Obs: $n>1$ pois $7 \equiv 0 \mod 1$

Congruência módulo n

DEFINIÇÃO: Seja $n \in \mathbb{Z}$, $n>1$. Diz-se que dois números $a, b \in \mathbb{Z}$ são congruentes módulo n, se os restos se sua divisão euclidiana por n são iguais.

$$a \equiv b \pmod{n}$$

EXEMPLOS:

a) $-56 \equiv -11 \pmod{9}$

Congruência módulo n

DEFINIÇÃO: Seja $n \in \mathbb{Z}$, $n>1$. Diz-se que dois números $a, b \in \mathbb{Z}$ são congruentes módulo n, se os restos se sua divisão euclidiana por n são iguais.

$$a \equiv b \pmod{n}$$

EXEMPLOS:

a) $-56 \equiv -11 \pmod{9}$

$$\begin{array}{r|l} -56 & 9 \\ \underline{+63} & -7 \\ +7 & \end{array}$$

Congruência módulo n

DEFINIÇÃO: Seja $n \in \mathbb{Z}$, $n>1$. Diz-se que dois números $a, b \in \mathbb{Z}$ são congruentes módulo n, se os restos se sua divisão euclidiana por n são iguais.

$$a \equiv b \pmod{n}$$

EXEMPLOS:

a) $-56 \equiv -11 \pmod{9}$

$$\begin{array}{r|l} -56 & 9 \\ \underline{+63} & -7 \\ +7 & \end{array} \qquad \begin{array}{r|l} -11 & 9 \\ \underline{+18} & -2 \\ +7 & \end{array}$$

Congruência módulo n

DEFINIÇÃO: Seja $n \in \mathbb{Z}$, $n>1$. Diz-se que dois números $a, b \in \mathbb{Z}$ são congruentes módulo n, se os restos se sua divisão euclidiana por n são iguais.

$$a \equiv b \pmod{n}$$

EXEMPLOS:

a) $-56 \equiv -11 \pmod{9}$

$$\begin{array}{r|l} -56 & 9 \\ \underline{+63} & -7 \\ +7 & \end{array}$$

$$\begin{array}{r|l} -11 & 9 \\ \underline{+18} & -2 \\ +7 & \end{array}$$

$$-56 = (-7)\cdot 9 + 7$$
$$-11 = (-2)\cdot 9 + 7$$

Congruência módulo n

DEFINIÇÃO: Seja $n \in \mathbb{Z}$, $n>1$. Diz-se que dois números $a, b \in \mathbb{Z}$ são congruentes módulo n, se os restos se sua divisão euclidiana por n são iguais.

$$a \equiv b \pmod{n}$$

EXEMPLOS:

a) $-56 \equiv -11 \pmod{9}$

Sua vez!

b) $-31 \_\_\_ 11 \pmod{7}$

O QUE VOCÊ ACHA?
SÃO CONGRUENTES?

Congruência módulo n

DEFINIÇÃO: Seja $n \in \mathbb{Z}$, $n>1$. Diz-se que dois números $a, b \in \mathbb{Z}$ são congruentes módulo n, se os restos se sua divisão euclidiana por n são iguais.

$$a \equiv b \pmod{n}$$

EXEMPLOS:

a) $-56 \equiv -11 \pmod{9}$

Sua vez!

b) $-31 \_\_\_ 11 \pmod{7}$

$$-31 = 7q + r$$

$$11 = 7q + r$$

Congruência módulo n

DEFINIÇÃO: Seja $n \in \mathbb{Z}$, $n>1$. Diz-se que dois números são congruentes módulo n, se os restos se sua divisão euclidiana por n são iguais.

$$a \equiv b \pmod{n}$$

EXEMPLOS:

a) $-56 \equiv -11 \pmod{9}$

Sua vez!

b) $-31 \_\_\_ 11 \pmod{7}$

$$-31 = 7q + r \quad \Rightarrow \quad -31 = 7(-5) + 4$$

$$11 = 7q + r$$

Congruência módulo n

DEFINIÇÃO: Seja $n \in \mathbb{Z}$, $n>1$. Diz-se que dois números $a, b \in \mathbb{Z}$ são congruentes módulo n, se os restos se sua divisão euclidiana por n são iguais.

$$a \equiv b \pmod{n}$$

EXEMPLOS:

a) $-56 \equiv -11 \pmod{9}$

Sua vez!

b) $-31 \_\_\_ 11 \pmod{7}$

$$-31 = 7q + r \quad \Rightarrow \quad -31 = 7(-5) + 4$$

$$11 = 7q + r \quad \Rightarrow \quad 11 = 7(1) + 4$$

Congruência módulo n

DEFINIÇÃO: Seja $n \in \mathbb{Z}$, $n>1$. Diz-se que dois números $a, b \in \mathbb{Z}$ são congruentes módulo n, se os restos se sua divisão euclidiana por n são iguais.

$$a \equiv b \pmod{n}$$

EXEMPLOS:

a) $-56 \equiv -11 \pmod{9}$

Sua vez!

b) $-31 \equiv \ 11 \pmod{7}$

$$-31 = 7q + r \quad \Rightarrow \quad -31 = 7(-5) + 4$$

$$11 = 7q + r \quad \Rightarrow \quad 11 = 7(1) + 4$$

Congruência módulo n

Voltemos à idéia inicial!

$$7+6=1$$

Matemáticamente:

$$7+6=13$$

Logo,

$$7+6\equiv 1\,(mod\,12)$$

Congruência módulo n

PROPOSIÇÃO: Sejam $a, b, n \in \mathbb{Z}$, $n > 1$, temos:

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad n \mid a - b$$

ou seja, $a \equiv b \pmod{n} \quad \Leftrightarrow \quad a - b$ é divisível por n.

Congruência módulo n

PROPOSIÇÃO: Sejam $a, b, n \in \mathbb{Z}$, $n > 1$, temos:

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad n \mid a-b$$

ou seja, $a \equiv b \pmod{n} \quad \Leftrightarrow \quad a-b$ é divisível por n.

