Matemática Discreta

Teoria dos Números e Aritmética Modular

Profa. Helena Caseli
helenacaseli@ufscar.br

Teoria dos Números

- **Objetivos desta aula**
  - Apresentar alguns conceitos, propriedades e teoremas relativos aos inteiros
    - Divisibilidade
    - Máximo divisor comum
    - Números relativamente primos
    - Fatoração de primos
  - Capacitar o aluno a utilizar os conceitos da teoria dos números para modelar e resolver problemas computacionais

Teoria dos Números

- **Objetivos desta aula**
  - Apresentar a aritmética modular
    - O conjunto $\mathbb{Z}_n$
    - Adição modular e multiplicação modular e suas propriedades
    - Subtração modular
    - Inverso modular e $\mathbb{Z}_n^*$
    - Divisão modular
  - Capacitar o aluno a utilizar os conceitos da aritmética modular para modelar e resolver problemas computacionais

Problema #13

- **Liste os elementos do conjunto**

$$\mathbb{Z}_{14}^*$$

Teoria dos Números

- **Divisibilidade**

Fonte: https://pixabay.com/

- 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

$a = 12$ e $b = 3$

$12 = 3q + r$

$q = 4$ e $r = 0$

$a = 12$ e $b = 5$

$12 = 5q + r$

$q = 2$ e $r = 2$

- **Divisibilidade**
  - **Teorema da Divisão**
    - Sejam $a, b \in \mathbb{Z}$ com $b > 0$. Então, existem inteiros q e r tais que

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

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

Teoria dos Números

- **Máximo Divisor Comum (MDC)**

Fonte: https://pixabay.com/

- 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)**
  - 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 <u>único</u>

Teoria dos Números

mdc(54,8)
a = 54 e b = 8
54 = 8q + r
q = 6 e r = 6
mdc(8,6)

a = 8 e b = 6
8 = 6q + r
q = 1 e r = 2
mdc(6,2)
a = 6 e b = 2
6 = 2*3 + 0

- **Máximo Divisor Comum (MDC)**
  - **Algoritmo de Euclides**
    - **Proposição**
      - Sejam *a* e *b* inteiros positivos com b ≠ 0, 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

- **Números relativamente primos**

Fonte: https://pixabay.com/

- 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**

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 <u>única</u> 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

- **Aritmética modular**

Fonte: https://pixabay.com/

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

Teoria dos Números

- **Aritmética modular**
  - O conjunto $\mathbb{Z}_n$
    - O conjunto $\mathbb{Z}_n$, onde *n* é um inteiro positivo, é o conjunto de todos os números naturais de 0 a *n*-1, inclusive:

$$\mathbb{Z}_n = \{0, 1, 2, ..., n - 1\}$$

    - Exemplos
      - $\mathbb{Z}_1 = \{0\}$ $\mathbb{Z}_2 = \{0, 1\}$ $\mathbb{Z}_3 = \{0, 1, 2\}$
      - $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

→ Define o contexto no qual as operações da aritmética modular serão realizadas

Teoria dos Números

- **Aritmética modular**
  - Adição ($\oplus$) e multiplicação ($\otimes$) modulares
    - Sejam n um inteiro positivo e a, $b \in \mathbb{Z}_n$. Definimos

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

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

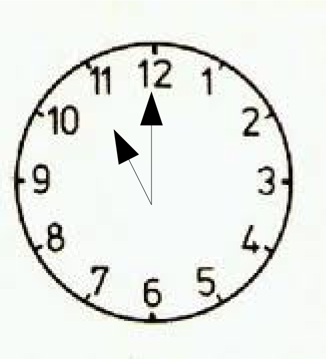
- *"a soma modular de a e b no contexto Z_n é igual ao resto da divisão inteira da soma de a e b por n"*
- *"o produto modular de a e b no contexto Z_n é igual ao resto da divisão inteira do produto de a e b por n"*

Teoria dos Números

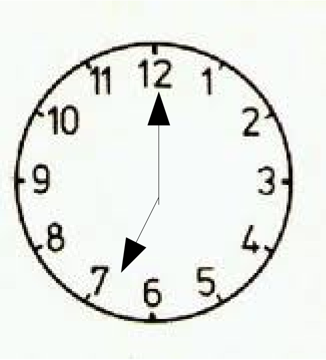
- **Aritmética modular**
  - Exemplos – adição ($\oplus$) e multiplicação ($\otimes$)
    - *Se* $n = 10$, $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
      - $5 \oplus 5 = (5 + 5) \bmod 10 = 10 \bmod 10 = 0$
      - $9 \oplus 8 = (9 + 8) \bmod 10 = 17 \bmod 10 = 7$
      - $5 \otimes 5 = (5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

Teoria dos Números

- **Aritmética modular**
  - Analogia do relógio
    - 11 horas + 8 horas = (11+8) mod 12 = 19 mod 12 = 7



+ 8 horas =



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

Teoria dos Números

- **Aritmética modular**
  - Exemplos – adição ($\oplus$) e multiplicação ($\otimes$)
    - Se $n = 7$, $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
      - $5 \oplus 5 =$ **?**
      - $3 \oplus 6 =$ **?**
      - $5 \otimes 5 =$ **?**
      - $3 \otimes 6 =$ **?**

