Def. $\forall a \in \mathbb{Z}$, o **módulo de a** é:

$$|a| = \begin{cases} a \text{ se } a \geq 0 \\ -a \text{ se } a < 0 \end{cases}$$

Algoritmo da divisão euclidiana

Sejam $m, n \in \mathbb{Z}$, com $m \neq 0$. Então existem, e são unicamente determinados, $q, r \in \mathbb{Z}$ tais que:

$$n = qm + r \quad \text{e} \quad 0 \leq r < |m|.$$

Dem.

Já demonstramos o teorema para $n, m \in \mathbb{N}$.

Então $\forall m \in \mathbb{Z}$, $\exists\, q', r \in \mathbb{N}$ t.q. $n = q'|m| + r$ e $0 \leq r < |m|$.

Se $m > 0$, podemos escolher $q = q'$. Se $m < 0$, $q = -q'$.

Suponha-se, agora, $n < 0$. Então $\exists\, q', r'$ t.q.

$|m| = q'm + r'$ e $0 \leq r' < |m|$.

Logo, $n = -q'm - r'$. Se $r' = 0$, terminamos ($q = -q'$ e $r = 0$).

Seja $r' > 0$ e vamos distinguir os casos: $m < 0$, $m > 0$.

Se $m > 0$, $n = -q'm - r' = (-q' - 1)m + m - r'$ e $0 \leq m - r' < m$

pois $0 < r' < m$. Então $n = qm + r$, com $q = -q' - 1$ e $r = m - r'$.

Se $m < 0$, $n = -q'm - r' = (-q' + 1)m - m - r' = (-q' + 1)m + |m| - r'$

Então $n = qm + r$ com $q = -q' + 1$ e $r = |m| - r'$.

Unicidade: Se $n = mq + r = mq_1 + r_1$, com $0 \leq r, r_1 < |m|$, então $0 = n - n = mq + r - mq_1 - r_1 = (q - q_1)m + r - r_1$.

De $(q - q_1)m + r - r_1 = 0$ segue $(q - q_1)m = r_1 - r$. Sem perda, podemos supor $r_1 \geq r$. Logo:

$$|q - q_1||m| = |r_1 - r| = r_1 - r \leq r_1 < |m| \Rightarrow$$

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

$q = q_1$ e, consequentemente, $r = r_1$.

$3 \mid 2$ $\quad 3 = 2 \cdot \underset{q}{1} + \underset{r}{1}$

$-3 \mid 2$ $\quad -3 = 2 \cdot (-2) + 1$ (q, r)

$11 \mid 3$ $\quad 11 = 3 \cdot \underset{q}{3} + \underset{r}{2}$

$-11 \mid 3$ $\quad -11 = 3 \cdot (-4) + \underset{r}{1}$ (q) $\quad 3 \cdot (-3)$ ~~-2~~

Def. $\forall a, b \in \mathbb{Z}$, dizemos que a divide b, e denotaremos isto por $a|b$, sse $\exists\, c \in \mathbb{Z}$ t.q. $ac = b$.

(a divide b, ou a é um divisor de b, ou b é um múltiplo de a).

$|$ é reflexiva e transitiva (pré-ordem).

$\forall a \in \mathbb{Z}$, $a \cdot 1 = a \Rightarrow a|a$.

$\forall a, b, c \in \mathbb{Z}$, $a|b$ e $b|c \Rightarrow \exists\, d, e \in \mathbb{Z}$ t.q. $ad = b$ e $be = c$. Logo, $c = be = a(de) \Rightarrow a|c$.

Não é simétrica pois, por exemplo, $1|2$ mas $2 \nmid 1$

Não é antissimétrica pois $\forall a \in \mathbb{Z}$, $a|-a$ e $-a|a$, mas $-a = a$ sse $a = 0$. $2 = -2 \cdot (-1)$ e $-2 = 2 \cdot (-1)$.

A restrição de $|$ a $\mathbb{N}$ é sim antissimétrica e, então é uma ordem (não total).

