Divisibilidade e Aritmética Modular

QXD0008 – Matemática Discreta

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Prof. Lucas Ismaily
ismailybf@ufc.br

Universidade Federal do Ceará

2º semestre/2025

Tópicos desta aula

Esta apresentação:

- Introduz os conceitos de divisibilidade e divisão inteira
- Discute propriedades da relação de divisibilidade
- Inclui exemplos de aplicação dos conceitos em demonstrações
- Introduz conceitos de Aritmética Modular
- Explora teoremas sobre congruências modulares e propriedades das operações em uma aritmética modular.

Referências para esta aula

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- **Seção 3.4** do livro: Matemática Discreta e suas Aplicações.
  Autor: Kenneth H. Rosen. Sexta Edição.

- **Seção 4.1** do livro: Discrete Mathematics and Its Applications.
  Author: Kenneth H. Rosen. Seventh Edition. **(English version)**

Introdução

Divisibilidade

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- **Definição:** Dados inteiros a e b com $a \neq 0$, dizemos que a **divide** b se e somente se existe um inteiro c tal que $b = ac$.

  Quando a **divide** b representamos isso pela notação $a|b$.

  Quando a **não divide** b representamos isso pela notação $a\nmid b$.

Divisibilidade

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- **Definição:** Dados inteiros a e b com $a \neq 0$, dizemos que a **divide** b se e somente se existe um inteiro c tal que $b = ac$.

  Quando a **divide** b representamos isso pela notação $a|b$.

  Quando a **não divide** b representamos isso pela notação $a\nmid b$.

Exemplo:

- 3 divide 6, pois $6 = 3 \cdot 3$
  ou seja, existe um inteiro c tal que $6 = 3 \cdot c$. Neste caso, temos $c = 2$

Divisibilidade

- **Definição:** Dados inteiros a e b com $a \neq 0$, dizemos que a **divide** b se e somente se existe um inteiro c tal que $b = ac$.

  Quando a **divide** b representamos isso pela notação $a|b$.

  Quando a **não divide** b representamos isso pela notação $a \nmid b$.

Exemplo:

- 3 divide 6, pois $6 = 3 \cdot 3$
  ou seja, existe um inteiro c tal que $6 = 3 \cdot c$. Neste caso, temos $c = 2$
- 2 divide -30, pois $-30 = 2 \cdot (-15)$
  ou seja, existe um inteiro c tal que $-30 = 2c$. Neste caso, temos $d = -15$.

Divisibilidade

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- **Definição:** Dados inteiros a e b com $a \neq 0$, dizemos que a **divide** b se e somente se existe um inteiro c tal que $b = ac$.

  Quando a **divide** b representamos isso pela notação $a|b$.

  Quando a **não divide** b representamos isso pela notação $a \nmid b$.

Exemplo:

- 3 divide 6, pois $6 = 3 \cdot 3$
  ou seja, existe um inteiro c tal que $6 = 3 \cdot c$. Neste caso, temos $c = 2$
- 2 divide -30, pois $-30 = 2 \cdot (-15)$
  ou seja, existe um inteiro c tal que $-30 = 2c$. Neste caso, temos $d = -15$.
- -4 divide 68, pois $68 = (-4) \cdot (-17)$
  ou seja, existe um inteiro c tal que $68 = -4c$. Neste caso, $c = -17$.

Divisibilidade

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- **Definição:** Dados inteiros a e b com $a \neq 0$, dizemos que a **divide** b se e somente se existe um inteiro c tal que $b = ac$.

  Quando a **divide** b representamos isso pela notação $a|b$.

  Quando a **não divide** b representamos isso pela notação $a \nmid b$.

Divisibilidade

- **Definição:** Dados inteiros a e b com $a \neq 0$, dizemos que a **divide** b se e somente se existe um inteiro c tal que $b = ac$.

  Quando a **divide** b representamos isso pela notação $a|b$.

  Quando a **não divide** b representamos isso pela notação $a \nmid b$.

Exemplo:

- 3 não divide 16, pois não existe nenhum inteiro c tal que $16 = 3c$.
  Como verificar?

Divisibilidade

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- **Definição:** Dados inteiros a e b com $a \neq 0$, dizemos que a **divide** b se e somente se existe um inteiro c tal que $b = ac$.

  Quando a **divide** b representamos isso pela notação $a|b$.

  Quando a **não divide** b representamos isso pela notação $a \nmid b$.

Exemplo:

- 3 não divide 16, pois não existe nenhum inteiro c tal que $16 = 3c$.
  Como verificar?

1. Por absurdo, suponha que existe $c \in \mathbb{Z}$ tal que $16 = 3c$.
2. Observe que $3 \cdot 5 = 15$ e que $3 \cdot 6 = 18$.
3. Como $15 < 16 < 18$, temos que $3 \cdot 5 < 3 \cdot c < 3 \cdot 6$.

Divisibilidade

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- **Definição:** Dados inteiros a e b com $a \neq 0$, dizemos que a **divide** b se e somente se existe um inteiro c tal que $b = ac$.

  Quando a **divide** b representamos isso pela notação $a|b$.

  Quando a **não divide** b representamos isso pela notação $a\nmid b$.

Exemplo:

- 3 não divide 16, pois não existe nenhum inteiro c tal que $16 = 3c$.
  Como verificar?

1. Por absurdo, suponha que existe $c \in \mathbb{Z}$ tal que $16 = 3c$.
2. Observe que $3 \cdot 5 = 15$ e que $3 \cdot 6 = 18$.
3. Como $15 < 16 < 18$, temos que $3 \cdot 5 < 3 \cdot c < 3 \cdot 6$.
4. Dividindo todos os termos da inequação por 3, obtemos $5 < c < 6$.
5. Absurdo, pois não existem inteiros entre 5 e 6.
6. Concluímos que não existe $c \in \mathbb{Z}$ tal que $16 = 3c$.

Divisibilidade

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Proposição 7.1: Sejam a e b números inteiros com $a \neq 0$. Então, a divide b se e somente se $\frac{b}{a}$ é um inteiro.

$$\forall a \forall b[a \neq 0 \ \rightarrow \ (a|b \ \leftrightarrow \ \frac{b}{a} \in \mathbb{Z})]$$

Divisibilidade

Proposição 7.1: Sejam a e b números inteiros com $a \neq 0$. Então, a divide b se e somente se $\frac{b}{a}$ é um inteiro.

$$\forall a \forall b [a \neq 0 \rightarrow (a | b \leftrightarrow \frac{b}{a} \in \mathbb{Z})]$$

Demonstração:

Divisibilidade

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Proposição 7.1: Sejam a e b números inteiros com $a \neq 0$. Então, a divide b se e somente se $\frac{b}{a}$ é um inteiro.

$$\forall a \forall b[a \neq 0 \ \rightarrow \ (a|b \ \leftrightarrow \ \frac{b}{a} \in \mathbb{Z})]$$

Demonstração:
Sejam a,b inteiros quaisquer com $a \neq 0$ (Instanciação).

($\Rightarrow$) Suponha que a divide b (Hipótese da PD). Pela definição de divisibilidade, existe um inteiro c tal que $b = ac$. Como $a \neq 0$, obtemos $\frac{b}{a} = c$ e, portanto, que $\frac{b}{a}$ é um inteiro.

Divisibilidade

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Proposição 7.1: Sejam a e b números inteiros com $a \neq 0$. Então, a divide b se e somente se $\frac{b}{a}$ é um inteiro.

$$\forall a \forall b [a \neq 0 \rightarrow (a|b \leftrightarrow \frac{b}{a} \in \mathbb{Z})]$$

Demonstração:
Sejam a,b inteiros quaisquer com $a \neq 0$ (Instanciação).

($\Rightarrow$) Suponha que a divide b (Hipótese da PD). Pela definição de divisibilidade, existe um inteiro c tal que $b = ac$. Como $a \neq 0$, obtemos $\frac{b}{a} = c$ e, portanto, que $\frac{b}{a}$ é um inteiro.

($\Leftarrow$) Suponha que $\frac{b}{a}$ é um inteiro (Hipótese da PD). Isso implica $\frac{b}{a} = c$ para $c \in \mathbb{Z}$. Multiplicando ambos os lados da igualdade por a, obtemos $b = ac$. Pela definição de divisibilidade, temos que a divide b. $\square$

Divisibilidade

Proposição 7.1: Sejam a e b números inteiros com $a \neq 0$. Então, a divide b se e somente se $\frac{b}{a}$ é um inteiro.

Exemplos:

- 2 divide -30, pois $-30 = 2 \cdot (-15)$
  da mesma forma, $\frac{-30}{2}$ é um inteiro, pois $\frac{-30}{2} = -15$

Divisibilidade

Proposição 7.1: Sejam a e b números inteiros com $a \neq 0$. Então, a divide b se e somente se $\frac{b}{a}$ é um inteiro.

Exemplos:

- 2 divide -30, pois $-30 = 2 \cdot (-15)$
  da mesma forma, $\frac{-30}{2}$ é um inteiro, pois $\frac{-30}{2} = -15$

- 3 não divide 16, pois não existe $c \in \mathbb{Z}$ tal que $6 = 3c$
  da mesma forma, $\frac{16}{3}$ não é um inteiro, pois $\frac{16}{3} = 5,33333...$

Divisibilidade

Terminologia (Fator, Divisor, Múltiplo)

Quando a divide b, dizemos, de forma sinônima, que

- a é um **fator** de b
- a é um **divisor** de b
- b é um **múltiplo** de a
- b é **divisível** por a

Divisibilidade

Terminologia (Fator, Divisor, Múltiplo)

Quando a divide b, dizemos, de forma sinônima, que

- a é um **fator** de b
- a é um **divisor** de b
- b é um **múltiplo** de a
- b é **divisível** por a

Exemplo:

Vimos que **3 divide 6**. Da mesma forma, podemos dizer que
3 é fator de 6, que 3 é divisor de 6,
que 6 é multiplo de 3 e que 6 é divisível por 3.

