

1 TEORIA DOS NÚMEROS

A **teoria dos números** é o ramo da Matemática pura que estuda as propriedades dos números em geral, e em particular as propriedades dos números inteiros. Além disso, estuda-se as diversas classes de problemas que surge no seu estudo.

1.1 Divisibilidade

Uma equação do tipo $ax = b$ pode ou não ter solução no conjunto dos números inteiros; isso dependerá dos coeficientes a e b da equação. Quando tal solução existe, diz-se que **b é divisível por a**. Mais precisamente:

Definição: Sejam a e b inteiros. Dizemos que **a divide b**, denotado por $a \mid b$, se existe um inteiro c tal que $b = a \cdot c$.

Se $a \mid b$ também se diz que **a é um divisor de b**, que **b é um múltiplo de a**, que **a é um fator de b** ou que **b é divisível por a**.

Observações:

1. se **a não divide b** escrevemos $a \nmid b$;
2. \mid é um símbolo de relação e não de operação.

Exemplos:

1. $2 \mid 6$, pois existe $3 \in \mathbb{Z}$ tal que $6 = 2 \cdot 3$;
2. $-5 \mid 30$, pois existe $-6 \in \mathbb{Z}$ tal que $30 = (-5) \cdot (-6)$;
3. $3 \mid 0$, pois existe $0 \in \mathbb{Z}$ tal que $0 = 3 \cdot 0$;
4. $3 \nmid 10$, pois não existe $c \in \mathbb{Z}$ tal que $10 = 3 \cdot c$;

Observação: Se $a \neq 0$, o inteiro c nas condições da definição é único.

PROVA

Suponha que existe outro inteiro c' tal que $b = ac'$. Daí, temos $ac = ac'$ e como $a \neq 0$, pela propriedades do cancelamento, $c = c'$. Logo, c é único.

O inteiro assim definido chama-se **quociente** de b por a e indicado por

$$c = \frac{b}{a}.$$

Nota: $0 \mid b$, se e somente se, $b = 0$.

Observe que neste caso o quociente não é único, pois $0 = 0 \cdot c$, para todo $c \in \mathbb{Z}$. Por causa disso, costuma-se excluir o caso em que o divisor é nulo.

Observações: Se a é divisor de b , então $-a$ também é divisor de b . Assim, os divisores de um inteiro qualquer são dois a dois iguais em valor absoluto e de sinais opostos.

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

Corolários.

1. Os únicos divisores de 1 são 1 e -1 ;
2. Se $a \mid b$ e $b \mid a$, então $a = \pm b$.

Proposição. Quaisquer que $a, b, c, d \in \mathbb{Z}$, valem:

1. $a \mid 0$, $1 \mid a$ e $a \mid a$;
2. Se $a \mid b$ e $b \mid c$, então $a \mid c$;
3. Se $a \mid b$ e $c \mid d$, então $ac \mid bd$;
4. Se $a \mid b$ e $a \mid c$, então $a \mid (b + c)$;
5. Se $a \mid b$, então para todo $m \in \mathbb{Z}$, tem-se que $ac \mid mb$;
6. Se $a \mid b$ e $a \mid c$, então para todo $m, n \in \mathbb{Z}$ tem-se que $a \mid (mb + nc)$;
7. Se $c \mid a$, $c \mid b$ e $a \leq b$, então $c \mid (b - a)$;
8. Seja $a = b + c$ e suponhamos que $d \mid b$. Então $d \mid a$ se, e somente se, $d \mid c$.

Exercícios. Demonstrar as proposições acima que foram demonstradas em aula.

1.2 Algoritmo da Divisão

É evidente que há infinitos casos de pares de inteiros tais que nenhum dos dois é divisor do outro. Por exemplo, $2 \nmid 3$ nem $3 \nmid 2$. O algoritmo da divisão estabelece uma “divisão com resto” e é a base da teoria dos números.

Algoritmo da Divisão. Sejam a e d inteiros com $d > 0$. Então existem inteiros q e r , únicos, com $0 \leq r < d$, tais que $a = dq + r$. Os elementos a, d, q e r são chamados, respectivamente, **dividendo**, **divisor**, **quociente** e **resto**.

Teorema. Sejam a e d inteiros com $d \neq 0$. Então existem inteiros q e r , únicos, com $0 \leq r < |d|$, tais que $a = dq + r$.

Exemplo. Temos que $20 = 3 \cdot 6 + 2$ e $-20 = (-4) \cdot 6 + 4$, ou seja, o resto da divisão de 20 por 6 é 2 e o resto da divisão de -20 por 6 é 4. Note que o resto não pode ser negativo.

1.3 Paridade de um inteiro

Na divisão de um inteiro qualquer $a \neq 0$ por $d = 2$ os possíveis restos são $r = 0$ e $r = 1$. Se $r = 0$, então o inteiro $a = 2q$ é denominado **par**; se $r = 1$, então o inteiro $a = 2q + 1$ é denominado **ímpar**.

Proposição. Na divisão do quadrado de um inteiro qualquer a por 4 o resto é 0 ou 1.

Exercício. Mostre que o quadrado de qualquer inteiro ímpar é da forma $8k + 1$

1.4 Máximo divisor comum de dois inteiros

Definição. Sejam a e b dois inteiros, não simultaneamente nulos, chama-se **máximo divisor comum de a e b** e, indica-se por $\text{mdc}(a, b)$, o inteiro positivo d ($d > 0$) que satisfaz as seguintes condições:

- (i) $d \mid a$ e $d \mid b$;
- (ii) Se $c \mid a$ e se $c \mid b$, então $c \leq d$.