Teoria dos Números

- **Aritmética modular**
  - Exemplos – adição ($\oplus$) e multiplicação ($\otimes$)
    - Se $n = 7$, $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
      - $5 \oplus 5 = (5 + 5) \bmod 7 = 10 \bmod 7 = 3$
      - $3 \oplus 6 = (3 + 6) \bmod 7 = 9 \bmod 7 = 2$
      - $5 \otimes 5 = (5 * 5) \bmod 7 = 25 \bmod 7 = 4$
      - $3 \otimes 6 = (3 * 6) \bmod 7 = 18 \bmod 7 = 4$

Teoria dos Números

- **Aritmética modular**
  - Propriedades das operações
    - **Fechamento**
      - Sejam a, b $\in \mathbb{Z}_n$. Então $a \oplus b$ e $a \otimes b \in \mathbb{Z}_n$

    → Essa propriedade diz que o resultado da soma ou da multiplicação modular entre elementos de um dado contexto também está no mesmo contexto
    - **Elemento identidade**
      - Para todo a $\in \mathbb{Z}_n$

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

Teoria dos Números

- **Aritmética modular**
  - Propriedades das operações
    - **Comutatividade**
      - Para todos a, b $\in \mathbb{Z}_n$

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

    - **Associatividade**
      - Para todos os valores a, b, c $\in \mathbb{Z}_n$

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

    - ***Distributividade***
      - Para todos os valores a, b, c $\in \mathbb{Z}_n$

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

Teoria dos Números

- **Aritmética modular**
  - **Proposição**
    - Seja n um inteiro positivo e sejam a, b $\in \mathbb{Z}_n$. Então, existe <u>um e um só</u> $x \in \mathbb{Z}_n$ tal que a = b $\oplus$ x
    - Exemplo
      - Considere o contexto $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
      - Qual é o valor de x que satisfaz a equação $6 = 2 \oplus x$?
        R. $2 \oplus 4 = 6$
      - Qual é o valor de x que satisfaz a equação $7 = 2 \oplus x$?
        R. $2 \oplus 5 = 7$

Teoria dos Números

- **Aritmética modular**
  - **Proposição**
    - Seja n um inteiro positivo e sejam a, b $\in \mathbb{Z}_n$. Então, existe <u>um e um só</u> $x \in \mathbb{Z}_n$ tal que a = b $\oplus$ x
      - O mesmo não pode ser afirmado sobre a multiplicação modular
  - Exemplo
    - Considere o contexto $\mathbb{Z}_{10}$ = {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 ($\ominus$) modular
    - Seja n um inteiro positivo e sejam a, b $\in \mathbb{Z}_n$
    - Então,

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

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

Teoria dos Números

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

$$\boldsymbol{a \otimes b = 1}$$

- ➔ O inverso de um elemento a é denotado por a^{-1}
- ➔ Um elemento de $\mathbb{Z}_n$ que tenha inverso é chamado **inversível**
- ➔ Nem todos os elementos de $\mathbb{Z}_n$ têm inverso
- ➔ Se o inverso existir, esse inverso é <u>único</u>

Teoria dos Números

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

    R. 2 não tem inverso

    - O inverso do elemento 3 é o elemento $x \in \mathbb{Z}_{10}$ 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 $\mathbb{Z}_{10}$, 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 $\mathbb{Z}_{10}$ que têm inverso são exatamente aqueles que são relativamente primos com 10

Teoria dos Números

- **Aritmética modular**
  - No contexto $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, diga quais são os elementos invertíveis em $\mathbb{Z}_9$ e quais não são

Teoria dos Números

- **Aritmética modular**
  - No contexto $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, diga quais são os elementos invertíveis em $\mathbb{Z}_9$ e quais não são
    - Os elementos invertíveis em $\mathbb{Z}_9$ são 1, 2, 4, 5, 7 e 8, todos relativamente primos com 9
    - Os elementos não invertíveis em $\mathbb{Z}_9$ são 0, 3 e 6

Teoria dos Números

- **Aritmética modular**
  - Definição ($\mathbb{Z}^*_n$)
    - Seja n um inteiro positivo. Definimos

$$\mathbb{Z}^*_{\mathbf{n}} = \{ a \in \mathbb{Z}_n \mid \mathrm{mdc}(a, n) = 1 \}$$

    - Exemplo
      - $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$
      - Elementos invertíveis em Z_9 são: 1, 2, 4, 5, 7, 8

$$\mathbb{Z}^*_9 = \{1, 2, 4, 5, 7, 8\}$$

      - Inversos

$\mathbf{1^{-1} = 1}$ $\mathbf{2^{-1} = 5}$ $\mathbf{4^{-1} = 7}$

$\mathbf{5^{-1} = 2}$ $\mathbf{7^{-1} = 4}$ $\mathbf{8^{-1} = 8}$

Teoria dos Números

- **Aritmética modular**
  - Divisão ($\oslash$) modular
    - Seja n um inteiro positivo e seja b um elemento invertível de $\mathbb{Z}_n$
    - Seja $a \in \mathbb{Z}_n$ arbitrário
    - Então, definimos a divisão modular como

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

    - Exemplo
      - Em $\mathbb{Z}_{10}$, $2 \oslash 7$ é calculado com base em 7^{-1}
      - $7^{-1} = 3$
      - $2 \oslash 7 = 2 \otimes 3 = 6$

Problema #13

- **Liste os elementos do conjunto**

$$\mathbb{Z}_{14}{}^{*}$$

Problema #13

- **Liste os elementos do conjunto**

$$\mathbb{Z}_{14}{}^{*} = \{\ 1,\ 3,\ 5,\ 9,\ 11,\ 13\ \}$$