Estruturas Discretas

Teoria dos Números
Aritmética Modular

Profa. Helena Caseli
helenacaseli@dc.ufscar.br

Teoria dos Números

- **Conceitualização**
  - Teoria dos Números
    - Se preocupa com as propriedades e relações entre os números

Teoria dos Números

- **Conceitualização**
  - Teoria dos Números
    - Se preocupa com as propriedades e relações entre os números
  - Aritmética Modular
    - Estuda as operações básicas como adição e multiplicação no contexto dos números inteiros módulo n

Teoria dos Números

- **Conceitualização**
  - Teoria dos Números
    - Se preocupa com as propriedades e relações entre os números
  - Aritmética Modular
    - Estuda as operações básicas como adição e multiplicação no contexto dos números inteiros módulo n

RELEMBRANDO

- Função módulo (ou resto)
  - Para qualquer inteiro x e qualquer inteiro positivo n, a função módulo n, denotada por

$$f(x) = x \bmod n$$

  - Associa a cada x o resto da sua divisão (inteira) por n

Teoria dos Números

- **O que é?**
  - Um dos ramos mais antigos da matemática que engloba, basicamente, a teoria das propriedades dos inteiros (divisibilidade, paridade, primos relativos)

Teoria dos Números

- **O que é?**
  - Um dos ramos mais antigos da matemática que engloba, basicamente, a teoria das propriedades dos inteiros (divisibilidade, paridade, primos relativos)
- **Por que estudar?**
  - A Teoria dos Números se tornou central na criptografia e na segurança dos computadores

Teoria dos Números

- **O que é?**
  - Um dos ramos mais antigos da matemática que engloba, basicamente, a teoria das propriedades dos inteiros (divisibilidade, paridade, primos relativos)
- **Por que estudar?**
  - A Teoria dos Números se tornou central na criptografia e na segurança dos computadores
  - Neste curso
    - Não serão apresentados métodos para criptografia, mas veremos a aritmética modular, que é fundamental para esses métodos

Teoria dos Números

- **Divisibilidade**
  - Sejam a e b dois inteiros com $b \neq 0$. Dizemos que b divide a se há um inteiro c tal que $a = bc$
    - Denotamos $b|a$

Teoria dos Números

- **Divisibilidade**
  - Sejam a e b dois inteiros com b ≠ 0. Dizemos que b divide a se há um inteiro c tal que a = bc
    - Denotamos b|a

Teorema – Divisão

Sejam $a, b \in \mathbb{Z}$ com $b > 0$. Então, existem inteiros q e r tais que

$$a = qb + r \text{ e } 0 \leq r < b$$

Teoria dos Números

- **Divisibilidade**
  - Sejam a e b dois inteiros com b ≠ 0. Dizemos que b divide a se há um inteiro c tal que a = bc
    - Denotamos b|a

Teorema – Divisão

Sejam $a, b \in \mathbb{Z}$ com $b > 0$. Então, existem inteiros q e r tais que

$$a = qb + r \text{ e } 0 \leq r < b$$

- Além disso, existe um único par de tais inteiros (q, r) que satisfaz essas condições
- O inteiro q é chamado **quociente** e o inteiro r é chamado **resto**
- O resto nunca é negativo e só é igual a 0 se b|a

Teoria dos Números

- **Divisibilidade**

$$a = qb + r$$

  - Exemplos
    - Sejam a = 35 e b = 10
    - Sejam *a* = -37 e *b* = 5 (Atenção!! Divisão de um inteiro negativo)
    - Sejam *a* = -19 e *b* = 4

Teoria dos Números

- **Divisibilidade**

$$a = qb + r$$

  - Exemplos
    - Sejam a = 35 e b = 10

      Então o quociente é $q = 3$ e o resto é $r = 5$, porque

      $35 = 3 * 10 + 5$ e $0 \leq 5 < 10$

    - Sejam $a = -37$ e $b = 5$ (Atenção!! Divisão de um inteiro negativo)

      Então o quociente é $q = -8$ e o resto é $r = 3$, porque

      $-37 = -8 * 5 + 3$ e $0 \leq 3 < 5$

    - Sejam $a = -19$ e $b = 4$

      Então o quociente é $q = -5$ e o resto é $r = 1$, porque

      $-19 = -5 * 4 + 1$ e $0 \leq 1 < 4$

Teoria dos Números

- **Div e Mod**
  - São operações associadas ao processo de divisão
    - Div – retorna o quociente da divisão
    - Mod – retorna o resto da divisão

