Números Inteiros

Prof. Eanes Torres Pereira

FMCC2

Roteiro

1. O Algoritmo da Divisão

2. Divisibilidade

3. O Algoritmo de Euclides

3. Números Primos

O Algoritmo da Divisão

- Consideramos $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$
- **Princípio da Boa Ordenação - PBO**. Todo subconjunto não-vazio do conjunto dos inteiros não-negativos contém um menor elemento.
- O PBO não é válido para o conjunto de todos os inteiros.
- **Divisão Inteira**. dividendo = (divisor)(quociente) + (resto)
- **Teorema 1.1 (O algoritmo da divisão)**. Sejam a, b inteiros com $b > 0$. Então, existem inteiros únicos q e r tais que: $a = bq + r$ e $0 \leq r < b$.

O Algoritmo da Divisão

- Observações sobre o Algoritmo da Divisão:
  1. Esse teorema permite a possibilidade de que o divisor, a, seja negativo.
  2. Por isso, há uma afirmação adicional indicando que o quociente, q, e o resto, r, são únicos e r é não-negativo.
  3. A ideia fundamental para a prova do Teorema 1.1 é que a divisão é apenas a repetição de subtrações.

Exercícios

Determine o quociente e o resto quando a é dividido por b:

1. $a = 302$, $b = 19$
2. $a = 0$, $b = 19$
3. $a = 2001$, $b = 17$

Respostas do Exercícios

1. quociente 15; resto 17;
2. quociente 0; resto 0;
3. quociente 117; resto 12

O Algoritmo da Divisão

- **Corolário 1.2**. Sejam a e c inteiros, com $c \neq 0$. Então, existem inteiros únicos q e r, tal que: $a = cq + r$ e $0 \leq r < |c|$.
- Como **Exercício**, prove o Corolário 1.2.

Roteiro

Divisibilidade

- **Definição**. Sejam a e b inteiros com $b \neq 0$. Dizemos que b divide a (ou que b é divisor de a ou que b é um fator de a) se $a = bc$ para algum inteiro c. Em símbolos, "b divide a" escrito $b \mid a$ e "b não divide a" é escrito $b \nmid a$.
- **Exemplo 1.** $3|24$ por que $24 = 3 \cdot 8$. Mas $3 \nmid 7$. Divisores negativos são permitidos: $-6|54$ por que $54 = (-6)(-9)$, mas $-6 \nmid (-13)$.
- **Exemplo 2.** Todo inteiro b diferente de zero divide zero, por que $0 = b \cdot 0$. Para todo inteiro a, temos $1|a$, por que $a = 1 \cdot a$.

Máximo Divisor Comum

- **Definição**. Sejam a e b inteiros, diferentes de zero. O maior divisor comum (mdc) de a e de b é o maior inteiro d que divide ambos, a e b. Em outras palavras, d é o mdc de a e de b desde que:
  (i) $d|a$ e $d|b$;
  (ii) se $c|a$ e $c|b$, então $c \leq d$.
- Vamos denotar o mdc de a e de b como $\text{mdc}(a, b)$.
- **Exemplo**. $\text{mdc}(12, 30) = 6$. Os únicos divisores comuns de 10 e de 21 são 1 e -1. Portanto, $\text{mdc}(10, 21) = 1$. Dois inteiros cujo mdc é 1, são chamados de **primos entre si** ou primos relativos.

Máximo Divisor Comum

- **Teorema 1.3** Sejam a e b inteiros, ambos não são zero simultaneamente, e seja d seu mdc. Então, existem inteiros u e v, não necessariamente únicos, tais que $d = au + bv$.
- **Exercício**. Para cada par de números a seguir, determine o mdc.
  1. 56 e 72
  2. 24 e 138
- Respostas:

Máximo Divisor Comum

- **Teorema 1.3** Sejam a e b inteiros, ambos não são zero simultaneamente, e seja d seu mdc. Então, existem inteiros u e v, não necessariamente únicos, tais que $d = au + bv$.
- **Exercício**. Para cada par de números a seguir, determine o mdc.
  1. 56 e 72
  2. 24 e 138
- Respostas:
  1. mdc(56,72) = 8

Máximo Divisor Comum

- **Teorema 1.3** Sejam a e b inteiros, ambos não são zero simultaneamente, e seja d seu mdc. Então, existem inteiros u e v, não necessariamente únicos, tais que $d = au + bv$.
- **Exercício**. Para cada par de números a seguir, determine o mdc.
  1. 56 e 72
  2. 24 e 138
- Respostas:
  1. mdc(56,72) $= 8$
  2. mdc(24, 138) $= 6$