Obs.: $\forall a \in \mathbb{Z}$, $a|0$ pois $a \cdot 0 = 0$.

Em $\mathbb{N}$: $\forall x,y\,(xy=1 \leftrightarrow x=y=1)$

← já sabemos

Iremos provar que $(xy=1 \rightarrow y=1)$

Se $y=0 \rightarrow xy=0$.

Então $y>0 \Rightarrow \exists z\,(y=s(z))$, então

$$1 = xy = xs(z) = xz + x \rightarrow \begin{cases} xz=0 \text{ e } x=1 \\ \text{ou} \\ xz=1 \text{ e } x=0 \end{cases}$$

$xz=0$ e $x=1 \Rightarrow z=0$ e, então, $y=1$ $(e\ x=1)$ ✓

$xz=1$ e $x=0$ absurdo, pois $xz = 0\cdot z = 0 \neq 1$

Em $\mathbb{Z}$, $xy=1$ sse $x=y=-1$ ou $x=y=1$.

$x>0$ e $y<0$ ou vice-versa $\Rightarrow xy<0$.

Então $x,y>0$ ou $x,y<0$. Se $x,y>0$, pela dem. anterior, $x=y=1$. Se $x,y<0$, então $|x|,|y|>0$ e $|x||y| = |1| = 1 \Rightarrow |x| = |y| = 1 \Rightarrow x = y = -1$.

Sejam $a, b \in \mathbb{Z}$. Um número $d \in \mathbb{Z}$ é dito um máximo divisor comum (mdc) de a e b se: $d|a$, $d|b$ e $\forall c \in \mathbb{Z}\,((c|a \text{ e } c|b) \to c|d)$.

d é um mdc de a e b sse $-d$ também é

$m \in \mathbb{Z}$ é um mínimo múltiplo comum (mmc) de a e b se: $a|m$, $b|m$ e $\forall c \in \mathbb{Z}\,((a|c \text{ e } b|c) \to m|c)$.

Lema $\forall a, b \in \mathbb{Z}$ valem:

(1) $a|b$ e $b|a \Rightarrow a = \pm b$.

(2) $c|a$ e $c|b \Rightarrow c|ah+bk$ $\forall h, k \in \mathbb{Z}$.

Dem.

(2) $c|a$ e $c|b \Rightarrow \exists u, v \in \mathbb{Z}\,(a = cu \text{ e } b = cv)$.

Então $\forall h, k \in \mathbb{Z}$, $ah + bk = cuh + cvk = c(uh + vk)$

$\Rightarrow c|ah+bk$.

$d \in mdc(a,b)$ — d é um mdc de a e b

$m \in mmc(a,b)$ — m é um mmc de a e b

Algoritmo das divisões subsequentes (Euclides)

$\forall a,b \in \mathbb{Z}$ $\exists d \in mdc(a,b)$ e $\exists u,v \in \mathbb{Z}$ t.q.

$au + bv = d$.

Dem.:

Se $a = b = 0$, então $mdc(0,0) = \{0\}$ e u, v são quaisquer.

Se $a = 0$ e $b \neq 0$, então $mdc(0,b) = \{\pm b\}$ e $u = 0$ e $v = 1$.

Vamos supor a e b não nulos e observemos que

$mdc(a,b) = mdc(a,-b) = mdc(-a,b) = mdc(-a,-b) =$

$= mdc(|a|,|b|)$. Sem perda, podemos supor $a, b > 0$.

$\exists\, q_1, r_1 \in \mathbb{N}$ t.q. $a = bq_1 + r_1$ e $0 \leq r_1 < b$

$\exists\, q_2, r_2 \in \mathbb{N}$ t.q. $b = r_1 q_2 + r_2$ e $0 \leq r_2 < r_1 < b$

$\forall i \geq 2$, se $r_i > 0$, $\exists\, q_{i+1}, r_{i+1}$ t.q. $r_{i-1} = r_i q_{i+1} + r_{i+1}$

e $0 \leq r_{i+1} < r_i < \dots < b = r_0$

$\exists k$ t.q. $r_{k+1}=0$. Vamos provar que $r_k=d$.