Teoria dos Números

- **Div e Mod**
  - São operações associadas ao processo de divisão
    - Div – retorna o quociente da divisão
    - Mod – retorna o resto da divisão

Sejam $a, b \in Z$ com $b > 0$. Pelo Teorema da Divisão, existe um único par de inteiros q e r tais que

$$a = qb + r \text{ e } 0 \leq r < b$$

Definimos as operações div e mod como:

$$a \text{ div } b = q \qquad \text{e} \qquad a \text{ mod } b = r$$

Teoria dos Números

- **Div e Mod**
  - Calcule
    - 12 div 5 = ? 12 mod 5 = ?
    - 35 div 3 = ? 35 mod 3 = ?
    - 30 div 6 = ? 30 mod 6 = ?
    - -7 div 4 = ? -7 mod 4 = ?
    - -19 div 7 = ? -19 mod 7 = ?
    - 11 div 3 = ? 11 mod 3 = ?
    - 23 div 10 = ? 23 mod 10 = ?

Teoria dos Números

- **Div e Mod**
  - Calcule
    - 12 div 5 = 2 12 mod 5 = 2
    - 35 div 3 = 11 35 mod 3 = 2
    - 30 div 6 = 5 30 mod 6 = 0
    - -7 div 4 = -2 -7 mod 4 = 1 *(-7 = -2 * 4 + 1 e 0 ≤ 1 < 4)*
    - -19 div 7 = -3 -19 mod 7 = 2
    - 11 div 3 = 3 11 mod 3 = 2
    - 23 div 10 = 2 23 mod 10 = 3

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - O máximo divisor comum de a, $b \in \mathbb{Z}$ é o maior inteiro que divide a e b
    - Denotamos mdc(a,b)

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - O máximo divisor comum de a, $b \in \mathbb{Z}$ é o maior inteiro que divide a e b
    - Denotamos mdc(a,b)

Sejam a, $b \in \mathbb{Z}$. Dizemos que um inteiro d é o **máximo divisor comum** de a e b se

- d é um divisor comum de a e b, e

- se c é um divisor comum de a e b, então $c \leq d$

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - O máximo divisor comum de a, $b \in \mathbb{Z}$ é o maior inteiro que divide a e b
    - Denotamos mdc(a,b)

Sejam a, $b \in \mathbb{Z}$. Dizemos que um inteiro d é o **máximo divisor comum** de a e b se

- d é um divisor comum de a e b, e

- se c é um divisor comum de a e b, então $c \leq d$

Se existir o mdc(a, b) então ele é único

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - Exemplos
    - mdc(18, 24) = **?**
    - mdc(30, 20) = **?**
    - mdc(30, 24) = **?**
    - mdc(-30, -24) = **?**

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - Exemplos
    - mdc(18, 24) = 6
    - mdc(30, 20) = 10
    - mdc(30, 24) = 6
    - mdc(-30, -24) = 6

Como calcular?

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - Algoritmo de Euclides

Proposição

Sejam a e b inteiros positivos, então

$\text{mdc}(a, b) = \text{mdc}(b, a \bmod b)$

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - Algoritmo de Euclides

Proposição

Sejam *a* e *b* inteiros positivos, então

mdc (*a*, *b*) = mdc (*b*, *a* mod *b*)

    - Entrada: dois inteiros positivos a e b

    - Saída: o b utilizado no último cálculo de mdc

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - Algoritmo de Euclides

Proposição

Sejam *a* e *b* inteiros positivos, então

mdc (*a*, *b*) = mdc (*b*, *a* mod *b*)

    - Entrada: dois inteiros positivos a e b
    - Passos
      - Dividir a por b e armazenar o resto em r
      - Se r = 0 retorna b
      - Senão calcular o mdc(b, r)
  - Saída: o b utilizado no último cálculo de mdc

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - Algoritmo de Euclides

Proposição

Sejam *a* e *b* inteiros positivos, então

mdc (*a*, *b*) = mdc (*b*, *a* mod *b*)

    - Entrada: dois inteiros positivos a e b
    - Passos
      - Dividir a por b e armazenar o resto em r
      - Se r = 0 retorna b
      - Senão calcular o mdc(b, r)
  - Saída: o b utilizado no último cálculo de mdc
  - ➔ Quando a < b, a primeira iteração do algoritmo de Euclides apenas inverte a ordem dos valores