Máximo Divisor Comum

- **Teorema 1.3** Sejam a e b inteiros, ambos não são zero simultaneamente, e seja d seu mdc. Então, existem inteiros u e v, não necessariamente únicos, tais que $d = au + bv$.
- **Exercício**. Para cada par de números a seguir, determine o mdc.
  1. 56 e 72
  2. 24 e 138
- Respostas:
  1. mdc(56,72) = 8
  2. mdc(24, 138) = 6

Máximo Divisor Comum

- **Corolário 1.4**. Sejam a e b inteiros, não zero simultaneamente, e seja d um inteiro positivo. Então, d é o mdc de a e de b se, e somente se, d satisfaz estas condições:
  (i) $d|a$ e $d|b$;
  (ii) se $c|a$ e $c|b$, então $c|d$.
- **Teorema 1.5**. Se $a|bc$ e mdc(a,b)=1, então $a|c$.

Roteiro

O Algoritmo de Euclides

- **Teorema 1.6**. Sejam a e b inteiros positivos com $a \geq b$. Se $b|a$, então $\mathrm{mdc}(a, b) = b$. Se $b \nmid a$, então aplique o algoritmo da divisão repetidamente como segue:

  $a = bq_0 + r_0$, $0 < r_0 < b$

  $b = r_0 q_1 + r_1$, $0 \leq r_1 < r_0$

  $r_0 = r_1 q_2 + r_2$, $0 \leq r_2 < r_1$

  $r_1 = r_2 q_3 + r_3$, $0 \leq r_3 < r_2$

  $\ldots$

  $\ldots$

  $\ldots$

- Esse processo para quando um resto igual a zero for obtido. O último resto não-zero é o mdc de a e de b.

Exemplo

- Use o algoritmo de Euclides para calcular mdc(324, 148).

  Solução:

  $324 = 148 \cdot 2 + 28$

  $148 = 28 \cdot 5 + 8$

  $28 = 8 \cdot 3 + \mathbf{4}$

  $8 = 4 \cdot 2 + 0$
- Use substituição retroativa para escrever 4 como uma combinação linear de 324 e 148.
- Resposta:

Exemplo

- Use o algoritmo de Euclides para calcular mdc(324, 148).

  Solução:

  $324 = 148{\cdot}2 + 28$

  $148 = 28{\cdot}5 + 8$

  $28 = 8{\cdot}3 + \mathbf{4}$

  $8 = 4{\cdot}2 + 0$

- Use substituição retroativa para escrever 4 como uma combinação linear de 324 e 148.
- Resposta:

  $\mathrm{mdc}(324{,}148) = 4$; $4 = 16 \cdot 324 - 35 \cdot 148$.

O Algoritmo de Euclides

- **Lema 1.7**. Se a, b, q, $r \in \mathbb{Z}$ e $a = bq + r$, então mdc(a,b) = mdc(b,r).
- **Exercício**. Expresse cada um dos mdc(a,b) a seguir como uma combinação linear de a e de b:
  - mdc(56, 72)
  - mdc(24,138)
  - mdc(143, 227)
  - mdc(314, 159)

Roteiro

Números Primos

- **Definição**. Um inteiro p é chamado de *primo* se $p \neq 0$, $p \neq \pm 1$ e os únicos divisores de p são ± 1 e $\pm p$.
- **Exemplo**. 3, -5, 7, -11, 13 e -17 são primos, mas 15 não é. O inteiro 4567 é primo
- **Teorema 1.8**. Seja p um inteiro com $p \neq 0$, $p \neq \pm 1$. Então p é primo se, e somente se, p tem esta propriedade: sempre que $p|bc$, então $p|b$ ou $p|c$.
- **Corolário 1.9**. Se p é primo e $p|a_1 a_2 \ldots a_n$, então p divide pelo menos um dos a_i.

O Teorema Fundamental da Aritmética

- **Teorema 1.10**. Todo inteiro n exceto 0, ± 1 é o produto de primos.
- **Teorema 1.11**. A fatoração de um inteiro em números primos é única.
- **Corolário 1.12**. Todo inteiro $n > 1$ pode ser escrito apenas na forma $n = p_1 p_2 p_3 \ldots p_r$, em que os p_i são primos positivos tais que $p_1 \leq p_2 \leq p_3 \leq \ldots \leq p_r$.

Exercício

- Busque em livros texto de Álgebra Abstrata demonstrações para os teoremas, corolários e lemas vistos neste slide e estude-os.

Referência

- Abstract Algebra an Introduction. Thomas W. Hungerford.