CAPÍTULO 4

DIVISIBILIDADE

4.1 RELAÇÃO DE DIVISIBILIDADE EM Z

Definição 4.1 Sejam a e b dois inteiros, com $a \neq 0$. Diz-se que a *divide* b se e somente se existe um inteiro q tal que $b = aq$.

Se a *divide* 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.

Com a notação "$a|b$" indica-se que $a \neq 0$ *divide* b e, portanto, a notação "$a \nmid b$" significa que $a \neq 0$ *não divide* b.

A relação "a divide b ($a|b$)" denomina-se *relação de divisibilidade em Z*.

Se a é um *divisor* de b, então $-a$ também é um *divisor* de b, porque a igualdade $b = aq$ implica $b = (-a)(-q)$, de modo que os *divisores* de um inteiro qualquer são dois a dois iguais em valor absoluto e de sinais opostos (simétricos).

Assim, p.ex.:

$2|6$, porque $6 = 2.3$

$-5|30$, porque $30 = (-5)(-6)$

$7|-21$, porque $-21 = 7(-3)$

$3 \nmid 10$, porque não existe $q \in Z$ tal que $10 = 3z$

Teorema 4.1 Quaisquer que sejam os inteiros *a*, *b* e *c*, tem se:

(1) $a|0$, $1|a$ e $a|a$

(2) Se $a|1$, então $a = \pm 1$

(3) Se $a|b$ e se $c|d$, então $ac|bd$

(4) Se $a|b$ e se $b|c$, então $a|c$

(5) Se $a|b$ e se $b|a$, então $a = \pm b$

(6) Se $a|b$, com $b \neq 0$, então $|a| \leq |b|$

(7) Se $a|b$ e se $a|c$, então $a|(bx+cy)$, $\forall\, x,y \in Z$

Demonstração:

(1) Com efeito:

$$0 = a.0, \quad a = 1.a, \quad a = a.1$$

(2) Com efeito, se $a|1$, então $1 = aq$, com $q \in Z$, o que

implica $a = 1$ e $q = 1$ ou $a = -1$ e $q = -1$, isto é: $a = \pm 1$.

(3) Com efeito:

$$a|b \Longrightarrow b = aq, \quad \text{com} \quad q \in Z$$

$$c|d \Longrightarrow d = cq_1, \quad \text{com} \quad q_1 \in Z$$

Portanto:

$$bd = (ac)(qq_1) \Longrightarrow ac|bd$$

(4) Com efeito:

$$a|b \Longrightarrow b = aq, \quad \text{com} \quad q \in Z$$

$$b|c \Longrightarrow c = bq_1, \quad \text{com} \quad q_1 \in Z$$

Portanto:

$$c = a(qq_1) \Longrightarrow a|c$$

(5) Com efeito:

$$a|b \Longrightarrow b = aq, \quad \text{com} \quad q \in Z$$

$$b|a \Longrightarrow a = bq_1, \quad \text{com} \quad q_1 \in Z$$

Portanto:

$$a = a(qq_1) \Longrightarrow qq_1 = 1 \Longrightarrow q_1 | 1$$

$$\Longrightarrow q_1 = \pm 1 \Longrightarrow a = \pm b$$

(6) Com efeito:

$$a|b,\ b \neq 0 \Longrightarrow b = aq,\quad q \neq 0 \qquad |b| = |a|\,|q|$$

Como $q \neq 0$, segue-se que $|q| \geq 1$ e, portanto:

$$|b| \geq |a|$$

(7) Com efeito:

$$a|b \Longrightarrow b = aq, \quad \text{com } q \in Z$$

$$a|c \Longrightarrow c = aq_1, \quad \text{com } q_1 \in Z$$

Portanto, quaisquer que sejam os inteiros x e y:

$$bx+cy = aqx+aq_1y = a(qx+q_1y) \Longrightarrow a|(bx+cy)$$

Esta propriedade (7) admite uma óbvia generalização; isto é, se

$$a|b_k, \quad \text{para } k = 1, 2, \ldots, n$$

então, quaisquer que sejam os inteiros

$$x_1, x_2, \ldots, x_n:$$

$$a|(b_1x_1 + b_2x_2 + \ldots + b_nx_n)$$

Consoante as propriedades (1) e (4), a relação de divisibilidade Z é *reflexiva* e *transitiva*, mas *não é simétrica*, porque, p.ex., $3|6$ e $6 \nmid 3$.