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - Algoritmo de Euclides

Proposição

Sejam *a* e *b* inteiros positivos, então

mdc (*a*, *b*) = mdc (*b*, *a* mod *b*)

    - Entrada: dois inteiros positivos a e b
    - Passos
      - Dividir a por b e armazenar o resto em r
      - Se r = 0 retorna b
      - Senão calcular o mdc(b, r)
  - Saída: o b utilizado no último cálculo de mdc
  - ➔ Quando a < b, a primeira iteração do algoritmo de Euclides apenas inverte a ordem dos valores

Recursividade

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - Exemplos
    - mdc (18, 24)

mdc (18, 24) ⇒

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - Exemplos
    - mdc (18, 24)

mdc (18, 24) ⇒ 18 mod 24 = ?

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - Exemplos
    - mdc (18, 24)

mdc (18, 24) ⇒ 18 mod 24 = 18

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - Exemplos
    - mdc (18, 24)

mdc (18, 24) ⇒ 18 mod 24 = 18

mdc (24, 18) ⇒

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - Exemplos
    - mdc (18, 24)

mdc (18, 24) ⇒ 18 mod 24 = 18

mdc (24, 18) ⇒ 24 mod 18 = ?

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - Exemplos
    - mdc (18, 24)

mdc (18, 24) ⇒ 18 mod 24 = 18

mdc (24, 18) ⇒ 24 mod 18 = 6

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - Exemplos
    - mdc (18, 24)

mdc (18, 24) ⇒ 18 mod 24 = 18

mdc (24, 18) ⇒ 24 mod 18 = 6

mdc (18, 6) ⇒

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - Exemplos
    - mdc (18, 24)

mdc (18, 24) ⇒ 18 mod 24 = 18

mdc (24, 18) ⇒ 24 mod 18 = 6

mdc (18, 6) ⇒ 18 mod 6 = ?

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - Exemplos
    - mdc (18, 24)

mdc (18, 24) ⇒ 18 mod 24 = 18

mdc (24, 18) ⇒ 24 mod 18 = 6

mdc (18, 6) ⇒ 18 mod 6 = 0

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - Exemplos
    - mdc (18, 24)

mdc (18, 24) ⇒ 18 mod 24 = 18

mdc (24, 18) ⇒ 24 mod 18 = 6

mdc (18, 6) ⇒ 18 mod 6 = 0

⇒ 6

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - Calcule
    - mdc (75, 67)

mdc (75, 67) ⇒ ?

Teoria dos Números

- **Máximo Divisor Comum (MDC)**
  - Calcule
    - mdc (75, 67)

mdc (75, 67) ⇒ 75 mod 67 = 8

mdc (67, 8) ⇒ 67 mod 8 = 3

mdc (8, 3) ⇒ 8 mod 3 = 2

mdc (3, 2) ⇒ 3 mod 2 = 1

mdc (2, 1) ⇒ 2 mod 1 = 0

⇒ 1

Teoria dos Números

- **Números relativamente primos e número primo**
  - Sejam *a* e *b* inteiros. Dizemos que *a* e *b* são **relativamente primos** (ou primos entre si) se e somente se mdc(*a*, *b*) = 1
    - Dois inteiros são relativamente primos se os únicos divisores que eles têm em comum são 1 e -1

Teoria dos Números

- **Números relativamente primos e número primo**
  - Sejam *a* e *b* inteiros. Dizemos que *a* e *b* são **relativamente primos** (ou primos entre si) se e somente se mdc(*a*, *b*) = 1
    - Dois inteiros são relativamente primos se os únicos divisores que eles têm em comum são 1 e -1
  - Um inteiro positivo p > 1 é **primo** se ele é divisível por 1 e por ele mesmo (p)
    - Se n > 1 não é primo, então n é dito **composto**
      - 0 e 1 não são nem primos nem compostos!
      - 2 é o único primo par

Teoria dos Números

- **Fatoração em primos**

Teorema Fundamental da Aritmética

- Seja n um número inteiro positivo
- Então n se fatora (decompõe) em um produto de números primos
- Além disso, essa fatoração é única a menos da ordem dos primos

Teoria dos Números

- **Fatoração em primos**

Teorema Fundamental da Aritmética

- Seja n um número inteiro positivo
- Então n se fatora (decompõe) em um produto de números primos
- Além disso, essa fatoração é única a menos da ordem dos primos

