AULA

Números Inteiros: Continuação

5

META:

Apresentar as propriedades aritméticas dos números inteiros

OBJETIVOS:

Ao fim da aula os alunos deverão ser capazes de:

Entender o conceito de divisibilidade nos números inteiros.

Entender o conceito de números primos.

PRÉ-REQUISITOS

Propriedades de adição e multiplicação dos números inteiros. Indução sobre os números inteiros.

5.1 Introdução

Nesta aula apresentaremos o conceito de divisibilidade entre dois números inteiros bem como o conceito de números primos. Você, caro aluno, perceberá uma pequena diferença entre o conceito aprendido no ensino fundamental e o exposto aqui.

5.2 Propriedades Aritméticas dos Números Inteiros

5.2.1 Divisibilidade

Definição 5.1. Dados dois números $x, y \in \mathbb{Z}$, dizemos que x divide y se existe $z \in \mathbb{Z}$ tal que $y = x.z$. Neste caso dizemos que y é um múltiplo de x. (x é um divisor de y).

Escrevemos $x|y$ para dizer que x divide y.

Exemplo 5.1. $1|10$; $2|-2$;

As seguintes propriedades seguem imediatamente da definição de divisão.

Proposição 5.10. *As seguintes afirmações são verdadeiras para números inteiros.*

a) $x|x$

b) $x|y \ e \ y|x \Rightarrow x = \pm y$

c) $x|y \ e \ y|z \Rightarrow x|z$

d) $x|y \ e \ x|z \Rightarrow x|ay + bz, \ \forall a, b \in \mathbb{Z}$

Demonstração.

a) $x|x$ pois $x = x.1$

b) Temos que existe $z_1 \in \mathbb{Z}$ tal que $y = x.z_1$ e existe $z_2 \in \mathbb{Z}$ tal que $x = yz_2$. Então $y = y(z_1z_2)$. Assim $y - y(z_1 - z_2) = 0 \Rightarrow y(1 - z_1z_2) = 0$. Logo $y = 0$ ou $z_1z_2 = 1$. Se $y = 0, x = 0$. Se $z_1z_2 = 1$, $z_1 = z_2 = 1$ ou $z_1 = z_2 = -1$ (Exercício).

c) Existem k_1 e k_2 tais que $y = xk_1$ e $z = yk_2$. Segue-se que $z = x(k_1k_2)$. Donde $x|z$.

d) De $x|y$ temos que existe $k_1 \in \mathbb{Z}$ tal que $y = xk_1$ (1). De $x|z$ temos que existe $k_2 \in \mathbb{Z}$ tal que $z = xk_2$ (2). Logo $ay + bz = x(k_1a + k_2b)$. Fazendo $k_3 = k_1a + k_2b$, temos que $ay + bz = xk_3$, o que significa $x|ay + bz$.

e) Como $x|y$ e $x, y \in \mathbb{Z}_+$, existe $q \in \mathbb{Z}_+$ tal que $y = xq$. Se $q = 1$, $x = y$. Se $q > 1$, existe $q_0 \in \mathbb{Z}_+$ tal que $q = q_0 + 1$. Logo $y = x(q_0 + 1) = xq_0 + x > x$. Em todo caso $x \leq y$.

■

Definição 5.2. Para todo $a \in \mathbb{Z}$, o valor absoluto de a (ou módulo de a) representado por $|a|$ é definido como:

$$|a| = \begin{cases} a, & a \in \mathbb{Z}_+ \cup \{0\} \\ -a, & a \in \mathbb{Z}_- \cup \{0\} \end{cases}$$

Proposição 5.11. *Se $a, b \in \mathbb{Z}$ então:*

a) $|a| = |-a|$

b) $|ab| = |a||b|$

c) $-|a| \leq a \leq |a|$

d) $|a + b| \leq |a| + |b|$

Demonstração.

a) Se $a \geq 0$, $|-a| = -(-a) = a = |a|$. Se $a \leq 0$, $|-a| = -a = |a|$.

b) Suponhamos que $ab > 0$. Então $a > 0$ e $b > 0$ ou $a < 0$ e $b < 0$. No primeiro caso $a = |a|$ e $b = |b|$. Donde $|ab| = ab = |a||b|$. No segundo caso $|a| = -a$ e $|b| = -b$, donde temos $|ab| = ab = (-a)(-b) = |a||b|$.

