DIVISIBILIDADE

Definição: Sejam $a, b \in \mathbb{Z}$. Dizemos que $b|a$ (b divide a ou a é múltiplo de b) se existir $c \in \mathbb{Z}$ tal que $a = bc$.

Observação: Se $a = 0$, então $b|a$, para todo $b \in \mathbb{Z}$, já que $0 = b.0$, para todo $b \in \mathbb{Z}$.

Se $b = 0$ e $0|a$ então $a = 0$. (Pois se existe $c \in \mathbb{Z}$ tal que $a = c.0$ então $a = 0$).

Se $b \neq 0$ e $b|a$ então c é único.

($a = bc$ LCM $\underset{b \neq 0}{\Rightarrow}$ Se $a = bc = bc'$ então $c = c'$)

(Podemos denotar c por $\frac{a}{b}$.)

Se $b|a$ então b é DIVISOR de a.

Vamos supor daqui em diante que $b \neq 0$ (os divisores são diferentes de zero.)

Proposição: Se $b|a$ e $a \neq 0$ então $|b| \leq |a|$.

Demonstração: Como $b|a$, existe $c \in \mathbb{Z}$ tal que $a = bc$. Então $|a| = |bc| = |b||c|$.

Como $a \neq 0$, $c \neq 0$, então $|c| \geq 1$. Logo, por OM

$$\underbrace{|b||c|}_{|a|} \geq |b| \quad \text{. Logo } |a| \geq |b|.$$

COROLÁRIO: (i) Se $b|1$ então $b = \pm 1$.

(ii) Se $a|b$ e $b|a$ então $|a| = |b|$.

Demonstração: (i) $b|1 \Rightarrow \exists\, c \in \mathbb{Z}$ tal que $bc = 1$. Logo $|b| \leq 1$. Como $b \neq 0$, temos que $|b| \geq 1$. Portanto $|b| = 1 \Rightarrow b = \pm 1$.

(ii) Se $a|b \Rightarrow |a| \leq |b|$ e se $b|a$, então $|b| \leq a$

Logo $|a| = |b| \Rightarrow a = \pm b$.

Proposição: Sejam $a, b, c, d \in \mathbb{Z}$. Então:

(i) $a \mid a$ (É claro pois $a = 1 \cdot a$.)

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

$a \mid b \Rightarrow \exists\, k$ tal que $b = ak$.
$b \mid c \Rightarrow \exists\, l$ tal que $c = bl$.

Então $c = bl = (ak)l = a(kl)$. Logo $a \mid c$.

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

$$\left.\begin{array}{l} a \mid b \Rightarrow b = ka \\ a \mid c \Rightarrow c = la \end{array}\right\} \; b + c = ka + la = (k+l)a.$$

(iv) Se $a \mid b$ então $a \mid mb$ para todo $m \in \mathbb{Z}$.

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

$$\left.\begin{array}{l} a \mid b \Rightarrow b = ka \\ c \mid d \Rightarrow d = lc \end{array}\right\} \Rightarrow bd = (ka)(lc) = (kl)(ac)$$

$$\Rightarrow ac \mid bd.$$

(vi) $a \mid b$ e $a \mid c \Rightarrow a \mid mb + nc$ para todos $m, n \in \mathbb{Z}$.

TEOREMA: (Algoritmo da Divisão) Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$. Então existem $q, r \in \mathbb{Z}$ únicos tais que $a = qb + r$, com $0 \leq r < |b|$.

$$\begin{array}{r|l} 37 & 7 \\ \hline 2 & 5 \end{array} \qquad \begin{array}{r|l} a & b \\ \hline r & q \end{array}$$

Demonstração:

1º caso: $a \geq 0$ e $b > 0$.

Consequência do PBO.

Seja $S = \{ a - xb,\ x \in \mathbb{Z} \text{ e } a - xb \geq 0 \}$.

$S \neq \emptyset$ pois $a - 0 \cdot b = a \geq 0$.

S é limitado inferiormente.

Logo existe $r = \text{mín } S$.

Só falta mostrar que $r < b$.

Se $r \geq b$ então

$$a = qb + r - b + b = (q+1)b + (r-b)$$

$0 \leq r - b = a - (q+1)b$

Como $b > 0 \Rightarrow -b < 0$ e $r - b < r$.

Logo $r - b \in S$ e $r - b < r = \min S$, absurdo.

Portanto $0 \leq r < b$.

2º caso:

Se $a < 0$, então $|a| > 0$

e $b > 0$

$|a| = q'b + r'$, com $0 \leq r' < b$

Se $r' = 0$, então $a = -|a| = \underbrace{(-q')}_{q} b$.