Sua vez!

EXEMPLOS: Verifique se as afirmações a seguir são verdadeiras:

a) $1 \equiv 7 \pmod{6}$

b) $7 \equiv -5 \pmod{6}$

c) $-5 \equiv -11 \pmod{6}$

Congruência módulo n

PROPOSIÇÃO: Sejam $a, b, n \in \mathbb{Z}$, $n > 1$, temos:

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad n \mid a-b$$

ou seja, $a \equiv b \pmod{n} \quad \Leftrightarrow \quad a-b$ é divisível por n.

Sua vez!

EXEMPLOS: Verifique se as afirmações a seguir são verdadeiras:

a) $1 \equiv 7 \pmod{6} \longrightarrow 1-7=-6$

b) $7 \equiv -5 \pmod{6}$

c) $-5 \equiv -11 \pmod{6}$

Congruência módulo n

PROPOSIÇÃO: Sejam $a, b, n \in \mathbb{Z}$, $n > 1$, temos:

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad n \mid a - b$$

ou seja, $a \equiv b \pmod{n} \quad \Leftrightarrow \quad a - b$ é divisível por n.

Sua vez!

EXEMPLOS: Verifique se as afirmações a seguir são verdadeiras:

a) $1 \equiv 7 \pmod{6} \longrightarrow 1 - 7 = -6 \longrightarrow +6 \mid -6$

b) $7 \equiv -5 \pmod{6}$

c) $-5 \equiv -11 \pmod{6}$

Congruência módulo n

PROPOSIÇÃO: Sejam $a, b, n \in \mathbb{Z}$, $n > 1$, temos:

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad n \mid a-b$$

ou seja, $a \equiv b \pmod{n} \quad \Leftrightarrow \quad a-b$ é divisível por n.

Sua vez!

EXEMPLOS: Verifique se as afirmações a seguir são verdadeiras:

a) $1 \equiv 7 \pmod{6} \longrightarrow 1-7=-6 \longrightarrow +6 \mid -6$ Ok!

b) $7 \equiv -5 \pmod{6}$

c) $-5 \equiv -11 \pmod{6}$

Congruência módulo n

PROPOSIÇÃO: Sejam $a, b, n \in \mathbb{Z}$, $n > 1$, temos:

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad n \mid a-b$$

ou seja, $a \equiv b \pmod{n} \quad \Leftrightarrow \quad a-b$ é divisível por n.

Sua vez!

EXEMPLOS: Verifique se as afirmações a seguir são verdadeiras:

a) $1 \equiv 7 \pmod{6} \longrightarrow 1-7=-6 \longrightarrow +6 \mid -6$ Ok!

b) $7 \equiv -5 \pmod{6} \longrightarrow 7-(-5)=12 \longrightarrow +6 \mid 12$ Ok!

c) $-5 \equiv -11 \pmod{6}$

Congruência módulo n

PROPOSIÇÃO: Sejam $a, b, n \in \mathbb{Z}$, $n > 1$, temos:

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad n \mid a-b$$

ou seja, $a \equiv b \pmod{n} \quad \Leftrightarrow \quad a-b$ é divisível por n.

Sua vez!

EXEMPLOS: Verifique se as afirmações a seguir são verdadeiras:

a) $1 \equiv 7 \pmod{6} \longrightarrow 1-7=-6 \longrightarrow +6 \mid -6$ Ok!

b) $7 \equiv -5 \pmod{6} \longrightarrow 7-(-5)=12 \longrightarrow +6 \mid 12$ Ok!

c) $-5 \equiv -11 \pmod{6} \longrightarrow -5-(-11)=6 \longrightarrow 6 \mid 6$ Ok!

Congruência módulo n

PROPOSIÇÃO: Sejam $a, b, n \in \mathbb{Z}$, $n > 1$, temos:

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad n \mid a-b$$

ou seja, $a \equiv b \pmod{n} \quad \Leftrightarrow \quad a-b$ é divisível por n.

Sua vez!

EXEMPLOS: Verifique se as afirmações a seguir são verdadeiras:

a) $1 \equiv 7 \pmod{6} \longrightarrow 1-7=-6 \longrightarrow +6 \mid -6$ Ok!

b) $7 \equiv -5 \pmod{6} \longrightarrow 7-(-5)=12 \longrightarrow +6 \mid 12$ Ok!

c) $-5 \equiv -11 \pmod{6} \longrightarrow -5-(-11)=6 \longrightarrow 6 \mid 6$ Ok!

$$1 \equiv 7 \equiv -5 \equiv -11 \pmod{6}$$

Congruência módulo n

PROPOSIÇÃO: Sejam $a, b, n \in \mathbb{Z}$, $n > 1$, temos:

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad n \mid a-b$$

ou seja, $a \equiv b \pmod{n} \quad \Leftrightarrow \quad a-b$ é divisível por n.

Obs:
Para:

$$n=0 \quad \Rightarrow \quad a \equiv b \pmod{0} \quad \Leftrightarrow \quad a=b$$

$$n=1 \quad \Rightarrow \quad a \equiv b \pmod{1} \quad \text{sempre!}$$

$$n=2 \quad \Rightarrow \quad a \equiv b \pmod{2} \quad \Leftrightarrow \quad a \ \ e \ \ b$$ são ambos pares ou ambos ímpares

Sua vez!

EXEMPLO: Verifique

a) $a=11 \ , \ b=3 \ , \ n=2$

b) $a=17 \ , \ b=11 \ , \ n=3$

c) $a=17 \ , \ b=11 \ , \ n=5$

Sua vez!

EXEMPLO: Verifique

a) $a=11 \ , \ b=3 \ , \ n=2 \quad \Rightarrow \quad 11-3=8$

b) $a=17 \ , \ b=11 \ , \ n=3$

c) $a=17 \ , \ b=11 \ , \ n=5$

Sua vez!

