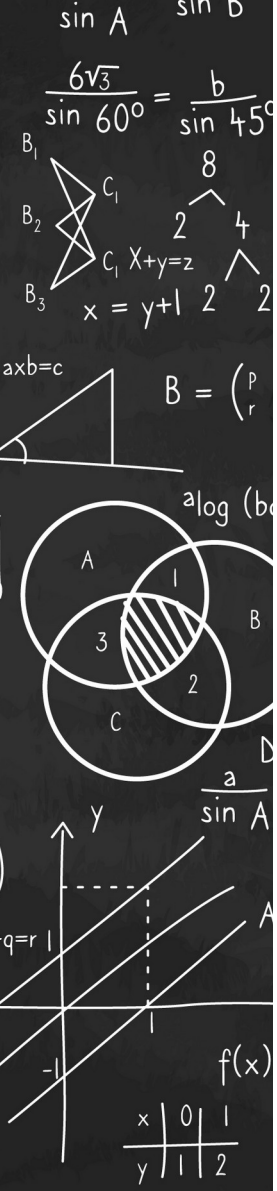


Matemática Discreta 2

Aulas 07 e 08
Aritmética Modular

Cristiane Loesch

Brasília
2025

RELEMBRANDO

DIV e **MOD**

→ Operações associadas ao processo de divisão

→ Dados $a, b \in \mathbb{Z}$ com $b \neq 0$ e $q, r \in \mathbb{Z}$ tem-se que:

$$a = q\,b + r \qquad 0 \leq r < |b|$$

com,

$$a \;\; div \;\; b = q$$

$$a \;\; mod \;\; b = r$$

Aritmética Modular

→ Aritmética dos Restos

→ números inteiros e racionais

→ operações básicas com significados ligeiramente diferentes

→ aritmética finita

Aritmética Modular

Seja o conjunto Z_n no qual $n \in \mathbb{Z}$, positivo dado por:

$$Z_n = \{0,1,2,\ldots,n-1\}$$

Tal conjunto é denominado conjunto dos números inteiros *mod n*.

Aritmética Modular

Seja o conjunto Z_n no qual $n \in \mathbb{Z}$, positivo dado por:

$$Z_n = \{0, 1, 2, \ldots, n-1\}$$

Tal conjunto é denominado conjunto dos números inteiros *mod n*.

As operações definidas neste conjunto são:

- $\oplus \rightarrow$ adição *mod n*
- $\otimes \rightarrow$ multiplicação *mod n*
- $\ominus \rightarrow$ subtração *mod n*
- $\oslash \rightarrow$ divisão *mod n*

ADIÇÃO E MULTIPLICAÇÃO MODULARES

Seja n um inteiro positivo e $a, b \in Z_n$. Definimos:

$$a \oplus b = (a + b) \bmod n$$

$$a \otimes b = (a \dot{b}) \bmod n$$

EXEMPLO:

Aritmética Modular

ADIÇÃO E MULTIPLICAÇÃO MODULARES

ATENÇÃO AO CONTEXTO!

$$Z_{10} \longrightarrow 5 \oplus 5 = 0$$

$$Z_{9} \longrightarrow 5 \oplus 5 = 1$$

Observe que o resultado da operação de adição mod n será diferente em cada conjunto!!!

Vamos relembrar o por que?!

Aritmética Modular

ADIÇÃO E MULTIPLICAÇÃO MODULARES

ATENÇÃO AO CONTEXTO!

$$Z_{10} \longrightarrow 5 \oplus 5 = 0$$

$$Z_{9} \longrightarrow 5 \oplus 5 = 1$$

$$(5+5)\ mod\ 10 = 10\ mod\ 10 = 0$$

$$\begin{array}{r|l} 10 & 10 \\ \cline{2-2} -\ 10 & 1 \\ \cline{1-1} 0 & \end{array}$$

Aritmética Modular

ADIÇÃO E MULTIPLICAÇÃO MODULARES

ATENÇÃO AO CONTEXTO!

$$Z_{10} \longrightarrow 5 \oplus 5 = 0$$

$$Z_{9} \longrightarrow 5 \oplus 5 = 1$$

$$(5+5)\ mod\ 10 = 10\ mod\ 10 = 0$$

$$\begin{array}{r|l} 10 & 10 \\ \cline{2-2} -\ 10 & 1 \\ \cline{1-1} 0 & \end{array}$$

$$(5+5)\ mod\ 9 = 10\ mod\ 9 = 1$$

$$\begin{array}{r|l} 10 & 9 \\ \cline{2-2} -\ 9 & 1 \\ \cline{1-1} 1 & \end{array}$$

ADIÇÃO E MULTIPLICAÇÃO MODULARES

Propriedades:

→ ambas as operações gozam das propriedades algébricas usuais.

ADIÇÃO E MULTIPLICAÇÃO MODULARES

Propriedades:

→ ambas as operações gozam das propriedades algébricas usuais.

Proposições:

I) Sejam $a, b \in Z_n \Rightarrow a \oplus b$ e $a \otimes b \in Z_n$ (ppdde do fechamento).

ADIÇÃO E MULTIPLICAÇÃO MODULARES

Propriedades:

→ ambas as operações gozam das propriedades algébricas usuais.

Proposições:

I) Sejam $a, b \in Z_n \Rightarrow a \oplus b$ e $a \otimes b \in Z_n$ (ppdde do fechamento).

II) Seja $n \in \mathbb{Z}$ e $n \geq \alpha$

ADIÇÃO E MULTIPLICAÇÃO MODULARES

Propriedades:

→ ambas as operações gozam das propriedades algébricas usuais.

Proposições:

I) Sejam $a, b \in Z_n \Rightarrow a \oplus b$ e $a \otimes b \in Z_n$ (ppdde do fechamento).

II) Seja $n \in \mathbb{Z}$ e $n \geq \alpha$

* comutativa: $\forall a, b \in Z_n \longrightarrow a \oplus b = b \oplus a$ e $a \otimes b = b \otimes a$

ADIÇÃO E MULTIPLICAÇÃO MODULARES

Propriedades:

→ ambas as operações gozam das propriedades algébricas usuais.

Proposições:

I) Sejam $a, b \in Z_n \Rightarrow a \oplus b$ e $a \otimes b \in Z_n$ (ppdde do fechamento).

II) Seja $n \in \mathbb{Z}$ e $n \geq \alpha$

* comutativa: $\forall a, b \in Z_n \longrightarrow a \oplus b = b \oplus a$ e $a \otimes b = b \otimes a$

* associativa: $\forall a, b, c \in Z_n \longrightarrow a \oplus (b \oplus c) = (a \oplus b) \oplus c$ e $a \otimes (b \otimes c) = (a \otimes b) \otimes c$

ADIÇÃO E MULTIPLICAÇÃO MODULARES

Propriedades:

→ ambas as operações gozam das propriedades algébricas usuais.

Proposições:

I) Sejam $a, b \in Z_n \Rightarrow a \oplus b$ e $a \otimes b \in Z_n$ (ppdde do fechamento).

II) Seja $n \in \mathbb{Z}$ e $n \geq \alpha$

* comutativa: $\forall a, b \in Z_n \longrightarrow a \oplus b = b \oplus a$ e $a \otimes b = b \otimes a$

* associativa: $\forall a, b, c \in Z_n \longrightarrow a \oplus (b \oplus c) = (a \oplus b) \oplus c$ e $a \otimes (b \otimes c) = (a \otimes b) \otimes c$

* elemento identidade: $\forall a \in Z_n \longrightarrow a \oplus 0 = 0 \oplus a = a$ e $a \otimes 1 = 1 \otimes a = a$

ADIÇÃO E MULTIPLICAÇÃO MODULARES

Propriedades:

→ ambas as operações gozam das propriedades algébricas usuais.

Proposições:

I) Sejam $a, b \in Z_n \Rightarrow a \oplus b$ e $a \otimes b \in Z_n$ (ppdde do fechamento).