Suponha então $r' > 0$ e $r' < b$

$$a = -|a| = (-q')b - r' = (-q')b + b - b - r'$$

$$= \underbrace{(-q' - 1)}_{q} b + \underbrace{b - r'}_{r}$$

$b - r' > 0$ e $b - r' < b$ pois $r' > 0$.

3º caso a qualquer e $b < 0$.

Pelo 2º caso, podemos determinar q' e r' tais que

$a = q'|b| + r'$, onde $0 \leq r' < |b|$.

Mas então $a = q'(-b) + r' = \underbrace{(-q')}_{q} b + \underbrace{r'}_{r}$, $0 \leq r' < |b|$

UNICIDADE:

Suponha que $a, b \in \mathbb{Z}$, $b \neq 0$, e $a = qb + r = q_1 b + r_1$ com $0 \leq r, r_1 < |b|$. Mostrar que $q = q_1$ e $r = r_1$.

$a = qb + r = q_1 b + r_1 \Rightarrow (q - q_1) b + r - r_1 = 0$.

Logo $(q - q_1) b = r_1 - r$. Suponha que $r_1 \geq r$.

$0 \leq \underbrace{r_1 - r}_{} < |b|$, pois $0 \leq r_1 < |b|$

$0 \leq |r_1 - r| = |q - q_1||b| < |b|$.

Portanto $|q - q_1| < 1 \Rightarrow |q - q_1| = 0 \Rightarrow q = q_1$

$\Rightarrow r = r_1$. //

Exemplos

Se n é um inteiro, então $n = 2q$ ou $n = 2q+1$.

O quadrado de um inteiro é da forma $4k$ ou $4k+1$.

Se $n = 2q \Rightarrow n^2 = 4q^2$

$n = 2q+1 \Rightarrow n^2 = 4q^2 + 4q + 1 = 4\underbrace{(q^2+q)}_{k} + 1$.

n inteiro $\Rightarrow n = 3q$ ou $n = 3q+1$ ou $n = 3q+2$.

Logo $n^2 = 9q^2$ ou $n^2 = 9q^2 + 6q + 1 = 3\underbrace{(q^2+2q)}_{k} + 1$

ou $n^2 = 9q^2 + 12q + 4 = 3\underbrace{(3q^2+4q+1)}_{k} + 1$

O quadrado de um inteiro é da forma $3k$ ou $3k+1$.

10 (a) Mostrar que para todo $n \geq 1$

$$a^n - b^n = (a-b) \sum_{i=0}^{n-1} a^{n-1-i} b^i .$$

$n = 1$

$$a - b = (a-b) \cdot 1$$

Suponha que a fórmula é valida para $k \geq 1$ (Hipótese de Indução)

Mostrar que

$$a^{k+1} - b^{k+1} = (a-b) \sum_{j=0}^{k} a^{k-j} b^j .$$

$$a^{k+1} - b^{k+1} = a^{k+1} - a^k b + a^k b - b^{k+1}$$

$$= a^k (a-b) + b (a^k - b^k) \underset{\text{H I}}{=} a^k (a-b) + b (a-b) \sum_{i=0}^{k-1} a^{k-1-i} b^i$$

$$= (a-b) \left[a^k + \sum_{i=0}^{k-1} a^{k-(i+1)} b^{i+1} \right] = (a-b) \left[a^k + \sum_{j=1}^{k} a^{k-j} b^j \right]$$

Faça

$j = i+1$

$i = 0 \Rightarrow j = 1$

$i = k-1 \Rightarrow j = k$

(b) $a^{2n+1} + b^{2n+1}$

Aplique a fórmula de (a) para

$a^{2n+1} + b^{2n+1} = a^{2n+1} - (-b)^{2n+1}$.

Tudo o que tem que saber é:

$$\square^n - \Delta^n = (\square - \Delta)(\square^{n-1} + \square^{n-2}\Delta + \cdots + \square\Delta^{n-2} + \Delta^{n-1})$$

(15) $2^{333} + 3^{222} = (2^3)^{111} + (3^2)^{111} = (2^3)^{111} - (-3^2)^{111}$

$$= (2^3 + 3^2) \sum_{i=0}^{110} (2^3)^{110-i} \cdot (-3^2)^i$$

$2^3 + 3^2 = 17$

Qual é o resto da divisão de 4^{5000} por 3?

$$4^{5000} = (3+1)^{5000} = \sum_{i=0}^{5000} \binom{5000}{i} 3^{5000-i}$$

$$4^{5000} - 1^{5000} = (4-1) \sum_{i=0}^{4999} 4^{4999-i} \Rightarrow 4^{5000} = 3q + 1$$

$(4-1) = 3$

Como $0 \leq 1 < 4$ pela unicidade