Divisibilidade

Matemática Discreta

Prof. Samy Sá

Universidade Federal do Ceará
Campus de Quixadá

21 de agosto de 2020

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Roteiro

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Prévia

Requisitos

- Técnicas de Demonstração de Teoremas
- Propriedades de operações aritméticas

Esta apresentação...

- introduz os conceitos de divisibilidade e divisão inteira
- discute propriedades da relação de divisibilidade
- inclui exemplos de aplicação dos conceitos em demonstrações

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Roteiro

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

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** $b = ac$.*

Exemplo

- 3 *divide* 6, *pois* $6 = 3.2$

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

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

  ou seja, existe um inteiro e tal que $68 = -4e$. ***Neste caso, temos*** $e = -17$.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

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 $b = ac$.***

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 $3.5 = 15$ e que $3.6 = 18$.*
  3. *Como $15 < 16 < 18$, temos que $3.5 < 3.c < 3.6$.*
  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 $16 = 3c$.*

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

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** $b = ac$.*

Proposição

Sejam a e b números inteiros com $a \neq 0$, dizemos que a divide b se e somente se $\frac{b}{a}$ é um inteiro.

$$\forall a \, \forall b \, [a \neq 0 \rightarrow (\, a \text{ divide } b \, \leftrightarrow \, \frac{b}{a} \text{ é um inteiro}) \,]$$

Prova

($\Rightarrow$) Sejam a, b inteiros quaisquer com $a \neq 0$ (Instanciação), suponha que a divide b (Hipótese da PD). Pela definição, 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.

($\Leftarrow$) Deixada como exercício.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

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 $b = ac$**.*

Proposição

Sejam a e b números inteiros com $a \neq 0$, dizemos que a divide b se e somente se $\frac{b}{a}$ é um inteiro

Exemplo

- 3 *divide* 6, *pois* $6 = 3.2$;
  da mesma forma, $\frac{6}{3}$ *é um inteiro, pois* $\frac{6}{3} = 2$.
- 2 *divide* -30, *pois* $-30 = 2.(-15)$;
  da mesma forma, $\frac{-30}{2}$ *é um inteiro, pois* $\frac{-30}{2} = -15$.

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** $b = ac$.*

Proposição

Sejam a e b números inteiros com $a \neq 0$, dizemos que a divide b se e somente se $\frac{b}{a}$ é um inteiro

Exemplo

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

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

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** $b = ac$.*

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 dividor de** 6, que 6 **é múltiplo de** 3 e que 6 **é divisível por** 3.*

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

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** $b = ac$.*

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 **não divide** 16. Da mesma forma, podemos dizer que*

*3 **não é fator de** 16, 3 **não é divisor de** 16, que 16 **não é múltiplo de** 3 e que 16 **não é divisível por** 3.*

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

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** $b = ac$.*

Notação

- *Quando **a divide b**, escremos "$a \mid b$"*
- *Quando a **não** divide b, escremos "$a \nmid b$"*

Exemplo

- *Vimos que 3 divide 6, então escrevemos $3 \mid 6$;*
- *Vimos que 2 divide -30, então escrevemos $2 \mid -30$;*
- *Vimos que 3 não divide 16, então escrevemos $3 \nmid 16$.*

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Roteiro

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Divisibilidade e 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 mais recente...

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 $b = ac$.*

* dica: se existe um inteiro k tal que $n = 2k$, então 2 divide n.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Divisibilidade e 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 mais recente...

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 reescrever...

Definição (Número Par (Alternativa 2))

Seja n um inteiro, dizemos que

*n é par se e somente se 2 **divide** n.*

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Divisibilidade e 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 mais recente...

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 reescrever...

Definição (Número Par (Alternativa 3))

Seja n um inteiro, dizemos que
*n é par se e somente se n **é divisível por** 2.*

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Roteiro

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Propriedades de $|$

Teorema

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

1. *Se $a \mid b$ e $a \mid c$, então $a \mid (b + c)$;*
2. *Se $a \mid b$, então $a \mid b.c$ para todo c inteiro;*
3. *Se $a \mid b$ e $b \mid c$, então $a \mid c$.*

Prova

1. *Sejam a, b, c inteiros quaisquer com $a \neq 0$ **(Instanciação)**, suponha que $a \mid b$ e $a \mid c$ **(Hipótese da PD)**.*

   Então existem inteiros s e t tais que $b = a.s$ e $c = a.t$ **(Divisibilidade)**.

   Portanto, $b + c = a.s + a.t = a.(s + t)$ **(Igualdades + Distributididade)**.

   Como s, t são inteiros, $s + t$ é inteiro. Portanto, $a \mid b + c$ **(Divisibilidade)**.
2. *Deixada como exercício.*
3. *Deixada como exercício.*

Samy Sá (samy@ufc.br)

Propriedades de $|$

Teorema

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

1. *Se $a \mid b$ e $a \mid c$, então $a \mid (b + c)$;*
2. *Se $a \mid b$, então $a \mid b.c$ para todo c inteiro;*
3. *Se $a \mid b$ e $b \mid c$, então $a \mid c$.*

Corolário

Se a, b e c são inteiros tais que $a \neq 0$, $a \mid b$ e $a \mid c$, então $a \mid m.b + n.c$ para quaisquer m, n inteiros.