II) Seja $n \in \mathbb{Z}$ e $n \geq \alpha$

* comutativa: $\forall a, b \in Z_n \longrightarrow a \oplus b = b \oplus a$ e $a \otimes b = b \otimes a$

* associativa: $\forall a, b, c \in Z_n \longrightarrow a \oplus (b \oplus c) = (a \oplus b) \oplus c$ e $a \otimes (b \otimes c) = (a \otimes b) \otimes c$

* elemento identidade: $\forall a \in Z_n \longrightarrow a \oplus 0 = 0 \oplus a = a$ e $a \otimes 1 = 1 \otimes a = a$

* distributiva: $\forall a, b, c \in Z_n \longrightarrow a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

ADIÇÃO E MULTIPLICAÇÃO MODULARES

EXEMPLO: Mostre as propriedades da adição e multiplicação modulares nos exemplos abaixo:

SUA VEZ! Z_{10}

a) comutativa

$$3 \oplus 7 = 7 \oplus 3$$
$$2 \otimes 6 = 6 \otimes 2$$

b) associativa

$$3 \oplus (2 \oplus 4) = (3 \oplus 2) \oplus 4$$

c) elemento identidade

$$1 \oplus 0 = 0 \oplus 1 = 1$$
$$2 \otimes 1 = 1 \otimes 2 = 2$$

d) distributiva

$$3 \otimes (2 \oplus 4) = (3 \otimes 2) \oplus (3 \otimes 4)$$

Aritmética Modular

ADIÇÃO E MULTIPLICAÇÃO MODULARES

Obs:

$$(X * Y) \bmod Z = (X \bmod Z * Y \bmod Z) \bmod Z$$

Aritmética Modular

ADIÇÃO E MULTIPLICAÇÃO MODULARES

Obs:

$$(X * Y) \bmod Z = (X \bmod Z * Y \bmod Z) \bmod Z$$

EXEMPLOS:

$$(11 \bmod 10 + 100 \bmod 10) \bmod 10 =$$

$$(77 \bmod 31 \cdot 31 \bmod 31) \bmod 31 =$$

Aritmética Modular

ADIÇÃO E MULTIPLICAÇÃO MODULARES

Obs:

$$(X * Y) \bmod Z = (X \bmod Z * Y \bmod Z) \bmod Z$$

EXEMPLOS:

$$(11 \bmod 10 + 100 \bmod 10) \bmod 10 = (11 + 100) \bmod 10 =$$

$$(77 \bmod 31 \cdot 31 \bmod 31) \bmod 31 =$$

Aritmética Modular

ADIÇÃO E MULTIPLICAÇÃO MODULARES

Obs:

$$(X * Y) \bmod Z = (X \bmod Z * Y \bmod Z) \bmod Z$$

EXEMPLOS:

$$(11 \bmod 10 + 100 \bmod 10) \bmod 10 = (11 + 100) \bmod 10 = 111 \bmod 10$$

$$(77 \bmod 31 \cdot 31 \bmod 31) \bmod 31 =$$

Aritmética Modular

ADIÇÃO E MULTIPLICAÇÃO MODULARES

Obs:

$$(X * Y) \bmod Z = (X \bmod Z * Y \bmod Z) \bmod Z$$

EXEMPLOS:

$$(11 \bmod 10 + 100 \bmod 10) \bmod 10 = (11 + 100) \bmod 10 = 111 \bmod 10$$

$$(77 \bmod 31 \cdot 31 \bmod 31) \bmod 31 = (77 \cdot 31) \bmod 31 =$$

Aritmética Modular

ADIÇÃO E MULTIPLICAÇÃO MODULARES

Obs:

$$(X * Y) \bmod Z = (X \bmod Z * Y \bmod Z) \bmod Z$$

EXEMPLOS:

$$(11 \bmod 10 + 100 \bmod 10) \bmod 10 = (11 + 100) \bmod 10 = 111 \bmod 10$$

$$(77 \bmod 31 \cdot 31 \bmod 31) \bmod 31 = (77 \cdot 31) \bmod 31 = 2387 \bmod 31$$

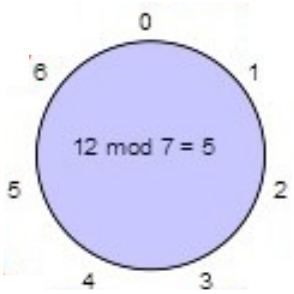
CÍRCULO MODULAR

EXEMPLO: $12+9 \mod 7$

Aritmética Modular

CÍRCULO MODULAR

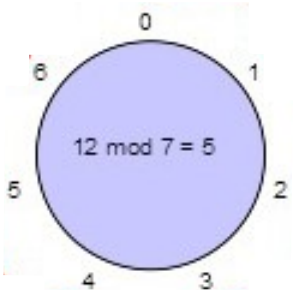
EXEMPLO: $12+9 \mod 7$



FONTE:
https://pt.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/modular-addition-and-subtraction

CÍRCULO MODULAR

EXEMPLO: $12+9 \mod 7$

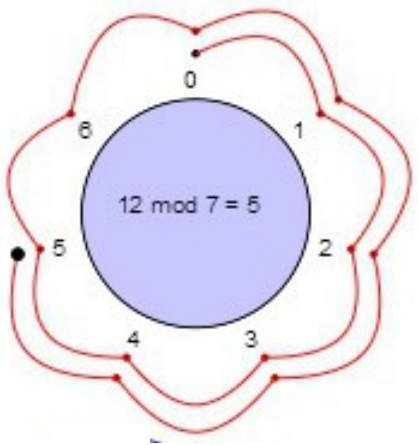


→ sequência de passos para a direita

FONTE:
https://pt.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/modular-addition-and-subtraction

CÍRCULO MODULAR

EXEMPLO: $12+9 \mod 7$



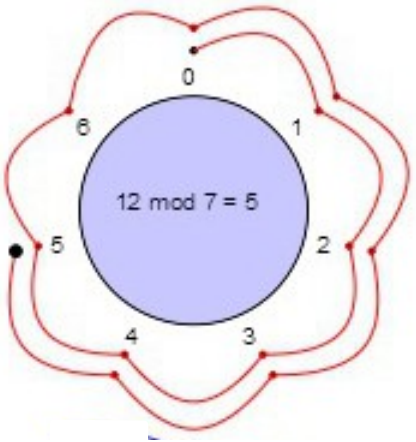
→ sequência de passos para a direita

→ observe que 7 passos terminarão sempre na mesma posição do círculo

FONTE:
https://pt.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/modular-addition-and-subtraction

CÍRCULO MODULAR

EXEMPLO: $12+9 \mod 7$

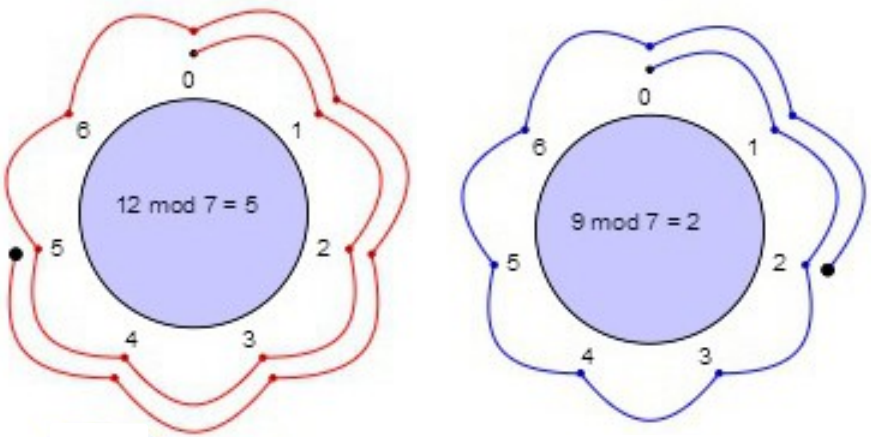


→ sequência de passos para a direita
→ observe que 7 passos terminarão sempre na mesma posição do círculo
→voltas completas não contribuem para posição final

FONTE:
https://pt.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/modular-addition-and-subtraction