EXEMPLO: Verifique

a) $a=11 \;,\; b=3 \;,\; n=2 \quad \Rightarrow \quad 11-3=8 \;,\; 2|8$

b) $a=17 \;,\; b=11 \;,\; n=3$

c) $a=17 \;,\; b=11 \;,\; n=5$

Sua vez!

EXEMPLO: Verifique

a) $a=11 \;,\; b=3 \;,\; n=2 \quad \Rightarrow \quad 11-3=8 \;,\; 2|8 \;,\; 2|(11-3)$

b) $a=17 \;,\; b=11 \;,\; n=3$

c) $a=17 \;,\; b=11 \;,\; n=5$

Sua vez!

EXEMPLO: Verifique

a) $a=11 \;,\; b=3 \;,\; n=2 \quad \Rightarrow \quad 11-3=8 \;,\; 2|8 \;,\; 2|(11-3)$

logo $11 \equiv 3 \pmod 2$

b) $a=17 \;,\; b=11 \;,\; n=3$

c) $a=17 \;,\; b=11 \;,\; n=5$

Sua vez!

EXEMPLO: Verifique

a) $a=11 \;,\; b=3 \;,\; n=2 \quad \Rightarrow \quad 11-3=8 \;,\; 2|8 \;,\; 2|(11-3)$

logo $11\equiv 3\,(mod\,2)$

b) $a=17 \;,\; b=11 \;,\; n=3 \quad \Rightarrow \quad 17-11=6 \quad \Rightarrow \quad 3|6$

logo $17\equiv 11\,(mod\,3)$

c) $a=17 \;,\; b=11 \;,\; n=5$

Sua vez!

EXEMPLO: Verifique

a) $a=11 \;,\; b=3 \;,\; n=2 \quad \Rightarrow \quad 11-3=8 \;,\; 2|8 \;,\; 2|(11-3)$

logo $11 \equiv 3 \pmod 2$

b) $a=17 \;,\; b=11 \;,\; n=3 \quad \Rightarrow \quad 17-11=6 \quad \Rightarrow \quad 3|6$

logo $17 \equiv 11 \pmod 3$

c) $a=17 \;,\; b=11 \;,\; n=5 \quad \Rightarrow \quad 17-11=6 \quad \Rightarrow \quad 5 \nmid 6$

logo $17 \not\equiv 11 \pmod 5$

Congruência módulo n

PROPOSIÇÃO: Seja $n \in \mathbb{Z}$ e n positivo. Os inteiros a e b são congruentes módulo n se, e somente se, existe um inteiro k de forma que:

$$a = b + k \cdot n$$

Congruência módulo n

PROPOSIÇÃO: Seja $n \in \mathbb{Z}$ e n positivo. Os inteiros a e b são congruentes módulo n se, e somente se, existe um inteiro k de forma que:

$$a = b + k \cdot n$$

EXEMPLO:

$$73 \equiv 13 \pmod{5}$$

Congruência módulo n

PROPOSIÇÃO: Seja $n \in \mathbb{Z}$ e n positivo. Os inteiros a e b são congruentes módulo n se, e somente se, existe um inteiro k de forma que:

$$a = b + k \cdot n$$

EXEMPLO:

$$73 \equiv 13 \pmod 5$$

$$73 = 13 + 5k$$

Congruência módulo n

PROPOSIÇÃO: Seja $n \in \mathbb{Z}$ e n positivo. Os inteiros a e b são congruentes módulo n se, e somente se, existe um inteiro k de forma que:

$$a = b + k \cdot n$$

EXEMPLO:

$$73 \equiv 13 \pmod{5}$$

$$73 = 13 + 5k$$

$$5 \mid (73 - 13) \quad \Rightarrow \quad 5 \mid 60 \quad \Rightarrow \quad 12 = k$$

Congruência módulo n

PROPOSIÇÃO: Seja $n \in \mathbb{Z}$ e n positivo. Os inteiros a e b são congruentes módulo n se, e somente se, existe um inteiro k de forma que:

$$a = b + k \cdot n$$

EXEMPLO:

$$73 \equiv 13 \pmod{5}$$

$$73 = 13 + 5k$$

$$5 \mid (73 - 13) \quad \Rightarrow \quad 5 \mid 60 \quad \Rightarrow \quad 12 = k$$

$$73 = 13 + 12 \cdot 5$$

Congruência módulo n

PROPRIEDADES: Seja $n \in \mathbb{Z}$, $n>1$, um inteiro fixo e $\forall a, b, c, d, \in \mathbb{Z}$, as seguintes propriedades são válidas:

i) $a \equiv a \pmod{n}$

Congruência módulo n

PROPRIEDADES: Seja $n \in \mathbb{Z}$, $n>1$, um inteiro fixo e $\forall a, b, c, d, \in \mathbb{Z}$, as seguintes propriedades são válidas:

i) $a \equiv a \pmod{n}$

ii) se $a \equiv b \pmod{n} \quad \Rightarrow \quad b \equiv a \pmod{n}$

Congruência módulo n

PROPRIEDADES: Seja $n \in \mathbb{Z}$, $n>1$, um inteiro fixo e $\forall\, a, b, c, d, \in \mathbb{Z}$, as seguintes propriedades são válidas:

i) $a \equiv a \pmod{n}$

ii) se $a \equiv b \pmod{n} \quad \Rightarrow \quad b \equiv a \pmod{n}$

iii) se $a \equiv b \pmod{n} \quad$ e $\quad b \equiv c \pmod{n} \quad \Rightarrow \quad a \equiv c \pmod{n}$

Congruência módulo n

PROPRIEDADES: Seja $n \in \mathbb{Z}$, $n>1$, um inteiro fixo e $\forall a, b, c, d, \in \mathbb{Z}$, as seguintes propriedades são válidas:

i) $a \equiv a \pmod{n}$

ii) se $a \equiv b \pmod{n} \quad \Rightarrow \quad b \equiv a \pmod{n}$

iii) se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \quad \Rightarrow \quad a \equiv c \pmod{n}$

