1.3. Divisibilidade

Teorema (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* $0 \leq r < |m|$.

Exemplo

Sejam $n = 234$ e $m = 5$. Então $234 = 5 \times 46 + 4$ (donde $q = 46$ e $r = 4$).
Para $n = 234$ e $m = -5$, temos $234 = (-5) \times (-46) + 4$ (i.e. $q = -46$ e $r = 4$).
Se $n = -234$ e $m = 5$, então $-234 = 5 \times (-47) + 1$ (observe que

$234 = 5\times46+4 \Rightarrow -234 = -5\times46-4 = 5\times(-46)-5+5-4 = 5\times(-47)+1$),

donde $q = -47$ e $r = 1$.
Para $n = -234$ e $m = -5$, temos $-234 = (-5) \times 47 + 1$ (i.e. $q = 47$ e $r = 1$).

Definição

Nas condições do teorema anterior, os inteiros q e r designam-se respectivamente por *cociente* e *resto* da divisão inteira de n por m.

O algoritmo da divisão justifica a representação usual dos inteiros:
Seja $t \geq 2$ um inteiro. Sendo x um inteiro positivo, pelo algoritmo da divisão, temos:

$$\begin{aligned} x &= tq_0 + r_0, \text{ com } 0 \leq r_0 < t, \\ q_0 &= tq_1 + r_1, \text{ com } 0 \leq r_1 < t, \\ &\vdots \\ q_{i-2} &= tq_{i-1} + r_{i-1}, \text{ com } 0 \leq r_{i-1} < t \\ q_{i-1} &= tq_i + r_i, \text{ com } 0 \leq r_i < t, \\ &\vdots \end{aligned}$$

O processo termina quando encontramos $k \in \mathbb{N}$ tal que $q_k = 0$ (notemos que $q_0 > q_1 > \cdots > q_i > \cdots \geq 0$). Eliminando (por substituição) os sucessivos quocientes q_i, obtemos

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

Desta forma, x está representado (com respeito à base t) pela sequência dos restos e escreve-se

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

Exemplo

Vamos escrever 245 na base 2. Dividindo (os cocientes obtidos) sucessivamente por 2, obtemos

$$\begin{array}{rcrcr} 245 & = & 2 \times 122 & + & 1 \\ 122 & = & 2 \times 61 & + & 0 \\ 61 & = & 2 \times 30 & + & 1 \\ 30 & = & 2 \times 15 & + & 0 \\ 15 & = & 2 \times 7 & + & 1 \\ 7 & = & 2 \times 3 & + & 1 \\ 3 & = & 2 \times 1 & + & 1 \\ 1 & = & 2 \times 0 & + & 1\,, \end{array}$$

Então $(245)_{10} = (11110101)_2$.

Sejam $a, b \in \mathbb{Z}$. Escrevemos $a|b$ para denotar que a *divide* b (ou que a é um *divisor* de b ou ainda que b é um *múltiplo* de a), i.e. quando existe $c \in \mathbb{Z}$ tal que $ac = b$.

Observemos que a relação $|$ não é uma relação de ordem parcial sobre $\mathbb{Z}$ (porquê?), ao contrário, como vimos atrás, da sua restrição a $\mathbb{N}$.

Teorema

Dados dois números inteiros não nulos a e b, existe um único número natural d (designado por máximo divisor comum de a e b e denotado por $\text{mdc}\{a, b\}$) 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] Para $a > b > 0$ tais que $b \nmid a$ (se $b|a$ então $b = \text{mdc}\{a, b\}$), determinamos sucessivamente os inteiros q_i e r_i, $1 \leq i \leq k+1$, com $k \geq 1$ (e tomando $r_{-1} = a$ e $r_0 = b$, se necessário), tais que

$$\begin{array}{ll} a = bq_1 + r_1\,, & 0 < r_1 < b\,, \\ b = r_1 q_2 + r_2\,, & 0 < r_2 < r_1\,, \\ r_1 = r_2 q_3 + r_3\,, & 0 < r_3 < r_2\,, \\ r_2 = r_3 q_4 + r_4\,, & 0 < r_4 < r_3\,, \\ \quad\vdots & \\ r_{k-2} = r_{k-1} q_k + r_k\,, & 0 < r_k < r_{k-1}\,, \\ r_{k-1} = r_k q_{k+1}\,, & r_{k+1} = 0\,. \end{array}$$

