Teoria de Números

Algoritmo da divisão

Teorema Dados $a, b \in \mathbb{Z}$ com $b > 0$ existe um e um só $q \in \mathbb{Z}$ e um e um só $r \in \mathbb{Z}$ tais que

$$a = bq + r \quad , \quad \text{com} \quad 0 \leq r < b$$

Demonstração (ver sebenta)

A demonstração não é construtiva e baseia-se no princípio ordenação.

Terminologia: Nas condições do teorema anterior:

a diz-se o dividendo, b o divisor, q o quociente e r o resto

Corolário Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$. Então existem q e r, univocamente determinados tais que $a = bq + r$ com $0 \leq r < |b|$

Demonstração: Se $b > 0$ usa-se o teorema anterior.

Se $b < 0$ então existem q' e r' tais que $a = (-b)q' + r'$

como $0 \leq r' < -b$ $(-b > 0)$, pelo teorema anterior. Então

$a = (-q')b + r'$ e toma-se $q = -q'$ e $r' = r$.

$\square$

Exemplos

- $a = 7$ e $b = 6$ então $7 = 1 \times 6 + 1$ $q = 1$ e $r = 1$
  $0 \leq r < 6$
- $a = 1$ e $b = 6$ então $1 = 0 \times 6 + 1$ $q = 0$ e $r = 1$
- $a = -2$ e $b = -7$ então $-2 = -7 + 5$ $q = 1$ e $r = 5$
  $0 \leq r < |-7|$
- $a = 61$ e $b = -7$ então $61 = 8 \times 7 + 5$
  $= (-8) \times (-7) + 5$ $q = -8$
  $r = 5$

Aplicações do Teorema do Algoritmo da divisão

- O resto da divisão do quadrado de um número inteiro por 4 ou é 0 ou é 1.

Seja n um quadrado. Então $n = a^2$ para algum $a \in \mathbb{Z}$.

Então $a = 2q + r$ onde $r \in \{0, 1\}$

- se $r = 0$, temos $a^2 = 4q^2$ logo o resto da divisão de a^2 por 4 é 0

- se $r = 1$, temos $a^2 = (2q+1)^2 = 4q^2 + 4q + 1 = 4(\underbrace{q^2+q}_{q'}) + 1$

logo o resto da divisão de a^2 por 4 é 1.

- Para qualquer $a \in \mathbb{Z}$ então $a(a^2+2)$ é divisível por 3

Temos que $a = 3q + r$ com $r \in \{0, 1, 2\}$

- se $r = 0$ então $a = 3q$ e

$$a(a^2+2) = 3q(9q^2+2) = 3[q(9q^2+2)] \checkmark$$

- se $r = 1$ então $a = 3q+1$ e

$$a(a^2+2) = (3q+1)((3q+1)^2+2) = (3q+1)(9q^2+6q+1+2)$$

$$= 3[(3q+1)(3q^2+2q+1)] \checkmark$$

- se $r = 2$ então $a = 3q+2$

$$a(a^2+2) = (3q+2)((3q+2)^2+2) = (3q+2)(9q^2+12q+4+2)$$

$$= 3[(3q+2)(3q^2+4q+2)] \checkmark$$

Em qualquer caso $a(a^2+2)$ é divisível por 3.

$\square$

Máximo divisor comum

Definição: Sejam $a, b \in \mathbb{Z}$. Diz-se que a divide b e escreve-se $a \mid b$ se existe $c \in \mathbb{Z}$ tal que $b = ac$.

Escreveremos $a \nmid b$ se a não divide b.

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

(1) $a \mid 0$, $1 \mid a$, $a \mid a$

(2) $a \mid 1 \iff a = \pm 1$ e $0 \mid a \iff a = 0$

(3) $a \mid b$ e $c \mid d \implies ac \mid bd$

(4) $a \mid b$ e $b \mid c \implies a \mid c$

(5) $a \mid b$ e $b \mid a \implies b = \pm a$

(6) $a \mid b \ (b \neq 0) \implies |a| \leq |b|$

(7) $a \mid b$ e $a \mid c$ $\Rightarrow$ $a \mid (bx + cy)$, para todos os $x, y \in \mathbb{Z}$.

<u>Demonstração:</u> (1), (2) exercício, (6) e (7) sebenta

(3) Sejam $a, b, c, d \in \mathbb{Z}$ tais que $a \mid b$ e $c \mid d$. Queremos mostrar que $ac \mid bd$.