Vamos provar que $r_k \mid r_i \ \forall i \leq k$, por indução sobre $k-i$.

Base $k-i=0$, ou seja, $k=i$ óbvio $r_k \mid r_k$.

Passo Hp.: $r_k \mid r_j \forall j \geq i$ Tese: $r_k \mid r_{i-1}$

$$\left.\begin{array}{l} r_k \mid r_i \Rightarrow \exists c \,(r_k c = r_i) \\ r_k \mid r_{i+1} \Rightarrow \exists c' \,(r_k c' = r_{i+1}) \end{array}\right\} \text{e } r_{i-1} = r_i q_{i+1} + r_{i+1} \Rightarrow$$

$$r_{i-1} = r_k c q_{i+1} + r_k c' = r_k \left(c q_{i+1} + c'\right) \Rightarrow r_k \mid r_{i-1}$$

Pela indução, segue $r_k \mid r_i \ \forall i$ e, em particular,

$\exists h, h'$ t.q. $r_k h = b$ e $r_k h' = r_1 \Rightarrow a = b q_1 + r_1 =$

$= r_k h q_1 + r_k h' = r_k \left(h q_1 + h'\right) \Rightarrow r_k \mid a$.

Seja $z \in \mathbb{Z}$ t.q. $z \mid a$ e $z \mid b$ e vamos provar que $z \mid r_k$.

(Chamemos r_k de d).

$z \mid a$ e $z \mid b \Rightarrow z \mid a - b q_1 = r_1$

$\forall i > 1$, vamos supor $z \mid r_j \ \forall j < i$.

$z \mid r_{i-2} - r_{i-1} q_i = r_i$ (pois $r_{i-2} = r_{i-1} q_i + r_i$)

$\Rightarrow z \mid r_i \ \forall i$ pelo princípio de indução $\Rightarrow z \mid r_k = d$.

d é $mdc(a,b)$. (Teorema de Bézout)

d é $mdc(a,b)$. (Teorema de Bézout)

Vamos provar que $\exists u,v\ (au+bv=d)$.

Indução em k.

$k=0$, $d=r_0=b \Rightarrow b|a$ e então $b=a\cdot 0+b\cdot 1$

vale com $u=0$ e $v=1$

Seja $k>0$ e vemos supor, por hip. de indução, que $\forall i<k\ \exists u_i,v_i\in\mathbb{Z}$ t.q. $r_i=au_i+bv_i$.

$$r_k=r_{k-2}-r_{k-1}q_k=(au_{k-2}+bv_{k-2})-(au_{k-1}+bv_{k-1})q_k=$$

$$=a(u_{k-2}-u_{k-1}q_k)+b(v_{k-2}-v_{k-1}q_k)$$

vale com $u=u_{k-2}-u_{k-1}q_k$ e $v=v_{k-2}-v_{k-1}q_k$

Exemplo $\text{mdc}(36, 42)$

r_i	42	36	6	r_{k+1}
q_i		1	6	

$\text{mdc}(36, 42) = \{\pm 6\}$

$6 = 42 - 36 \cdot 1 \Rightarrow 6 = 36 \cdot (-1) + 42 \cdot 1$

$u \qquad v$

$\text{mdc}(764, 48) = \{\pm 4\}$

764	48	44	4	0
	15	1	11	

$4 = 48 - 44 \cdot 1 = 48 - (764 - 48 \cdot 15) =$

$= 764 \cdot (-1) + 48 \cdot 16$

$u \qquad v$

$\text{mdc}(39, 7) = \{\pm 1\}$

39	7	4	3	1	0
	5	1	1	3	

$1 = 4 - 3 = 39 + 7 \cdot (-5) - (7 - 4) =$

$= 39 + 7 \cdot (-6) + 4 = 39 + 7(-6) + 39 + 7(-5) =$

$= 39 \cdot 2 + 7(-11)$

$u \qquad v$