Divisibilidade

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Terminologia (Fator, Divisor, Múltiplo)

Quando a divide b, dizemos, de forma sinônima, que

- a é um **fator** de b
- a é um **divisor** de b
- b é um **múltiplo** de a
- b é **divisível** por a

Exemplo:

Vimos que **3 divide 6**. Da mesma forma, podemos dizer que
3 é fator de 6, que 3 é divisor de 6,
que 6 é multiplo de 3 e que 6 é divisível por 3.

Como **3 não divide 16**, podemos dizer que
3 não é fator de 16, que 3 não é divisor de 16,
que 16 não é multiplo de 3 e que 16 não é divisível por 3.

Divisibilidade e números pares

Divisibilidade e números pares

- **Definição (número par):** Seja n um inteiro. Dizemos que n **é par** se e somente se existe um inteiro k tal que $n = 2k$.

Compare com a definição de divisibilidade:

- **Definição (divisibilidade):** Sejam a e b números inteiros com $a \neq 0$, dizemos que a **divide** b se e somente se existe um inteiro c tal que $b = ac$.

Divisibilidade e números pares

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- **Definição (número par):** Seja n um inteiro. Dizemos que n **é par** se e somente se existe um inteiro k tal que $n = 2k$.

Compare com a definição de divisibilidade:

- **Definição (divisibilidade):** Sejam a e b números inteiros com $a \neq 0$, dizemos que a **divide** b se e somente se existe um inteiro c tal que $b = ac$.

Podemos então reescrever:

- **Definição (número par (Alternativa 2)):** Seja n um inteiro. Dizemos que n **é par** se e somente se 2 **divide** n.

Par e ímpar

Proposição 7.2: Nenhum inteiro é ao mesmo tempo par e ímpar.

Reexpressa na forma "se-então", essa proposição é "se x é um inteiro, então x não pode ser simultaneamente par e ímpar".

Demonstração:

Par e ímpar

Proposição 7.2: Nenhum inteiro é ao mesmo tempo par e ímpar.

Reexpressa na forma "se-então", essa proposição é "se x é um inteiro, então x não pode ser simultaneamente par e ímpar".

Demonstração:

- Seja x um inteiro. Suponha por contradição que x seja par e ímpar.

Par e ímpar

Proposição 7.2: Nenhum inteiro é ao mesmo tempo par e ímpar.

Reexpressa na forma "se-então", essa proposição é "se x é um inteiro, então x não pode ser simultaneamente par e ímpar".

Demonstração:

- Seja x um inteiro. Suponha por contradição que x seja par e ímpar.
- Como x é par, sabemos que $2|x$, isto é, existe um inteiro a de modo que $x = 2a$.

Par e ímpar

Proposição 7.2: Nenhum inteiro é ao mesmo tempo par e ímpar.

Reexpressa na forma "se-então", essa proposição é "se x é um inteiro, então x não pode ser simultaneamente par e ímpar".

Demonstração:

- Seja x um inteiro. Suponha por contradição que x seja par e ímpar.
- Como x é par, sabemos que $2|x$, isto é, existe um inteiro a de modo que $x = 2a$.
- Como x é ímpar, sabemos que existe um inteiro b de modo que $x = 2b + 1$.

Par e ímpar

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Proposição 7.2: Nenhum inteiro é ao mesmo tempo par e ímpar.

Reexpressa na forma “se-então”, essa proposição é “se x é um inteiro, então x não pode ser simultaneamente par e ímpar”.

Demonstração:

- Seja x um inteiro. Suponha por contradição que x seja par e ímpar.
- Como x é par, sabemos que $2|x$, isto é, existe um inteiro a de modo que $x = 2a$.
- Como x é ímpar, sabemos que existe um inteiro b de modo que $x = 2b + 1$.
- Portanto, $2a = 2b + 1$. Dividindo ambos os termos por 2, obtemos $a = b + \frac{1}{2}$, de forma que $(a - b) = \frac{1}{2}$. Note que $a - b$ é um inteiro (pois a e b o são), mas $\frac{1}{2}$ não é inteiro.

Par e ímpar

Proposição 7.2: Nenhum inteiro é ao mesmo tempo par e ímpar.

Reexpressa na forma "se-então", essa proposição é "se x é um inteiro, então x não pode ser simultaneamente par e ímpar".

Demonstração:

- Seja x um inteiro. Suponha por contradição que x seja par e ímpar.
- Como x é par, sabemos que $2|x$, isto é, existe um inteiro a de modo que $x = 2a$.
- Como x é ímpar, sabemos que existe um inteiro b de modo que $x = 2b + 1$.
- Portanto, $2a = 2b + 1$. Dividindo ambos os termos por 2, obtemos $a = b + \frac{1}{2}$, de forma que $(a - b) = \frac{1}{2}$. Note que $a - b$ é um inteiro (pois a e b o são), mas $\frac{1}{2}$ não é inteiro.
- Logo, x não é ao mesmo tempo par e ímpar. $\square$

Propriedades da relação de divisibilidade

Propriedades da divisibilidade

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.3: Sejam a, b e c números inteiros com $a \neq 0$. Então:

(1) Se $a|b$ e $a|c$, então $a|(b+c)$.

(2) Se $a|b$, então $a|bc$ para todo c inteiro.

(3) Se $a|b$ e $b|c$, então $a|c$.

Demonstração:

Propriedades da divisibilidade

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.3: Sejam a, b e c números inteiros com $a \neq 0$. Então:

(1) Se $a|b$ e $a|c$, então $a|(b+c)$.

(2) Se $a|b$, então $a|bc$ para todo c inteiro.

(3) Se $a|b$ e $b|c$, então $a|c$.

Demonstração:

Prova do condicional 1: Sejam a, b e c inteiros quaisquer com $a \neq 0$ (Instanciação universal).

Propriedades da divisibilidade

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.3: Sejam a, b e c números inteiros com $a \neq 0$. Então:

(1) Se $a|b$ e $a|c$, então $a|(b+c)$.

(2) Se $a|b$, então $a|bc$ para todo c inteiro.

(3) Se $a|b$ e $b|c$, então $a|c$.

Demonstração:

Prova do condicional 1: Sejam a, b e c inteiros quaisquer com $a \neq 0$ (Instanciação universal).Suponha que $a|b$ e $a|c$ (Hipótese da PD).

Propriedades da divisibilidade

Teorema 7.3: Sejam a, b e c números inteiros com $a \neq 0$. Então:

(1) Se $a|b$ e $a|c$, então $a|(b+c)$.

(2) Se $a|b$, então $a|bc$ para todo c inteiro.

(3) Se $a|b$ e $b|c$, então $a|c$.

Demonstração:

Prova do condicional 1: Sejam a, b e c inteiros quaisquer com $a \neq 0$ (Instanciação universal).Suponha que $a|b$ e $a|c$ (Hipótese da PD).

Pela definição de divisibilidade, existem inteiros s e t tais que $b = as$ e $c = at$.

Propriedades da divisibilidade

Teorema 7.3: Sejam a, b e c números inteiros com $a \neq 0$. Então:

(1) Se $a|b$ e $a|c$, então $a|(b+c)$.

(2) Se $a|b$, então $a|bc$ para todo c inteiro.

(3) Se $a|b$ e $b|c$, então $a|c$.

Demonstração:

Prova do condicional 1: Sejam a, b e c inteiros quaisquer com $a \neq 0$ (Instanciação universal).Suponha que $a|b$ e $a|c$ (Hipótese da PD).

Pela definição de divisibilidade, existem inteiros s e t tais que $b = as$ e $c = at$.

Portanto, $b + c = as + at = a(s+t)$ (Igualdades + Distributividade).

Propriedades da divisibilidade

Teorema 7.3: Sejam a, b e c números inteiros com $a \neq 0$. Então:

(1) Se $a|b$ e $a|c$, então $a|(b+c)$.

(2) Se $a|b$, então $a|bc$ para todo c inteiro.

(3) Se $a|b$ e $b|c$, então $a|c$.

Demonstração:

Prova do condicional 1: Sejam a, b e c inteiros quaisquer com $a \neq 0$ (Instanciação universal).Suponha que $a|b$ e $a|c$ (Hipótese da PD).

Pela definição de divisibilidade, existem inteiros s e t tais que $b = as$ e $c = at$.

Portanto, $b + c = as + at = a(s + t)$ (Igualdades + Distributividade).

Como s e t são inteiros, $s + t$ é inteiro. Portanto, $a|(b+c)$. (Divisibilidade).

Propriedades da divisibilidade

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.3: Sejam a, b e c números inteiros com $a \neq 0$. Então:

(1) Se $a|b$ e $a|c$, então $a|(b+c)$.

(2) Se $a|b$, então $a|bc$ para todo c inteiro.

(3) Se $a|b$ e $b|c$, então $a|c$.

Demonstração:

Prova do condicional 1: Sejam a, b e c inteiros quaisquer com $a \neq 0$ (Instanciação universal).Suponha que $a|b$ e $a|c$ (Hipótese da PD).

Pela definição de divisibilidade, existem inteiros s e t tais que $b = as$ e $c = at$.

Portanto, $b + c = as + at = a(s + t)$ (Igualdades + Distributividade).