4.2 CONJUNTO DOS DIVISORES DE UM INTEIRO

O conjunto de todos os *divisores* de um inteiro qualquer a indica-se por D(a), isto é:

$$D(a) = \{x \in Z^* \mid x|a\}$$

onde Z^* denota o conjunto dos inteiros *não nulos* ($\neq 0$).

Assim, p.ex.:

$$D(0) = \{x \in Z^* \mid x|0\} = Z^*$$

$$D(1) = \{x \in Z^* \mid x|1\} = \{-1, 1\}$$

$$D(2) = \{x \in Z^* \mid x|2\} = \{\pm 1, \pm 2\}$$

$$D(-8) = \{x \in Z^* \mid x|-8\} = \{\pm 1, \pm 2, \pm 4, \pm 8\}$$

É imediato que, para todo inteiro $\underline{a}$, se tem $D(a) = D(-a)$, e como

$$a = a.1 = (-a).(-1)$$

segue-se que 1, -1, $\underline{a}$ e $-\underline{a}$ são *divisores* de $\underline{a}$, denominados *divisores triviais* de $\underline{a}$. Em particular, o inteiro 1 (ou -1) só admite *divisores triviais*.

Qualquer que seja o inteiro $a \neq 0$, se $x|a$, então:

$$-a \leqslant x \leqslant a \Longrightarrow D(a) \subset [-a, a]$$

e isto significa que qualquer inteiro $a \neq 0$ tem um número *finito* de divisores.

4.3 DIVISORES COMUNS DE DOIS INTEIROS

Definição 4.2 Chama-se *divisor comum* de dois inteiros $\underline{a}$ e $\underline{b}$ todo inteiro $d \neq 0$ tal que $d|a$ e $d|b$.

Em outros termos, *divisor comum* de dois inteiros a e b é todo inteiro $d \neq 0$ que pertence simultaneamente aos conjuntos D(a) e D(b).

O conjunto de todos os *divisores comuns* a dois inteiros a e b indica-se por D(a,b). Portanto, simbolicamente:

$$D(a,b) = \{x \in Z^* \mid x|a \quad e \quad x|b\}$$

ou seja:

$$D(a,b) = \{x \in Z^* \mid x \in D(a) \quad e \quad x \in D(b)\}$$

e, portanto:

$$D(a,b) = D(a) \cap D(b)$$

A *interseção* ($\cap$) é uma *operação comutativa*, de modo que D(a,b) não depende da *ordem* dos inteiros dados a e b, isto é: $D(a,b) = D(b,a)$.

Como -1 e 1 são *divisores comuns* de dois inteiros quaisquer a e b, segue-se que o conjunto D(a,b) dos *divisores comuns* de a e b *nunca é vazio*: $D(a,b) \neq \phi$. Em particular, se $a = b = 0$, então todo inteiro não nulo é um *divisor comum* de a e b, isto é: $D(a,b) = Z^*$.

Exemplo 4.1 Sejam os inteiros $a = 12$ e $b = -15$. Temos:

$$D(12) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$$

$$D(-15) = \{\pm 1, \pm 3, \pm 5, \pm 15\}$$

Portanto:

$$D(12,-15) = D(12) \cap D(-15) = \{\pm 1, \pm 3\}$$

4.4 ALGORITMO DA DIVISÃO

Teorema 4.2 Se a e b são dois inteiros, com $b > 0$, então *existem* e são *únicos* os inteiros q e r que satisfazem às condições:

$$a = bq + r \quad e \quad 0 \leq r < b$$

Demonstração:

