

1.3 Divisibilidade

Teorema 1.3.1 (Algoritmo da Divisão)

Sejam $n, m \in \mathbb{Z}$ tais que $m \neq 0$. Então, existem dois únicos inteiros q e r tais que

$$n = mq + r,$$

com $0 \leq r < |m|$.

Resto
Quociente

Exemplo:

- $n = 172, \quad m = 20$

Então, $172 = 20 \times 8 + 12$

r
 q

- $n = 172, \quad m = -20$

$$172 = 20 \times 8 + 12 \Rightarrow 172 = -20 \times (-8) + 12$$

r
 q

Dividendo

$$\begin{array}{r} 172 \\ -160 \\ \hline 12 \end{array}$$

Divisor

$$\begin{array}{r} 20 \\ \hline 8 \end{array}$$

Quociente

Resto

$$172 = 20 \times 8 + 12$$

1.3 Divisibilidade

Teorema 1.3.1 (Algoritmo da Divisão)

Sejam $n, m \in \mathbb{Z}$ tais que $m \neq 0$. Então, existem dois únicos inteiros q e r tais que

$$n = mq + r,$$

Quociente

Resto

com $0 \leq r < |m|$.

Exemplo:

● $n = 172, \quad m = 20$

Então, $172 = 20 \times 8 + 12$

$\swarrow$ r
 $\nwarrow$ q

● $n = 172, \quad m = -20$

$$172 = 20 \times 8 + 12 \Rightarrow 172 = -20 \times (-8) + 12$$

$\swarrow$ r
 $\nwarrow$ q

● $n = -172, \quad m = 20$

$$172 = 20 \times 8 + 12 \Rightarrow -172 = -20 \times 8 - 12$$

$\Downarrow$

$$-172 = 20 \times (-8) - 12$$

$\Downarrow$

$$-172 = 20 \times (-8) - 12 + 20 - 20$$

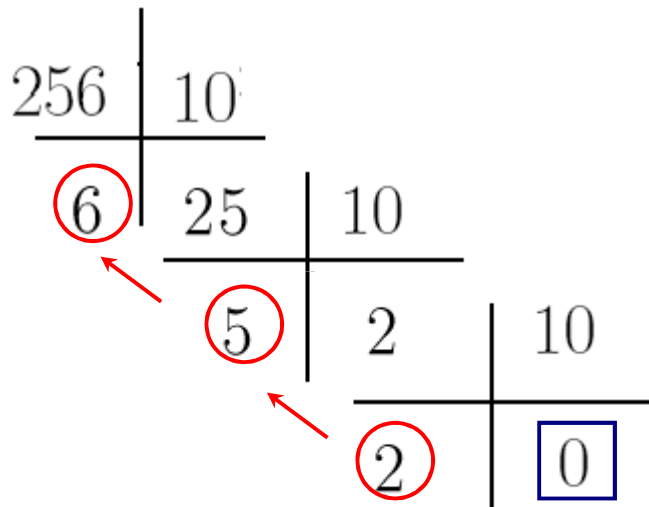
$\Downarrow$

$$-172 = 20 \times (-9) + 8$$

$\swarrow$ r
 $\nwarrow$ q

Sistema Decimal:

$$x = 256 = \underset{\uparrow}{2} \times 10^2 + \underset{\uparrow}{5} \times 10^1 + \underset{\uparrow}{6} \times 10^0$$



$$256 = \textcircled{2} \textcircled{5} \textcircled{6}$$

Sistema Binário:

$$x = 245 = r_k 2^k + r_{k-1} 2^{k-1} + r_{k-2} 2^{k-2} + \dots + r_1 2^1 + r_0 2^0$$

↑ ? ↑ ? ↑ ? ↑ ? ↑ ?

245	2
1	122
0	61
1	30
0	15
1	7
1	3
1	1
1	0

r_0 r_1 r_2 r_3 r_4 r_5 r_6 r_7

$$x = 245 = \underline{(11110101)}_2$$

Geralmente:

O algoritmo da divisão justifica a representação usual dos inteiros.

Seja $t \geq 2$ um inteiro. Sendo x um inteiro positivo,

$$x = tq_0 + r_0, \text{ com } 0 \leq r_0 < t \quad (\text{Algoritmo da Divisão})$$

$$q_0 = tq_1 + r_1, \text{ com } 0 \leq r_1 < t \quad (\text{Algoritmo da Divisão})$$

$$\vdots \quad (\text{Algoritmo da Divisão})$$

$$q_{k-2} = tq_{k-1} + r_{k-1}, \text{ com } 0 \leq r_{k-1} < t \quad (\text{Algoritmo da Divisão})$$

$$q_{k-1} = tq_k + r_k, \text{ com } 0 \leq r_k < t. \quad (\text{Algoritmo da Divisão})$$

$\parallel$
0

(Tem-se que $0 \leq r_{k-2} < \dots < r_2 < r_1 < r_0 < x$)