  - Exemplos
    - 30 = **?**
    - 45 = **?**
    - 24 = **?**

Teoria dos Números

- **Fatoração em primos**

Teorema Fundamental da Aritmética

- Seja n um número inteiro positivo
- Então n se fatora (decompõe) em um produto de números primos
- Além disso, essa fatoração é única a menos da ordem dos primos

  - Exemplos
    - 30 = 2 * 3 * 5 (ou 5 * 2 * 3 ou 3 * 2 * 5)
    - 45 = 3 * 3 * 5
    - 24 = 2 * 2 * 2 * 3

Teoria dos Números

- **Fatoração em primos**

Teorema Fundamental da Aritmética

- Seja n um número inteiro positivo
- Então n se fatora (decompõe) em um produto de números primos
- Além disso, essa fatoração é única a menos da ordem dos primos

  - Exemplos
    - 30 = 2 * 3 * 5 (ou 5 * 2 * 3 ou 3 * 2 * 5)
    - 45 = 3 * 3 * 5
    - 24 = 2 * 2 * 2 * 3

    Qual o mdc(30,24)?

Teoria dos Números

- **Fatoração em primos & mdc**
  - Calculando mdc usando fatoração em primos
    - Sejam a e b inteiros positivos. Podemos fatorá-los em números primos como

      $a = 2^{e2}3^{e3}5^{e5}7^{e7}...$ $b = 2^{f2}3^{f3}5^{f5}7^{f7}...$

    - Assim, d = mdc(a, b) pode ser escrito como

      $d = 2^{x2}3^{x3}5^{x5}7^{x7}...$

    - Onde x2 = min{e2, f2}, x3 = min{e3, f3} e assim por diante
    - Exemplo
      - mdc(30,24)

        $30 = 2 * 3 * 5$

        $24 = 2^3 * 3$

      - $mdc(30,24) = 2^1 * 3^1 * 5^0 = 6$

Teoria dos Números

- **Fatoração em primos & mdc**
  - Calcule o mdc usando fatoração em primos
    a) mdc(15, 28)
    b) mdc(40, 78)
    c) mdc(13, 7)

Teoria dos Números

- **Fatoração em primos & mdc**
  - Calcule o mdc usando fatoração em primos

    a) mdc(15, 28) = 1

    $15 = 3^1 * 5^1$

    $28 = 2^2 * 7^1$

    b) mdc(40, 78) = 2

    $40 = 2^3 * 5^1$

    $78 = 2^1 * 3^1 * 13^1$

    c) mdc(13, 7) = 1

    $13 = 13^1$

    $7 = 7^1$

Teoria dos Números

- **Aritmética modular**
  - É o estudo das operações básicas (adição, subtração, multiplicação e divisão) no contexto dos números inteiros módulo n

Teoria dos Números

- **Aritmética modular**
  - É o estudo das operações básicas (adição, subtração, multiplicação e divisão) no contexto dos números inteiros módulo n
  - O conjunto Z_n
    - O conjunto Z_n, onde *n* é um inteiro positivo, é o conjunto de todos os números naturais de 0 a *n*-1, inclusive:

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

Teoria dos Números

- **Aritmética modular**
  - É o estudo das operações básicas (adição, subtração, multiplicação e divisão) no contexto dos números inteiros módulo n
  - O conjunto Z_n
    - O conjunto Z_n, onde *n* é um inteiro positivo, é o conjunto de todos os números naturais de 0 a *n*-1, inclusive:

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

    - Exemplos
      - $Z_1 = \{0\}$ $Z_2 = \{0, 1\}$ $Z_3 = \{0, 1, 2\}$
      - $Z_4 = \{0, 1, 2, 3\}$ ... $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
      - ...