Seja S o conjunto de todos os inteiros não negativos (≥ 0) que são da forma $a - bx$, com $x \in Z$, isto é:

$$S = \{a - bx \mid x \in Z,\ a - bx \geq 0\}$$

Este conjunto S não é vazio ($S \neq \phi$), porque, sendo $b > 0$, temos $b \geq 1$ e, portanto, para $x = -|a|$, resulta:

$$a - bx = a + b|a| \geq a + |a| \geq 0$$

Assim sendo, pelo *"Princípio da boa ordenação"*, existe o *elemento mínimo* r de S tal que

$$r \geq 0 \quad e \quad r = a - bq \quad ou \quad a = bq + r, \quad com \quad q \in Z$$

Além disso, temos $r < b$, pois, se fosse $r \geq b$, teríamos:

$$0 \leq r - b = a - bq - b = a - b(q + 1) < r$$

isto é, r não seria o *elemento mínimo* de S.

Para demonstrar a *unicidade* de q e r, suponhamos que *existem* dois outros inteiros q_1 e r_1 tais que

$$a = bq_1 + r_1 \quad e \quad 0 \leq r_1 < b$$

Então, teremos:

$$bq_1 + r_1 = bq + r \Longrightarrow r_1 - r = (q - q_1)b \Longrightarrow b \mid (r_1 - r)$$

Por outro lado, temos:

$$-b < -r \leq 0 \quad e \quad 0 \leq r_1 < b$$

o que implica:

$$-b < r_1 - r < b, \text{ isto é: } \quad |r_1 - r| < b$$

Assim, $b \mid (r_1 - r)$ e $|r_1 - r| < b$ e, portanto: $r_1 - r = 0$, e como $b \neq 0$, também temos $q - q_1 = 0$. Logo, $r_1 = r$ e $q_1 = q$.

Corolário 4.1 Se a e b são dois inteiros, com $b \neq 0$, *existem* e são *únicos* os inteiros q e r que satisfazem as condições:

$$a = bq + r \quad e \quad 0 \leq r < |b|$$

Demonstração:

Com efeito, se $b > 0$, nada há que demonstrar, e se $b < 0$, então $|b| > 0$, e por conseguinte *existem* e são *únicos* os inteiros q_1 e $\underline{r}$ tais que

$$a = |b|q_1 + r \quad e \quad 0 \leqslant r < |b|$$

ou seja, por ser $|b| = -b$:

$$a = b(-q_1) + r \quad e \quad 0 \leqslant r < |b|$$

Portanto, *existem* e são *únicos* os inteiros $q = -q_1$ e $\underline{r}$ tais que

$$a = bq + r \quad e \quad 0 \leqslant r < |b|$$

Os inteiros $\underline{q}$ e $\underline{r}$ chamam-se respectivamente o *quociente* e o *resto* na divisão de $\underline{a}$ por $\underline{b}$.

Observe-se que $\underline{b}$ é *divisor* de $\underline{a}$ se e somente se o *resto* $r = 0$. Neste caso, temos $a = bq$ e o *quociente* $\underline{q}$ na divisão exata de $\underline{a}$ por $\underline{b}$ indica-se também por $\frac{a}{b}$ ou

$$a/b \quad (q = \frac{a}{b} = a/b),$$

que se lê "a sobre b".

Exemplo 4.2 Achar o *quociente* $\underline{q}$ e o *resto* $\underline{r}$ na divisão de $a = 59$ por $b = -14$ que satisfazem às condições do *algoritmo da divisão*.

Efetuando a divisão usual dos *valores absolutos* de $\underline{a}$ e $\underline{b}$, obtemos:

$$59 = 14.4 + 3$$

o que implica:

$$59 = (-14)(-4) + 3 \quad e \quad 0 \leqslant 3 < |-14|$$

Logo, o *quociente* $q = -4$ e o *resto* $r = 3$.

Exemplo 4.3 Achar o *quociente* $\underline{q}$ e o *resto* $\underline{r}$ na divisão de $a = -79$ por $b = 11$ que satisfazem às condições do *algoritmo da divisão*.