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

Exemplo

Vamos calcular $\text{mdc}\{51975, 31752\}$, usando o Algoritmo de Euclides:

$$\begin{aligned} 51975 &= 31752 \cdot 1 + 20223 \\ 31752 &= 20223 \cdot 1 + 11529 \\ 20223 &= 11529 \cdot 1 + 8694 \\ 11529 &= 8694 \cdot 1 + 2835 \\ 8694 &= 2835 \cdot 3 + 189 \\ 2835 &= 189 \cdot 15 + 0. \end{aligned}$$

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

Teorema (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. Nas condições da demonstração anterior, sejam $d = \text{mdc}\{a, b\}$ e (pelo Algoritmo de Euclides)

$$\begin{aligned} a &= bq_1 + r_1\ ,\ \ 0 < r_1 < b \\ b &= r_1 q_2 + r_2\ ,\ \ 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3\ ,\ \ 0 < r_3 < r_2 \end{aligned} \tag{1}$$

$$\begin{aligned} r_2 &= r_3 q_4 + r_4\ ,\ \ 0 < r_4 < r_3 \\ &\cdots \\ r_{k-2} &= r_{k-1} q_k + d\ ,\ \ 0 < d = r_k < r_{k-1}, \end{aligned}$$

para certo $k \in \mathbb{N}$. Então, $d = r_{k-2} - r_{k-1} q_k$ $(*)$ e, mais geralmente, para $i \in \{1, \ldots, k\}$, $r_i = r_{i-2} - r_{i-1} q_i$ $(**)$ (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. □

Exemplo

Vamos calcular coeficientes da Igualdade de Bezout para os inteiros do exemplo anterior ($189 = \text{mdc}\{51975, 31752\}$):

$$\begin{aligned} 51975 &= 31752 \cdot 1 + 20223 \\ 31752 &= 20223 \cdot 1 + 11529 \\ 20223 &= 11529 \cdot 1 + 8694 \\ 11529 &= 8694 \cdot 1 + 2835 \\ 8694 &= 2835 \cdot 3 + 189 \\ 2835 &= 189 \cdot 15 + 0 \end{aligned} \quad \Rightarrow \quad \begin{aligned} 189 &= 8694 - 2835 \cdot 3 \\ &= 8694 - (11529 - 8694) \cdot 3 \\ &= 8694 \cdot 4 - 11529 \cdot 3 \\ &= (20223 - 11529) \cdot 4 - 11529 \cdot 3 \\ &= 20223 \cdot 4 - 11529 \cdot 7 \\ &= 20223 \cdot 4 - (31752 - 20223) \cdot 7 \\ &= 20223 \cdot 11 - 31752 \cdot 7 \\ &= (51975 - 31752) \cdot 11 - 31752 \cdot 7 \\ &= 51975 \cdot 11 - 31752 \cdot 18\ . \end{aligned}$$

Assim $189 = 51975 \cdot \mathbf{11} + 31752 \cdot (\mathbf{-18})$.

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

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

Teorema

Dados dois números inteiros não nulos a e b, existe um único número natural m (designado por mínimo múltiplo comum *de a e b e denotado por $\text{mmc}\{a, b\}$) tal que:*

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

Teorema

Dados dois inteiros não nulos a e b, então $\text{mmc}\{a,\ b\} = \frac{|ab|}{\text{mdc}\{a,\ b\}}$.

Exemplo

Vamos calcular $\text{mmc}\{32060,\ 31652\}$. Como

$$\begin{aligned} 32060 &= 31652 \times 1 + 408 \\ 31652 &= 408 \times 77 + 236 \\ 408 &= 236 \times 1 + 172 \\ 236 &= 172 \times 1 + 64 \\ 172 &= 64 \times 2 + 44 \\ 64 &= 44 \times 1 + 20 \\ 44 &= 20 \times 2 + 4 \\ 20 &= 4 \times 5 + 0\ , \end{aligned}$$

então $\text{mdc}\{32060,\ 31652\} = 4$, donde

$$\text{mmc}\{32060,\ 31652\} = \frac{32060 \times 31652}{4} = 253690780.$$

Definições

Um número inteiro p diz-se *primo* de $p > 1$ e p apenas possui como divisores positivos 1 e p. Dois números inteiros não nulos a e b dizem-se *primos entre si* se $\text{mdc}\{a, b\} = 1$.