Sabemos que $b = xa$ e $d = yc$. Logo $bd = (xa)(yc)$ $= (xy)(ac)$. Portanto $ac \mid bd$.

(4) Sejam $a, b, c \in \mathbb{Z}$ tais que $a \mid b$ e $b \mid c$. Queremos mostrar que $a \mid c$.

Sabemos que $b = xa$ e $c = yb$, para alguns $x, y \in \mathbb{Z}$.

Então $c = yb = y(xa) = (yx)a$. Logo $a \mid c$.

(5) Sejam $a, b \in \mathbb{Z}$ tais que $a | b$ e $b | a$. Queremos ver que $b = \pm a$.

Se $a = 0$ então de $0 | b$, por (2), temos $b = 0$. Logo $b = \pm a$

Se $a \neq 0$. Temos $a | b \Rightarrow b = xa$
$b | a \Rightarrow a = yb$

Logo $a = yb = yxa$. Assim $a = yxa$. Logo $xy = 1$

Como $xy \in \mathbb{Z}$ então ou ($x = 1$ e $y = 1$) ou $x = -1$ e $y = -1$. No primeiro caso, $b = a$ e no segundo caso $b = -a$.

$\square$.

Sejam $a, b \in \mathbb{Z}$. Como $1 | a$ e $1 | b$, temos que:

$$D = \{ d \in \mathbb{N} : d | a \text{ e } d | b \} \neq \emptyset$$

Se $a = 0 = b$ então $D = \mathbb{N}$

Se $a \neq 0$ ou $b \neq 0$ então se $d \in \mathbb{N}$ e $d | a$ e $d | b$ temos $d \leq |a|$ e $d \leq |b|$, pelo que D tem um máximo

Definição Sejam $a, b \in \mathbb{Z}$, $a \neq 0$ ou $b \neq 0$. Chama-se máximo divisor comum de a e b e representa-se por $m.d.c\,(a, b)$ ao inteiro positivo d tal que:

i) $d | a$ e $d | b$

ii) $\forall c \in \mathbb{N}$, $c | a$ e $c | b \Rightarrow c \leq d$

Teorema: Para quaisquer $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$, existem $x, y \in \mathbb{Z}$ tais que $m.d.c(a,b) = ax + by$

Demonstração: (ver sebenta)

Corolário Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$, então o conjunto $T = \{ax + by \mid x, y \in \mathbb{Z}\}$ é exactamente o conjunto dos múltiplos de $d = m.d.c(a,b)$

Demonstração Seja $d = m.d.c(a,b)$. Pelo teorema anterior existem $x_0, y_0 \in \mathbb{Z}$ tais que $d = a x_0 + b y_0$, pelo que $d \in T$. Além disso, para todo o $n \in \mathbb{Z}$, temos que

$$nd = a(n x_0) + b(n y_0)$$

pelo que os múltiplos de d pertencem a T.

Temos que de $d \mid a$ e $d \mid b$ resulta que

$d \mid ax+by$, para quaisquer $x, y \in \mathbb{Z}$

Logo todos os elementos de T são múltiplos de d. $\square$

Teorema

Sejam $a, b \in \mathbb{Z}$, $a \neq 0$ ou $b \neq 0$, e seja $d \in \mathbb{N}$. Então

$d = m.d.c(a,b)$ se e só se:

i) $d \mid a$ e $d \mid b$

ii) $\forall c \in \mathbb{Z}$ $c \mid a$ e $c \mid b \Rightarrow c \mid d$.

Demonstração (ver sebenta)

Números primos entre si

Definição: Dois números dizem-se a e b, $a \neq 0$ ou $b \neq 0$, dizem-se primos entre si se $m.d.c(a,b) = 1$.

Teorema: Sejam a, b números inteiros a, b com $a \neq 0$ ou $b \neq 0$

Então a e b são primos entre si sse existem $x, y \in \mathbb{Z}$ tais que

$1 = ax + by$.

Demonstração Se a e b são primos entre si então $m.d.c(a,b) = 1$ e pelo teorema anterior existem $x, y \in \mathbb{Z}$ tais que $1 = ax + by$.