Efetuando a divisão usual dos *valores absolutos* de $\underline{a}$ e $\underline{b}$, obtemos:

$$79 = 11.7 + 2$$

o que implica:

$$-79 = 11(-7) - 2$$

Como o termo $r = -2 < 0$ não satisfaz à condição $0 \leqslant r < 11$, somando e subtraindo o valor 11 de $\underline{b}$ ao segundo membro da igualdade anterior, obtemos:

$$-79 = 11(-7) - 11 + 11 - 2 = 11(-8) + 9$$

com $0 \leqslant 9 < 11$. Logo, o *quociente* $q = -8$ e o *resto* $r = 9$.

Exemplo 4.4 Sejam os inteiros $a = 1, -2, 61, -59$ e $b = -7$. Temos:

$$1 = (-7).0 + 1 \quad e \quad 0 \leqslant 1 < |-7| \implies q = 0 \text{ e } r = 1$$

$$-2 = (-7).1 + 5 \quad e \quad 0 \leqslant 5 < |-7| \implies q = 1 \text{ e } r = 5$$

$$61 = (-7)(-8) + 5 \quad e \quad 0 \leqslant 5 < |-7| \Longrightarrow q = -8 \ e \ r = 5$$

$$-59 = (-7).9 + 4 \quad e \quad 0 \leqslant 4 < |-7| \Longrightarrow q = 9 \quad e \quad r = 4$$

4.5 PARIDADE DE UM INTEIRO

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

Observe-se que

$$a^2 = (2q)^2 = 4q^2 \quad ou \quad a^2 = 4(q^2 + q) + 1$$

de modo que na divisão do quadrado a^2 de um inteiro qualquer $\underline{a}$ por 4 o *resto* é 0 ou 1.

Exemplo 4.5 Mostrar que o *quadrado* de qualquer inteiro *ímpar* é da forma $8k + 1$.

Com efeito, pelo algorítmo da divisão, qualquer inteiro é de uma das seguintes formas:

$$4q, \ 4q+1, \ 4q + 2, \ 4q + 3$$

Nesta classificação, somente os inteiros das formas $4q+1$ e $4q+3$ são *ímpares* e, portanto, os seus *quadrados* são da forma:

$$(4q+1)^2 = 8(2q^2 + q) + 1 = 8k + 1$$

$$(4q+3)^2 = 8(2q^2 + 3q + 1) + 1 = 8k + 1$$

Assim, p.ex., 7 e 13 são inteiros *ímpares*, e temos:

$$7^2 = 49 = 8.6 + 1$$

$$13^2 = 169 = 8.21 + 1$$

EXERCÍCIOS

1. Mostrar que, se $a|b$, então $(-a)|b$, $a|(-b)$ e $(-a)|(-b)$.

2. Sejam <u>a</u>, <u>b</u> e <u>c</u> inteiros. Mostrar:

   (a) se $a|b$, então $a|bc$

   (b) se $a|b$ e se $a|c$, então $a^2|bc$

   (c) $a|b$ se e somente se $ac|bc$ $(c \neq 0)$

3. Verdadeiro ou falso:
   se $a|(b+c)$, então $a|b$ ou $a|c$.

4. Mostrar que, se <u>a</u> é um inteiro qualquer, então um dos inteiros: a, $a+2$, $a+4$ é divisível por 3.

5. Sendo <u>a</u> um inteiro qualquer, mostrar:

   (a) $2|a(a+1)$ (b) $3|a(a+1)(a+2)$

6. Mostrar que um inteiro qualquer da forma $6k+5$ também é da forma $3k+2$.

7. Mostrar que todo inteiro *ímpar* é da forma $4k+1$ ou $4k+3$.

8. Mostrar que o *quadrado* de um inteiro qualquer é da forma $3k$ ou $3k+1$.

9. Mostrar que o *cubo* de um inteiro qualquer é de uma das formas: $9k$, $9k+1$ ou $9k+8$.

10. Mostrar que $n(n+1)(2n+1)/6$ é um inteiro, qualquer que seja o inteiro positivo n.

11. Mostrar que, se $a \mid (2x - 3y)$ e se $a \mid (4x - 5y)$, então $a \mid y$.

12. Sendo a e b dois inteiros quaisquer, mostrar que os inteiros a e $a+2b$ têm sempre a mesma *paridade*.

13. Sendo m e n dois inteiros quaisquer, mostrar que os inteiros $m+n$ e $m-n$ têm sempre a mesma *paridade*.

14. Determinar os inteiros positivos que divididos por 17 deixam um resto igual ao quadrado do quociente.

15. Achar inteiros a, b e c tais que $a \mid bc$, mas $a \nmid b$ e $a \nmid c$.

16. Verdadeiro ou falso: se $a \mid c$ e se $b \mid c$, então $a \mid b$.

17. Demonstrar:

(a) Se a é um inteiro *ímpar*, então $24 \mid a(a^2 - 1)$.

(b) Se a e b são inteiros *ímpares*, então $8 \mid (a^2 - b^2)$.

18. Mostrar que a diferença entre os cubos de dois inteiros consecutivos nunca é divisível por 2.

19. Na divisão do inteiro $a = 427$ por um inteiro positivo $\underline{b}$ o *quociente* é 12 e o *resto* é $\underline{r}$. Achar o *divisor* $\underline{b}$ e o *resto* $\underline{r}$.

20. Na divisão do inteiro 525 por um inteiro positivo o *resto* é 27. Achar os inteiros que podem ser o *divisor* e o *quociente*.

21. Na divisão de dois inteiros positivos o *quociente* é 16 e o *resto* é o *maior possível*. Achar os dois inteiros, sabendo que a sua soma é 341.

22. Achar os inteiros positivos menores que 150 e que divididos por 39 deixam um resto igual ao quociente.

23. Seja $\underline{d}$ um divisor de $n(d|n)$. Mostrar que $cd|n$ se e somente se $c|(n/d)$.

24. Sejam $\underline{n}$, $\underline{r}$ e $\underline{s}$ inteiros tais que $0 \leqslant r < n$ e $0 \leqslant s < n$. Mostrar que, se $n|(r - s)$, então $r = s$.

25. Mostrar que o produto de dois inteiros *ímpares* é um inteiro *ímpar*.

26. Demonstrar que, se $\underline{m}$ e $\underline{n}$ são inteiros ímpares, então $8|(m^4 + n^4 - 2)$.

27. Demonstrar que $30|(n^5 - n)$.

28. Mostrar que, para todo inteiro $\underline{n}$, existem inteiros $\underline{k}$ e $\underline{r}$ tais que

$$n = 3k+r \quad e \quad r = -1,0,1$$

29. Mostrar que

$$(1 + 2 + \ldots + n) \mid 3(1^2 + 2^2 + \ldots + n^2)$$

para todo $n \geqslant 1$.

30. Mostrar que todo inteiro ímpar, quadrado perfeito, é da forma $4n+1$.

31. Na divisão de 392 por 45, determinar:
   (a) o maior inteiro que se pode somar ao dividendo sem alterar o quociente;
   (b) o maior inteiro que se pode subtrair do dividendo sem alterar o quociente.

32. Numa divisão de dois inteiros, o quociente é 16 e o resto é 167. Determinar o maior inteiro que se pode somar ao dividendo e ao divisor sem alterar o quociente.

33. Achar o maior inteiro de quatro algarismos divisível por 13 e o menor inteiro de cinco algarismos divisível por 15.

34. Achar um inteiro de quatro algarismos, quadrado perfeito, divisível por 27 e terminado em 6.

CAPÍTULO 5

MÁXIMO DIVISOR COMUM

5.1 MÁXIMO DIVISOR COMUM DE DOIS INTEIROS

<u>Definição 5.1</u> Sejam a e b dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$). Chama-se *máximo divisor comum* de a e b o inteiro *positivo* d ($d > 0$) que satisfaz às condições:

(1) $d \mid a$ e $d \mid b$

(2) se $c \mid a$ e se $c \mid b$, então $c \leqslant d$.

Observe-se que, pela condição (1), d é um *divisor comum* de a e b, e pela condição (2), d é o *maior* dentre todos os divisores comuns de a e b.

O *máximo divisor comum* de a e b indica-se pela notação mdc(a,b).