EXEMPLO: $5 \equiv 9 \pmod{4}$ e $9 \equiv 13 \pmod{4}$

Congruência módulo n

PROPRIEDADES: Seja $n \in \mathbb{Z}$, $n>1$, um inteiro fixo e $\forall a, b, c, d, \in \mathbb{Z}$, as seguintes propriedades são válidas:

i) $a \equiv a \pmod{n}$

ii) se $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

iii) se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

EXEMPLO: $5 \equiv 9 \pmod{4}$ e $9 \equiv 13 \pmod{4} \Rightarrow 5 \equiv 13 \bmod 4$

Divisões por 4 com resto 1

Congruência módulo n

PROPRIEDADES: Seja $n \in \mathbb{Z}$, $n>1$, um inteiro fixo e $\forall a, b, c, d, \in \mathbb{Z}$, as seguintes propriedades são válidas:

i) $a \equiv a \pmod{n}$

ii) se $a \equiv b \pmod{n} \quad \Rightarrow \quad b \equiv a \pmod{n}$

iii) se $a \equiv b \pmod{n} \quad \text{e} \quad b \equiv c \pmod{n} \quad \Rightarrow \quad a \equiv c \pmod{n}$

iv) se $a \equiv b \pmod{n} \quad \text{e} \quad c \equiv d \pmod{n} \quad \Rightarrow \begin{cases} a+c \equiv b+d \pmod{n} \\ a \cdot c \equiv b \cdot d \pmod{n} \end{cases}$

Congruência módulo n

PROPRIEDADES: Seja $n \in \mathbb{Z}$, $n>1$, um inteiro fixo e $\forall a, b, c, d, \in \mathbb{Z}$, as seguintes propriedades são válidas:

i) $a \equiv a \pmod{n}$

ii) se $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

iii) se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

iv) se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n} \Rightarrow \begin{cases} a+c \equiv b+d \pmod{n} \\ a \cdot c \equiv b \cdot d \pmod{n} \end{cases}$

EXEMPLO:

$1 \equiv 5 \pmod{4}$ *e* $6 \equiv 10 \pmod{4}$

Divisões por 4 com resto 1

Divisões por 4 com resto 2

Congruência módulo n

PROPRIEDADES: Seja $n \in \mathbb{Z}$, $n>1$, um inteiro fixo e $\forall a, b, c, d, \in \mathbb{Z}$, as seguintes propriedades são válidas:

i) $a \equiv a \pmod{n}$

ii) se $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

iii) se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

iv) se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n} \Rightarrow \begin{cases} a+c \equiv b+d \pmod{n} \\ a \cdot c \equiv b \cdot d \pmod{n} \end{cases}$

EXEMPLO:

$1 \equiv 5 \pmod{4}$ *e* $6 \equiv 10 \pmod{4} \Rightarrow 1+6 \equiv 5+10 \bmod 4$

Divisões por 4 com resto 1

Divisões por 4 com resto 2

Congruência módulo n

PROPRIEDADES: Seja $n \in \mathbb{Z}$, $n>1$, um inteiro fixo e $\forall a, b, c, d, \in \mathbb{Z}$, as seguintes propriedades são válidas:

i) $a \equiv a \pmod{n}$

ii) se $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

iii) se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

iv) se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n} \Rightarrow \begin{cases} a+c \equiv b+d \pmod{n} \\ a \cdot c \equiv b \cdot d \pmod{n} \end{cases}$

EXEMPLO:

$$1 \equiv 5 \pmod{4} \quad e \quad 6 \equiv 10 \pmod{4} \Rightarrow 1+6 \equiv 5+10 \bmod 4 \rightarrow 7 \equiv 15 \bmod 4$$

Divisões por 4 com resto 1

Divisões por 4 com resto 2

Divisões por 4 com resto 3

Congruência módulo n

PROPRIEDADES: Seja $n \in \mathbb{Z}$, $n>1$, um inteiro fixo e $\forall a, b, c, d, \in \mathbb{Z}$, as seguintes propriedades são válidas:

i) $a \equiv a \pmod{n}$

ii) se $a \equiv b \pmod{n} \quad \Rightarrow \quad b \equiv a \pmod{n}$

iii) se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \quad \Rightarrow \quad a \equiv c \pmod{n}$

iv) se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n} \quad \Rightarrow \begin{cases} a+c \equiv b+d \pmod{n} \\ a \cdot c \equiv b \cdot d \pmod{n} \end{cases}$

v) se $a \equiv b \pmod{n} \Rightarrow \begin{cases} a+c \equiv b+c \pmod{n} \\ a \cdot c \equiv b \cdot c \pmod{n} \end{cases}$

Congruência módulo n

PROPRIEDADES: Seja $n \in \mathbb{Z}$, $n>1$, um inteiro fixo e $\forall a, b, c, d, \in \mathbb{Z}$, as seguintes propriedades são válidas:

i) $a \equiv a \pmod{n}$

ii) se $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

iii) se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

iv) se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n} \Rightarrow \begin{cases} a+c \equiv b+d \pmod{n} \\ a \cdot c \equiv b \cdot d \pmod{n} \end{cases}$

v) se $a \equiv b \pmod{n} \Rightarrow \begin{cases} a+c \equiv b+c \pmod{n} \\ a \cdot c \equiv b \cdot c \pmod{n} \end{cases}$