Reciprocamente, suponhamos que existem $x, y \in \mathbb{Z}$ tais que $1 = ax + by$. Pelo corolário anterior, 1 é múltiplo de $d = m.d.c(a,b)$ logo como $1, d \in \mathbb{N}$ então $d = 1$ $\square$

Corolário: Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$ ou $b \neq 0$. Se m.d.c $(a,b) = d$ então $\frac{a}{d} \in \mathbb{Z}$ e $\frac{b}{d} \in \mathbb{Z}$ e m.d.c $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demonstração: Temos m.d.c $(a,b) = d$

$\Rightarrow \exists\, x, y \in \mathbb{Z}$ tais que $d = ax + by$

$\Rightarrow \exists\, x, y \in \mathbb{Z}$ tais que $1 = \frac{a}{d} x + \frac{b}{d} y$

Como $\frac{a}{d}$ e $\frac{b}{d}$ são inteiros, pelo teorema anterior, m.d.c $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. $\square$

Corolário Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$ ou $b \neq 0$. Se $a \mid c$ e $b \mid c$ e m.d.c$(a,b) = 1$, então, $ab \mid c$.

Demonstração Como $a \mid c$ e $b \mid c$ existem $x, y \in \mathbb{Z}$ tais que $c = ax$ e $c = by$.

Como $m.d.c(a,b) = 1$ então existem $x_0, y_0 \in \mathbb{Z}$ tais que $1 = a x_0 + b y_0$.

Logo $c = c \cdot 1 = c(a x_0 + b y_0) = ac\, x_0 + bc\, y_0$

$= a(by)\, x_0 + b(ax)\, y_0 = (ab)(y x_0 + x y_0)$

Portanto $c \mid ab$ $\square$

Observação: No corolário anterior a condição $m.d.c.(a,b) = 1$ não pode ser omitida. Por exemplo, $2 \mid 2$ e $2 \mid 2$ mas $4 \nmid 2$.

Corolário (Lema de Euclides) Sejam $a, b, c \in \mathbb{Z}$, $a \neq 0$ ou $b \neq 0$, se $a \mid bc$ e $m.d.c(a,b) = 1$ então $a \mid c$.

Demonstração: Se $1 = m.d.c\,(a,b)$ então $\exists\, x, y \in \mathbb{Z}$ tais que $1 = ax + by$. Assim, $c = c \cdot 1 = acx + bcy$

Como $a \mid ac$ e, por hipótese, $a \mid bc$ então $a \mid acx + bcy$ logo $a \mid c$. $\square$

Observação: A condição $m.d.c\,(a,b) = 1$ não pode ser omitida. Temos $6 \mid 2 \times 3$ mas $6 \nmid 2$ e $6 \nmid 3$. Note-se que $m.d.c\,(6,2) = 2$ e $m.d.c\,(6,3) = 3$.

Algoritmo de Euclides

Lema: Sejam $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$, $q, r \in \mathbb{Z}$ tais que

$$a = qb + r, \quad 0 \leq r < b. \text{ Então } d = m.d.c\,(a,b) \iff d = m.d.c\,(b,r)$$

Demonstração : (vez sobenta)

Teorema (Algoritmo de Euclides)

Sejam a e $b \in \mathbb{Z}$ tais que $a \geq b > 0$. Se existem $q_1, q_2, \ldots, q_{n+1}$, $r_1, r_2, \ldots, r_n \in \mathbb{Z}$ tais que

$$a = q_1 b + r_1 \qquad 0 < r_1 < b$$

$$b = q_2 r_1 + r_2 \qquad 0 < r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3 \qquad 0 < r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n \qquad 0 < r_n < r_{n-1}$$

$$r_{n-1} = q_{n+1} r_n + 0$$

Então $m.d.c(a,b) = r_n$.

Demonstração: Imediata do lema anterior

$\square$

Exemplo: $m.d.c(12378, 3054) = ?$

$$12378 = 4 \times \underline{3054} + \underline{162}$$

$$3054 = 18 \times \underline{162} + \underline{138}$$

$$162 = 1 \times \underline{138} + \underline{24}$$

$$138 = 5 \times \underline{24} + \underline{18}$$

$$24 = 1 \times \underline{18} + \underline{6}$$

$$18 = 3 \times \underline{6} + 0$$

Portanto $m.d.c(12378, 3054) =$

Além disso

$$6 = 24 - 1 \times 18$$

$$= 24 - (138 - 5 \times 24)$$

$$= 6 \times 24 - 1 \times 138$$

$$= 6(162 - 1 \times 138) - 138$$

$$\vdots$$

$$\boxed{6 = 132 \times \underline{12378} - 535 \times \underline{3054}}$$