Lema

Sejam a e b dois números inteiros não nulos e primos entre si. Seja $c \in \mathbb{Z}$ tal que $a|bc$. Então $a|c$.

Demonstração. Atendendo à Igualdade de Bezout, existem inteiros m e n tais que

$$1 = am + bn.$$

Donde $c = amc + bnc$. Como $a|bc$, então em particular $a|bnc$. Além disso, claramente, $a|amc$. Logo $a|(amc + bnc)$, ou seja, $a|c$. □

Lema

Seja p um número primo e sejam $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ (com $n \in \mathbb{N}^+$) tais que $p|a_1 a_2 \cdots a_n$. Então $p|a_i$, para algum $i \in \{1, \ldots, n\}$.

Demonstração. Por indução em n. Para $n = 1$ é imediato. Admitamos então o resultado válido para $n-1$, para certo $n > 1$. Sejam $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ tais que $p|a_1 a_2 \cdots a_n$. Ora, se $p|a_1 a_2 \cdots a_{n-1}$, por hipótese de indução, $p|a_i$, para algum $i \in \{1, \ldots, n-1\}$. Se, pelo contrário $p \not| a_1 a_2 \cdots a_{n-1}$, então

$$\text{mdc}\{p, a_1 a_2 \cdots a_{n-1}\} = 1,$$

visto que p é um número primo. Neste caso, pelo lema anterior, deduzimos que $p|a_n$. □

Teorema (Teorema Fundamental da Aritmética)

Todo o número inteiro maior do que um pode ser escrito como um produto de números primos (com um só factor, no caso do número ser primo). Além disso, uma tal decomposição em números primos é essencialmente única, i.e. duas decomposições apenas diferem na ordem pela qual os primos são escritos.

Observação/Definição

Por reordenação dos factores de uma decomposição em números primos, um inteiro $n > 1$ pode ser escrito na forma

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}, \text{ com } p_1 < p_2 < \cdots < p_k,$$

em que $p_1, p_2, \ldots, p_k$ são números primos e $k, r_1, r_2, \ldots, r_k \in \mathbb{N}^+$ (unicamente determinados por n). Uma decomposição deste tipo é designada por *forma standard* de n.

Por exemplo, a forma standard de 300 é $2^2 \cdot 3 \cdot 5^2$:

300	2
150	2
75	3
25	5
5	5
1	

Teorema

Sejam

$$m = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} \quad e \quad n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$$

($k \in \mathbb{N}$), em que $p_1 < p_2 < \cdots < p_k$ são números primos e s_i e t_i são números inteiros não negativos, para $i = 1, 2, \ldots, k$. Sejam

$$u_i = min\{s_i, t_i\} \quad e \quad v_i = max\{s_i, t_i\},$$

para qualquer $i = 1, 2, \ldots, k$. Então:

1. $mdc\{m, n\} = p_1^{u_1} p_2^{u_2} \cdots p_k^{u_k}$;
2. $mmc\{m, n\} = p_1^{v_1} p_2^{v_2} \cdots p_k^{v_k}$.

Outras aplicações do Teorema Fundamental da Aritmética:

1. *Se m e n forem dois naturais maiores ou iguais a 2, então $m^2 \neq 2n^2$.*

   Prova. Suponhamos que $m = 2^s a$ e $n = 2^t b$, em que $s, t \in \mathbb{N}_0$ e $a, b \in \mathbb{N}$ não são divisíveis por 2. Então a^2 e b^2 também não são divisíveis por 2 e temos $m^2 = 2^{2s} a^2$ e $2n^2 = 2^{2t+1} b^2$. Como $2s$ é um número par e $2t+1$ um número ímpar, não podemos ter $m^2 = 2n^2$.

2. *Se $n \geq 2$ não é um número primo, então existe um número primo p tal que $p|n$ e $p^2 \leq n$.*

   Prova. Como $n \geq 2$ e n não é primo, então $n = pqa$, com p e q primos tais que $p \leq q$ e $a \in \mathbb{N}$. Donde $p^2 \leq pq \leq n$.

Exemplo

O número 79 é primo: de facto, se 79 não fosse primo, pela propriedade 2 anterior, teria de existir um número primo p divisor de 79 tal que $p^2 \leq 79$. Como $11^2 = 121 > 79$, então $p \in \{2, 3, 5, 7\}$. Mas nenhum destes quatro primos é divisor de 79.