Teoria dos Números

- **Aritmética modular**
  - Adição ($\oplus$) e multiplicação ($\otimes$) modulares
    - Para trabalhar com operações modulares, é necessário definir previamente qual o contexto em que as operações serão realizadas, ou seja o conjunto Z_n

Teoria dos Números

- **Aritmética modular**
  - Adição ($\oplus$) e multiplicação ($\otimes$) modulares
    - Para trabalhar com operações modulares, é necessário definir previamente qual o contexto em que as operações serão realizadas, ou seja o conjunto Z_n
    - Sejam n um inteiro positivo e $a, b \in Z_n$. Definimos

$$a \oplus b = (a + b) \bmod n \qquad \text{(adição modular)}$$

$$a \otimes b = (a * b) \bmod n \qquad \text{(multiplicação modular)}$$

Teoria dos Números

- **Aritmética modular**
  - Adição (⊕) e multiplicação (⊗) modulares
    - Para trabalhar com operações modulares, é necessário definir previamente qual o contexto em que as operações serão realizadas, ou seja o conjunto Z_n
    - Sejam n um inteiro positivo e $a, b \in Z_n$. Definimos

$$a \oplus b = (a + b) \bmod n \qquad \text{(adição modular)}$$

$$a \otimes b = (a * b) \bmod n \qquad \text{(multiplicação modular)}$$

- *"a soma modular de a e b no contexto Z_n é igual ao resto da divisão inteira da soma de a e b por n"*
- *"o produto modular de a e b no contexto Z_n é igual ao resto da divisão inteira do produto de a e b por n"*

Teoria dos Números

- **Aritmética modular**
  - Exemplos – adição (⊕) e multiplicação (⊗)
    - *Se n = 10,* $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
      - $5 \oplus 5 =$ **?**
      - $9 \oplus 8 =$ **?**
      - $5 \otimes 5 =$ **?**
      - $9 \otimes 8 =$ **?**

Teoria dos Números

- **Aritmética modular**
  - Exemplos – adição (⊕) e multiplicação (⊗)
    - *Se n = 10,* $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
      - $5 \oplus 5 = (5 + 5) \bmod 10 = 10 \bmod 10 = 0$
      - $9 \oplus 8 = (9 + 8) \bmod 10 = 17 \bmod 10 = 7$
      - $5 \otimes 5 = (5 * 5) \bmod 10 = 25 \bmod 10 = 5$
      - $9 \otimes 8 = (9 * 8) \bmod 10 = 72 \bmod 10 = 2$

Teoria dos Números

- **Aritmética modular**
  - Exemplos – adição (⊕) e multiplicação (⊗)
    - *Se $n = 10$,* $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
      - $5 \oplus 5 = (5 + 5) \bmod 10 = 10 \bmod 10 = 0$
      - $9 \oplus 8 = (9 + 8) \bmod 10 = 17 \bmod 10 = 7$
      - $5 \otimes 5 = (5 * 5) \bmod 10 = 25 \bmod 10 = 5$
      - $9 \otimes 8 = (9 * 8) \bmod 10 = 72 \bmod 10 = 2$
    - Se $n = 7$, $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$
      - $5 \oplus 5 =$ **?**
      - $3 \oplus 6 =$ **?**
      - $5 \otimes 5 =$ **?**
      - $3 \otimes 6 =$ **?**

Teoria dos Números

- **Aritmética modular**
  - Exemplos – adição (⊕) e multiplicação (⊗)
    - *Se $n = 10$,* $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
      - $5 \oplus 5 = (5 + 5) \bmod 10 = 10 \bmod 10 = 0$
      - $9 \oplus 8 = (9 + 8) \bmod 10 = 17 \bmod 10 = 7$
      - $5 \otimes 5 = (5 * 5) \bmod 10 = 25 \bmod 10 = 5$
      - $9 \otimes 8 = (9 * 8) \bmod 10 = 72 \bmod 10 = 2$
    - Se $n = 7$, $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$
      - $5 \oplus 5 = (5 + 5) \bmod 7 = 10 \bmod 7 = 3$
      - $3 \oplus 6 = (3 + 6) \bmod 7 = 9 \bmod 7 = 2$
      - $5 \otimes 5 = (5 * 5) \bmod 7 = 25 \bmod 7 = 4$
      - $3 \otimes 6 = (3 * 6) \bmod 7 = 18 \bmod 7 = 4$

