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 inteiros c tal que $b = a \cdot c$.

Se $a|b$ 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 inteiros 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 | 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 $a \mid mb$;
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 $a = 2q$ e é denominado **par**; se $r = 1$, então o inteiro $a = 2q + 1$ e 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 $mdc(a, b)$, 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 $mdc(a, b) = mdc(b, a)$. Em particular:

(i) o $mdc(0, 0)$ não existe;

(ii) o $mdc(a, 1) = 1$;

(iii) se $a \neq 0$, então o $mdc(a, 0) = |a|$;

(iv) se $a \mid b$, então o $mdc(a, b) = |a|$.

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

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

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

$$mdc(a,b) = ax + by,$$

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

Observação. O $mdc(a,b)$ 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

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

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

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

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

Lema. Se $a = bq + r$, então $mdc(a,b) = mdc(b,r)$.

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;

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

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

Além disso, como $mdc(a,b) = mdc(|a|,|b|)$, a determinação do $mdc(a,b)$ 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 =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 $mdc(372, 162) = 6$.

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

Exemplo. Escreva o $mdc(372, 162)$ 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,

$$6 = 18 - 1 \cdot 12 = 18 - 1 \cdot (48 - 2 \cdot 18) = 3 \cdot 18 - 48 = 3 \cdot (162 - 3 \cdot 48) - 48 =$$
$$= 3 \cdot 162 - 10 \cdot 48 = 3 \cdot 162 - 10 \cdot (372 - 2 \cdot 162) = 23 \cdot 162 - 10 \cdot 372,$$

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

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

1.5 Inteiros primos entre si

Definição. Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. Diz-se que a e b são **primos entre si** se, e somente se, o $mdc(a,b) = 1$.

Exemplo. 9 e 10, -9 e 16 são primos entre si, pois o $mdc(9,10) = mdc(-9,16) = 1$.

Teorema. Sejam a e b inteiros, não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$), são **primos entre si** se, e somente se, existem inteiros x e y tais que $ax + by = 1$.

Prova

$\Longrightarrow$) Se a e b são *primos entre si*, então o $mdc(a,b) = 1$. Como o $mdc(a,b) = 1$, pelo Teorema Bèzout, existem inteiros x e y tais que $ax + by = 1$.

$\Longleftarrow$) Suponha que existem inteiros x e y tais que $ax + by = 1$. Seja $d = mdc(a,b)$, então $d \mid a$ e $a \mid b$. $d \mid a$ implica que $d \mid ax$ e $d \mid b$ implica que $d \mid by$, com x e y inteiros. Segue que $d \mid ax + by$, ou seja, $d \mid 1$. Portanto, $d = 1$, ou seja, o $mdc(a,b) = 1$. Logo a e b são *primos entre si*.

Corolário. Se o $mdc(a,b) = d$, então o $mdc(\frac{a}{d}, \frac{b}{d}) = 1$.

Antes de iniciarmos a demonstração, observe que $\frac{a}{d}$ e $\frac{b}{d}$ são inteiros, pois d é um divisor comum de a e b.

Prova

Suponha que $mdc(a,b) = d$, então existem inteiros x e y tais que $ax + by = d$. Dividindo esta igualdade por d, temos:

$$\frac{a}{d}x+\frac{b}{d}y=1.$$

Logo, pelo teorema anterior, os inteiros $\frac{a}{d}$ e $\frac{b}{d}$ são *primos entre si*, isto é, o $mdc(\frac{a}{d},\frac{b}{d})=1$.

Exemplo. $mdc(-12,30)=6$ e $mdc(\frac{-12}{6},\frac{30}{6})=mdc(-2,5)=1$.

Corolário. Se $a \mid b$ e se o $mdc(b,c)=1$, então o $mdc(a,c)=1$.

Corolário. Se $a \mid c$, $b \mid c$ e se o $mdc(a,b)=1$, então $ab \mid c$.