CÍRCULO MODULAR

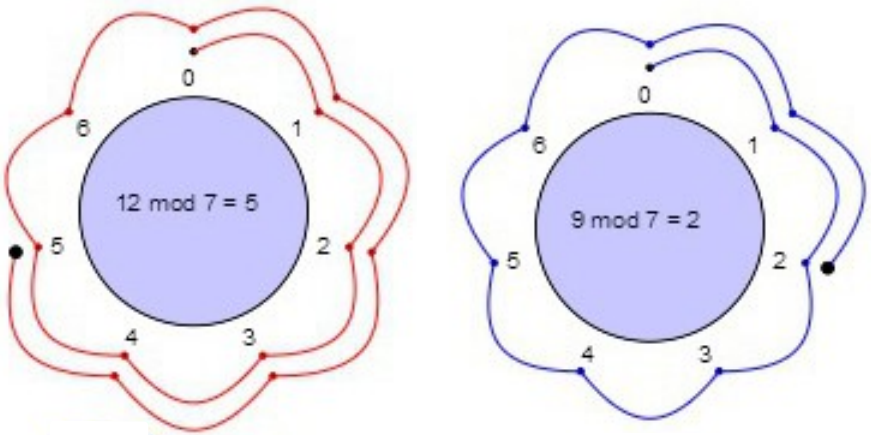
EXEMPLO: $12+9 \mod 7$



FONTE: https://pt.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/modular-addition-and-subtraction

CÍRCULO MODULAR

EXEMPLO: $12+9 \mod 7$

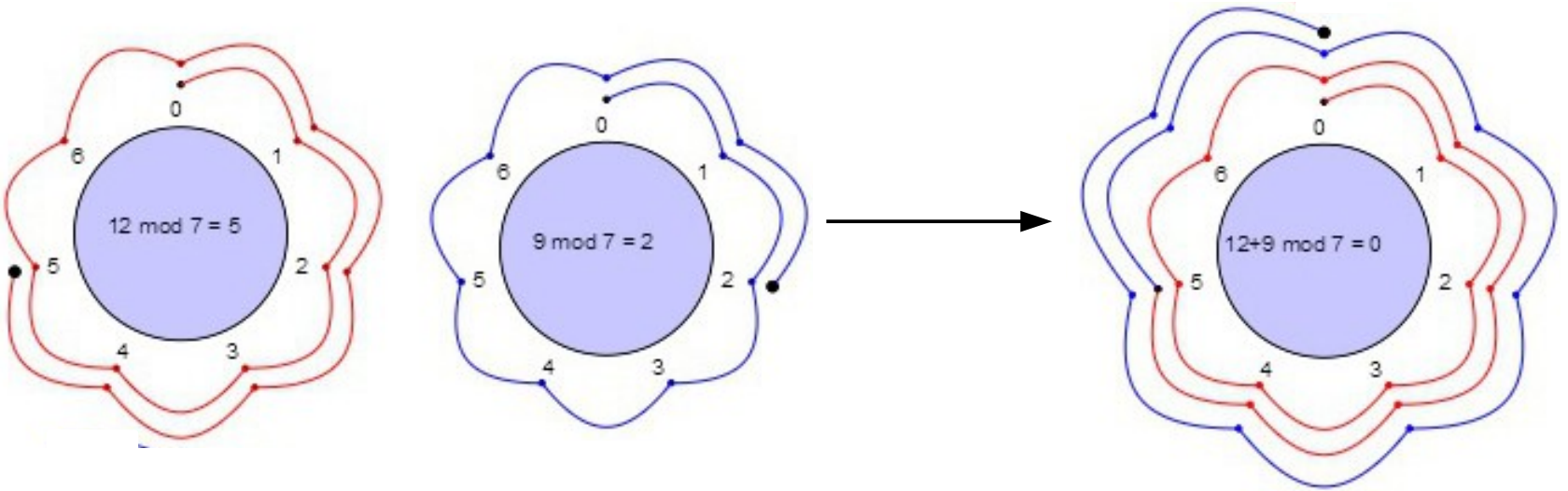


$12+9 \mod 7$ → 12 + 9 passos

FONTE:
https://pt.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/modular-addition-and-subtraction

CÍRCULO MODULAR

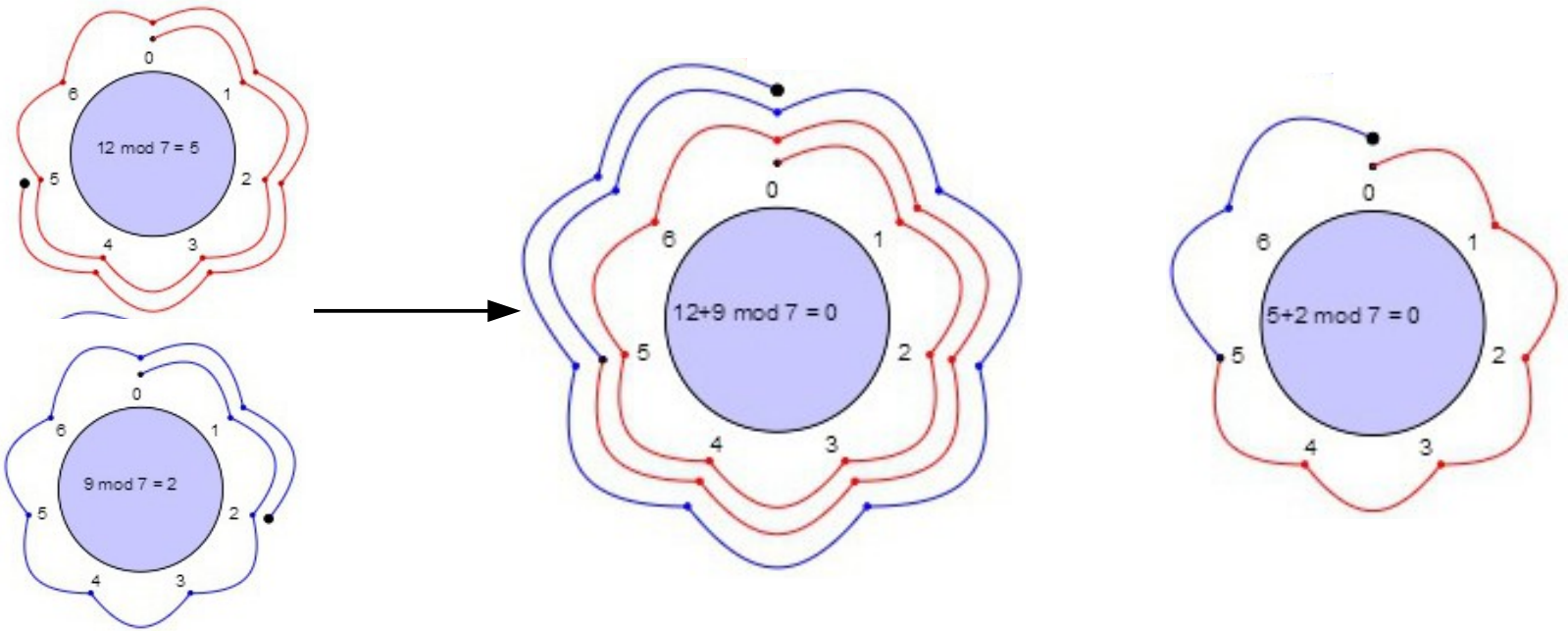
EXEMPLO: $12+9 \mod 7$



FONTE:
https://pt.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/modular-addition-and-subtraction

CÍRCULO MODULAR

EXEMPLO: $12+9 \mod 7$



FONTE: https://pt.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/modular-addition-and-subtraction

SUBTRAÇÃO MODULAR

DEFINIÇÃO:

Seja $n \in \mathbb{Z}_+$ e $a, b \in Z_n$ Define-se $a \ominus b$ como o único valor $x \in Z_n$, tal que $a = b \oplus x$. Assim,

$$a \ominus b = (a - b) \mod n$$

SUBTRAÇÃO MODULAR

DEFINIÇÃO:

Seja $n \in \mathbb{Z}_+$ e $a, b \in Z_n$ Define-se $a \ominus b$ como o único valor $x \in Z_n$, tal que $a = b \oplus x$. Assim,

$$a \ominus b = (a - b) \mod n$$

EXEMPLO: Z_{10}

$$8 \ominus 5 =$$

SUBTRAÇÃO MODULAR

DEFINIÇÃO:

Seja $n \in \mathbb{Z}_+$ e $a, b \in Z_n$ Define-se $a \ominus b$ como o único valor $x \in Z_n$, tal que $a = b \oplus x$. Assim,

$$a \ominus b = (a - b) \mod n$$

EXEMPLO: Z_{10}

$$8 \ominus 5 = (8 - 5) \mod 10$$

SUBTRAÇÃO MODULAR

DEFINIÇÃO:

Seja $n \in \mathbb{Z}_+$ e $a, b \in Z_n$ Define-se $a \ominus b$ como o único valor $x \in Z_n$, tal que $a = b \oplus x$. Assim,

$$a \ominus b = (a - b) \mod n$$

EXEMPLO: Z_{10}

$$8 \ominus 5 = (8 - 5) \mod 10 = 3 \mod 10 = 3$$

DIVISÃO MODULAR

→ significativamente diferente de quaisquer outras operações modulares

DIVISÃO MODULAR

→ significativamente diferente de quaisquer outras operações modulares

→ multiplicação e divisão modulares são inversas?

DIVISÃO MODULAR

→ significativamente diferente de quaisquer outras operações modulares

→ multiplicação e divisão modulares são inversas?

EXEMPLO: Dados $a, b \in Z_{10}$ ($b \neq 0$) existe uma solução para $a = b \otimes x$? Tal solução é única?

a) $a = 6, b = 2$

DIVISÃO MODULAR

→ significativamente diferente de quaisquer outras operações modulares

→ multiplicação e divisão modulares são inversas?

EXEMPLO: Dados $a, b \in Z_{10}$ ($b \neq 0$) existe uma solução para $a = b \otimes x$? Tal solução é única?

a) $a = 6, b = 2 \longrightarrow 6 = 2 \otimes x$

DIVISÃO MODULAR

→ significativamente diferente de quaisquer outras operações modulares

→ multiplicação e divisão modulares são inversas?

EXEMPLO: Dados $a, b \in Z_{10}$ ($b \neq 0$) existe uma solução para $a = b \otimes x$? Tal solução é única?

a) $a = 6, b = 2 \longrightarrow 6 = 2 \otimes x \longrightarrow x = 3 \quad \text{ou} \quad x = 8$

Lembre-se: $(2 \cdot 3) \bmod 10 = 6 \bmod 10 = 6$

DIVISÃO MODULAR

→ significativamente diferente de quaisquer outras operações modulares

→ multiplicação e divisão modulares são inversas?

EXEMPLO: Dados $a, b \in Z_{10}$ ($b \neq 0$) existe uma solução para $a = b \otimes x$? Tal solução é única?

a) $a = 6, b = 2 \longrightarrow 6 = 2 \otimes x \longrightarrow x = 3 \quad \text{ou} \quad x = 8$

Lembre-se: $(2 \cdot 3) \, mod \, 10 = 6 \, mod \, 10 = 6$

$(2 \cdot 8) \, mod \, 10 = 16 \, mod \, 10 = 6$

DIVISÃO MODULAR

→ significativamente diferente de quaisquer outras operações modulares

→ multiplicação e divisão modulares são inversas?

EXEMPLO: Dados $a, b \in Z_{10}$ ($b \neq 0$) existe uma solução para $a = b \otimes x$? Tal solução é única?

a) $a = 6, b = 2 \longrightarrow 6 = 2 \otimes x \longrightarrow x = 3 \quad \text{ou} \quad x = 8$

b) $a = 7, b = 2$

DIVISÃO MODULAR

→ significativamente diferente de quaisquer outras operações modulares

→ multiplicação e divisão modulares são inversas?

EXEMPLO: Dados $a, b \in Z_{10}$ ($b \neq 0$) existe uma solução para $a = b \otimes x$? Tal solução é única?

a) $a=6, b=2 \longrightarrow 6=2 \otimes x \longrightarrow x=3 \quad \text{ou} \quad x=8$

b) $a=7, b=2 \longrightarrow 7=2 \otimes x$

DIVISÃO MODULAR

→ significativamente diferente de quaisquer outras operações modulares

→ multiplicação e divisão modulares são inversas?

EXEMPLO: Dados $a, b \in Z_{10}$ ($b \neq 0$) existe uma solução para $a = b \otimes x$? Tal solução é única?

a) $a=6, b=2 \longrightarrow 6=2 \otimes x \longrightarrow x=3 \quad \text{ou} \quad x=8$

b) $a=7, b=2 \longrightarrow 7=2 \otimes x \longrightarrow \nexists x$

DIVISÃO MODULAR

→ significativamente diferente de quaisquer outras operações modulares

→ multiplicação e divisão modulares são inversas?

EXEMPLO: Dados $a, b \in Z_{10}$ ($b \neq 0$) existe uma solução para $a = b \otimes x$? Tal solução é única?

a) $a=6, b=2 \longrightarrow 6=2 \otimes x \longrightarrow x=3 \quad \text{ou} \quad x=8$

b) $a=7, b=2 \longrightarrow 7=2 \otimes x \longrightarrow \nexists x$

c) $a=7, b=3$

DIVISÃO MODULAR

→ significativamente diferente de quaisquer outras operações modulares

→ multiplicação e divisão modulares são inversas?

EXEMPLO: Dados $a, b \in Z_{10}$ ($b \neq 0$) existe uma solução para $a = b \otimes x$? Tal solução é única?

a) $a=6, b=2 \longrightarrow 6=2 \otimes x \longrightarrow x=3 \quad \text{ou} \quad x=8$

b) $a=7, b=2 \longrightarrow 7=2 \otimes x \longrightarrow \nexists x$

c) $a=7, b=3 \longrightarrow 7=3 \otimes x$

DIVISÃO MODULAR

→ significativamente diferente de quaisquer outras operações modulares

→ multiplicação e divisão modulares são inversas?

EXEMPLO: Dados $a, b \in Z_{10}$ ($b \neq 0$) existe uma solução para $a = b \otimes x$? Tal solução é única?

a) $a=6, b=2 \longrightarrow 6=2 \otimes x \longrightarrow x=3 \quad \text{ou} \quad x=8$

b) $a=7, b=2 \longrightarrow 7=2 \otimes x \longrightarrow \nexists x$

c) $a=7, b=3 \longrightarrow 7=3 \otimes x \longrightarrow x=9$

DIVISÃO MODULAR

→ significativamente diferente de quaisquer outras operações modulares

→ multiplicação e divisão modulares são inversas?

EXEMPLO: Dados $a, b \in Z_{10}$ ($b \neq 0$) existe uma solução para $a = b \otimes x$? Tal solução é única?

a) $a=6, b=2 \longrightarrow 6 = 2 \otimes x \longrightarrow x=3 \quad \text{ou} \quad x=8$

b) $a=7, b=2 \longrightarrow 7 = 2 \otimes x \longrightarrow \nexists x$

c) $a=7, b=3 \longrightarrow 7 = 3 \otimes x \longrightarrow x=9 \longrightarrow 7 \oslash 3 = 9$

INVERSO

Seja n um inteiro positivo e $a \in Z_n$. O inverso de a é um elemento $b \in Z_n$, tal que $a \otimes b = 1 \Rightarrow a \cdot b \mod n = 1$.

→ um elemento de Z_n que tenha inverso, é chamado invertível

→ se a tem inverso em Z_n , então tem apenas um inverso

→ supondo que a seja invertível. Se $b = a^{-1} \Rightarrow b$ é invertível e $a = b^{-1}$ logo,

$$\left(a^{-1}\right)^{-1} = a$$

INVERSO

DEFINIÇÃO:

Seja n um inteiro positivo e seja b um elemento invertível de Z_n .

Seja $a \oslash b$ arbitrário. Então, $a \otimes b^{-1}$.

INVERSO

DEFINIÇÃO:

Seja n um inteiro positivo e seja b um elemento invertível de Z_n .