EXEMPLO: $2 \equiv 6 \pmod{4}$

Divisões por 4
com resto 2

Congruência módulo n

PROPRIEDADES: Seja $n \in \mathbb{Z}$, $n>1$, um inteiro fixo e $\forall a, b, c, d, \in \mathbb{Z}$, as seguintes propriedades são válidas:

i) $a \equiv a \pmod{n}$

ii) se $a \equiv b \pmod{n} \quad \Rightarrow \quad b \equiv a \pmod{n}$

iii) se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \quad \Rightarrow \quad a \equiv c \pmod{n}$

iv) se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n} \quad \Rightarrow \begin{cases} a+c \equiv b+d \pmod{n} \\ a \cdot c \equiv b \cdot d \pmod{n} \end{cases}$

v) se $a \equiv b \pmod{n} \Rightarrow \begin{cases} a+c \equiv b+c \pmod{n} \\ a \cdot c \equiv b \cdot c \pmod{n} \end{cases}$

EXEMPLO: $2 \equiv 6 \pmod{4} \Rightarrow 2+3 \equiv 6+3 \bmod 4$

Divisões por 4
com resto 2

Congruência módulo n

PROPRIEDADES: Seja $n \in \mathbb{Z}$, $n>1$, um inteiro fixo e $\forall a, b, c, d, \in \mathbb{Z}$, as seguintes propriedades são válidas:

i) $a \equiv a \pmod{n}$

ii) se $a \equiv b \pmod{n} \quad \Rightarrow \quad b \equiv a \pmod{n}$

iii) se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \quad \Rightarrow \quad a \equiv c \pmod{n}$

iv) se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n} \quad \Rightarrow \begin{cases} a+c \equiv b+d \pmod{n} \\ a \cdot c \equiv b \cdot d \pmod{n} \end{cases}$

v) se $a \equiv b \pmod{n} \Rightarrow \begin{cases} a+c \equiv b+c \pmod{n} \\ a \cdot c \equiv b \cdot c \pmod{n} \end{cases}$

EXEMPLO: $2 \equiv 6 \pmod{4} \Rightarrow 2+3 \equiv 6+3 \bmod 4 \rightarrow 5 \equiv 9 \bmod 4$

Divisões por 4 com resto 2

Divisões por 4 com resto 1

Congruência módulo n

PROPRIEDADES: Seja $n \in \mathbb{Z}$, $n>1$, um inteiro fixo e $\forall a, b, c, d, \in \mathbb{Z}$, as seguintes propriedades são válidas:

i) $a \equiv a \pmod{n}$

ii) se $a \equiv b \pmod{n} \quad \Rightarrow \quad b \equiv a \pmod{n}$

iii) se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \quad \Rightarrow \quad a \equiv c \pmod{n}$

iv) se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n} \quad \Rightarrow \begin{cases} a+c \equiv b+d \pmod{n} \\ a \cdot c \equiv b \cdot d \pmod{n} \end{cases}$

v) se $a \equiv b \pmod{n} \Rightarrow \begin{cases} a+c \equiv b+c \pmod{n} \\ a \cdot c \equiv b \cdot c \pmod{n} \end{cases}$

vi) se $a \equiv b \pmod{n} \quad \Rightarrow a^k \equiv b^k \pmod{n}$, $\forall k \in \mathbb{Z}$, $z>0$

Congruência módulo n

Proposição 1:
Seja $n \in \mathbb{N}$ e $a, b, c, d \in \mathbb{Z}$. Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então:
(a) $a \pm c \equiv b \pm d \pmod{n}$;
(b) $ac \equiv bd \pmod{n}$.

Demonstração: (a) Por hipótese temos que $a - b = nk_1$ e $c - d = nk_2$. Somando as duas expressões obtemos $(a + c) - (b + d) = n(k_1 + k_2)$. Portanto, $a + c \equiv b + d \pmod{n}$. De forma análoga, fazendo a subtração entre as duas expressões acima obtemos $a - c \equiv b - d \pmod{n}$.

(b) Além disso, multiplicando $a = b + nk_1$ e $c = d + nk_2$, temos

$$\begin{aligned} ac &= (b + nk_1)(d + nk_2) \\ &= bd + n(bk_2 + dk_1 + nk_1k_2) \\ &= bd + nk_3. \end{aligned}$$

Portanto, $ac \equiv bd \pmod{n}$.

Congruência módulo n

Proposição 2:
Se $(c, n) = g$, então

$$ac \equiv bc \pmod{n}$$

se, e somente se,

$$a \equiv b \pmod{n/g}.$$

Demonstração: ($\Rightarrow$) Sejam $a, b, c \in \mathbb{Z}$ e $n, g \in \mathbb{N}$ tal que $ac \equiv bc \pmod{n}$ e $(c, n) = g$. Sabemos que

$$\left(\frac{c}{g}, \frac{n}{g}\right) = 1$$

e que $n|(a-b)c$, para algum $k \in \mathbb{Z}$. Dividindo a última expressão por g, temos

$$(n/g)|(a-b)(c/g).$$

Como $(c/g, n/g) = 1$, então n/g deve dividir $a - b$ e portanto $a \equiv b \pmod{n/g}$.

($\Leftarrow$) Por outro lado, suponha que $a \equiv b \pmod{n/g}$. Temos que existe $k \in \mathbb{Z}$ tal que $a = b + (n/g)k$. Multiplicando os dois lados por c obtemos o resultados, pois $ac = bc + n(c/g)k$, i.e., $ac \equiv bc \pmod{n}$.

Congruência módulo n

Proposição 3:

Sejam $a, b, c \in \mathbb{Z}$, $m, n \in \mathbb{N}$ e $a \equiv b \pmod{n}$. Então cada uma das afirmações é válida:

(a) $am \equiv bm \pmod{mn}$;

(b) $a^m \equiv b^m \pmod{n}$;

(c) Se $m|n$, então $a \equiv b \pmod{m}$.

(b) por indução. Por hipótese $a \equiv b \pmod{n}$, ou seja, a afirmação é verdadeira para $m = 1$. Suponha que $a^m \equiv b^m \pmod{n}$ seja válida para algum $m \in \mathbb{N}$, assim pela **Proposição 1** temos que $a^m \cdot a \equiv b^m \cdot b \pmod{n}$, i.e., $a^{m+1} \equiv b^{m+1} \pmod{n}$. Portanto, por indução, a fórmula $a^m \equiv b^m \pmod{n}$ é válida para todo $m \in \mathbb{N}$.