Como s e t são inteiros, $s + t$ é inteiro. Portanto, $a|(b + c)$. (Divisibilidade).

Condicional 2: Deixado como exercício.
Condicional 3: Provado em aulas passadas.

Propriedades da divisibilidade

Teorema 7.3: Sejam a, b e c números inteiros com $a \neq 0$. Então:

(1) Se $a|b$ e $a|c$, então $a|(b+c)$.

(2) Se $a|b$, então $a|bc$ para todo c inteiro.

(3) Se $a|b$ e $b|c$, então $a|c$.

Propriedades da divisibilidade

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.3: Sejam a, b e c números inteiros com $a \neq 0$. Então:

(1) Se $a|b$ e $a|c$, então $a|(b+c)$.

(2) Se $a|b$, então $a|bc$ para todo c inteiro.

(3) Se $a|b$ e $b|c$, então $a|c$.

Corolário 7.4: Se a, b e c são inteiros tais que $a \neq 0$, $a|b$ e $a|c$, então $a|(mb+nc)$, para quaisqer m e n inteiros.

Demonstração:

Propriedades da divisibilidade

Teorema 7.3: Sejam a, b e c números inteiros com $a \neq 0$. Então:

(1) Se $a|b$ e $a|c$, então $a|(b+c)$.

(2) Se $a|b$, então $a|bc$ para todo c inteiro.

(3) Se $a|b$ e $b|c$, então $a|c$.

Corolário 7.4: Se a, b e c são inteiros tais que $a \neq 0$, $a|b$ e $a|c$, então $a|(mb+nc)$, para quaisqer m e n inteiros.

Demonstração:
Pela afirmação (2) do teorema 7.2, vemos que $a|mb$ para todo inteiro m e que $a|nc$ para todo inteiro n.

Propriedades da divisibilidade

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.3: Sejam a, b e c números inteiros com $a \neq 0$. Então:

(1) Se $a|b$ e $a|c$, então $a|(b+c)$.

(2) Se $a|b$, então $a|bc$ para todo c inteiro.

(3) Se $a|b$ e $b|c$, então $a|c$.

Corolário 7.4: Se a, b e c são inteiros tais que $a \neq 0$, $a|b$ e $a|c$, então $a|(mb+nc)$, para quaisqer m e n inteiros.

Demonstração:
Pela afirmação (2) do teorema 7.2, vemos que $a|mb$ para todo inteiro m e que $a|nc$ para todo inteiro n.
Daí, podemos usar a afirmação (1) para concluir que $a|(mb+nc)$. $\square$

Algoritmo da divisão

Divisão

Teorema 7.5 (Algoritmo da divisão): Seja n um inteiro qualquer e d um inteiro positivo. Então, existe **um único par de inteiros** q e r com $0 \leq r < d$ tais que $n = dq + r$.

Divisão

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.5 (Algoritmo da divisão): Seja n um inteiro qualquer e d um inteiro positivo. Então, existe **um único par de inteiros** q e r com $0 \leq r < d$ tais que $n = dq + r$.

Este teorema trata da divisão de inteiros:

$$\begin{array}{r|l} n & d \\ \cline{2-2} r & q \end{array}$$

Numa divisão como esta acima,

- n é chamado **dividendo**
- d é chamado **divisor**
- q é chamado **quociente**
- r é chamado **resto**

Divisão

Teorema 7.5 (Algoritmo da divisão): Seja n um inteiro qualquer e d um inteiro positivo. Então, existe **um único par de inteiros** q e r com $0 \leq r < d$ tais que $n = dq + r$.

Observação: A condição $0 \leq r < d$ é fundamental, pois sem ela existirão infinitos pares q, r tais que $n = dq + r$.

Divisão

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.5 (Algoritmo da divisão): Seja n um inteiro qualquer e d um inteiro positivo. Então, existe **um único par de inteiros** q e r com $0 \leq r < d$ tais que $n = dq + r$.

Observação: A condição $0 \leq r < d$ é fundamental, pois sem ela existirão infinitos pares q, r tais que $n = dq + r$.

Exemplo

Considere $n = 10$ e $d = 3$. Se não restringirmos r, teremos:

Divisão

Teorema 7.5 (Algoritmo da divisão): Seja n um inteiro qualquer e d um inteiro positivo. Então, existe **um único par de inteiros** q e r com $0 \leq r < d$ tais que $n = dq + r$.

Observação: A condição $0 \leq r < d$ é fundamental, pois sem ela existirão infinitos pares q, r tais que $n = dq + r$.

Exemplo

Considere $n = 10$ e $d = 3$. Se não restringirmos r, teremos:

- ...
- $10 = 3(-3) + 19$
- $10 = 3(-2) + 16$
- $10 = 3(-1) + 13$
- $10 = 3 \cdot 0 + 10$
- $10 = 3 \cdot 1 + 7$
- $10 = 3 \cdot 2 + 4$
- $10 = 3 \cdot 3 + 1$
- $10 = 3 \cdot 4 + (-2)$
- $10 = 3 \cdot 5 + (-5)$
- $10 = 3 \cdot 6 + (-8)$
- ...

Divisão

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.5 (Algoritmo da divisão): Seja n um inteiro qualquer e d um inteiro positivo. Então, existe **um único par de inteiros** q e r com $0 \leq r < d$ tais que $n = dq + r$.

Observação: A condição $0 \leq r < d$ é fundamental, pois sem ela existirão infinitos pares q, r tais que $n = dq + r$.

Exemplo

Considere $n = 10$ e $d = 3$. Se não restringirmos r, teremos:

- ...
- $10 = 3(-3) + 19$
- $10 = 3(-2) + 16$
- $10 = 3(-1) + 13$
- $10 = 3 \cdot 0 + 10$
- $10 = 3 \cdot 1 + 7$
- $10 = 3 \cdot 2 + 4$
- $10 = 3 \cdot 3 + 1$
- $10 = 3 \cdot 4 + (-2)$
- $10 = 3 \cdot 5 + (-5)$
- $10 = 3 \cdot 6 + (-8)$
- ...

...mas haverá apenas um caso em que $0 \leq r < 3$.

Pares e ímpares

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.6: Todo inteiro é par ou ímpar, mas não os dois.

Demonstração:

Pares e ímpares

Teorema 7.6: Todo inteiro é par ou ímpar, mas não os dois.

Demonstração:

Provamos anteriormente que nenhum inteiro pode ser simultaneamente par e ímpar. Com isso, resta mostrar que todo inteiro é um ou outro. Vamos usar o Teorema do Algoritmo da Divisão para mostrar isso.

Pares e ímpares

Universidade Federal do Ceará
Campus Quixadá

Teorema 7.6: Todo inteiro é par ou ímpar, mas não os dois.

Demonstração:

Provamos anteriormente que nenhum inteiro pode ser simultaneamente par e ímpar. Com isso, resta mostrar que todo inteiro é um ou outro. Vamos usar o Teorema do Algoritmo da Divisão para mostrar isso.

Seja n qualquer inteiro. Pelo Teorema 7.5, podemos encontrar os inteiros q e r, de forma que $n = 2q + r$, em que $0 \leq r < 2$.

Pares e ímpares

Universidade Federal do Ceará
Campus Quixadá

Teorema 7.6: Todo inteiro é par ou ímpar, mas não os dois.

Demonstração:

Provamos anteriormente que nenhum inteiro pode ser simultaneamente par e ímpar. Com isso, resta mostrar que todo inteiro é um ou outro. Vamos usar o Teorema do Algoritmo da Divisão para mostrar isso.

Seja n qualquer inteiro. Pelo Teorema 7.5, podemos encontrar os inteiros q e r, de forma que $n = 2q + r$, em que $0 \leq r < 2$.

Observe que, se $r = 0$, então n é par, e se $r = 1$, então n é ímpar. $\square$

Operações **div** e **mod**

Universidade Federal do Ceará
Campus Quixadá

Definição

Sejam n, d, q, r inteiros tais que

- $d > 0$ e
- $n = dq + r$, com $0 \leq r < d$,

definimos as funções **div** e **mod** tais que

- $n \ \mathbf{div} \ d = q$ **(divisão inteira/sem resto)**
- $n \ \mathbf{mod} \ d = r$ **(módulo/resto da divisão)**

Operações **div** e **mod**

Na divisão de 110 por 9 temos

$$
\begin{array}{r|l}
110 & 9 \\ \cline{2-2}
-9 & 12 \\ \cline{1-1}
20 & \\
-18 & \\ \cline{1-1}
2 &
\end{array}
$$

Isso nos dá que

- $110 = 9 \cdot 12 + 2$
- 110 **div** $9 = 12$
- 110 **mod** $9 = 2$

Operações **div** e **mod**

Na divisão de -110 por 9 temos

$$\begin{array}{r|l} -110 & \;\; 9 \\ \cline{2-2} +9 & -13 \\ \cline{1-1} -20 & \\ +27 & \\ \cline{1-1} 7 & \end{array}$$

Operações **div** e **mod**

Na divisão de -110 por 9 temos

$$\begin{array}{r|l} -110 & \quad 9 \\ \cline{2-2} +9 & -13 \\ \cline{1-1} -20 & \\ +27 & \\ \cline{1-1} 7 & \end{array}$$

Isso nos dá que

- $-110 = 9 \cdot (-13) + 7$
- -110 **div** $9 = -13$
- -110 **mod** $9 = 7$

Operações **div** e **mod**

Na divisão de -110 por 9 temos

$$\begin{array}{r|l} -110 & \;9 \\ \cline{2-2} +9 & -13 \\ \cline{1-1} -20 & \\ +27 & \\ \cline{1-1} 7 & \end{array}$$

Por que o quociente não é 12?