Prova

*Pela afirmação **2.** do teorema anterior, vemos que $a \mid m.b$ para todo inteiro m e que $a \mid n.c$ para todo inteiro n.*
*Daí podemos usar a afirmação **1.** para concluir que $a \mid m.b + n.c$.*

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Roteiro

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

O Algoritmo de Divisão

No caso geral, quando tentamos dividir um inteiro por outro...

Teorema (Algoritmo da Divisão)

Seja n um inteiro qualquer e d um inteiro positivo, existe ***um único par de inteiros*** *q e r com $0 \leq r < d$ tais que $n = d.q + r$.*

Este teorema trata da divisão entre inteiros:

$$\begin{array}{l|l} n & \underline{\quad d \quad} \\ r & \quad q \end{array}$$

Numa divisão como esta acima,

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

É este formato de divisão que nos dá

$$n = d.q + r$$

que será chave para o próximo tópico

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

O Algoritmo de Divisão

No caso geral, quando tentamos dividir um inteiro por outro...

Teorema (Algoritmo da Divisão)

Seja n um inteiro qualquer e d um inteiro positivo, existe ***um único par de inteiros*** *q e r com $0 \leq r < d$ tais que $n = d.q + r$.*

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

Exemplo

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

- $\ldots$
- $10 = 3.(-3) + 19$
- $10 = 3.(-2) + 16$
- $10 = 3.(-1) + 13$
- $10 = 3.0 + 10$
- $10 = 3.1 + 7$
- $10 = 3.2 + 4$
- $10 = 3.3 + 1$
- $10 = 3.4 + (-2)$
- $10 = 3.5 + (-5)$
- $10 = 3.6 + (-8)$
- $\ldots$

O Algoritmo de Divisão

No caso geral, quando tentamos dividir um inteiro por outro...

Teorema (Algoritmo da Divisão)

Seja n um inteiro qualquer e d um inteiro positivo, existe ***um único par de inteiros*** *q e r com $0 \leq r < d$ tais que $n = d.q + r$.*

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

Exemplo

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

- $\ldots$
- $10 = 3.(-3) + 19$
- $10 = 3.(-2) + 16$
- $10 = 3.(-1) + 13$
- $10 = 3.0 + 10$
- $10 = 3.1 + 7$
- $10 = 3.2 + 4$
- $10 = 3.3 + 1$
- $10 = 3.4 + (-2)$
- $10 = 3.5 + (-5)$
- $10 = 3.6 + (-8)$
- $\ldots$

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

O Algoritmo de Divisão

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 ***div*** $d = q$ ***(divisão inteira ou sem resto)***
- n ***mod*** $d = r$ ***(módulo/resto da divisão)***

Obs.: Também é admissível escrever **div** $(n, d) = q$ e **mod** $(n, d) = r$.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

O Algoritmo de Divisão

Exemplo

Na divisão de 110 *por* 9*, teremos (Parte 1/2)*

$$\begin{array}{rl} \overset{\frown}{11}0 & \underline{|\ \ 9\ \ } \\ \underline{-9\ } & \ \ \ 1 \\ 2\ & \end{array}$$

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

O Algoritmo de Divisão

Exemplo

Na divisão de 110 *por* 9*, teremos (Parte 2/2)*

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

Isso nos dá que

- $110 = 9.12 + 2$,
- 110 **div** $9 = 12$, e
- 110 **mod** $9 = 2$.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

O Algoritmo de Divisão

O Algoritmo da Divisão também permite dividendos negativos.

Exemplo

Na divisão de -110 *por* 9*, teremos (Parte 1/2)*

$$
\begin{array}{r|l}
-110 & \underline{\;9\;} \\
\underline{+9} & -1 \\
-2 &
\end{array}
$$

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

O Algoritmo de Divisão

Exemplo

Na divisão de -110 *por* 9*, teremos (Parte 2/2)*

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

Isso nos dá que

- $-110 = 9.(-13) + 7$,
- -110 **div** $9 = -13$, e
- -110 **mod** $9 = 7$.

Pera, por que o quociente não é -12?

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

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

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

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Roteiro

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Divisibilidade vs Algoritm da Divisão

Teorema (Algoritmo da Divisão)

*Seja n um inteiro qualquer e d um inteiro positivo, existe **um único par de inteiros** q e r com $0 \leq r < d$ tais que $n = d.q + r$.*

O que ocorre quando temos $r = 0$?

- Isto só é possível para alguns valores de n, d
- A expressão $n = d.q + r$ será escrita simplesmente como $n = d.q$
- Como q é inteiro, $n = d.q$ nos diz que d **divide** n

Teorema

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

Prova

(Nos próximos slides...)

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Divisibilidade vs Algoritm da Divisão

Teorema

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

Prova (1/2)

($\Rightarrow$) Sejam a, b inteiros com $a \neq 0$ (Instanciação),

- *suponha que a divide b (Hipótese da PD).*
- *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** $a = 0$.*

($\Leftarrow$) No próximo slide.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Divisibilidade vs Algoritm da Divisão

Teorema

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

Prova (2/2)

($\Rightarrow$) Concluído.
($\Leftarrow$) Sejam a, b inteiros com $a \neq 0$ (Instanciação),

- *suponha que b **mod** $a = 0$ (Hipótese da PD).*
- *Seja b **div** $a = c$, pelo algoritmo da divisão, teremos $b = a.c + 0$.*
- $\ldots$
- *Logo, a divide b.*

Exercício: conclua a demonstração indicando os passos que faltam.