É imediato que o 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 $\text{mdc}(a,0) = |a|$

(iv) se $a|b$, então o $\text{mdc}(a,b) = |a|$

Assim, p.ex.:

$\text{mdc}(8,1) = 1$, $\text{mdc}(-3,0) = |-3| = 3$

$\text{mdc}(-6,12) = |-6| = 6$

Exemplo 5.1 Sejam os inteiros $a = 16$ e $b = 24$. Os *divisores comuns positivos* de 16 e 24 são 1, 2, 4 e 8, e como o *maior* deles é 8, segue-se que o $\text{mdc}(16,24) = 8$.

Observe-se que

$$\text{mdc}(-16,24) = \text{mdc}(16,-24) = \text{mdc}(-16,-24) = 8.$$

Exemplo 5.2 Sejam os inteiros $a = -24$ e $b = 60$. Os *divisores comuns positivos* de -24 e 60 são 1,2,3,4,6 e 12, e como o *maior* deles é 12, segue-se que o $\text{mdc}(-24,60) = 12$.

5.2 EXISTÊNCIA E UNICIDADE DO MDC

Teorema 5.1 Se a e b são dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$), 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.

Demonstração:

Seja S o conjunto de todos os inteiros *positivos* da forma $au + bv$, com $u, v \in Z$, isto é:

$$S = \{ au + bv \mid au + bv > 0 \ \text{ e } \ u, v \in Z \}$$

Este conjunto S *não é vazio* ($S \neq \phi$), porque, p.ex., se $a \neq 0$, então um dos dois inteiros:

$$a = a.1 + b.0 \quad \text{ e } \quad -a = a.(-1) + b.0$$

é *positivo* e pertence a S. Logo, pelo *"Princípio da boa ordenação"*, *existe* e é *único* o *elemento mínimo* d de S: $\min S = d > 0$. E, consoante a definição de S, *existem* inteiros x e y tais que $d = ax + by$.

Posto isto, vamos mostrar que $d = mdc(a,b)$. Com efeito, pelo *algoritmo da divisão*, temos:

$$a = dq + r, \quad \text{com} \quad 0 \leqslant r < d$$

o que dá:

$$r = a - dq = a - (ax + by)q = a(1 - qx) + b(-qy)$$

isto é, o *resto* r é uma *combinação linear* de a e b. Como $0 \leqslant r < d$ e $d > 0$ é o *elemento mínimo* de S, segue-se que $r = 0$ e $a = dq$, isto é, $d \mid a$.

Com raciocínio inteiramente análogo se conclui que também $d \mid b$. Logo, d é um *divisor comum positivo* de a e b.

Finalmente, se c é um *divisor comum positivo* qualquer de a e b ($c|a$ e $c|b$, $c > 0$), então:

$$c|(ax + by) \Longrightarrow c|d \Longrightarrow c \leqslant d$$

isto é, d é o *maior divisor comum positivo* de a e b, ou seja:

$$\text{mdc}(a,b) = d = ax + by, \quad x,y \in Z$$

e o teorema fica demonstrado.

NOTA. A demonstração do teorema 5.1 deixa ver que 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* do mdc(a,b) como *combinação linear* de a e b *não é única*, pois, temos:

$$\text{mdc}(a,b) = d = a(x + bt) + b(y - at)$$

qualquer que seja o inteiro t.

Importa ainda notar que, se

$$d = ar + bs$$

para algum par de inteiros r e s, então d não é necessariamente o mdc(a,b). Assim, p.ex., se:

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

então

$$t.\text{mdc}(a,b) = atx + bty$$

para todo inteiro t, isto é:

$$d = ar + bs$$

onde $d = t.\mathrm{mdc}(a,b)$, $r = tx$ e $s = ty$.

Exemplo 5.3 Sejam os inteiros $a = 6$ e $b = 27$. Temos:

$$\mathrm{mdc}(6,27) = 3 = 6\underbrace{(-4)}_{x} + 27.\underbrace{1}_{y}$$

e, portanto:

$d = a(x + bt) + b(y - at)$

$$\mathrm{mdc}(6,27) = 3 = 6(-4 + 27t) + 27(1 - 6t)$$

qualquer que seja o inteiro t.