Corolário. Se o $mdc(a,b)=1=mdc(a,c)$, então o $mdc(a,bc)=1$.

Corolário. Se o $mdc(a,bc)=1$, então $mdc(a,b)=1=mdc(a,c)$.

Teorema de Euclides. Se $a \mid bc$ e se $mdc(a,b)=1$, então $a \mid c$.

Note que apenas a condição $a \mid bc$ não implica que $a \mid c$. Por exemplo, $12 \mid 9\cdot 8$, mas $12 \nmid 9$ e $12 \nmid 8$. Perceba também que $mdc(12,9)\neq 1$ e $mdc(12,8)\neq 1$.

Exercícios. Demonstre os Corolários acima.

1.6 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 $mmc(a,b)$, 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 $mmc(a,b)=|b|$.

1.7 Relação entre o mdc e o mmc

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

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

Seja $d=mdc(a,b)$ e seja $m=mmc(a,b)$. Como $a \mid a\cdot\frac{b}{d}$ e $b \mid b\cdot\frac{a}{d}$, temos que $\frac{ab}{d}$ é múltiplo comum de a e de b. Portanto, existe $k\in\mathbb{Z}^*$ tal que $\frac{ab}{d}=mk$ (*). Assim,

$$\frac{ab}{d} = mk \Rightarrow \frac{a}{d} = \frac{m}{b} \cdot k \text{ e } \frac{b}{d} = \frac{m}{a} \cdot k,$$

isto é, k é um divisor comum dos inteiros $\frac{a}{d}$ e $\frac{b}{d}$. Usando o fato de que se o $mdc(a,b) = d$, então o $mdc(\frac{a}{d}, \frac{b}{d}) = 1$ e o fato que se o $mdc(\frac{a}{d}, \frac{b}{d}) = 1$, então $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si, conclui-se que $k = 1$. Assim, de (*), temos que $\frac{ab}{d} = m$ ou $ab = dm$, ou seja,

$$ab = mdc(a,b) \cdot mmc(a,b).$$

Exemplo. Determine o $mmc(372, 162)$.

Obtemos anteriormente que o $mdc(372, 162) = 6$. Portanto, $mmc(372, 162) = \frac{372 \cdot 162}{6} = \frac{60.264}{6} = 10.044$.

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

Exercício. Demonstre o Corolário acima.

1.8 Números Primos e Compostos

Definição. Diz-se que um número inteiro positivo $p > 1$ é um **número primo** se, e somente se, 1 e p são os seus únicos divisores positivos.

Um inteiro positivo $m > 1$ que não é primo chama-se **composto**.

Exemplos. $2, 3, 5$ e 7 são primos e os inteiros $4, 6, 8$ e 10 são compostos.

Observações:

a) 1 não é primo nem composto e, por conseguinte, se a é um inteiro positivo qualquer, então a é primo, a é composto ou $a = 1$.

b) 2 é o único inteiro positivo par que é primo.

Teorema. Se um primo p não divide um inteiro a, então a e p são **primos entre si**.

Corolário. Se p é primo tal que $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Corolário. Se p é primo tal que $p \mid a_1 \cdot a_2 \cdot a_3 \cdot \ldots cdot a_n$, então existe um índice k, com $1 \leq k \leq n$, tal que $p \mid a_k$.

Corolário. Se os inteiros $p, q_1, q_2, \ldots, q_n$ são todos primos e se$p \mid q_1 \cdot q_2 \cdot q_3 \cdot \ldots cdot q_n$, então existe um índice k, com $1 \leq k \leq n$, tal que $p = q_k$.

Teorema. Todo inteiro composto possui um divisor primo.

Teorema Fundamental da Aritmética. Todo inteiro positivo $n > 1$ é igual a um produto de fatores primos.