Teoria dos Números

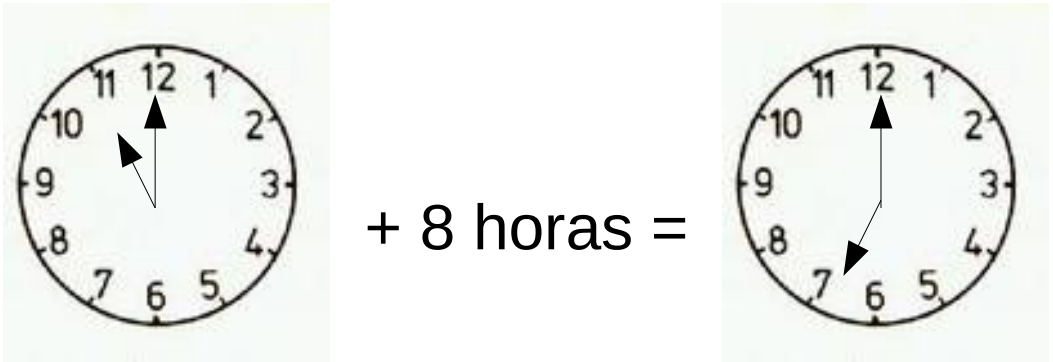
- **Aritmética modular**
  - Quanto é $11 \oplus 8$ em Z_{12}?

Teoria dos Números

- **Aritmética modular**
  - Quanto é $11 \oplus 8$ em Z_{12}?
    - (11+8) mod 12 = 19 mod 12 = 7

Teoria dos Números

- **Aritmética modular**
  - Quanto é $11 \oplus 8$ em Z_{12}?
    - (11+8) mod 12 = 19 mod 12 = 7
    - Analogia do relógio
      - 11 horas + 8 horas = (11+8) mod 12 = 19 mod 12 = 7



    - Por isso a aritmética modular também é chamada de aritmética do relógio ou circular

Teoria dos Números

- **Aritmética modular**
  - Propriedades das operações
    - **Fechamento**
      - Sejam $a, b \in Z_n$. Então $a \oplus b$ e $a \otimes b \in Z_n$
    - ➔ Essa propriedade diz que o resultado da soma ou da multiplicação modular entre elementos de um dado contexto também está no mesmo contexto

Teoria dos Números

- **Aritmética modular**
  - Propriedades das operações
    - **Fechamento**
      - Sejam $a, b \in Z_n$. Então $a \oplus b$ e $a \otimes b \in Z_n$
    - ➔ Essa propriedade diz que o resultado da soma ou da multiplicação modular entre elementos de um dado contexto também está no mesmo contexto
  - Exemplo
    - Se n = 10 e a = 9 e b = 8 (a, b $\in Z_{10}$)
    - $9 \oplus 8 = (9 + 8) \bmod 10 = 17 \bmod 10 = 7$ e $7 \in Z_{10}$

Teoria dos Números

- **Aritmética modular**
  - Propriedades das operações
    - **Comutatividade**
      - Seja n inteiro com $n \geq 2$
      - Para todos os valores $a, b \in Z_n$, temos que

$$\boldsymbol{a \oplus b = b \oplus a \text{ e } a \otimes b = b \otimes a}$$

    - **Associatividade**
      - Para todos os valores $a, b, c \in Z_n$, temos que

$$\boldsymbol{a \oplus (b \oplus c) = (a \oplus b) \oplus c \text{ e } a \otimes (b \otimes c) = (a \otimes b) \otimes c}$$

Teoria dos Números

- **Aritmética modular**
  - Propriedades das operações
    - **Elemento identidade**
      - Para todo $a \in Z_n$, temos que

$$\boldsymbol{a \oplus 0 = a,\ a \otimes 1 = a \text{ e } a \otimes 0 = 0}$$

    - **Distributividade**
      - Para todos os valores $a, b, c \in Z_n$, temos que

$$\boldsymbol{a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)}$$

Teoria dos Números

- **Aritmética modular**
  - Proposição
    - Seja n um inteiro positivo e sejam a, b $\in$ Z_n. Então, existe um e um só $x \in Z_n$ tal que a = b $\oplus$ x
      - O mesmo não pode ser afirmado sobre a multiplicação modular

Teoria dos Números

- **Aritmética modular**
  - Proposição
    - Seja n um inteiro positivo e sejam a, b $\in$ Z_n. Então, existe um e um só $x \in Z_n$ tal que a = b $\oplus$ x
      - O mesmo não pode ser afirmado sobre a multiplicação modular
  - Exemplo
    - Considere o contexto Z_{10} = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}
    - Qual é o valor de x que satisfaz a equação $2 \otimes x = 6$?
    - Qual é o valor de x que satisfaz a equação $2 \otimes x = 7$?

Teoria dos Números

- **Aritmética modular**
  - Proposição
    - Seja n um inteiro positivo e sejam a, b $\in$ Z_n. Então, existe um e um só $x \in Z_n$ tal que a = b $\oplus$ x
      - O mesmo não pode ser afirmado sobre a multiplicação modular
  - Exemplo
    - Considere o contexto Z_{10} = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}
    - Qual é o valor de x que satisfaz a equação $2 \otimes x = 6$?