Suponhamos agora $ab < 0$. Assim $a < 0$ e $b > 0$ ou $a > 0$ e $b < 0$. No primeiro destes casos $|a| = -a$ e $|b| = b$, donde $|a||b| = (-a)b = -(ab) = |ab|$. O outro caso fica como exercício. O caso $ab = 0$ é óbvio.

c) Se $a > 0$, $|a| = a$ e $-a < 0$, isto é, $-|a| < 0$. Logo $-|a| < 0 < |a|$. O caso $a < 0$ fica como exercício e o caso $a = 0$ é óbvio.

d) Se $a + b = 0$ claramente $|a + b| \leq |a| + |b|$. Se $a + b > 0$, $|a + b| = a + b \leq |a| + |b|$. Se $a + b < 0$, $|a + b| = -(a + b)$, isto é, $-|a + b| = a + b \geq -|a| + (-|b|) = -(|a| + |b|)$, o que implica $|a + b| \leq |a| + |b|$.

■

Notação: $a^n = \underbrace{aa...a}_{nvezes}$

Exercício 5.1. a) Mostre que se $a < 0$ entao $a^{2n+1} < 0$, para todo $n \geq 0$.

b) Mostre que $x^{2n+1}+1 = (x+1)(x^{2n}-x^{2n-1}+x^{2n-2}-...-x+1)$

c) Se $d|n$ então $ad|an$, para todo $a \in \mathbb{Z}$.

d) $|\sum_{i=1}^{n} a_i| \leq \sum_{i=1}^{n} |a_i|$ onde $\sum_{i=1}^{n} b_i = b_1 + b_2 + ... + b_n$.

Solução:

a) Mostremos por indução:

- A sentença é válida para n=o, pois $a^{2.0+1} = a^{0+1} = a < 0$
- Suponha que $a^{2n+1} < 0$. Devemos mostrar que $a^{2(n+1)+1} < 0$. Note que $a^{2(n+1)+1} = a^{2n+2+1} = a^{2n+1}a^2$. Mas, como $a \neq 0$, a^2. Logo $a^{2(n+1)+1} = a^{2n+1}a^2 < 0$.

b) Note que $(x+1).1 = x+1 = x^1+1 = x^{2.0+1}+1$, donde a sentença é válida para $n = 0$. Suponha que a expressão é válida para algum $n \geq 0$. Temos que $x^{2n+1}+1 = (x+1)(x^{2n} - x^{2n-1} + x^{2n-2} - ... - x + 1)$. Multiplicando a igualdade por x^2 obtemos $x^{2n+3} + x^2 = (x+1)(x^{2n+2} - x^{2n+1} + x^{2n} - ... - x^3 + x^2) \Rightarrow x^{2n+3} + 1 = (x+1)(x^{2n+2} - x^{2n+1} + x^{2n} - ... - x^3 + x^2) + 1 - x^2 = x^{2n+3} + 1 = (x+1)(x^{2n+2} - x^{2n+1} + x^{2n} - ... - x^3 + x^2) + (1+x)(1-x) \Rightarrow x^{2n+3} + 1 = (x+1)(x^{2n+2} - x^{2n+1} + x^{2n} - ... - x^3 + x^2 - x + 1)$

Definição 5.3. Um número $x \in \mathbb{Z}$ é dito um composto se o conjunto de seus divisores tem mais de 4 elementos, isto é,$x = yz$ com $y, z \notin \{1, x, -1, -x\}$

Definição 5.4. Um número $x \in \mathbb{Z}$ é dito ser primo, se o conjunto dos divisores positivos tem exatamente dois elementos 1 e $|x|$.

Observe que o conjunto dos divisores de um número inteiro é finito, pois $x|y \Rightarrow |x| \leq |y|$(exercício). Assim dados dois elementos $x, y \in \mathbb{Z}$, o conjunto dos divisores de x e y, isto é $\{z \in \mathbb{Z};\ z|x \text{ e} z|y\}$ tem finitos elementos e portanto considerando a ordem "$\leq$"tem um maior divisor comum. Isto nos motiva a seguinte definição:

Definição 5.5. Dados $x, y \in \mathbb{Z}$, não simultaneamente nulos, o maior divisor comum de x e y é o maior inteiro que divide x e y. Denotaremos este número por $mdc(x, y)$.