Isso nos dá que

- $-110 = 9 \cdot (-13) + 7$
- -110 **div** $9 = -13$
- -110 **mod** $9 = 7$

Operações **div** e **mod**

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Na divisão de -110 por 9 temos

$$\begin{array}{r|l} -110 & 9 \\ \cline{2-2} +9 & -13 \\ \cline{1-1} -20 & \\ +27 & \\ \cline{1-1} 7 & \end{array}$$

Por que o quociente não é 12?

Como $9 \cdot (-12) = -108$, se usássemos $q = -12$ na expressão $-110 = 9q + r$, teríamos $r = -2$.

Isso nos dá que

- $-110 = 9 \cdot (-13) + 7$
- -110 **div** $9 = -13$
- -110 **mod** $9 = 7$

Operações **div** e **mod**

Na divisão de -110 por 9 temos

$$\begin{array}{r|l} -110 & \ 9 \\ \cline{2-2} +9 & -13 \\ \hline -20 & \\ +27 & \\ \hline 7 & \end{array}$$

Isso nos dá que

- $-110 = 9 \cdot (-13) + 7$
- -110 **div** $9 = -13$
- -110 **mod** $9 = 7$

Por que o quociente não é 12?

Como $9 \cdot (-12) = -108$, se usássemos $q = -12$ na expressão $-110 = 9q + r$, teríamos $r = -2$.

$-110 = 9 \cdot (-12) + r \Rightarrow -110 = -108 + r \Rightarrow -110 - (-108) = r \Rightarrow -110 + 108 = r \Rightarrow r = -2$

Lembre-se que precisamos satisfazer
$0 \leq r < 9$

Relação entre divisibilidade e o Algoritmo da Divisão

Divisibilidade e Algoritmo da Divisão

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.5 (Algoritmo da divisão): Seja n um inteiro qualquer e d um inteiro positivo. Então, existe **um único par de inteiros** q e r com $0 \leq r < d$ tais que $n = dq + r$.

O que ocorre quando temos $r = 0$?

- Isto só é possível para alguns valores de n e d
- A expressão $n = dq + r$ torna-se simplesmente $n = dq$
- Como q é inteiro, $n = dq$ nos diz que d **divide** n

Divisibilidade e Algoritmo da Divisão

Universidade Federal do Ceará
Campus Quixadá

Teorema 7.7: Sejam a, b inteiros, com $a \neq 0$, temos que a divide b se e somente se b **mod** $a = 0$.

Demonstração:
Sejam a, b inteiros com $a \neq 0$.

Divisibilidade e Algoritmo da Divisão

Teorema 7.7: Sejam a, b inteiros, com $a \neq 0$, temos que a divide b se e somente se $b \textbf{ mod } a = 0$.

Demonstração:

Sejam a, b inteiros com $a \neq 0$.

$(\Rightarrow)$ Suponha que $a|b$.

Divisibilidade e Algoritmo da Divisão

Universidade Federal do Ceará
Campus Quixadá

Teorema 7.7: Sejam a, b inteiros, com $a \neq 0$, temos que a divide b se e somente se $b \textbf{ mod } a = 0$.

Demonstração:

Sejam a, b inteiros com $a \neq 0$.

$(\Rightarrow)$ Suponha que $a|b$.

Logo, existe um inteiro c tal que $b = ac$. (definição de divisibilidade)

Divisibilidade e Algoritmo da Divisão

Universidade Federal do Ceará
Campus Quixadá

Teorema 7.7: Sejam a, b inteiros, com $a \neq 0$, temos que a divide b se e somente se b **mod** $a = 0$.

Demonstração:
Sejam a, b inteiros com $a \neq 0$.

($\Rightarrow$) Suponha que $a|b$.
Logo, existe um inteiro c tal que $b = ac$. (definição de divisibilidade)
Podemos reescrever a igualdade como $b = ac + 0$. (Elemento neutro da soma)

Divisibilidade e Algoritmo da Divisão

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.7: Sejam a, b inteiros, com $a \neq 0$, temos que a divide b se e somente se b **mod** $a = 0$.

Demonstração:

Sejam a, b inteiros com $a \neq 0$.

($\Rightarrow$) Suponha que $a|b$.
Logo, existe um inteiro c tal que $b = ac$. (definição de divisibilidade)
Podemos reescrever a igualdade como $b = ac + 0$. (Elemento neutro da soma)
Neste ponto, o par de inteiros $c, 0$ satisfaz os requisitos do algoritmo da divisão.

Divisibilidade e Algoritmo da Divisão

Universidade Federal do Ceará
Campus Quixadá

Teorema 7.7: Sejam a, b inteiros, com $a \neq 0$, temos que a divide b se e somente se b **mod** $a = 0$.

Demonstração:

Sejam a, b inteiros com $a \neq 0$.

($\Rightarrow$) Suponha que $a|b$.
Logo, existe um inteiro c tal que $b = ac$. (definição de divisibilidade)
Podemos reescrever a igualdade como $b = ac + 0$. (Elemento neutro da soma)
Neste ponto, o par de inteiros $c, 0$ satisfaz os requisitos do algoritmo da divisão.
Portanto, na divisão de b por a temos b **div** $a = c$ e b **mod** $a = 0$.

Divisibilidade e Algoritmo da Divisão

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.7: Sejam a, b inteiros, com $a \neq 0$, temos que a divide b se e somente se b **mod** $a = 0$.

Demonstração:

Divisibilidade e Algoritmo da Divisão

Teorema 7.7: Sejam a, b inteiros, com $a \neq 0$, temos que a divide b se e somente se $b \textbf{ mod } a = 0$.

Demonstração:

Sejam a, b inteiros com $a \neq 0$.

Divisibilidade e Algoritmo da Divisão

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.7: Sejam a, b inteiros, com $a \neq 0$, temos que a divide b se e somente se $b \textbf{ mod } a = 0$.

Demonstração:

Sejam a, b inteiros com $a \neq 0$.

$(\Leftarrow)$ Suponha que $b \textbf{ mod } a = 0$.

Divisibilidade e Algoritmo da Divisão

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.7: Sejam a, b inteiros, com $a \neq 0$, temos que a divide b se e somente se b **mod** $a = 0$.

Demonstração:

Sejam a, b inteiros com $a \neq 0$.

($\Leftarrow$) Suponha que b **mod** $a = 0$.

Seja b **div** $a = c$, onde c é um inteiro. Pelo algoritmo da divisão, temos que $b = ac + 0$. Todo número somado com zero resulta no próprio número.

Divisibilidade e Algoritmo da Divisão

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.7: Sejam a, b inteiros, com $a \neq 0$, temos que a divide b se e somente se b **mod** $a = 0$.

Demonstração:

Sejam a, b inteiros com $a \neq 0$.

$(\Leftarrow)$ Suponha que b **mod** $a = 0$.

Seja b **div** $a = c$, onde c é um inteiro. Pelo algoritmo da divisão, temos que $b = ac + 0$. Todo número somado com zero resulta no próprio número.

Logo, $b = ac$ tal que $a \neq 0$ e c é um inteiro. Pela definição de divisibilidade, temos que a divide b. $\square$

Aritmética Modular

Congruência modular

Definição (Congruência módulo m):
Dados dois inteiros a e b e um inteiro positivo m, dizemos que a **é congruente a** b **módulo** m se e somente se $m|(a-b)$.

Congruência modular

Definição (Congruência módulo m):
Dados dois inteiros a e b e um inteiro positivo m, dizemos que
a **é congruente a** b **módulo** m se e somente se $m|(a-b)$.

Exemplos (Positivos)

- $370 - 114 = 256$,
  que é divisível por 256, pois $256 \textbf{ mod } 256 = 0$.
  Logo, 370 é congruente a 114 módulo 256.

Congruência modular

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Definição (Congruência módulo m):
Dados dois inteiros a e b e um inteiro positivo m, dizemos que
a **é congruente a** b **módulo** m se e somente se $m|(a-b)$.

Exemplos (Positivos)

- $370 - 114 = 256$,
  que é divisível por 256, pois $256 \textbf{ mod } 256 = 0$.
  Logo, 370 é congruente a 114 módulo 256.
- $370 - (-142) = 512$,
  que é divisível por 256, pois $512 \textbf{ mod } 256 = 0$.
  Logo, 370 é congruente a -142 módulo 256.

Congruência modular

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Definição (Congruência módulo m):
Dados dois inteiros a e b e um inteiro positivo m, dizemos que
a **é congruente a** b **módulo** m se e somente se $m|(a-b)$.

Exemplos (Positivos)

- $370 - 114 = 256$,
  que é divisível por 256, pois $256 \textbf{ mod } 256 = 0$.
  Logo, 370 é congruente a 114 módulo 256.

- $370 - (-142) = 512$,
  que é divisível por 256, pois $512 \textbf{ mod } 256 = 0$.
  Logo, 370 é congruente a -142 módulo 256.

- $-142 - 114 = -256$,
  que é divisível por 256, pois $-256 \textbf{ mod } 256 = 0$.
  Logo, -142 é congruente a 114 módulo 256.

Congruência modular

Definição (Congruência módulo m):
Dados dois inteiros a e b e um inteiro positivo m, dizemos que a **é congruente a** b **módulo** m se e somente se $m|(a-b)$.

Exemplos (Negativos)

Congruência modular

Definição (Congruência módulo m):
Dados dois inteiros a e b e um inteiro positivo m, dizemos que
a **é congruente a** b **módulo** m se e somente se $m|(a-b)$.