      R. $2 \otimes 3 = 6$ e que $2 \otimes 8 = 6$. Assim, x pode ser 3 ou 8
    - Qual é o valor de x que satisfaz a equação $2 \otimes x = 7$?

      R. não há valores para x que resolvam essa equação

Teoria dos Números

- **Aritmética modular**
  - Subtração (θ) modular
    - Seja n um inteiro positivo e sejam a, b $\in Z_n$
    - Então,

$$\mathbf{a \; \theta \; b = (a-b) \bmod n}$$

    - Ou, alternativamente, definimos a θ b como o único valor x $\in Z_n$ tal que a = b $\oplus$ x

Teoria dos Números

- **Aritmética modular**
  - Subtração (θ) modular
    - Seja n um inteiro positivo e sejam a, b $\in Z_n$
    - Então,

$$\mathbf{a \; \theta \; b = (a-b) \bmod n}$$

    - Ou, alternativamente, definimos a θ b como o único valor x $\in Z_n$ tal que a = b $\oplus$ x
  - Exemplos
    - Se n = 10, Z_{10} = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}
      - 3 θ 2 = **?** (é a solução para 3 = 2 $\oplus$ x)
      - 9 θ 8 = **?** (é a solução para 9 = 8 $\oplus$ x)
      - 4 θ 9 = **?** (é a solução para 4 = 9 $\oplus$ x)

Teoria dos Números

- **Aritmética modular**
  - Subtração (θ) modular
    - Seja n um inteiro positivo e sejam a, b $\in Z_n$
    - Então,

$$\mathbf{a \ \theta \ b = (a-b) \bmod n}$$

    - Ou, alternativamente, definimos a θ b como o único valor x $\in Z_n$ tal que a = b $\oplus$ x
  - Exemplos
    - Se $n = 10$, $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
      - 3 θ 2 = **1** (é a solução para 3 = 2 $\oplus$ x)
      - 9 θ 8 = **1** (é a solução para 9 = 8 $\oplus$ x)
      - 4 θ 9 = **5** (é a solução para 4 = 9 $\oplus$ x)

Teoria dos Números

- **Aritmética modular**
  - Inverso (a^{-1}) modular
    - Sejam n um inteiro positivo e $a \in Z_n$. O inverso de a é um elemento $b \in Z_n$ tal que

$$a \otimes b = 1$$

Teoria dos Números

- **Aritmética modular**
  - Inverso (a^{-1}) modular
    - Sejam n um inteiro positivo e a $\in$ Z_n. O inverso de a é um elemento b $\in$ Z_n tal que

$$a \otimes b = 1$$

      - O inverso de um elemento a é denotado por a^{-1}
      - Um elemento de Z_n que tenha inverso é chamado **inversível**
      - Nem todos os elementos de Z_n têm inverso. Porém, se ele tiver inverso, esse inverso é único

Teoria dos Números

- **Aritmética modular**
  - Inverso (a^{-1}) modular
    - Exemplos
      - Em $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
      - O inverso de 2 é o elemento $x \in Z_{10}$ tal que $2 \otimes x = 1$
      - O inverso do elemento 3 é o elemento $x \in Z_{10}$ tal que $3 \otimes x = 1$

Teoria dos Números

- **Aritmética modular**
  - Inverso (a^{-1}) modular
    - Exemplos
      - Em $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
      - O inverso de 2 é o elemento $x \in Z_{10}$ tal que $2 \otimes x = 1$

      R. 2 não tem inverso

    - O inverso do elemento 3 é o elemento $x \in Z_{10}$ tal que $3 \otimes x = 1$

      R. Podemos verificar que $3 \otimes 7 = (3*7) \bmod 10 = 21 \bmod 10 = 1$

      Logo, $x = 7$ é o inverso de 3 em Z_{10}. Escrevemos $3^{-1} = 7$

Teoria dos Números

- **Aritmética modular**
  - Inverso (a^{-1}) modular
    - Se calcularmos o inverso de todos os elementos de Z_{10}, vamos verificar que:
      - 0 não tem inverso
      - Os elementos 2, 4, 5, 6 e 8 não têm inversos
      - Os elementos 1, 3, 7 e 9 têm inversos, e esse inverso é único