Congruência módulo n

EXEMPLOS:

$$\left.\begin{array}{l} 19 \equiv 3 \pmod 4 \\ 2 \equiv 6 \pmod 4 \end{array}\right\} \quad (19+2) \equiv (3+6) \pmod 4$$

$$21 - 9 = 12 = 3 \cdot 4$$

Congruência módulo n

EXEMPLOS:

$$\left.\begin{array}{l} 19 \equiv 3 \pmod 4 \\ 2 \equiv 6 \pmod 4 \end{array}\right\} \quad (19+2) \equiv (3+6) \pmod 4 \qquad 21 - 9 = 12 = 3 \cdot 4$$

$$\left.\begin{array}{l} 15 \equiv 1 \pmod 7 \\ 51 \equiv 2 \pmod 7 \end{array}\right\} \quad 15 \cdot 51 \equiv 1 \cdot 2 \pmod 7 \qquad 765 - 2 = 763 = 109 \cdot 7$$

Congruência módulo n

EXEMPLOS:

$$\left.\begin{array}{l} 19 \equiv 3 \pmod 4 \\ 2 \equiv 6 \pmod 4 \end{array}\right\} \quad (19+2) \equiv (3+6) \pmod 4$$

$$21 - 9 = 12 = 3 \cdot 4$$

$$\left.\begin{array}{l} 15 \equiv 1 \pmod 7 \\ 51 \equiv 2 \pmod 7 \end{array}\right\} \quad 15 \cdot 51 \equiv 1 \cdot 2 \pmod 7$$

$$765 - 2 = 763 = 109 \cdot 7$$

$$32 \equiv 12 \pmod{10} \longrightarrow 16 \equiv 6 \pmod 5$$

$$(2, 10) = 2$$

Congruência módulo n

PROPOSIÇÃO: Sejam $a, b, c, n \in \mathbb{Z}$, $n > 1$ são satisfeitas as seguintes propriedades:

i) Reflexiva: $a \equiv a \pmod{n}$

ii) Simétrica: se $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

iii) Transitiva: se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

Congruência módulo n

PROPOSIÇÃO: Sejam $a, b, c, n \in \mathbb{Z}$, $n > 1$ são satisfeitas as seguintes propriedades:

i) Reflexiva: $a \equiv a \pmod{n}$

$$n \mid (a - a) = 0$$

ii) Simétrica: se $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

iii) Transitiva: se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

Congruência módulo n

PROPOSIÇÃO: Sejam $a, b, c, n \in \mathbb{Z}$, $n > 1$ são satisfeitas as seguintes propriedades:

i) Reflexiva: $a \equiv a \pmod{n}$

$$n \mid (a - a) = 0$$

ii) Simétrica: se $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

$$a \equiv b \pmod{n} \Rightarrow n \mid (a - b)$$

iii) Transitiva: se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

Congruência módulo n

PROPOSIÇÃO: Sejam $a, b, c, n \in \mathbb{Z}$, $n > 1$ são satisfeitas as seguintes propriedades:

i) Reflexiva: $a \equiv a \pmod{n}$

$$n \mid (a - a) = 0$$

ii) Simétrica: se $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

$$a \equiv b \pmod{n} \Rightarrow n \mid (a-b) \rightarrow n \mid -(a-b) \Rightarrow n \mid (b-a) \Rightarrow b \equiv a \pmod{n}$$

iii) Transitiva: se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

Congruência módulo n

PROPOSIÇÃO: Sejam $a, b, c, n \in \mathbb{Z}$, $n > 1$ são satisfeitas as seguintes propriedades:

i) Reflexiva: $a \equiv a \pmod{n}$

$$n \mid (a - a) = 0$$

ii) Simétrica: se $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

$$a \equiv b \pmod{n} \Rightarrow n \mid (a-b) \rightarrow n \mid -(a-b) \Rightarrow n \mid (b-a) \Rightarrow b \equiv a \pmod{n}$$

iii) Transitiva: se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

Congruência módulo n

PROPOSIÇÃO: Sejam $a, b, c, n \in \mathbb{Z}$, $n > 1$ são satisfeitas as seguintes propriedades:

i) Reflexiva: $a \equiv a \pmod{n}$

$$n \mid (a - a) = 0$$

ii) Simétrica: se $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

$$a \equiv b \pmod{n} \Rightarrow n \mid (a-b) \rightarrow n \mid -(a-b) \Rightarrow n \mid (b-a) \Rightarrow b \equiv a \pmod{n}$$

iii) Transitiva: se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

$$\left.\begin{array}{l} a \equiv b \pmod{n} \Rightarrow n \mid (a-b) \\ b \equiv c \pmod{n} \Rightarrow n \mid (b-c) \end{array}\right\} \longrightarrow n \mid (a-c) \Rightarrow a \equiv c \pmod{n}$$

Congruência módulo n

CLASSE DE CONGRUÊNCIA:

O conjunto de todos os números inteiros congruentes a um inteiro a módulo n é chamado de classe de congruência de a módulo n .

Congruência módulo n

CLASSE DE CONGRUÊNCIA:

O conjunto de todos os números inteiros congruentes a um inteiro a módulo n é chamado de classe de congruência de a módulo n .

EXEMPLO: Classes de congruência módulo 3

Congruência módulo n

CLASSE DE CONGRUÊNCIA:

O conjunto de todos os números inteiros congruentes a um inteiro a módulo n é chamado de classe de congruência de a módulo n .

EXEMPLO: Classes de congruência módulo 3

$\bar{0} =$

$\bar{1} =$

$\bar{2} =$

Congruência módulo n

CLASSE DE CONGRUÊNCIA:

O conjunto de todos os números inteiros congruentes a um inteiro a módulo n é chamado de classe de congruência de a módulo n .