Seja $a \oslash b$ arbitrário. Então, $a \otimes b^{-1}$.

EXEMPLO:

INVERSO

DEFINIÇÃO:

Seja n um inteiro positivo e seja b um elemento invertível de Z_n .

Seja $a \oslash b$ arbitrário. Então, $a \otimes b^{-1}$.

EXEMPLO: Calcule $2 \oslash 7$, ou seja 7^{-1}, em Z_{10}

INVERSO

EXEMPLO: Calcule $2 \oslash 7$, ou seja 7^{-1}, em Z_{10}

* usar a tabela
de multiplicação:

INVERSO

EXEMPLO: Calcule $2 \oslash 7$, ou seja 7^{-1}, em Z_{10}

* usar a tabela de multiplicação:

$\otimes$	0	1	2	3	4	5	6	7	8	9
0										
1										
2										
3										
4										
5										
6										
7										
8										
9										

INVERSO

EXEMPLO: Calcule $2 \oslash 7$, ou seja 7^{-1}, em Z_{10}

* usar a tabela de multiplicação:

$(0 \cdot 0) \, mod \, 10 = 0 \, mod \, 10 = 0$

$\otimes$	0	1	2	3	4	5	6	7	8	9
0										
1										
2										
3										
4										
5										
6										
7										
8										
9										

INVERSO

EXEMPLO: Calcule $2 \oslash 7$, ou seja 7^{-1}, em Z_{10}

* usar a tabela de multiplicação:

$(0 \cdot 0) \, mod \, 10 = 0 \, mod \, 10 = 0$

$\otimes$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0									
2	0									
3	0									
4	0									
5	0									
6	0									
7	0									
8	0									
9	0									

INVERSO

EXEMPLO: Calcule $2 \oslash 7$, ou seja 7^{-1}, em Z_{10}

* usar a tabela de multiplicação:

$(0 \cdot 0) \, mod \, 10 = 0 \, mod \, 10 = 0$

$(1 \cdot 2) \, mod \, 10 = 2 \, mod \, 10 = 2$

$\otimes$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2								
3	0	3								
4	0	4								
5	0	5								
6	0	6								
7	0	7								
8	0	8								
9	0	9								

INVERSO

EXEMPLO: Calcule $2 \oslash 7$, ou seja 7^{-1}, em Z_{10}

* usar a tabela de multiplicação:

$(0 \cdot 0) \, mod \, 10 = 0 \, mod \, 10 = 0$

$(1 \cdot 2) \, mod \, 10 = 2 \, mod \, 10 = 2$

$(2 \cdot 3) \, mod \, 10 = 6 \, mod \, 10 = 6$

$\otimes$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9						
4	0	4	8	2						
5	0	5	0	5						
6	0	6	2	8						
7	0	7	4	1						
8	0	8	6	4						
9	0	9	8	7						

INVERSO

EXEMPLO: Calcule $2 \oslash 7$, ou seja 7^{-1}, em Z_{10}

* usar a tabela de multiplicação:

$(0 \cdot 0) \, mod \, 10 = 0 \, mod \, 10 = 0$

$(1 \cdot 2) \, mod \, 10 = 2 \, mod \, 10 = 2$

$(2 \cdot 3) \, mod \, 10 = 6 \, mod \, 10 = 6$

$(5 \cdot 2) \, mod \, 10 = 10 \, mod \, 10 = 0$

$\otimes$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0				
7	0	7	4	1	8	5				
8	0	8	6	4	2	0				
9	0	9	8	7	6	5				

INVERSO

EXEMPLO: Calcule $2 \oslash 7$, ou seja 7^{-1}, em Z_{10}

* usar a tabela de multiplicação:

$\otimes$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2			
8	0	8	6	4	2	0	8			
9	0	9	8	7	6	5	4			

$(0 \cdot 0) \bmod 10 = 0 \bmod 10 = 0$

$(1 \cdot 2) \bmod 10 = 2 \bmod 10 = 2$

$(2 \cdot 3) \bmod 10 = 6 \bmod 10 = 6$

$(5 \cdot 2) \bmod 10 = 10 \bmod 10 = 0$

$(6 \cdot 2) \bmod 10 = 12 \bmod 10 = 2$

INVERSO

EXEMPLO: Calcule $2 \oslash 7$, ou seja 7^{-1}, em Z_{10}

* usar a tabela de multiplicação:

$\otimes$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9		
8	0	8	6	4	2	0	8	6		
9	0	9	8	7	6	5	4	3		

$(0 \cdot 0) \bmod 10 = 0 \bmod 10 = 0$

$(1 \cdot 2) \bmod 10 = 2 \bmod 10 = 2$

$(2 \cdot 3) \bmod 10 = 6 \bmod 10 = 6$

$(5 \cdot 2) \bmod 10 = 10 \bmod 10 = 0$

$(6 \cdot 2) \bmod 10 = 12 \bmod 10 = 2$

$(7 \cdot 4) \bmod 10 = 28 \bmod 10 = 8$

INVERSO

EXEMPLO: Calcule $2 \oslash 7$, ou seja 7^{-1}, em Z_{10}

* usar a tabela de multiplicação:

$\otimes$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4			

$(0 \cdot 0) \bmod 10 = 0 \bmod 10 = 0$

$(1 \cdot 2) \bmod 10 = 2 \bmod 10 = 2$

$(2 \cdot 3) \bmod 10 = 6 \bmod 10 = 6$

$(5 \cdot 2) \bmod 10 = 10 \bmod 10 = 0$

$(6 \cdot 2) \bmod 10 = 12 \bmod 10 = 2$

$(7 \cdot 4) \bmod 10 = 28 \bmod 10 = 8$

$(8 \cdot 3) \bmod 10 = 24 \bmod 10 = 4$

INVERSO

EXEMPLO: Calcule $2 \oslash 7$, ou seja 7^{-1}, em Z_{10}

* usar a tabela de multiplicação:

$\otimes$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

$(0 \cdot 0) \bmod 10 = 0 \bmod 10 = 0$

$(1 \cdot 2) \bmod 10 = 2 \bmod 10 = 2$

$(2 \cdot 3) \bmod 10 = 6 \bmod 10 = 6$

$(5 \cdot 2) \bmod 10 = 10 \bmod 10 = 0$

$(6 \cdot 2) \bmod 10 = 12 \bmod 10 = 2$

$(7 \cdot 4) \bmod 10 = 28 \bmod 10 = 8$

$(8 \cdot 3) \bmod 10 = 24 \bmod 10 = 4$

$(9 \cdot 5) \bmod 10 = 45 \bmod 10 = 5$

INVERSO

EXEMPLO: Calcule $2 \oslash 7$, ou seja 7^{-1}, em Z_{10}

* usar a tabela de multiplicação:

* buscar:

$$a \otimes b = 1$$

→ 1 é resto

$\otimes$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

INVERSO

EXEMPLO: Calcule $2 \oslash 7$, ou seja 7^{-1} em Z_{10}

* usar a tabela de multiplicação:

* buscar:

$$a \otimes b = 1$$

→ 1 é resto

* $7 \Rightarrow 3$

$\otimes$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

logo,

$$2 \oslash 7 \quad \Rightarrow \quad 2 \otimes 3 \quad \Rightarrow \quad 2 \cdot 3 \ mod \ 10 = 6$$

INVERSO

EXEMPLO: Calcule $2 \oslash 7$, ou seja 7^{-1} em Z_{10}

$\otimes$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Obs:
→ nem todas as classes tem inverso
→ 1, 3, 7, e 9 tem porque são primos
→ se fosse Z_{11} como 11 é primo todas as classes possuem inverso

logo,

$$2 \oslash 7 \quad \Rightarrow \quad 2 \otimes 3 \quad \Rightarrow \quad 2 \cdot 3 \ mod \ 10 = 6$$

Aritmética Modular

INVERSO

Teorema:
(Elementos Invertíveis de Z_n)

Seja n um inteiro positivo e seja $a \in Z_n$. Então, a é invertível se , e somente se, a e n são relativamente primos.