Teoria dos Números

- **Aritmética modular**
  - Inverso (a^{-1}) modular
    - Se calcularmos o inverso de todos os elementos de Z_{10}, vamos verificar que:
      - 0 não tem inverso
      - Os elementos 2, 4, 5, 6 e 8 não têm inversos
      - Os elementos 1, 3, 7 e 9 têm inversos, e esse inverso é único
    - ➔ Das afirmações colocadas, concluímos que os elementos de Z_{10} que têm inverso são exatamente aqueles que são relativamente primos com 10

Teoria dos Números

- **Aritmética modular**
  - Inverso (a^{-1}) modular

Teorema – Elementos invertíveis em 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

Teoria dos Números

- **Aritmética modular**
  - Inverso (a^{-1}) modular

Teorema – Elementos invertíveis em 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

  - Dois números inteiros são relativamente primos se o máximo divisor comum deles é 1, ou seja, mdc(a,b) = 1
  - De fato, os elementos de Z_{10} que são relativamente primos com 10 são exatamente aqueles que têm inverso em Z_{10}
    - mdc(1,10) = 1, mdc(3,10) = 1, mdc(7,10) = 1, mdc(9,10) = 1

Teoria dos Números

- **Aritmética modular**
  - No contexto $Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, diga quais são os elementos invertíveis em Z_9 e quais não são

Teoria dos Números

- **Aritmética modular**
  - No contexto $Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, diga quais são os elementos invertíveis em Z_9 e quais não são
    - Os elementos invertíveis em Z_9 são 1, 2, 4, 5, 7 e 8, todos relativamente primos com 9
    - Os elementos não invertíveis em Z_9 são 0, 3 e 6

Teoria dos Números

- **Aritmética modular**
  - Divisão (∅) modular
    - Seja n um inteiro positivo e seja b um elemento invertível de Z_n
    - Seja a $\in Z_n$ arbitrário
    - Então, definimos a divisão modular como

$$\mathbf{a \oslash b = a \otimes b^{-1}}$$

Teoria dos Números

- **Aritmética modular**
  - Divisão (∅) modular
    - Seja n um inteiro positivo e seja b um elemento invertível de Z_n
    - Seja a $\in Z_n$ arbitrário
    - Então, definimos a divisão modular como

$$\mathbf{a \varnothing b = a \otimes b^{-1}}$$

    - Exemplo
      - Em $\in Z_{10}$ calcule $2 \varnothing 7$
      - Como $7^{-1} = 3$, $2 \varnothing 7 = 2 \otimes 3 = 6$

Teoria dos Números

- **Aritmética modular**
  - Exemplo de aplicação
    - CPF – Cadastro de Pessoa Física
      - O CPF é composto por 11 dígitos, onde os primeiros oito dígitos são o número-base, o nono define a Região Fiscal, o penúltimo é o DV módulo 11 dos nove anteriores e o último é o DV módulo 11 dos dez anteriores
      - Exemplo: CPF = 280.012.389-38

Teoria dos Números

- **Aritmética modular**
  - Exemplo de aplicação
    - CPF – Cadastro de Pessoa Física
      - O CPF é composto por 11 dígitos, onde os primeiros oito dígitos são o número-base, o nono define a Região Fiscal, o penúltimo é o DV módulo 11 dos nove anteriores e o último é o DV módulo 11 dos dez anteriores
      - Exemplo: CPF = 280.012.389-38

S = 2*1 + 8*2 + 0*3 + 0*4 + 1*5 + 2*6 + 3*7 + 8*8 + 9*9

S = 2 + 16 + 0 + 0 + 5 + 12 + 21 + 64 + 81

201 mod 11 = 3

Teoria dos Números

- **Aritmética modular**
  - Exemplo de aplicação
    - CPF – Cadastro de Pessoa Física
      - O CPF é composto por 11 dígitos, onde os primeiros oito dígitos são o número-base, o nono define a Região Fiscal, o penúltimo é o DV módulo 11 dos nove anteriores e o último é o DV módulo 11 dos dez anteriores
      - Exemplo: CPF = 280.012.389-38

S = 2*0 + 8*1 + 0*2 + 0*3 + 1*4 + 2*5 + 3*6 + 8*7 + 9*8 + 3*9

S = 0 + 8 + 0 + 0 + 4 + 10 + 18 + 56 + 72 + 27

195 mod 11 = 8