Exemplos (Negativos)

- $400 - 114 = 286$,
  que não é divisível por 256, pois $286 \textbf{ mod } 256 = 30$,
  ou seja, 400 **não é** congruente a 11 módulo 256.

Congruência modular

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Definição (Congruência módulo m):
Dados dois inteiros a e b e um inteiro positivo m, dizemos que a **é congruente a** b **módulo** m se e somente se $m|(a-b)$.

Exemplos (Negativos)

- $400 - 114 = 286$,
  que não é divisível por 256, pois $286 \textbf{ mod } 256 = 30$,
  ou seja, 400 **não é** congruente a 11 módulo 256.

- $370 - 400 = -30$,
  que não é divisível por 256, pois $-30 \textbf{ mod } 256 = 226$.
  ou seja, 370 **não é** congruente a 400 módulo 256.

Congruência modular

Definição (Congruência módulo m):
Dados dois inteiros a e b e um inteiro positivo m, dizemos que
a **é congruente a** b **módulo** m se e somente se $m|(a-b)$.

Notação

- Escreve-se $a \equiv b \pmod{m}$ para dizer que a **é** congruente a b módulo m.
- Escreve-se $a \not\equiv b \pmod{m}$ para dizer que a **não é** congruente a b módulo m

Congruência modular

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Definição (Congruência módulo m):
Dados dois inteiros a e b e um inteiro positivo m, dizemos que
a **é congruente a** b **módulo** m se e somente se $m|(a-b)$.

Notação

- Escreve-se $a \equiv b \pmod{m}$ para dizer que a **é** congruente a b módulo m.
- Escreve-se $a \not\equiv b \pmod{m}$ para dizer que a **não é** congruente a b módulo m

Exemplo

- $370 \equiv 114 \pmod{256}$
- $370 \equiv -142 \pmod{256}$
- $-142 \equiv 114 \pmod{256}$
- $400 \not\equiv 114 \pmod{256}$
- $370 \not\equiv 400 \pmod{256}$

Congruência modular

Definição (Congruência módulo m):
Dados dois inteiros a e b e um inteiro positivo m, dizemos que a **é congruente a** b **módulo** m se e somente se $m|(a-b)$.

Notação

- Escreve-se $a \equiv b \pmod{m}$ para dizer que a **é** congruente a b módulo m.
- Escreve-se $a \not\equiv b \pmod{m}$ para dizer que a **não é** congruente a b módulo m

Observação 2: Dizemos que uma expressão do tipo "$a \equiv b \pmod{m}$" é uma **congruência** e que m é o seu módulo.

Congruência modular

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Definição (Congruência módulo m (Reescrita)):
Dados dois inteiros a e b e um inteiro positivo m, dizemos que $a \equiv b \pmod{m}$ se e somente se $m | (a - b)$.

Notação

- Escreve-se $a \equiv b \pmod{m}$ para dizer que a **é** congruente a b módulo m.
- Escreve-se $a \not\equiv b \pmod{m}$ para dizer que a **não é** congruente a b módulo m

Observação 2: Dizemos que uma expressão do tipo "$a \equiv b \pmod{m}$" é uma **congruência** e que m é o seu módulo.

Congruência modular

Observação 1: Embora a relação "$a \equiv b \pmod{m}$" e a função "$a \mathbf{\ mod\ } m = b$" sejam ambos escritos com a palavra "mod", estas expressões têm significados muito diferentes.

Congruência modular

Observação 1: Embora a relação "$a \equiv b \pmod{m}$" e a função "$a \ \mathbf{mod} \ m = b$" sejam ambos escritos com a palavra "mod", estas expressões têm significados muito diferentes.

Contudo, a relação "$a \equiv b \pmod{m}$" e a função "$a \ \mathbf{mod} \ m = b$" estão fortemente relacionadas:

Congruência modular

Observação 1: Embora a relação "$a \equiv b \pmod{m}$" e a função "$a \textbf{ mod } m = b$" sejam ambos escritos com a palavra "mod", estas expressões têm significados muito diferentes.

Contudo, a relação "$a \equiv b \pmod{m}$" e a função "$a \textbf{ mod } m = b$" estão fortemente relacionadas:

Teorema 7.10: Sejam a e b inteiros e seja m um inteiro positivo. Então $a \equiv b \pmod{m}$ se e somente se $a \textbf{ mod } m = b \textbf{ mod } m$

Demonstração: Deixada como exercício.

Congruência modular

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Observação 1: Embora a relação "$a \equiv b \pmod{m}$" e a função "$a \ \mathbf{mod}\ m = b$" sejam ambos escritos com a palavra "mod", estas expressões têm significados muito diferentes.

Contudo, a relação "$a \equiv b \pmod{m}$" e a função "$a \ \mathbf{mod}\ m = b$" estão fortemente relacionadas:

Teorema 7.10: Sejam a e b inteiros e seja m um inteiro positivo. Então $a \equiv b \pmod{m}$ se e somente se $a \ \mathbf{mod}\ m = b \ \mathbf{mod}\ m$

Demonstração: Deixada como exercício.

Teorema 7.11: Se a é um inteiro e m é um inteiro positivo, então $a \equiv (a \ \mathbf{mod}\ m) \pmod{m}$.

Demonstração: Deixada como exercício.

Propriedades de Congruências Modulares

Propriedades de Congruências Modulares

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- A notação $\equiv$ sugere que queremos considerar a relação de congruência modular como um análogo à relação de igualdade $=$.
- De fato, muitas das propriedades da igualdade são válidas para congruências, pelo menos quando mantemos o módulo fixo.

Propriedades de Congruências Modulares

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- A notação $\equiv$ sugere que queremos considerar a relação de congruência modular como um análogo à relação de igualdade $=$.
- De fato, muitas das propriedades da igualdade são válidas para congruências, pelo menos quando mantemos o módulo fixo.
- Assim, como a igualdade, a congruência modular também satisfaz as seguintes propriedades:

Propriedades de Congruências Modulares

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- A notação $\equiv$ sugere que queremos considerar a relação de congruência modular como um análogo à relação de igualdade $=$.
- De fato, muitas das propriedades da igualdade são válidas para congruências, pelo menos quando mantemos o módulo fixo.
- Assim, como a igualdade, a congruência modular também satisfaz as seguintes propriedades:
    - **Reflexividade:** $a \equiv a \pmod{m}$

Propriedades de Congruências Modulares

Universidade Federal do Ceará
Campus Quixadá

- A notação $\equiv$ sugere que queremos considerar a relação de congruência modular como um análogo à relação de igualdade $=$.
- De fato, muitas das propriedades da igualdade são válidas para congruências, pelo menos quando mantemos o módulo fixo.
- Assim, como a igualdade, a congruência modular também satisfaz as seguintes propriedades:
  - **Reflexividade:** $a \equiv a \pmod{m}$
  - **Simetria:** $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$

Propriedades de Congruências Modulares

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- A notação $\equiv$ sugere que queremos considerar a relação de congruência modular como um análogo à relação de igualdade $=$.
- De fato, muitas das propriedades da igualdade são válidas para congruências, pelo menos quando mantemos o módulo fixo.
- Assim, como a igualdade, a congruência modular também satisfaz as seguintes propriedades:
  - **Reflexividade:** $a \equiv a \pmod{m}$
  - **Simetria:** $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$
  - **Transitividade:**
    $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$

Propriedades de Congruências Modulares

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Proposição 7.12 (Reflexividade): Se a e m são inteiros, com $m \geq 1$, então $a \equiv a \pmod{m}$.

Demonstração:

Propriedades de Congruências Modulares

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Proposição 7.12 (Reflexividade): Se a e m são inteiros, com $m \geq 1$, então $a \equiv a \pmod{m}$.

Demonstração:

Seja m um inteiro positivo qualquer e a um inteiro qualquer.

Propriedades de Congruências Modulares

Proposição 7.12 (Reflexividade): Se a e m são inteiros, com $m \geq 1$, então $a \equiv a \pmod{m}$.

Demonstração:

Seja m um inteiro positivo qualquer e a um inteiro qualquer.

Note que $a - a = 0$ é múltiplo de m, pois existe um inteiro k tal que $0 = km$ (neste caso, temos $k = 0$).

Propriedades de Congruências Modulares

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Proposição 7.12 (Reflexividade): Se a e m são inteiros, com $m \geq 1$, então $a \equiv a \pmod{m}$.

Demonstração:

Seja m um inteiro positivo qualquer e a um inteiro qualquer.

Note que $a - a = 0$ é múltiplo de m, pois existe um inteiro k tal que $0 = km$ (neste caso, temos $k = 0$).

Pela definição de divisibilidade, $m|(a - a)$.

Propriedades de Congruências Modulares

Proposição 7.12 (Reflexividade): Se a e m são inteiros, com $m \geq 1$, então $a \equiv a \pmod{m}$.

Demonstração:

Seja m um inteiro positivo qualquer e a um inteiro qualquer.

Note que $a - a = 0$ é múltiplo de m, pois existe um inteiro k tal que $0 = km$ (neste caso, temos $k = 0$).

Pela definição de divisibilidade, $m|(a - a)$.

Logo, $a \equiv a \pmod{m}$ pela definição de congruência modular. $\square$

Propriedades de Congruências Modulares

Universidade Federal do Ceará
Campus Quixadá

Proposição 7.13 (Simetria): Sejam a, b e m inteiros, com $m \geq 1$. Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.

Demonstração:

Propriedades de Congruências Modulares

Proposição 7.13 (Simetria): Sejam a, b e m inteiros, com $m \geq 1$. Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.

Demonstração:

Seja m um inteiro positivo qualquer e a, b inteiros quaisquer.