Exemplo 5.4 Sejam os inteiros $a = -8$ e $b = -36$. Temos:

$$\mathrm{mdc}(-8,-36) = 4 = \underbrace{\overset{a}{(-8)}\overset{x}{4}}_{-32} + \underbrace{\overset{b}{(-36)}\overset{y}{(-1)}}_{+36}$$

Teorema 5.2 Se a e b são dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$), então o conjunto de todos os *múltiplos* do $\mathrm{mdc}(a,b) = d$ é

$$T = \{ax + by \mid x,y \in \mathbb{Z}\}$$

Demonstração:

Como $d|a$ e $d|b$, segue-se que $d|(ax + by)$, quaisquer que sejam os inteiros x e y, e por conseguinte todo elemento do conjunto T é um *múltiplo* de d.

Por outro lado, existem inteiros x_o e y_o tais que

$$d = ax_o + by_o,$$

de modo que todo *múltiplo* kd de d é da forma:

$$kd = k(ax_o + by_o) = a(kx_o) + b(ky_o)$$

isto é, kd é uma *combinação linear* de a e b e, portanto, kd é elemento do conjunto T.

5.3 INTEIROS PRIMOS ENTRE SI

Definição 5.2 Sejam a e b dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$). Diz-se que a e b são *primos entre si* se e somente se o $mdc(a,b) = 1$.

Assim, p.ex., são *primos entre si* os inteiros: 2 e 5, -9 e 16, -27 e -35, pois, temos:

$$mdc(2,5) = mdc(-9,16) = mdc(-27, -35) = 1$$

Dois inteiros a e b *primos entre si* admitem como *únicos divisores comuns* 1 e -1.

Teorema 5.3 Dois inteiros a e b, 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 $ax + by = 1$.

Demonstração:

($\Longrightarrow$) Se a e b são *primos entre si*, então o mdc(a,b) = = 1 e por conseguinte existem inteiros x e y tais que

$$ax + by = 1.$$

($\Longleftarrow$) Reciprocamente, se existem inteiros x e y tais que $ax + by = 1$ e se o mdc(a,b) = d, então $d \mid a$ e $d \mid b$. Logo, $d \mid (ax + by)$ e $d \mid 1$, o que implica $d = 1$ ou mdc(a,b) = 1, isto é, a e b são *primos entre si*.

Corolário 5.1 Se o mdc(a,b) = d, então o mdc(a/d, b/d) = = 1.

Demonstração:

Preliminarmente, observe-se que a/d e b/d são *inteiros*, porque d é um *divisor comum* de a e b.

Posto isto, se o mdc(a,b) = d, então existem inteiros x e y tais que $ax + by = d$, ou seja, dividindo ambos os membros desta igualdade por d:

$$(a/d)x + (b/d)y = 1$$

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

Assim, p.ex.:

$$\text{mdc}(-12,30) = 6 \quad \text{e} \quad \text{mdc}(-12/6,\ 30/6) = \text{mdc}(-2,5) = 1$$

<u>Corolário 5.2</u> Se $a|b$ e se o $mdc(b,c) = 1$, então o $mdc(a,c) = 1$.

<u>Demonstração:</u>

Com efeito:

$$a|b \Longrightarrow b = aq, \quad \text{com} \quad q \in Z$$

$$mdc(b,c) = 1 \Longrightarrow bx + cy = 1, \text{ com } \quad x,y \in Z$$

Portanto:

$$a(qx) + cy = 1 \Longrightarrow mdc(a,c) = 1$$

<u>Corolário 5.3</u> Se $a|c$, se $b|c$ e se o $mdc(a,b) = 1$, então $ab|c$.