O processo termina quando $q_k = 0$.

$$q_{k-1} = r_k$$

Eliminando os quocientes q_i , obtemos

$$x = tq_0 + r_0, \text{ com } 0 \leq r_0 < t \quad (\text{Algoritmo da Divisão})$$

$$q_0 = tq_1 + r_1, \text{ com } 0 \leq r_1 < t \quad (\text{Algoritmo da Divisão})$$

$\vdots$

$$q_{k-2} = tq_{k-1} + r_{k-1}, \text{ com } 0 \leq r_{k-1} < t \quad (\text{Algoritmo da Divisão})$$

$$q_{k-1} = tq_k + r_k, \text{ com } 0 \leq r_k < t. \quad (\text{Algoritmo da Divisão})$$

O processo termina quando $q_k = 0$.

Eliminando os quocientes q_i , obtemos $q_{k-1} = r_k$

$$q_{k-2} = r_k t + r_{k-1}$$

$$q_{k-3} = r_k t^2 + r_{k-1} t + r_{k-2}$$

$\vdots$

$$q_0 = r_k t^{k-1} + r_{k-1} t^{k-2} + \dots + r_1$$

$$x = (r_k r_{k-1} \dots r_1 r_0)_t$$

Representação base t

$$x = r_k t^k + r_{k-1} t^{k-1} + \dots + r_1 t + r_0.$$

Relação de Divisibilidade

$X = \mathbb{Z}$. Considere a relação $|$ definida por: $a, b \in \mathbb{Z}$

$$a|b \text{ (a divide b)} \iff (\exists k \in \mathbb{Z}) b = ak$$

b é múltiplo de a
(a é divisor de b)

Observação:

- $(\mathbb{N}, |)$ é um c.p.o..
- $(\mathbb{Z}, |)$ não é c.p.o.. A relação não é anti-simétrica em $\mathbb{Z}$

Máximo divisor comum

Dados dois números inteiros não nulos a e b , denotamos por

$$\text{mdc}\{a, b\}$$

o seu máximo divisor comum.

Definição 1.3.2

Dados dois números inteiros não nulos a e b , chama-se máximo divisor comum de a e b

ao número natural d (caso exista), tal que:

- ① $d|a$ e $d|b$;
- ② Se $c \in \mathbb{Z}$ é tal que $c|a$ e $c|b$ então $c|d$.

Exemplos:

● $\text{mdc}\{6, 9\} = 3$ pois: ① $3|6$ e $3|9$

② Se $c|6$ e $c|9$ então

$$\begin{array}{cc} \Downarrow & \Downarrow \end{array}$$

$$6 = ck_1 \quad 9 = ck_2 \quad k_1, k_2 \in \mathbb{Z}$$

Logo,

$$3 = 9 - 6 = ck_2 - ck_1 = c \underbrace{(k_2 - k_1)}_{k_3}$$

ou seja, $c|3$

- $\text{mdc}\{6, -9\} = \text{mdc}\{6, 9\} = 3$
- $\text{mdc}\{51975, 31752\} = ?$

51975	3 ←	31752	2
17325	3 ←	15876	2
5775	5	7938	2
1155	3 ←	3969	3 ←
385	5	1323	3 ←
77	11	441	3 ←
7	7 ←	147	3
1		49	7 ←
		7	7
		1	

Decompor em factores Primos

Decompor em factores Primos

$$\begin{aligned} \text{mdc}\{51975, 31752\} &= \\ &= 3 \times 3 \times 3 \times 7 = 189 \end{aligned}$$

Muitos cálculos

Algoritmo de Euclides

(300 a.c.)

Teorema 1.3.3: (Existência e unicidade do mdc)

Dados dois números inteiros não nulos a e b , existe um único número natural d (designado por máximo divisor comum de a e b) tal que:

- 1 $d|a$ e $d|b$;
- 2 Se $c \in \mathbb{Z}$ é tal que $c|a$ e $c|b$ então $c|d$.

Demonstração. [Algoritmo de Euclides] Determinamos sucessivamente os inteiros q_i e r_i , $1 \leq i \leq k+1$ (com $k \geq 2$), tais que

$$a = bq_1 + r_1, \quad 0 < r_1 < |b|, \quad \leftarrow \text{(Algoritmo da Divisão)}$$

$$b = r_1q_2 + r_2, \quad 0 < r_2 < r_1, \quad \leftarrow \text{(Algoritmo da Divisão)}$$

$$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2, \quad \leftarrow \text{(Algoritmo da Divisão)}$$

$$r_2 = r_3q_4 + r_4, \quad 0 < r_4 < r_3, \quad \leftarrow \text{(Algoritmo da Divisão)}$$