Propriedades de Congruências Modulares

Proposição 7.13 (Simetria): Sejam a, b e m inteiros, com $m \geq 1$. Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.

Demonstração:

Seja m um inteiro positivo qualquer e a, b inteiros quaisquer.

Suponha $a \equiv b \pmod{m}$.

Propriedades de Congruências Modulares

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Proposição 7.13 (Simetria): Sejam a, b e m inteiros, com $m \geq 1$. Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.

Demonstração:

Seja m um inteiro positivo qualquer e a, b inteiros quaisquer.

Suponha $a \equiv b \pmod{m}$. Por definição de congruência modular, $m|(a-b)$, ou seja, existe inteiro k tal que $a - b = km$.

Propriedades de Congruências Modulares

Universidade Federal do Ceará
Campus Quixadá

Proposição 7.13 (Simetria): Sejam a, b e m inteiros, com $m \geq 1$. Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.

Demonstração:

Seja m um inteiro positivo qualquer e a, b inteiros quaisquer.

Suponha $a \equiv b \pmod{m}$. Por definição de congruência modular, $m|(a-b)$, ou seja, existe inteiro k tal que $a - b = km$. Logo,

$$\begin{aligned} a - b &= km \\ -b &= -a + km \\ b &= a - km \\ b &= a + (-k)m \\ b - a &= (-k)m \end{aligned}$$

Propriedades de Congruências Modulares

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Proposição 7.13 (Simetria): Sejam a, b e m inteiros, com $m \geq 1$. Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.

Demonstração:

Seja m um inteiro positivo qualquer e a, b inteiros quaisquer.

Suponha $a \equiv b \pmod{m}$. Por definição de congruência modular, $m|(a-b)$, ou seja, existe inteiro k tal que $a - b = km$. Logo,

$$\begin{aligned}
a - b &= km \\
-b &= -a + km \\
b &= a - km \\
b &= a + (-k)m \\
b - a &= (-k)m
\end{aligned}$$

Segue da última igualdade que $m|(b-a)$. Logo, pela definição de congruência modular, $b \equiv a \pmod{m}$. $\square$

Propriedades de Congruências Modulares

Proposição 7.14 (Transitividade): Sejam a, b, c e m inteiros, com $m \geq 1$. Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

Demonstração: Deixada como exercício.

Propriedades de Congruências Modulares

Outros teoremas deixados como exercício:

Teorema 7.15: Sejam a e m inteiros, com $m \geq 1$.
Então, $a \equiv 0 \pmod{m}$ se e somente se $m | a$.

Propriedades de Congruências Modulares

Outros teoremas deixados como exercício:

Teorema 7.15: Sejam a e m inteiros, com $m \geq 1$.
Então, $a \equiv 0 \pmod{m}$ se e somente se $m | a$.

Teorema 7.16: Sejam a, b, c e m inteiros, com $m \geq 1$.
Se $a \equiv c \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv b \pmod{m}$.

Propriedades de Congruências Modulares

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Outros teoremas deixados como exercício:

Teorema 7.15: Sejam a e m inteiros, com $m \geq 1$.
Então, $a \equiv 0 \pmod{m}$ se e somente se $m|a$.

Teorema 7.16: Sejam a, b, c e m inteiros, com $m \geq 1$.
Se $a \equiv c \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv b \pmod{m}$.

Teorema 7.17: Sejam a, b e m inteiros, com $m \geq 1$.
Os inteiros a e b são congruentes módulo m se e somente se existe um inteiro k tal que $a = b + km$.

Propriedades de Congruências Modulares

Congruências também se comportam como igualdades no seguinte aspecto: Se você tiver duas congruências com o mesmo módulo:

$$a \equiv b \pmod{m} \qquad \text{e} \qquad c \equiv d \pmod{m}$$

então, podemos adicioná-las, subtraí-las ou multiplicá-las:

- $a + c \equiv b + d \pmod{m}$
- $a - c \equiv b - d \pmod{m}$
- $ac \equiv bd \pmod{m}$

Precisamos provar essas afirmações!

Propriedades de Congruências Modulares

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.18: Sejam a, b, c, d e m inteiros, com $m \geq 1$.
Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então

(1) $a + c \equiv b + d \pmod{m}$ e

(2) $a - c \equiv b - d \pmod{m}$ e

(3) $ac \equiv bd \pmod{m}$

Demonstração:

Vamos usar prova direta. Suponha $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$.

Propriedades de Congruências Modulares

Teorema 7.18: Sejam a, b, c, d e m inteiros, com $m \geq 1$.
Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então

(1) $a + c \equiv b + d \pmod{m}$ e

(2) $a - c \equiv b - d \pmod{m}$ e

(3) $ac \equiv bd \pmod{m}$

Demonstração:

Vamos usar prova direta. Suponha $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$.

Pelo Teorema 7.17, existem inteiros s e t tais que $b = a + sm$ e $d = c + tm$.

Propriedades de Congruências Modulares

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.18: Sejam a, b, c, d e m inteiros, com $m \geq 1$.
Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então

(1) $a + c \equiv b + d \pmod{m}$ e

(2) $a - c \equiv b - d \pmod{m}$ e

(3) $ac \equiv bd \pmod{m}$

Demonstração:

Vamos usar prova direta. Suponha $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$.

Pelo Teorema 7.17, existem inteiros s e t tais que $b = a + sm$ e $d = c + tm$. Deste modo, temos que

- $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$

Propriedades de Congruências Modulares

Teorema 7.18: Sejam a, b, c, d e m inteiros, com $m \geq 1$.
Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então

(1) $a + c \equiv b + d \pmod{m}$ e

(2) $a - c \equiv b - d \pmod{m}$ e

(3) $ac \equiv bd \pmod{m}$

Demonstração:

Vamos usar prova direta. Suponha $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$.

Pelo Teorema 7.17, existem inteiros s e t tais que $b = a + sm$ e $d = c + tm$. Deste modo, temos que

- $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$
- $b - d = (a + sm) - (c + tm) = (a - c) + m(s - t)$

Propriedades de Congruências Modulares

Teorema 7.18: Sejam a, b, c, d e m inteiros, com $m \geq 1$.
Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então

(1) $a + c \equiv b + d \pmod{m}$ e

(2) $a - c \equiv b - d \pmod{m}$ e

(3) $ac \equiv bd \pmod{m}$

Demonstração:

Vamos usar prova direta. Suponha $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$.

Pelo Teorema 7.17, existem inteiros s e t tais que $b = a + sm$ e $d = c + tm$.
Deste modo, temos que

- $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$
- $b - d = (a + sm) - (c + tm) = (a - c) + m(s - t)$
- $bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$

Propriedades de Congruências Modulares

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.18: Sejam a, b, c, d e m inteiros, com $m \geq 1$.
Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então

(1) $a + c \equiv b + d \pmod{m}$ e

(2) $a - c \equiv b - d \pmod{m}$ e

(3) $ac \equiv bd \pmod{m}$

Demonstração:

Vamos usar prova direta. Suponha $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$.

Pelo Teorema 7.17, existem inteiros s e t tais que $b = a + sm$ e $d = c + tm$.
Deste modo, temos que

- $b + d = (a + c) + m(s + t)$
- $b - d = (a - c) + m(s - t)$
- $bd = ac + m(at + cs + stm)$

Propriedades de Congruências Modulares

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Teorema 7.18: Sejam a, b, c, d e m inteiros, com $m \geq 1$.
Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então

(1) $a + c \equiv b + d \pmod{m}$ e

(2) $a - c \equiv b - d \pmod{m}$ e

(3) $ac \equiv bd \pmod{m}$

Demonstração:

Vamos usar prova direta. Suponha $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$.

Pelo Teorema 7.17, existem inteiros s e t tais que $b = a + sm$ e $d = c + tm$.
Deste modo, temos que

- $b + d = (a + c) + m(s + t)$
- $b - d = (a - c) + m(s - t)$
- $bd = ac + m(at + cs + stm)$

Então, pelo Teorema 7.17, temos que $a + c \equiv b + d \pmod{m}$ e
$a - c \equiv b - d \pmod{m}$ e $ac \equiv bd \pmod{m}$. □

Exercício:
Usando o Teorema 7.18, o Teorema 7.10 e o Teorema 7.11, prove:

Corolário 7.19: Seja m inteiro positivo e a, b inteiros. Então,

$$(a+b) \textbf{ mod } m = ((a \textbf{ mod } m) + (b \textbf{ mod } m) \textbf{ mod } m)$$

e

$$(a \cdot b) \textbf{ mod } m = ((a \textbf{ mod } m) \cdot (b \textbf{ mod } m) \textbf{ mod } m)$$

Demonstração: Deixada como exercício.

Universidade Federal do Ceará
Campus Quixadá

Aritmética módulo m

Aritmética módulo m

Suponha que agora são 2 horas (da tarde ou da madrugada, tanto faz). E considere as horas contadas no formato de 12h.
Ou seja, as horas possíveis estão no conjunto $\{0, 1, 2, \ldots, 11\}$
Em nosso relógio, a hora 0 corresponde aos ponteiros no número 12.

Aritmética módulo m

Suponha que agora são 2 horas (da tarde ou da madrugada, tanto faz). E considere as horas contadas no formato de 12h.
Ou seja, as horas possíveis estão no conjunto $\{0, 1, 2, \ldots, 11\}$
Em nosso relógio, a hora 0 corresponde aos ponteiros no número 12.

- Que horas serão daqui a 5 horas?

Aritmética módulo m

Suponha que agora são 2 horas (da tarde ou da madrugada, tanto faz). E considere as horas contadas no formato de 12h.
Ou seja, as horas possíveis estão no conjunto $\{0, 1, 2, \ldots, 11\}$
Em nosso relógio, a hora 0 corresponde aos ponteiros no número 12.