EXEMPLO: Classes de congruência módulo 3

$\bar{0} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}$

$\bar{1} =$

$\bar{2} =$

Congruência módulo n

CLASSE DE CONGRUÊNCIA:

O conjunto de todos os números inteiros congruentes a um inteiro a módulo n é chamado de classe de congruência de a módulo n .

EXEMPLO: Classes de congruência módulo 3

$$\bar{0} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}$$

$$\bar{1} = \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\}$$

$$\bar{2} =$$

Congruência módulo n

CLASSE DE CONGRUÊNCIA:

O conjunto de todos os números inteiros congruentes a um inteiro a módulo n é chamado de classe de congruência de a módulo n .

EXEMPLO: Classes de congruência módulo 3

$$\bar{0} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\} \qquad \ldots \equiv -6 \equiv -3 \equiv 0 \equiv 3 \equiv 6 \equiv 9 \equiv \ldots (mod\, 3)$$

$$\bar{1} = \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\}$$

$$\bar{2} = \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\}$$

Congruência módulo n

CLASSE DE CONGRUÊNCIA:

O conjunto de todos os números inteiros congruentes a um inteiro a módulo n é chamado de classe de congruência de a módulo n .

EXEMPLO: Classes de congruência módulo 3

$$\bar{0}=\{\ldots,-6,-3,0,3,6,9,\ldots\} \qquad \ldots\equiv -6\equiv -3\equiv 0\equiv 3\equiv 6\equiv 9\equiv \ldots (mod\,3)$$

$$\bar{1}=\{\ldots,-5,-2,1,4,7,10,\ldots\}$$

$$\bar{2}=\{\ldots,-7,-4,-1,2,5,8,\ldots\}$$

Obs: $-6\equiv -3\,mod\,3 \rightarrow -6-(-3)\,mod\,3=-6+3\,mod\,3=-3\,mod\,3=0$

Congruência módulo n

CLASSE DE CONGRUÊNCIA:

O conjunto de todos os números inteiros congruentes a um inteiro a módulo n é chamado de classe de congruência de a módulo n .

EXEMPLO: Classes de congruência módulo 3

$$\bar{0} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}$$

$$\bar{1} = \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\}$$

$$\bar{2} = \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\}$$

Congruência módulo n

CLASSE DE CONGRUÊNCIA:

O conjunto de todos os números inteiros congruentes a um inteiro a módulo n é chamado de classe de congruência de a módulo n .

EXEMPLO: Classes de congruência módulo 3

$$\bar{0} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\} \qquad \ldots \equiv -6 \equiv -3 \equiv 0 \equiv 3 \equiv 6 \equiv 9 \equiv \ldots (mod\, 3)$$

$$\bar{1} = \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\} \qquad \ldots \equiv -5 \equiv -2 \equiv 1 \equiv 4 \equiv 7 \equiv 10 \equiv \ldots (mod\, 3)$$

$$\bar{2} = \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\}$$

Congruência módulo n

CLASSE DE CONGRUÊNCIA:

O conjunto de todos os números inteiros congruentes a um inteiro a módulo n é chamado de classe de congruência de a módulo n .

EXEMPLO: Classes de congruência módulo 3

$$\bar{0} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\} \qquad \ldots \equiv -6 \equiv -3 \equiv 0 \equiv 3 \equiv 6 \equiv 9 \equiv \ldots (mod\, 3)$$

$$\bar{1} = \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\} \qquad \ldots \equiv -5 \equiv -2 \equiv 1 \equiv 4 \equiv 7 \equiv 10 \equiv \ldots (mod\, 3)$$

$$\bar{2} = \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\} \qquad \ldots \equiv -7 \equiv -4 \equiv -1 \equiv 2 \equiv 5 \equiv 8 \equiv \ldots (mod\, 3)$$

CLASSE DE RESÍDUOS MÓDULO n

CLASSE DE CONGRUÊNCIA:

O conjunto de todos os números inteiros congruentes a um inteiro a módulo n é chamado de classe de congruência de a módulo n .

EXEMPLO: Classes de congruência módulo 3

$$\bar{0}=\{\ldots,-6,-3,0,3,6,9,\ldots\} \qquad \ldots\equiv -6\equiv -3\equiv 0\equiv 3\equiv 6\equiv 9\equiv \ldots (mod\,3)$$

$$\bar{1}=\{\ldots,-5,-2,1,4,7,10,\ldots\} \qquad \ldots\equiv -5\equiv -2\equiv 1\equiv 4\equiv 7\equiv 10\equiv \ldots (mod\,3)$$

$$\bar{2}=\{\ldots,-7,-4,-1,2,5,8,\ldots\} \qquad \ldots\equiv -7\equiv -4\equiv -1\equiv 2\equiv 5\equiv 8\equiv \ldots (mod\,3)$$

CLASSE DE RESÍDUOS MÓDULO n

EXEMPLO:

Existem quatro classes de resíduos módulo 4, a saber

CLASSE DE RESÍDUOS MÓDULO n

EXEMPLO:

Existem quatro classes de resíduos módulo 4, a saber

$$\begin{aligned}
\overline{0} &= \{\cdots, -8, -4, 0, 4, 8, \cdots\} \\
\overline{1} &= \{\cdots, -7, -3, 1, 5, 9, \cdots\} \\
\overline{2} &= \{\cdots, -6, -2, 2, 6, 10, \cdots\} \\
\overline{3} &= \{\cdots, -5, -1, 3, 7, 11, \cdots\}
\end{aligned}$$

CLASSE DE RESÍDUOS MÓDULO n

EXEMPLO:

Existem quatro classes de resíduos módulo 4, a saber

$$\begin{aligned}
\overline{0} &= \{\cdots, -8, -4, 0, 4, 8, \cdots\} \\
\overline{1} &= \{\cdots, -7, -3, 1, 5, 9, \cdots\} \\
\overline{2} &= \{\cdots, -6, -2, 2, 6, 10, \cdots\} \\
\overline{3} &= \{\cdots, -5, -1, 3, 7, 11, \cdots\}
\end{aligned}$$