Observações. É imediato que $\text{mdc}(a, b) = \text{mdc}(b, a)$. Em particular:

- (i) o $\text{mdc}(0, 0)$ não existe;
- (ii) o $\text{mdc}(a, 1) = 1$;
- (iii) se $a \neq 0$, então o $\text{mdc}(a, 0) = |a|$;
- (iv) se $a \mid b$, então o $\text{mdc}(a, b) = |a|$.

Teorema. Se $k > 0$, então $\text{mdc}(ka.kb) = k \cdot \text{mdc}(a, b)$.

Corolário. Para todo $k \neq 0$, $\text{mdc}(ka.kb) = |k| \cdot \text{mdc}(a, b)$.

Teorema de Bézout. Se a e b são dois inteiros, não simultaneamente nulos, então existe e é único o $\text{mdc}(a, b)$, além disso, existem inteiros x e y tais que

$$\text{mdc}(a, b) = ax + by,$$

isto é, o $\text{mdc}(a, b)$ é uma **combinação linear** de a e b .

Observação. O $\text{mdc}(a, b)$ é o menor inteiro positivo da forma $ax + by$, isto é, que pode ser expresso como **combinação linear** de a e b . Mas esta representação não é única, pois

$$\text{mdc}(a, b) = a(x + bt) + b(y - at), \text{ qualquer que seja } t \in \mathbb{Z}.$$

Exemplo. Sejam $a = 6$ e $b = 27$, temos:

$$\text{mdc}(6, 27) = 3 = 6 \cdot (-4) + 27 \cdot 1.$$

Note também que $\text{mdc}(6, 27) = 3 = 6 \cdot (-4 + 27t) + 27 \cdot (1 - 6t)$.

Lema. Se $a = bq + r$, então $\text{mdc}(a, b) = \text{mdc}(b, r)$.

1.4.1 Algoritmo de Euclides

A ideia principal deste algoritmo é que o mdc pode ser calculado, recursivamente, usando o resto da divisão como entrada para o próximo passo. A ideia é embasada no Lema anterior;

$$\text{mdc}(a, b) = \text{mdc}(b, r),$$

onde r é o resto da divisão de a por b .

Além disso, como $\text{mdc}(a, b) = \text{mdc}(|a|, |b|)$, a determinação do $\text{mdc}(a, b)$ se reduz ao caso em que a e b são inteiros positivos distintos, tais que $b \nmid a$.

É usual o seguinte dispositivo de cálculo no emprego do algoritmo de Euclides:

- Inicialmente, efetuamos a divisão do maior inteiro pelo menor, $a = bq_1 + r_1$, e colocamos os números envolvidos no seguinte diagrama:

	q_1	q_2	
a	b	r_1	
r_1	r_2		

- A seguir, continuamos efetuando a divisão $b = r_1 q_2 + r_2$ e colocamos os números envolvidos no diagrama:

	q_1	q_2	
b	a	r_1	
r_1	r_2		

- Prosseguindo até obter resto nulo:

	q_1	q_2	q_3	\cdots	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	\cdots	r_{n-2}	r_{n-1}	$r_n = \text{mdc}(a,b)$
r_1	r_2	r_3	r_4	\cdots	r_n	0	

O último resto não nulo é o máximo divisor comum procurado.

Exemplo. Determine o mdc de 372 e 162.

Fazendo as divisões sucessivas e usando o dispositivo prático, temos:

	2	3	2	1	2
372	162	48	18	12	6
48	18	12	6		

Portanto, o $\text{mdc}(372, 162) = 6$.

O algoritmo de Euclides também pode ser usado para achar a expressão do $\text{mdc}(a, b) = r_n$ como **combinação linear** de a e b . Para isso, basta eliminar sucessivamente os restos $r_{n-1}, r_{n-2}, r_{n-3}, \dots, r_3, r_2, r_1$ entre as n primeiras igualdades anteriores.

Exemplo. Escreva o $\text{mdc}(372, 162)$ como combinação linear de 372 e 162.

Considerando os resultados obtidos no dispositivo acima, podemos escrever:

$$6 = 18 - 1 \cdot 12$$

$$12 = 48 - 2 \cdot 18$$

$$18 = 162 - 3 \cdot 48$$

$$48 = 372 - 2 \cdot 162$$

Assim,

$$\begin{aligned}6 &= 18 - 1 \cdot 12 = 18 - 1 \cdot (48 - 2 \cdot 18) = 3 \cdot 18 - 48 = 3 \cdot (162 - 3 \cdot 48) - 48 = \\&= 3 \cdot 162 - 10 \cdot 48 = 3 \cdot 162 - 10 \cdot (372 - 2 \cdot 162) = 23 \cdot 162 - 10 \cdot 372,\end{aligned}$$

isto é $6 = \text{mdc}(372, 162) = 372 \cdot x + 162 \cdot y$,

onde $x = -10$ e $y = 23$.

1.5 Mínimo múltiplo comum de dois inteiros

Definição. Sejam a e b dois inteiros, não simultaneamente nulos, chama-se **mínimo múltiplo comum de a e b** e, indica-se por $\text{mmc}(a, b)$, o inteiro positivo m ($m > 0$) que satisfaz as seguintes condições:

- (i) $a \mid m$ e $b \mid m$;
- (ii) Se $a \mid c$ e se $b \mid c$, $c > 0$, então $m \leq c$.

Proposição. Se $a \mid b$, então o $\text{mmc}(a, b) = |b|$.

1.6 Relação entre o mdc e o mmc

Teorema. Para todo par de inteiros positivos a e b subsiste a relação:

$$\text{mdc}(a, b) \cdot \text{mmc}(a, b) = a \cdot b.$$

Corolário. Para todo inteiro $a > 0$ e $b > 0$, o $\text{mmc}(a, b) = ab$ se, e somente se, o $\text{mdc}(a, b) = 1$.