- Que horas serão daqui a 5 horas?
  Resposta: $(2 + 5)$ **mod** $12 = 7$ horas

Aritmética módulo m

Suponha que agora são 2 horas (da tarde ou da madrugada, tanto faz). E considere as horas contadas no formato de 12h.
Ou seja, as horas possíveis estão no conjunto $\{0, 1, 2, \ldots, 11\}$
Em nosso relógio, a hora 0 corresponde aos ponteiros no número 12.

- Que horas serão daqui a 5 horas?
  Resposta: $(2 + 5)$ **mod** $12 = 7$ horas
- Que horas serão daqui a 24 horas?

Aritmética módulo m

Suponha que agora são 2 horas (da tarde ou da madrugada, tanto faz). E considere as horas contadas no formato de 12h.
Ou seja, as horas possíveis estão no conjunto $\{0, 1, 2, \ldots, 11\}$
Em nosso relógio, a hora 0 corresponde aos ponteiros no número 12.

- Que horas serão daqui a 5 horas?
  Resposta: $(2 + 5)$ **mod** $12 = 7$ horas
- Que horas serão daqui a 24 horas?
  Resposta: $(2 + 24)$ **mod** $12 = 26$ **mod** $12 = 2$ horas

Aritmética módulo m

Suponha que agora são 2 horas (da tarde ou da madrugada, tanto faz). E considere as horas contadas no formato de 12h.
Ou seja, as horas possíveis estão no conjunto $\{0, 1, 2, \ldots, 11\}$
Em nosso relógio, a hora 0 corresponde aos ponteiros no número 12.

- Que horas serão daqui a 5 horas?
  Resposta: $(2 + 5)$ **mod** $12 = 7$ horas
- Que horas serão daqui a 24 horas?
  Resposta: $(2 + 24)$ **mod** $12 = 26$ **mod** $12 = 2$ horas
- Que horas o relógio marcava há 4 horas atrás?

Aritmética módulo m

Suponha que agora são 2 horas (da tarde ou da madrugada, tanto faz). E considere as horas contadas no formato de 12h.
Ou seja, as horas possíveis estão no conjunto $\{0, 1, 2, \ldots, 11\}$
Em nosso relógio, a hora 0 corresponde aos ponteiros no número 12.

- Que horas serão daqui a 5 horas?
  Resposta: $(2 + 5)$ **mod** $12 = 7$ horas
- Que horas serão daqui a 24 horas?
  Resposta: $(2 + 24)$ **mod** $12 = 26$ **mod** $12 = 2$ horas
- Que horas o relógio marcava há 4 horas atrás?
  Resposta: $(2 - 4)$ **mod** $12 = -2$ **mod** $12 = 10$ horas

Aritmética módulo m

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

O que é "Aritmética"?

- É o ramo da matemática que estuda a manipulação de números e as propriedades sobre estes.

Aritmética módulo m

O que é "Aritmética"?

- É o ramo da matemática que estuda a manipulação de números e as propriedades sobre estes.

O que torna uma Aritmética "Modular"?

- É uma aritmética restrita aos restos de divisão pelo "**módulo**" m.
- Após cada operação, aplica-se a função " $\mathbf{mod}\ m$" para corrigir resultados.

Aritmética módulo m

Universidade Federal do Ceará
Campus Quixadá

O que é "Aritmética"?

- É o ramo da matemática que estuda a manipulação de números e as propriedades sobre estes.

O que torna uma Aritmética "Modular"?

- É uma aritmética restrita aos restos de divisão pelo "**módulo**" m.
- Após cada operação, aplica-se a função " **mod** m" para corrigir resultados.

Exemplo

Na aritmética de módulo 12, ao **somar** 5 e 130, faremos:

$$\underbrace{(5+130) \mathbf{\ mod\ } 12}_{\text{soma modular}} = 135 \mathbf{\ mod\ } 12 = \underbrace{3}_{\text{resultado}}$$

Aritmética módulo m

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

O que é "Aritmética"?

- É o ramo da matemática que estuda a manipulação de números e as propriedades sobre estes.

O que torna uma Aritmética "Modular"?

- É uma aritmética restrita aos restos de divisão pelo "**módulo**" m.
- Após cada operação, aplica-se a função " **mod** m" para corrigir resultados.

Exemplo

Na aritmética de módulo 12, ao **multiplicar** 5 e 130, faremos:

$$\underbrace{(5 \cdot 130) \textbf{ mod } 12}_{\text{multiplicação modular}} = 650 \textbf{ mod } 12 = \underbrace{2}_{\text{resultado}}$$

Domínio $\mathbb{Z}_m$

Definição (Domínio $\mathbb{Z}_m$)
Dado um inteiro $m > 0$, o **domínio da aritmética de módulo** m é o conjunto $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$.

Domínio $\mathbb{Z}_m$

Definição (Domínio $\mathbb{Z}_m$)
Dado um inteiro $m > 0$, o **domínio da aritmética de módulo** m é o conjunto $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$.

Exemplos:
A aritmética ...

- ... de módulo 1 tem como domínio $\mathbb{Z}_1 = \{0\}$

Domínio $\mathbb{Z}_m$

Definição (Domínio $\mathbb{Z}_m$)
Dado um inteiro $m > 0$, o **domínio da aritmética de módulo** m é o conjunto $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$.

Exemplos:
A aritmética ...

- ... de módulo 1 tem como domínio $\mathbb{Z}_1 = \{0\}$
- ... de módulo 2 tem como domínio $\mathbb{Z}_2 = \{0, 1\}$

Domínio $\mathbb{Z}_m$

Definição (Domínio $\mathbb{Z}_m$)
Dado um inteiro $m > 0$, o **domínio da aritmética de módulo** m é o conjunto $\mathbb{Z}_m = \{0, 1, \ldots, m - 1\}$.

Exemplos:
A aritmética ...

- ... de módulo 1 tem como domínio $\mathbb{Z}_1 = \{0\}$
- ... de módulo 2 tem como domínio $\mathbb{Z}_2 = \{0, 1\}$
- ... de módulo 5 tem como domínio $\mathbb{Z}_5 = \{0, 1, \ldots, 4\}$

Domínio $\mathbb{Z}_m$

Definição (Domínio $\mathbb{Z}_m$)
Dado um inteiro $m > 0$, o **domínio da aritmética de módulo m** é o conjunto $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$.

Exemplos:
A aritmética ...

- ... de módulo 1 tem como domínio $\mathbb{Z}_1 = \{0\}$
- ... de módulo 2 tem como domínio $\mathbb{Z}_2 = \{0, 1\}$
- ... de módulo 5 tem como domínio $\mathbb{Z}_5 = \{0, 1, \ldots, 4\}$
- ... de módulo 12 tem como domínio $\mathbb{Z}_{12} = \{0, 1, \ldots, 11\}$
- ... de módulo 60 tem como domínio $\mathbb{Z}_{60} = \{0, 1, \ldots, 59\}$
- ... de módulo 256 tem como domínio $\mathbb{Z}_{256} = \{0, 1, \ldots, 255\}$

Operações em $\mathbb{Z}_m$

Definição (Operações em $\mathbb{Z}_m$)

Dado um inteiro $m > 0$ e $a, b \in \mathbb{Z}_m$,

- $a +_m b \;=\; (a + b) \ \mathbf{mod}\ m$ “**soma módulo m**”
- $a \cdot_m b \;=\; (a \cdot b) \ \mathbf{mod}\ m$ “**multiplicação módulo m**”

Operações em $\mathbb{Z}_m$

Definição (Operações em $\mathbb{Z}_m$)

Dado um inteiro $m > 0$ e $a, b \in \mathbb{Z}_m$,

- $a +_m b \;=\; (a + b) \textbf{ mod } m$ "**soma módulo m**"
- $a \cdot_m b \;=\; (a \cdot b) \textbf{ mod } m$ "**multiplicação módulo m**"

Exemplo (Soma):

- $7 +_{11} 9 = (7 + 9) \textbf{ mod } 11 = 16 \textbf{ mod } 11 = 5$

Operações em $\mathbb{Z}_m$

Definição (Operações em $\mathbb{Z}_m$)

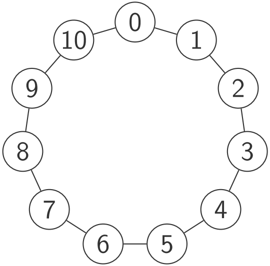
Dado um inteiro $m > 0$ e $a, b \in \mathbb{Z}_m$,

- $a +_m b \; = \; (a + b) \textbf{ mod } m$ “**soma módulo m**”
- $a \cdot_m b \; = \; (a \cdot b) \textbf{ mod } m$ “**multiplicação módulo m**”

Exemplo (Soma):

- $7 +_{11} 9 = (7 + 9) \textbf{ mod } 11 = 16 \textbf{ mod } 11 = 5$

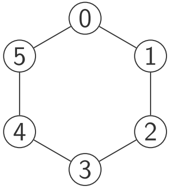
Operações aritméticas de módulo 11 funcionam como em um relógio hipotético de 11 horas.