PROVA

Se n é primo não há nada para demonstar. Se n é composto, então pelo Teorema anterior, n possui um divisor divisor primo p_1. Assim,

$$n = p_1 \cdot n_1, 1 < n_1 < n \ [1].$$

Se n_1 é primo, então n é um produto de fatores primos, mas se n_1 é composto, então pelo Teorema anterior, n_1 possui um divisor divisor primo p_2, isto é, $n_1 = p_2 \cdot n_2$. Daí,

$$n = p_1 \cdot p_2 \cdot n_2, 1 < n_2 < n_1.$$

Se n_2 é primo, então n é igual a um produto de fatores primos; se n_2 é composto, então pelo Teorema anterior, n_2 possui um divisor divisor primo p_3, isto é, $n_2 = p_3 \cdot n_3$. Assim,

$$n = p_1 \cdot p_2 \cdot p_3 \cdot n_3, 1 < n_3 < n_2.$$

Seguindo este raciocínio, obtemos a sequência decrescente

$$n > n_1 > n_2 > n_3 > \ldots > 1$$

e como existe um número finito de inteiros positivos menores que n e maiores que 1, necessariamente existe um n_k que é um número primo, ou seja, $n_k = p_k$, e consequentemente teremos:

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k.$$

Portanto, obtemos uma igualdade que representa o inteiro $n > 1$ como um produto de fatores primos.

[1] $n_1 < n$, pois se $n_1 = n$, teríamos $p_1 = 1$, mas p é primo; se $n_1 = 1$, recairíamos em n primo.

Corolário. A **decomposição** de um inteiro $n > 1$ como produto de fatores primos é única, a menos da ordem dos fatores.

Exemplo. A decomposição de 630 em um produto de fatores primos é dada por:

$$630 = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 7.$$

Corolário. Todo inteiro $n > 1$ admite uma única decomposição da forma:

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3} \cdot \ldots \cdot \ldots \cdot p_r^{k_r},$$

onde, para $i = 1, 2, 3, \ldots, r$, cada k_i é um inteiro positivo e cada p_i é um primo, com $p_1 < p_2 < \ldots < p_r$, denominada **decomposição canônica** do inteiro $n > 1$.

Exemplo. A decomposição canônica de $n = 630$ é dada por

$$360 = 2 \cdot 3^2 \cdot 5 \cdot 7.$$

Exemplo. A decomposição canônica de $n = 360$ é dada por

$$360 = 2^3 \cdot 3^2 \cdot 5.$$

Observações. Conhecidas as decomposições canônicas de dois inteiros positivos $a > 1$ e $b > 1$, o $mdc(a,b)$ é o produto dos fatores primos *comuns* às duas decomposições canônicas tomados cada um com o **menor** expoente; o $mmc(a,b)$ é o produto dos fatores primos *comuns* e *não comuns* às duas decomposições canônicas tomados cada um com o **maior** expoente;

Exemplo. As decomposições canônicas de 360 e 630 são dadas por $630 = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 7$ e $360 = 2 \cdot 3^2 \cdot 5 \cdot 7$ e, portanto,

$$mdc(630, 360) = 2 \cdot 3^2 \cdot 5 = 90$$

e

$$mmc(630, 360) = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520.$$

Teorema de Euclides. Há um número infinito de primos.

Teorema. Se um inteiro positivo $a > 1$ é composto, então a possui um divisor primo $p \leq \sqrt{a}$.

Corolário. Se $a > 1$ não é divisível por nenhum dos primos $p \leq \sqrt{a}$, então a é primo.

Nota. Estes resultados nos fornece um processo que permite reconhecer se um dado inteiro $a > 1$ é primo ou composto. O processo consiste em dividir a sucessivamente pelos primos que não excedem $\sqrt{a}$.

Exemplo. O número 509 é primo ou composto?

Como $22 \leq \sqrt{509} < 23$, os primos que não excedem $\sqrt{509}$ são $2, 3, 5, 7, 11, 13, 17$ e 19 e como 509 não é divisível por nenhum deles, segue que 509 é primo.