$\vdots$

$$\begin{array}{ll}
 a = bq_1 + r_1, & 0 < r_1 < |b|, \quad \text{(Algoritmo da Divisão)} \\
 b = r_1q_2 + r_2, & 0 < r_2 < r_1, \quad \text{(Algoritmo da Divisão)} \\
 r_1 = r_2q_3 + r_3, & 0 < r_3 < r_2, \quad \text{(Algoritmo da Divisão)} \\
 r_2 = r_3q_4 + r_4, & 0 < r_4 < r_3, \quad \text{(Algoritmo da Divisão)} \\
 \vdots & \\
 r_{k-2} = r_{k-1}q_k + r_k, & 0 < r_k < r_{k-1}, \quad \text{(Algoritmo da Divisão)} \\
 r_{k-1} = r_kq_{k+1}, & r_{k+1} = 0. \quad \text{(Algoritmo da Divisão)}
 \end{array}$$

$\text{mdc}\{a, b\}$

Nestas condições, $d = r_k$ verifica as condições (1) e (2) do teorema e é único.

- ① $d|a$ e $d|b$;
- ② Se $c \in \mathbb{Z}$ é tal que $c|a$ e $c|b$ então $c|d$.

Exemplo: Utilizar o algoritmo de Euclides para calcular $\text{mdc}\{51975, 31752\}$

(Algoritmo da Divisão)

$$51975 = 31752 \cdot 1 + 20223$$

(Algoritmo da Divisão)

$$31752 = 20223 \cdot 1 + 11529$$

(Algoritmo da Divisão)

$$20223 = 11529 \cdot 1 + 8694$$

(Algoritmo da Divisão)

$$11529 = 8694 \cdot 1 + 2835$$

(Algoritmo da Divisão)

$$8694 = 2835 \cdot 3 + 189$$

(Algoritmo da Divisão)

$$2835 = 189 \cdot 15 + 0.$$

Assim, $\text{mdc}\{51975, 31752\} = 189.$

$$189 = \text{mdc}\{51975, 31752\}$$

Igualdade de Bezout

$$51975 = 31752 \cdot 1 + 20223 \quad \leftarrow$$

$$31752 = 20223 \cdot 1 + 11529 \quad \leftarrow$$

$$20223 = 11529 \cdot 1 + 8694 \quad \leftarrow$$

$$11529 = 8694 \cdot 1 + 2835 \quad \leftarrow$$

$$8694 = 2835 \cdot 3 + \boxed{189} \quad \leftarrow$$

$$2835 = 189 \cdot 15 + 0$$

$$189 = 8694 - 2835 \cdot 3$$

$$= 8694 - (11529 - 8694) \cdot 3$$

$$= 8694 \cdot 4 - 11529 \cdot 3$$

$$= (20223 - 11529) \cdot 4 - 11529 \cdot 3$$

$$= 20223 \cdot 4 - 11529 \cdot 7$$

$$= 20223 \cdot 4 - (31752 - 20223) \cdot 7$$

$$= 20223 \cdot 11 - 31752 \cdot 7$$

$$= (51975 - 31752) \cdot 11 - 31752 \cdot 7$$

$$= 51975 \cdot 11 - 31752 \cdot 18$$

**Coeficientes da
igualdade de Bezout**

Assim $\underbrace{189}_{\text{mdc}\{a,b\}} = \underbrace{51975}_a \cdot \mathbf{11} + \underbrace{31752}_b \cdot (-\mathbf{18}).$

$$\text{mdc}\{a,b\} = am + bn$$

Teorema 1.3.4: (Igualdade de Bezout)

Dados dois números inteiros não nulos a e b , existem números inteiros m e n (designados por coeficientes da **Igualdade de Bezout**) tais que

$$\text{mdc}\{a, b\} = am + bn.$$

Demonstração. Seja $d = \text{mdc}\{a, b\}$. Pelo Algoritmo de Euclides, temos

$$\begin{aligned} a &= bq_1 + r_1, \quad 0 < r_1 < |b| \\ b &= r_1q_2 + r_2, \quad 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2 \end{aligned} \tag{1}$$

...

$$r_{k-2} = r_{k-1}q_k + d, \quad 0 < d = r_k < r_{k-1},$$

para certo $k \in \mathbb{N}$. Então, $d = r_{k-2} - r_{k-1}q_k$ (*) e, mais geralmente, para $i \in \{1, \dots, k\}$, $r_i = r_{i-2} - r_{i-1}q_i$ (**) (tomando $r_0 = b$ e $r_{-1} = a$). Assim, partindo de (*) e substituindo sucessivamente cada r_i usando (**), obtemos d como *combinação linear* de a e de b . □

Observação

Os coeficientes da Igualdade de Bezout, para dois números inteiros não nulos dados, não são únicos. Por exemplo, $1 = \text{mdc}\{2, 3\}$ e temos

$$1 = 2 \cdot (-1) + 3 \cdot 1 = 2 \cdot 2 + 3 \cdot (-1) = 2 \cdot (-4) + 3 \cdot 3 = \dots .$$

.