Aula 4. Divisibilidade e Algoritmo da divisão

4.1 Divisibilidade e suas propriedades

Uma equação da forma $bx = a$ pode ou não ter solução no conjunto dos números inteiros; isso dependerá dos coeficientes a e b da equação. Quando tal solução existe, diz-se que a é divisível por b. Mais precisamente:

Definição

Sejam a e b números inteiros. Diz-se que b *divide* a (ou que b é um *divisor* de a ou, ainda, que a é um *múltiplo* de b) se existe um inteiro c tal que $bc = a$.

Notação. Usaremos a notação $b \mid a$ para indicar que b divide a. A negação dessa afirmação será indicada por $b \nmid a$.

Observem que, se $b \neq 0$, o inteiro c nas condições da definição é único. De fato, se existisse outro c' tal que $bc' = a$, teríamos que

$$bc = bc'.$$

Assim, cancelando, vem que $c = c'$. Inteiro assim definido chama-se *quociente* de a por b e é indicado por $c = \frac{a}{b}$.

Por outro lado, note que $0 \mid a$ se e somente se $a = 0$. Nesse caso, o quociente não é único pois $0 \cdot c = 0$, para todo inteiro c.

Proposição 4.1

Se $b \mid a$ e $a \neq 0$, então $|b| \leq |a|$.

Prova

Se $b \mid a$ assim existe c inteiro tal que $bc = a$. Tomando os módulos em ambos os lados, tem-se que $|b||c| = |a|$.
Como $|c|$ é um inteiro positivo, temos que $1 \leq |c|$ e, multiplicando ambos os lados dessa desigualdade por $|b|$, temos que $|b| \leq |b||c| = |a|$.

Anotações MAT0123 (Draft). Prof. Kostiantyn

Corolário 4.1

(i) Os únicos divisores de 1 são 1 e -1.

(ii) Se $a \mid b$ e $b \mid a$, então $a = \pm b$.

Prova

(i) Se b é um divisor de 1, temos, pela proposição anterior, que $|b| \leq 1$. Além disso, da Aula 1, sabemos que não existem inteiros entre 0 e 1. Como $b \neq 0$, temos que $0 \leq b$. Logo, $|b| = 1$ e, portanto, $b = +1$ ou $b = -1$.

(ii) Se $a \mid b$ e $b \mid a$, existem inteiros c e d tais que $ac = b$ e $bd = a$. Substituindo na segunda igualdade o valor de b dado pela primeira, temos

$$acd = a.$$

Como $a \neq 0$, podemos cancelar a, assim $cd = 1$ Logo, d é um divisor de 1. Assim pela parte anterior, $d = \pm 1$. Consequentemente,

$$a = \pm b.$$

Proposição 4.2

Sejam os números inteiros a, b, c, d (lembrando que assumimos os divisores diferentes de zero, valem:

(i) $a \mid a$.

(ii) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

(iii) Se $a \mid b$ e $c \mid d$, então $ac \mid bd$.

(iv) Se $a \mid b$ e $a \mid c$, então $a \mid (b + c)$.

(v) Se $a \mid b$, então para todo inteiro m, tem-se que $a \mid mb$.

(vi) Se $a \mid b$ e $a \mid c$, então, para todos inteiros m, n, tem-se que $a \mid (mb + nc)$.

Prova

(i) Basta observar que podemos escrever $a \cdot 1 = a$.

(ii) Usando definição, existem inteiros d e d', tais que $ad = b$ e $bd' = c$. Substituindo o valor de b dado pela primeira igualdade, temos $c = (ad)d' = a\,(dd')$ logo $a \mid c$.

(iii) Novamente, por definição, existem inteiros f e f', tais que $af = b$ e $cf' = d$. Multiplicando ambas as igualdades, temos $ac(ff') = bd$, donde $ac \mid bd$.

(iv) Existem inteiros d e d', tais que $ad = b$ e $ad' = c$. Somando ambas as igualdades, temos $a\,(d + d') = b + c$, donde $a \mid (b + c)$.

(v) Se $a \mid b$, existe um inteiro c tal que $ac = b$. Multiplicando por m, temos $a(cm) = bm$ portanto, $a \mid bm$.

(vi) Segue diretamente de (v) e (iv).

4.2 *Algoritmo da divisão*

Theorem 4.1: (Algoritmo da divisão)

Sejam a e b dois inteiros, com $b > 0$. Então, existem únicos inteiros q e r, tais que

$$a = bq + r$$

e $0 \leq r \leq b$.