Como cada elemento de $\mathbb{Z}$ está em exatamente uma dessas classes disjuntas então

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3}.$$

CLASSE DE RESÍDUOS MÓDULO n

EXEMPLO:

Existem quatro classes de resíduos módulo 4, a saber

$$\begin{aligned}
\overline{0} &= \{\cdots, -8, -4, 0, 4, 8, \cdots\} \\
\overline{1} &= \{\cdots, -7, -3, 1, 5, 9, \cdots\} \\
\overline{2} &= \{\cdots, -6, -2, 2, 6, 10, \cdots\} \\
\overline{3} &= \{\cdots, -5, -1, 3, 7, 11, \cdots\}
\end{aligned}$$

Como cada elemento de $\mathbb{Z}$ está em exatamente uma dessas classes disjuntas então

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3}.$$

Além disso, $R = \{0, 1, 2, 3\}$ forma um sistema completo de resíduos módulo 4.

Aplicação - Congruência módulo n

EXEMPLO: Considere o mês de outubro de 2014, conforme ilustrado na tabela a seguir:

domingo	*segunda*	*terça*	*quarta*	*quinta*	*sexta*	*sábado*
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

em que as colunas indicam o dia da semana (matematicamente, números congruentes mod 7).

Neste exemplo, o dia 31 de outubro de 2014 é uma sexta-feira, 1º de novembro um sábado, 02 de novembro um domingo e assim por diante. Qual dia da semana será o dia 24 de novembro de 2014?

FONTE: http://www.sites.uem.br/profmat/GuilhermeLiegelLeopold.pdf

Aplicação - Congruência módulo n

EXEMPLO:

domingo	*segunda*	*terça*	*quarta*	*quinta*	*sexta*	*sábado*
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

→ considere a operação:

$$24 = 7q + r$$

FONTE: http://www.sites.uem.br/profmat/GuilhermeLiegelLeopold.pdf

Aplicação - Congruência módulo n

EXEMPLO:

domingo	*segunda*	*terça*	*quarta*	*quinta*	*sexta*	*sábado*
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

→ considere a operação:

$$24 = 7q + r$$

Vamos utilizá-la para encontrar um número entre 1 e 7 que seja congruente a 24.

FONTE: http://www.sites.uem.br/profmat/GuilhermeLiegelLeopold.pdf

Aplicação - Congruência módulo n

EXEMPLO:

domingo	*segunda*	*terça*	*quarta*	*quinta*	*sexta*	*sábado*
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

→ considere a operação:

$$24 = 7q + r$$

Vamos utilizá-la para encontrar um número entre 1 e 7 que seja congruente a 24.

$$24 = 7 \cdot 3 + 3$$

FONTE: http://www.sites.uem.br/profmat/GuilhermeLiegelLeopold.pdf

Aplicação - Congruência módulo n

EXEMPLO:

domingo	*segunda*	*terça*	*quarta*	*quinta*	*sexta*	*sábado*
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

→ considere a operação:

$$24 = 7q + r$$

Vamos utilizá-la para encontrar um número entre 1 e 7 que seja congruente a 24.

$$24 = 7 \cdot 3 + 3 \longrightarrow resto = 3$$

FONTE: http://www.sites.uem.br/profmat/GuilhermeLiegelLeopold.pdf

Aplicação - Congruência módulo n

EXEMPLO:

domingo	*segunda*	*terça*	*quarta*	*quinta*	*sexta*	*sábado*
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

→ considere a operação:

$$24 = 7q + r$$

Vamos utilizá-la para encontrar um número entre 1 e 7 que seja congruente a 24.

$$24 = 7 \cdot 3 + 3 \longrightarrow resto = 3$$

$$24 \equiv 3 \pmod 7$$

FONTE: http://www.sites.uem.br/profmat/GuilhermeLiegelLeopold.pdf

Aplicação - Congruência módulo n

EXEMPLO:

domingo	*segunda*	*terça*	*quarta*	*quinta*	*sexta*	*sábado*
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

→ considere a operação:

$$24 = 7q + r$$

Vamos utilizá-la para encontrar um número entre 1 e 7 que seja congruente a 24.

$$24 = 7 \cdot 3 + 3 \longrightarrow resto = 3$$

$$24 \equiv 3 \pmod 7$$

Logo, como $3/11/2014$ foi segunda-feira, o dia $24/11/2014$ foi segunda-feira

FONTE: http://www.sites.uem.br/profmat/GuilhermeLiegelLeopold.pdf

Aplicação - Congruência módulo n

A copa do mundo de futebol no Brasil foi em 2014. O jogo de abertura foi dia 12 de junho. Sem utilizar o calendário e sabendo que o dia 1º de janeiro de 2014 foi uma quarta-feira determine em que dia da semana ocorreu o jogo de abertura.

Aplicação - Congruência módulo n

A copa do mundo de futebol no Brasil foi em 2014. O jogo de abertura foi dia 12 de junho. Sem utilizar o calendário e sabendo que o dia 1º de janeiro de 2014 foi uma quarta-feira determine em que dia da semana ocorreu o jogo de abertura.

Dica: que dia do ano de 365 dias é o dia 12/06?

jan	*fev*	*mar*	*abr*	*maio*	*jun*
31	28	31	30	31	12

$$31+28+31+30+31+12=163$$

$$12/06 \longrightarrow 163^{o}$$

A que número entre 1 e 7, 163 é congruente?

domingo	*segunda*	*terça*	*quarta*	*quinta*	*sexta*	*sábado*
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

$$163=7q+r$$

$$163=7\cdot 23+2 \longrightarrow resto=2$$

$$163 \equiv 2 \pmod 7 \longrightarrow 12/06/2014 \text{ foi quinta-feira}$$