→ ou seja, se a é invertível → $\exists b \in Z_n / a \otimes b = 1 \rightarrow$ $a \cdot b \bmod n = 1$ $\Rightarrow$ $a\,b + k\,n = 1$, $\forall k \in \mathbb{Z}$

com a e n relativamente primos. Logo, $\exists x, y \in \mathbb{Z}$ tais que $a\,x + n\,y = 1$ e a é invertível em Z_n.

Se $b = x \mod n$ $\Rightarrow$ $b = x + k\,n$, $\forall k \in \mathbb{Z}$ temos:

Aritmética Modular

INVERSO

Teorema:
(Elementos Invertíveis de Z_n)

Seja n um inteiro positivo e seja $a \in Z_n$. Então, a é invertível se , e somente se, a e n são relativamente primos.

→ ou seja, se a é invertível → $\exists b \in Z_n / a \otimes b = 1 \rightarrow$ $a \cdot b \bmod n = 1$ $\Rightarrow$ $ab + kn = 1$, $\forall k \in \mathbb{Z}$

com a e n relativamente primos. Logo, $\exists x, y \in \mathbb{Z}$ tais que $ax + ny = 1$ e a é invertível em Z_n.

Se $b = x \mod n \Rightarrow b = x + kn$, $\forall k \in \mathbb{Z}$ temos:

$$ax + ny = 1 \longrightarrow 1 = ax + ny \longrightarrow 1 = a(b - kn) + ny \longrightarrow 1 = ab + (y - ka)n$$

então,

$$a \otimes b = ab \mod n = 1$$

e b é inverso de a → a é invertível em Z_n.

INVERSO

EXEMPLO: Determine 29^{-1} em Z_{431}

INVERSO

EXEMPLO: Determine 29^{-1} em Z_{431}

1º) escrever: $431\,x + 29\,y = 1$

INVERSO

EXEMPLO: Determine 29^{-1} em Z_{431}

1º) escrever: $431\,x + 29\,y = 1$

Na aula anterior, determinamos o valor de x e y a partir de $mdc(431,29)=1$

$$x=7 \qquad\qquad y=-104$$

INVERSO

EXEMPLO: Determine 29^{-1} em Z_{431}

1º) escrever: $431\,x + 29\,y = 1$

Na aula anterior, determinamos o valor de x e y a partir de $mdc(431,29)=1$

$$x=7 \qquad y=-104$$

2º) tem-se:

$$ab \mod n = 1 \longrightarrow (29\cdot(-104)) \mod 431 = 1$$

INVERSO

EXEMPLO: Determine 29^{-1} em Z_{431}

1º) escrever: $431\,x+29\,y=1$

Na aula anterior, determinamos o valor de x e y a partir de $mdc(431,29)=1$

$$x=7 \qquad y=-104$$

2º) tem-se:

$$ab \mod n=1 \longrightarrow (29\cdot(-104)) \mod 431=1$$

Mas, $-104 \notin Z_{431}$ então, fazemos:

INVERSO

EXEMPLO: Determine 29^{-1} em Z_{431}

1º) escrever: $431\,x + 29\,y = 1$

Na aula anterior, determinamos o valor de x e y a partir de $mdc(431,29)=1$

$$x=7 \qquad y=-104$$

2º) tem-se:

$$ab \mod n = 1 \longrightarrow (29\cdot(-104)) \mod 431 = 1$$

Mas, $-104 \notin Z_{431}$ então, fazemos:

$$b = -104 \mod 431 = 327$$

INVERSO

EXEMPLO: Determine 29^{-1} em Z_{431}

1º) escrever: $431\,x + 29\,y = 1$

Na aula anterior, determinamos o valor de x e y a partir de $mdc(431,29)=1$

$$x=7 \qquad y=-104$$

2º) tem-se:

$$ab \mod n = 1 \longrightarrow (29\cdot(-104)) \mod 431 = 1$$

Mas, $-104 \notin Z_{431}$ então, fazemos:

$$b = -104 \mod 431 = 327$$

$$29 \otimes 327 = (29\cdot 327) \mod 431$$

INVERSO

EXEMPLO: Determine 29^{-1} em Z_{431}

1º) escrever: $431\,x + 29\,y = 1$

Na aula anterior, determinamos o valor de x e y a partir de $mdc(431,29)=1$

$$x=7 \qquad y=-104$$

2º) tem-se:

$$ab \mod n = 1 \longrightarrow (29\cdot(-104)) \mod 431 = 1$$

Mas, $-104 \notin Z_{431}$ então, fazemos:

$$b = -104 \mod 431 = 327$$

$$29 \otimes 327 = (29\cdot 327) \mod 431 = 94383 \mod 431 = 1$$

INVERSO

EXEMPLO: Determine 29^{-1} em Z_{431}

1º) escrever: $431\,x+29\,y=1$

Na aula anterior, determinamos o valor de x e y a partir de $mdc(431,29)=1$

$$x=7 \qquad y=-104$$

2º) tem-se:

$$ab \mod n=1 \longrightarrow (29\cdot(-104)) \mod 431=1$$

Mas, $-104\notin Z_{431}$ então, fazemos:

$$b=-104 \mod 431=327$$

$$29\otimes 327=(29\cdot 327) \mod 431=94383 \mod 431=1$$

$$29^{-1}=327$$

INVERSO

EXEMPLO: Determine $30 \oslash 29$ em Z_{431}

INVERSO

EXEMPLO: Determine $30 \oslash 29$ em Z_{431}

$$30 \oslash 29 = 30 \otimes 327$$

INVERSO

EXEMPLO: Determine $30 \oslash 29$ em Z_{431}

$$30 \oslash 29 = 30 \otimes 327$$
$$= (30 \cdot 327) \mod 431$$

INVERSO

EXEMPLO: Determine $30 \oslash 29$ em Z_{431}

$$
\begin{aligned}
30 \oslash 29 &= 30 \otimes 327 \\
&= (30 \cdot 327) \ \ mod \ \ 431 \\
&= 9810 \ \ mod \ \ 431
\end{aligned}
$$

INVERSO

EXEMPLO: Determine $30 \oslash 29$ em Z_{431}

$$
\begin{aligned}
30 \oslash 29 &= 30 \otimes 327 \\
&= (30 \cdot 327) \ \ mod \ \ 431 \\
&= 9810 \ \ mod \ \ 431 \\
&= 328
\end{aligned}
$$

EXPONENCIAÇÃO MODULAR

$$A^B \mod C = (A \mod C)^B \mod C$$

OBS: Se B muito grande, então A^B torna-se muito grande

EXPONENCIAÇÃO MODULAR

$$A^B \mod C = (A \mod C)^B \mod C$$

OBS: Se B muito grande, então A^B torna-se muito grande

EXEMPLO:

$$2^{90} = 1\,237\,940\,039\,290\,000\,000\,000\,000\,000$$

* calculadoras tem dificuldade em representar números tão grandes

$$2^{90} \mod 13 = ?$$

Aritmética Modular

EXPONENCIAÇÃO MODULAR $A^B \mod C = (A \mod C)^B \mod C$

EXEMPLO: $2^{90} \mod 13 = ?$

Aritmética Modular

EXPONENCIAÇÃO MODULAR $A^B \mod C = (A \mod C)^B \mod C$

EXEMPLO: $2^{90} \mod 13 = ?$

$$2^{90} = 2^{50} \cdot 2^{40}$$

Aritmética Modular

EXPONENCIAÇÃO MODULAR $A^B \mod C = (A \mod C)^B \mod C$

EXEMPLO: $2^{90} \mod 13 = ?$

$$2^{90} = 2^{50} \cdot 2^{40} \longrightarrow 2^{50} \mod 13 = 4 \; ; \; 2^{40} \mod 13 = 3$$