Prova

Consideremos o seguinte conjunto

$$S = \{a - bx \mid x \in Z, a - bx \geq 0\}.$$

Quando $x = -|a|$, temos que $a - bx = a + b|a| \geq 0$ pois $b > 0$. Logo S não-vazio. Pelo Princípio da Boa Ordem, existe $r = \min S$. Como $r \in S$, ele também é da forma $r = a - bq \geq 0$, para algum $q \in \mathbb{Z}$.
Para mostrar que as condições do enunciado estão verificadas, basta provar que $r < b$. De fato, se fosse $r \geq b$, teríamos que:

$$a - b(q+1) = a - bq - b = r - b \geq 0,$$

logo, $a - b(q+1)$ também pertenceria a S. Mas $a - b(q+1) = r - b < r = \min S$, uma contradição.
Agora, provaremos que, se (q, r) e (q', r') são dois pares de inteiros verificando as condições do enunciado, então $q = q'$ e $r = r'$. De fato, temos que

$$qb + r = a = q'b + r'.$$

Podemos supor, por exemplo, que $r' \neq r$. Da igualdade acima, temos $q - q'b = r' - r$, logo $b|r' - r$. Como $r' - r \neq 0$, assim pelo Proposição 4.1 temos que $b \leq |r' - r|$. Por outro lado $0 \leq r < b$ e $0 \leq r' < b$, assim

$$-b < r' - r < b,$$

Ou seja $|r' - r| < b$ (contradição com $b \leq |r' - r|$). Assim $r' = r$. Logo

$$a - bq = a - bq' \Rightarrow bq = bq' \Rightarrow q = q'.$$

Os números q e r determinados no Teorema anterior chamam-se, respectivamente, *quociente* e *resto* da divisão de a por b.

4.3 Aplicações e exemplos

Exemplo 4.1

Mostre que dados 3 inteiros consecutivos um deles é múltiplo de 3.
Seja a um inteiro. Usando algoritmo de divisão de a por 3, temos que a tem forma

$$a = 3q + r,$$

onde $0 \leq r < 3$, assim temos três possibilidades

$$a = 3q, a = 3q + 1, \quad \text{ou} \quad a = 3q + 2.$$

Agora se

$$\begin{aligned} r = 0, &\quad \text{assim} \quad a \quad \text{é multiplo de 3,} \\ r = 1, &\quad \text{assim} \quad a + 2 = 3q + 3 \quad \text{é multiplo de 3,} \\ r = 2, &\quad \text{assim} \quad a + 1 = 3q + 3 \quad \text{é multiplo de 3.} \end{aligned}$$

Assim para qualquer r temos que um dos a, $a + 1$ ou $a + 2$ é múltiplo de 3.

Exercício 4.1

Mostre que o quadrado de um inteiro é da forma $4k$ ou $4k + 1$.

Solução 4.1

Um quadrado tem forma $b = a^2$, para algum inteiro a. Usando algoritmo de divisão de a por 2, temos que a tem forma

$$a = 2q + r,$$

onde $0 \leq r < 2$, assim temos dois possibilidades

$$a = 2q, \quad \text{ou} \quad a = 2q + 1.$$

Agora se

$$\begin{aligned} r = 0, &\quad \text{assim} \quad b = a^2 = 4q^2, \quad b \text{ tem forma } 4k, \\ r = 1, &\quad \text{assim} \quad b = a^2 = 4q^2 + 4q + 1, \quad b \text{ tem forma } 4k + 1. \end{aligned}$$

Exercício 4.2

Mostre que o $3 \mid n^3 - n$ para todo inteiro n.

Solução 4.2

Temos

$$n^3 - n = n(n^2 - 1) = (n-1)n(n+1).$$

Assim $n^3 - n$ é o produto de 3 inteiros consecutivos. Um deles é múltiplo de 3 pelo Exemplo 4.1. Assim $n^3 - n$ é múltiplo de 3, ou seja $3 \mid n^3 - n$.

Exercício 4.3: (Trabalho p/ casa)

Mostre que o quadrado de cada número inteiro ímpar tem a forma de $8m + 1$.

Exercício 4.4: (Trabalho p/ casa)

Mostre que o quadrado de qualquer inteiro tem a forma $3m$ ou $3m + 1$, mas não a forma $3m + 2$.

Exercício 4.5: (Trabalho p/ casa)

Mostre que se $ac \mid bc$ e $c \neq 0$, então $a \mid b$.

Anotações MAT0120 (... Prof. Kostiantyn