Teorema 5.1. *Dado um número $x \notin \{1, 0, -1\}$ tem-se que x é primo ou x é um produto finito de números primos.*

Demonstração. É suficiente mostrar que que todo inteiro positivo maior que 1 é primo ou um produto finito de números primos. $(-x = (-1).x)$.
Para demonstrar, usaremos o segundo princípio de indução. Considere $B = \{z \in \mathbb{Z}_+;\ z > 1 \text{ e} z \text{ ou é primo ou produto finito de números primos}\}$. Note que $2 \in B$. Suponha que a tese seja válida para todo $2 \leq y < x$. Se x é primo, $x \in B$. Suponha que x não seja primo. Assim existem $a, b \notin \{0, 1\}$ tais que $x = a.b$. Note que pela relação de ordem $2 \leq < x$ e $2 \leq b < x$. Por hipótese de indução, a, b são primos ou produto finito de números primos. Em qualquer caso, x é um produto finito de fatores primos. Portanto $x \in B$. O segundo princípio de indução garante que todo número inteiro positivo é produto finito de números primos. ■

Teorema 5.2. *Existem infinitos números primos.*

Demonstração. Suponha que a afirmação é falsa e considere $p_1 < p_2 < ... < p_n$ todos os números primos em ordem crescente. Seja $x = p_1 p_2 ... p_n + 1$. Como x é maior que $p_1 p_2 ... p_n$ e x é produto finito de números primos (Pelo teorema anterior). Assim deve existir $p \in \{p_1, p_2, ..., p_n\}$ e y inteiro tal que $x = py$. Assim $p|x$ e $p|p_1 p_2 ... p_n$. Logo $p|x - p_1 p_2 ... p_n \Rightarrow p|1$, o que é um absurdo, pois p é primo. Logo existem infinitos números primos. ■

RESUMO

Divisibilidade

Dados dois números $x, y \in \mathbb{Z}$, dizemos que x divide y se existe $z \in \mathbb{Z}$ tal que $y = x.z$. Neste caso dizemos que y é um múltiplo de x. (x é um divisor de y).

Valor absoluto

Para todo $a \in \mathbb{Z}$, o valor absoluto de a (ou módulo de a) representado por $|a|$ é definido como:

$$|a| = \begin{cases} a, & a \in \mathbb{Z}_+ \cup \{0\} \\ -a, & a \in \mathbb{Z}_- \cup \{0\} \end{cases}$$

Números primos e compostos

Um número $x \in \mathbb{Z}$ é dito um composto se o conjunto de seus divisores tem mais de 4 elementos, isto é,$x = yz$ com $y, z \notin \{1, x, -1, -x\}$

Um número $x \in \mathbb{Z}$ é dito ser primo, se o conjunto dos divisores positivos tem exatamente dois elementos 1 e $|x|$.

Dados $x, y \in \mathbb{Z}$, não simultaneamente nulos, o maior divisor comum de x e y é o maior inteiro que divide x e y.

Denotaremos este número por $mdc(x, y)$.

PRÓXIMA AULA

Na próxima aula, apresentaremos o algoritmo da divisão, sistemas de numeração posicionais (bases) além de elencar alguns critérios de divisibilidade e o importante Teorema Fundamental da Aritmética.

ATIVIDADES

ATIV. 5.1. Seja $a \in \mathbb{Z}_-$. Então $a^{2n} > 0, \forall n \in \mathbb{Z}_+$.

ATIV. 5.2. Sejam $x, y, z \in \mathbb{Z}$. Mostre que se $x|yz$, então $x|y$ ou $x|z$.

ATIV. 5.3. Analise cada uma das afirmações abaixo. Demonstre as verdadeiras e dê contra exemplo para as falsas.

a) Sejam $x, y, z \in \mathbb{Z}$. Se $x|z$ e $y|z$, então $xy|z$.

b) Sejam $x, y, z \in \mathbb{Z}$. Se $x|(y+z)$, então $x|y$ e $x|z$.

c) Sejam $x, y \in \mathbb{Z}$. Então $||x| - |y|| \leq |x - y|$.

ATIV. 5.4. Se $d|n$ então $ad|an$, para todo $a \in \mathbb{Z}$.

ATIV. 5.5. $|\sum_{i=1}^{n} a_i| \leq \sum_{i=1}^{n} |a_i|$ onde $\sum_{i=1}^{n} b_i = b_1 + b_2 + ... + b_n$ e $a_i \in \mathbb{Z}$.

LEITURA COMPLEMENTAR

LIMA, Elon L., Análise na Reta Vol. 1, IMPA, Projeto Euclides, 5.ed., Rio de Janeiro, 2008.

LIMA, Elon L., Matemática para o Ensino Médio 1.

DOMINGUES, H. Fundamentos de Aritmética.

GONÇALVES, Adilson, Introdução à álgebra, IMPA, Projeto Euclides, 5.ed., Rio de Janeiro, 2008.

HUNGERFORD, Thomas W., Abstract algebra: an introduction, Saunders College Publishing, 1990.

Bahiano, C. Notas de aula. UFBA