Operações em $\mathbb{Z}_m$

Similarmente, teremos:

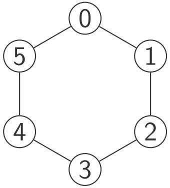
- $4 +_5 3 = (4+3) \textbf{ mod } 5 = 7 \textbf{ mod } 5 = 2$



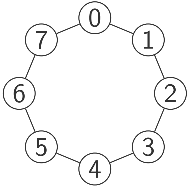
Operações em $\mathbb{Z}_m$

Similarmente, teremos:

- $4 +_5 3 = (4+3) \textbf{ mod } 5 = 7 \textbf{ mod } 5 = 2$



- $5 +_8 3 = (5+3) \textbf{ mod } 8 = 8 \textbf{ mod } 8 = 0$



Definição: Aritmética de módulo m

Definição (Domínio $\mathbb{Z}_m$)
Dado um inteiro $m > 0$, o **domínio da aritmética de módulo** m é o conjunto $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$.

Definição (Operações em $\mathbb{Z}_m$)
Dado um inteiro $m > 0$ e $a, b \in \mathbb{Z}_m$,

- $a +_m b \;=\; (a + b) \textbf{ mod } m$ "**soma módulo m**"
- $a \cdot_m b \;=\; (a \cdot b) \textbf{ mod } m$ "**multiplicação módulo m**"

Definição: Aritmética de módulo m

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Definição (Domínio $\mathbb{Z}_m$)
Dado um inteiro $m > 0$, o **domínio da aritmética de módulo** m é o conjunto $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$.

Definição (Operações em $\mathbb{Z}_m$)
Dado um inteiro $m > 0$ e $a, b \in \mathbb{Z}_m$,

- $a +_m b \;=\; (a + b) \textbf{ mod } m$ "**soma módulo m**"
- $a \cdot_m b \;=\; (a \cdot b) \textbf{ mod } m$ "**multiplicação módulo m**"

Definição (Aritmética de módulo m)
Dado um inteiro $m > 0$, a **aritmética de módulo m** é a estrutura

$$\langle \mathbb{Z}_m, +_m, \cdot_m \rangle$$

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Propriedades das Operações no Módulo m

Propriedades das operações no módulo m

Dado um inteiro $m > 0$, as operações $+_m$ e $\cdot_m$ satisfazem às propriedades abaixo para todos $a, b, c \in \mathbb{Z}_m$

(**Fechamento**)

1. $a +_m b \in \mathbb{Z}_m$
2. $a \cdot_m b \in \mathbb{Z}_m$

Propriedades das operações no módulo m

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Dado um inteiro $m > 0$, as operações $+_m$ e $\cdot_m$ satisfazem às propriedades abaixo para todos $a, b, c \in \mathbb{Z}_m$

(**Fechamento**)

1. $a +_m b \in \mathbb{Z}_m$
2. $a \cdot_m b \in \mathbb{Z}_m$

(**Associatividade**)

1. $(a +_m b) +_m c = a +_m (b +_m c)$
2. $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

Propriedades das operações no módulo m

Universidade Federal do Ceará
Campus Quixadá

Dado um inteiro $m > 0$, as operações $+_m$ e $\cdot_m$ satisfazem às propriedades abaixo para todos $a, b, c \in \mathbb{Z}_m$

(**Fechamento**)

1. $a +_m b \in \mathbb{Z}_m$
2. $a \cdot_m b \in \mathbb{Z}_m$

(**Associatividade**)

1. $(a +_m b) +_m c = a +_m (b +_m c)$
2. $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

(**Comutatividade**)

1. $a +_m b = b +_m a$
2. $a \cdot_m b = b \cdot_m a$

Propriedades das operações no módulo m

Universidade Federal do Ceará
Campus Quixadá

Dado um inteiro $m > 0$, as operações $+_m$ e $\cdot_m$ satisfazem às propriedades abaixo para todos $a, b, c \in \mathbb{Z}_m$

(**Fechamento**)

1. $a +_m b \in \mathbb{Z}_m$
2. $a \cdot_m b \in \mathbb{Z}_m$

(**Associatividade**)

1. $(a +_m b) +_m c = a +_m (b +_m c)$
2. $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

(**Comutatividade**)

1. $a +_m b = b +_m a$
2. $a \cdot_m b = b \cdot_m a$

(**Distributividade**)

1. $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$

Propriedades das operações no módulo m

Dado um inteiro $m > 0$, as operações $+_m$ e $\cdot_m$ satisfazem às propriedades abaixo para todos $a, b, c \in \mathbb{Z}_m$

(**Fechamento**)

1. $a +_m b \in \mathbb{Z}_m$
2. $a \cdot_m b \in \mathbb{Z}_m$

(**Associatividade**)

1. $(a +_m b) +_m c = a +_m (b +_m c)$
2. $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

(**Comutatividade**)

1. $a +_m b = b +_m a$
2. $a \cdot_m b = b \cdot_m a$

(**Distributividade**)

1. $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$

(**Elemento Neutro**)

1. $a +_m 0 = a$
2. $a \cdot_m 1 = a$

Propriedades das operações no módulo m

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Dado um inteiro $m > 0$, as operações $+_m$ e $\cdot_m$ satisfazem às propriedades abaixo para todos $a, b, c \in \mathbb{Z}_m$

(**Fechamento**)

1. $a +_m b \in \mathbb{Z}_m$
2. $a \cdot_m b \in \mathbb{Z}_m$

(**Associatividade**)

1. $(a +_m b) +_m c = a +_m (b +_m c)$
2. $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

(**Comutatividade**)

1. $a +_m b = b +_m a$
2. $a \cdot_m b = b \cdot_m a$

(**Distributividade**)

1. $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$

(**Elemento Neutro**)

1. $a +_m 0 = a$
2. $a \cdot_m 1 = a$

(**Inverso Aditivo**)

1. se $a \neq 0$, $a +_m (m - a) = 0$
2. $0 +_m 0 = 0$

Propriedades das operações no módulo m

Dado um inteiro $m > 0$, as operações $+_m$ e $\cdot_m$ satisfazem às propriedades abaixo para todos $a, b, c \in \mathbb{Z}_m$

(**Fechamento**)

1. $a +_m b \in \mathbb{Z}_m$
2. $a \cdot_m b \in \mathbb{Z}_m$

(**Associatividade**)

1. $(a +_m b) +_m c = a +_m (b +_m c)$
2. $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

(**Comutatividade**)

1. $a +_m b = b +_m a$
2. $a \cdot_m b = b \cdot_m a$

(**Distributividade**)

1. $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$

(**Elemento Neutro**)

1. $a +_m 0 = a$
2. $a \cdot_m 1 = a$

(**Inverso Aditivo**)

1. se $a \neq 0$, $a +_m (m - a) = 0$
2. $0 +_m 0 = 0$

Demonstrar estas propriedades é um excelente exercício.

Propriedades das operações no módulo m

A título de exemplo, demonstraremos a comutatividade da soma.

Teorema 7.20 (Comutatividade de $+_m$): Dado um inteiro $m > 0$, se $a, b \in \mathbb{Z}_m$, então $a +_m b = b +_m a$.

Demonstração:

Propriedades das operações no módulo m

A título de exemplo, demonstraremos a comutatividade da soma.

Teorema 7.20 (Comutatividade de $+_m$): Dado um inteiro $m > 0$, se $a, b \in \mathbb{Z}_m$, então $a +_m b = b +_m a$.

Demonstração:

Sejam m um inteiro positivo qualquer e a, b inteiros quaisquer.

Propriedades das operações no módulo m

A título de exemplo, demonstraremos a comutatividade da soma.

Teorema 7.20 (Comutatividade de $+_m$): Dado um inteiro $m > 0$, se $a, b \in \mathbb{Z}_m$, então $a +_m b = b +_m a$.

Demonstração:

Sejam m um inteiro positivo qualquer e a, b inteiros quaisquer.

Por prova direta, suponha que $a, b \in \mathbb{Z}_m$.

Propriedades das operações no módulo m

A título de exemplo, demonstraremos a comutatividade da soma.

Teorema 7.20 (Comutatividade de $+_m$): Dado um inteiro $m > 0$, se $a, b \in \mathbb{Z}_m$, então $a +_m b = b +_m a$.

Demonstração:

Sejam m um inteiro positivo qualquer e a, b inteiros quaisquer.

Por prova direta, suponha que $a, b \in \mathbb{Z}_m$.

Pela definição da soma modular, temos

Propriedades das operações no módulo m

A título de exemplo, demonstraremos a comutatividade da soma.

Teorema 7.20 (Comutatividade de $+_m$): Dado um inteiro $m > 0$, se $a, b \in \mathbb{Z}_m$, então $a +_m b = b +_m a$.

Demonstração:

Sejam m um inteiro positivo qualquer e a, b inteiros quaisquer.

Por prova direta, suponha que $a, b \in \mathbb{Z}_m$.

Pela definição da soma modular, temos

$$\begin{aligned} a +_m b &= (a + b) \textbf{ mod } m \\ &= (b + a) \textbf{ mod } m \quad \text{(comutatividade em } \mathbb{Z}) \\ &= b +_m a \quad \text{(definição de } +_m) \end{aligned}$$

Propriedades das operações no módulo m

A título de exemplo, demonstraremos a comutatividade da soma.

Teorema 7.20 (Comutatividade de $+_m$): Dado um inteiro $m > 0$, se $a, b \in \mathbb{Z}_m$, então $a +_m b = b +_m a$.

Demonstração:

Sejam m um inteiro positivo qualquer e a, b inteiros quaisquer.

Por prova direta, suponha que $a, b \in \mathbb{Z}_m$.

Pela definição da soma modular, temos

$$\begin{aligned} a +_m b &= (a + b) \textbf{ mod } m \\ &= (b + a) \textbf{ mod } m \quad \text{(comutatividade em } \mathbb{Z}) \\ &= b +_m a \quad \text{(definição de } +_m) \end{aligned}$$

Portanto, $a +_m b = b +_m a$. □

Como exercício, demonstre as demais propriedades.

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

FIM