Aritmética Modular

EXPONENCIAÇÃO MODULAR $A^B \ mod \ C = (A \ mod \ C)^B \ mod \ C$

EXEMPLO: $2^{90} \ mod \ 13 = ?$

$$2^{90} = 2^{50} \cdot 2^{40} \longrightarrow 2^{50} \ mod \ 13 = 4 \ ; \ 2^{40} \ mod \ 13 = 3$$

$$2^{90} \ mod \ 13 = (2^{50} \cdot 2^{40}) \ mod \ 13$$

Aritmética Modular

EXPONENCIAÇÃO MODULAR $A^B \ mod \ C = (A \ mod \ C)^B \ mod \ C$

EXEMPLO: $2^{90} \ mod \ 13 = ?$

$$2^{90} = 2^{50} \cdot 2^{40} \longrightarrow 2^{50} \ mod \ 13 = 4 \ ; \ 2^{40} \ mod \ 13 = 3$$

$$2^{90} \ mod \ 13 = (2^{50} \cdot 2^{40}) \ mod \ 13$$

$$2^{90} \ mod \ 13 = (2^{50} \ mod \ 13 \cdot 2^{40} \ mod \ 13) \ mod \ 13$$

Aritmética Modular

EXPONENCIAÇÃO MODULAR $A^B \ mod \ C = (A \ mod \ C)^B \ mod \ C$

EXEMPLO: $2^{90} \ mod \ 13 = ?$

$$2^{90} = 2^{50} \cdot 2^{40} \longrightarrow 2^{50} \ mod \ 13 = 4 \ ; \ 2^{40} \ mod \ 13 = 3$$

$$2^{90} \ mod \ 13 = (2^{50} \cdot 2^{40}) \ mod \ 13$$

$$2^{90} \ mod \ 13 = (2^{50} \ mod \ 13 \cdot 2^{40} \ mod \ 13) \ mod \ 13$$

$$2^{90} \ mod \ 13 = (4 \cdot 3) \ mod \ 13$$

Aritmética Modular

EXPONENCIAÇÃO MODULAR $A^B \ mod \ C = (A \ mod \ C)^B \ mod \ C$

EXEMPLO: $2^{90} \ mod \ 13 = ?$

$$2^{90} = 2^{50} \cdot 2^{40} \longrightarrow 2^{50} \ mod \ 13 = 4 \ ; \ 2^{40} \ mod \ 13 = 3$$

$$2^{90} \ mod \ 13 = (2^{50} \cdot 2^{40}) \ mod \ 13$$

$$2^{90} \ mod \ 13 = (2^{50} \ mod \ 13 \cdot 2^{40} \ mod \ 13) \ mod \ 13$$

$$2^{90} \ mod \ 13 = (4 \cdot 3) \ mod \ 13$$

$$2^{90} \ mod \ 13 = 12 \ mod \ 13$$

Aritmética Modular

EXPONENCIAÇÃO MODULAR $A^B \ mod \ C = (A \ mod \ C)^B \ mod \ C$

EXEMPLO: $2^{90} \ mod \ 13 = ?$

$$2^{90} = 2^{50} \cdot 2^{40} \longrightarrow 2^{50} \ mod \ 13 = 4 \ ; \ 2^{40} \ mod \ 13 = 3$$

$$2^{90} \ mod \ 13 = (2^{50} \cdot 2^{40}) \ mod \ 13$$

$$2^{90} \ mod \ 13 = (2^{50} \ mod \ 13 \cdot 2^{40} \ mod \ 13) \ mod \ 13$$

$$2^{90} \ mod \ 13 = (4 \cdot 3) \ mod \ 13$$

$$2^{90} \ mod \ 13 = 12 \ mod \ 13$$

$$2^{90} \ mod \ 13 = 12$$

EXPONENCIAÇÃO MODULAR

EXEMPLO: 7^{256} ?

* nem todo cálculo é simples, como o anterior. Neste caso, por exemplo, o cálculo exige 5 divisões.

Existem outras possibilidades como, por exemplo, o conceito binário.

Para ilustrar tal exemplo verifique o exemplo disponibilizado na *timeline* da disciplina para $5^{117} \mod 19$ (Khan academy).

EXERCÍCIOS:

1) Calcule em Z_{10}

a) $3 \oplus 3$

b) $6 \oplus 6$

c) $3 \otimes 3$

d) $6 \otimes 6$

e) $5 \ominus 8$

2) Faça a tabela para Z_8 e verifique a existência de elementos invertíveis. Eles existem? Quem são eles?

3) Calcule Y dados:

a) $A \bmod 11 = 6 \;\; ; \;\; B \bmod 11 = 7 \;\; e \;\; (A+B) \bmod 11 = Y$

b) $A \bmod 12 = 5 \;\; ; \;\; B \bmod 12 = 11 \;\; e \;\; (A \cdot B) \bmod 12 = Y$

Lembre-se: $(X * Y) \bmod Z = (X \bmod Z * Y \bmod Z) \bmod Z$

EXERCÍCIOS:

4) Quais das opções a seguir são equivalentes a (894-573)mod 7?

a) $(5+1) mod\, 7$

b) 5

c) $2\, mod\, 7$

d) $6\, mod\, 7$

e) $(7-5) mod\, 7$

f) $(2+3) mod\, 7$

5) Utilizando a técnica do circulo modular determine:

$8 \bmod 4$

$7 \bmod 2$

$-5 \bmod 3$

EXERCÍCIOS:

6) (Khan Academy)

Quais das seguintes expressões são equivalentes a $111 \bmod 10$?

$A : (110 \bmod 10 + 1 \bmod 10) \bmod 10$

$B : (1 \bmod 10 + 1 \bmod 10 + 1 \bmod 10) \bmod 10$

$C : (100 \bmod 10 + 10 \bmod 10 + 1 \bmod 10) \bmod 10$

$D : (11 \bmod 10 + 100 \bmod 10) \bmod 10$

RESOLUÇÃO EXERCÍCIOS:

1) Z_{10}

a) $3 \oplus 3 = (3 + 3) \bmod 10 = 6 \bmod 10 = 6$

b) $6 \oplus 6 = (6 + 6) \bmod 10 = 12 \bmod 10 = 2$

c) $3 \otimes 3 = (3 \cdot 3) \bmod 10 = 9 \bmod 10 = 9$

d) $6 \otimes 6 = (6 \cdot 6) \bmod 10 = 36 \bmod 10 = 6$

e) $5 \ominus 8 = (5-8) \bmod 10 = -3 \bmod 10 = 7$

$a = n\,q + r$

$-3 = 10\,q + r$

$-3 = 10\,(-1) + r$

$-3 = -10 + r$

$10-3 = r \rightarrow r = 7$

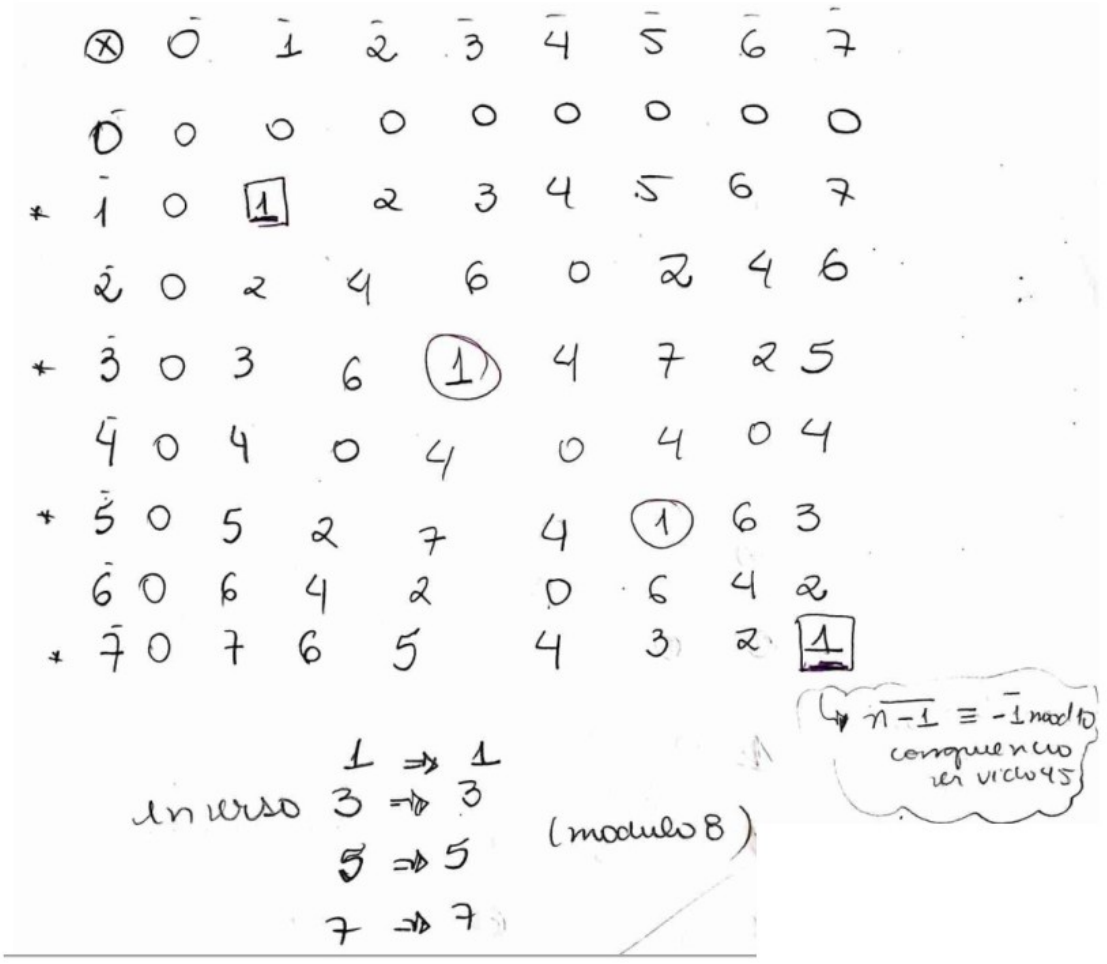
RESOLUÇÃO EXERCÍCIOS:

0 . 0 mod 8

0 mod 8

0

2)



em Z8

2 divido mod n por 3

= 2 x 3 mod n

em Z10

2 divido mod n por 3

= 2 x 7 mod n

pq lá a inversa do 3 é o 7

RESOLUÇÃO EXERCÍCIOS:

3)

a) $A \bmod 11 = 6 \;;\; B \bmod 11 = 7 \;\; e \;\; (A+B) \bmod 11 = Y$

$$(A + B) \bmod 11 = (A \bmod 11 + B \bmod 11) \bmod 11$$

$$(A + B) \bmod 11 = (6 + 7) \bmod 11$$

$$(A + B) \bmod 11 = 13 \bmod 11$$

$$(A + B) \bmod 11 = 2$$

$$Y = 2$$

b) $A \bmod 12 = 5 \;;\; B \bmod 12 = 11 \;\; e \;\; (A \cdot B) \bmod 12 = Y$

$$(A \cdot B) \bmod 12 = (A \bmod 12 \cdot B \bmod 12) \bmod 12$$

$$(A \cdot B) \bmod 12 = (5 \cdot 11) \bmod 12$$

$$(A \cdot B) \bmod 12 = 55 \bmod 12$$

$$(A \cdot B) \bmod 12 = 7$$

$$Y = 7$$

RESOLUÇÃO EXERCÍCIOS:

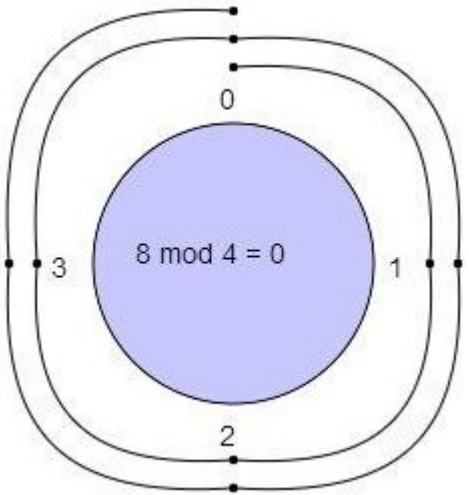
4)

- [x] $(5 + 1) \bmod 7$
- [ ] 5
- [ ] $2 \bmod 7$
- [x] $6 \bmod 7$
- [ ] $(7 - 5) \bmod 7$
- [ ] $(2 + 3) \bmod 7$

RESOLUÇÃO EXERCÍCIOS:

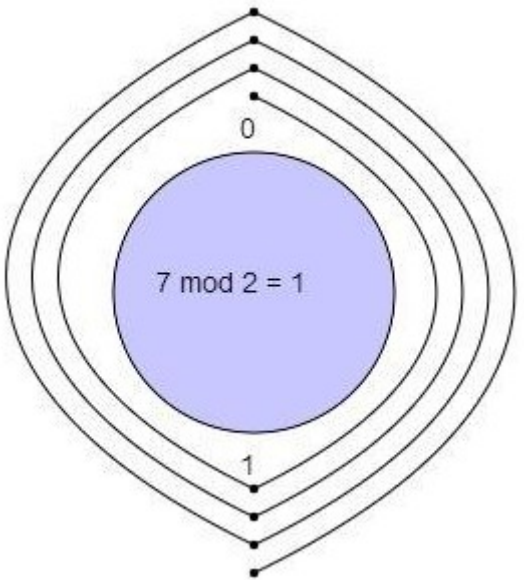
5)

$8 \bmod 4$



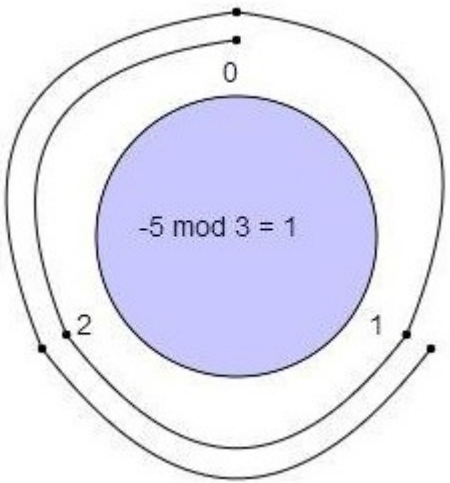
$8 \bmod 4 = \mathbf{0}$

$7 \bmod 2$



$7 \bmod 2 = \mathbf{1}$

$-5 \bmod 3$



$-5 \bmod 3 = \mathbf{1}$

RESOLUÇÃO EXERCÍCIOS:

6)

Lembre-se que:

$$(X + Y) \bmod Z = (X \bmod Z + Y \bmod Z) \bmod Z$$

OU mais geralmente:

$$(u_1 + u_2 + ... + u_n) \bmod Z = (u_1 \bmod Z + u_2 \bmod Z + ... + u_n \bmod Z) \bmod Z$$

Verifcar a declaração de A:

$$(110 \bmod 10 + 1 \bmod 10) \bmod 10 = (110 + 1) \bmod 10$$

$$(110 \bmod 10 + 1 \bmod 10) \bmod 11 = 111 \bmod 11$$

Verifcar a declaração de B:

$$(1 \bmod 10 + 1 \bmod 10 + 1 \bmod 10) \bmod 10 = (1 + 1 + 1) \bmod 10$$

$$(1 \bmod 10 + 1 \bmod 10 + 1 \bmod 10) \bmod 10 = 3 \bmod 10$$

RESOLUÇÃO EXERCÍCIOS:

Verificar a declaração de C:

$$C : (100 \bmod 10 + 10 \bmod 10 + 1 \bmod 10) \bmod 10 = (100 + 10 + 1) \bmod 10$$

$$C : (100 \bmod 10 + 10 \bmod 10 + 1 \bmod 10) \bmod 10 = 111 \bmod 10$$

Verificar a declaração de D:

$$D : (11 \bmod 10 + 100 \bmod 10) \bmod 10 = (11 + 100) \bmod 10$$

$$D : (11 \bmod 10 + 100 \bmod 10) \bmod 10 = 111 \bmod 10$$

$$111 \bmod 10 = 1$$

$$3 \bmod 10 = 3$$

A, C e D **são declarações equivalentes a** $111 \bmod 10$