<u>Demonstração:</u>

Com efeito:

$$a|c \Longrightarrow c = aq_1, \quad \text{com} \quad q_1 \in Z$$

$$b|c \Longrightarrow c = bq_2, \quad \text{com} \quad q_2 \in Z$$

$$mdc(a,b) = 1 \Longrightarrow ax + by = 1, \quad \text{com} \quad x,y \in Z$$

$$\Longrightarrow acx + bcy = c$$

Portanto:

$$c = a(bq_2)x + b(aq_1)y = ab(q_2x + q_1y) \Longrightarrow ab|c$$

Observe-se que somente as condiçoes $a|c$ e $b|c$ não implicam $ab|c$.

Assim, p.ex., $6|24$ e $8|24$, mas $6.8 \nmid 24$ (o modc$(6,8) =$ $= 2 \neq 1)$.

<u>Corolário 5.4</u> Se $\text{mdc}(a,b) = 1 = \text{mdc}(a,c)$, então o $\text{mdc}(a,bc) = 1$.

<u>Demonstração:</u>

Com efeito:

$$\text{mdc}(a,b) = 1 \Longrightarrow ax + by = 1, \text{ com } x,y \in Z$$

$$\text{mdc}(a,c) = 1 \Longrightarrow az + ct = 1, \text{ com } z,t \in Z$$

Portanto:

$$1 = ax + by(az + ct) = a(x + byz) + bc(yt)$$

o que implica $\text{mdc}(a,bc) = 1$.

<u>Corolário 5.5</u> Se o $\text{mdc}(a,bc) = 1$, então $\text{mdc}(a,b) = 1 = \text{mdc}(a,c)$.

<u>Demonstração:</u>

Com efeito:

$$\text{mdc}(a,bc) = 1 \Longrightarrow ax + (bc)y = 1, \text{ com } x,y \in Z$$

Portanto:

$$ax + b(cy) = 1 \Longrightarrow \text{mdc}(a,b) = 1$$

$$ax + c(by) = 1 \Longrightarrow \text{mdc}(a,c) = 1$$

Note-se que esta proposição é a *recíproca* da anterior.

Teorema 5.4 (de EUCLIDES) Se $a|bc$ e se o $mdc(a,b) = 1$, então $a|c$.

Demonstração:

Com efeito:

$$a|bc \Longrightarrow bc = aq, \quad \text{com } q \in Z$$
$$mdc(a,b) = 1 \Longrightarrow ax + by = 1, \quad \text{com } x,y \in Z$$
$$\Longrightarrow acx + bcy = c$$

Portanto:

$$c = acx + aqy = a(cx + qy) \Longrightarrow a|c$$

Note-se que somente a condição $a|bc$ não implica que $a|c$. Assim, p.ex., $12|9.8$, mas $12 \nmid 9$ e $12 \nmid 8$ $mdc(12,9) \neq 1$ e $mdc(12,8) \neq 1$).

5.4 CARACTERIZAÇÃO DO MDC DE DOIS INTEIROS

Teorema 5.5 Sejam $\underline{a}$ e $\underline{b}$ dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$). Um inteiro *poditivo* $\underline{d}$ ($d > 0$) é o $mdc(a,b)$ se e somente se satisfaz às condições:

(1) $d|a$ e $d|b$

(2) se $c|a$ e se $c|b$, então $c|d$

Demonstração:

($\Longrightarrow$) Suponhamos que o mdc(a,b) = d. Então, $d \mid a$ e $d \mid b$, isto é, a condição (1) é satisfeita. Por outra parte, existem inteiros x e y tais que $ax + by = d$ e, portanto, se $c \mid a$ e se $c \mid b$, então $c \mid (ax + by)$ e $c \mid d$, isto é, a condição (2) também é satisfeita.

($\Longrightarrow$) Reciprocamente, seja d um inteiro positivo qualquer que satisfaz às condições (1) e (2). Então, pela condição (2), todo divisor comum c de a e b também é divisor de d, isto é, $c \mid d$, e isto implica $c \leqslant d$. Logo, d é o mdc(a,b).

5.5 MDC DE VÁRIOS INTEIROS

O conceito de *máximo divisor comum*, definido para dois inteiros a e b, estende-se de maneira natural a mais de dois inteiros. No caso de três inteiros a, b e c, não todos nulos, o mdc(a,b,c) é o inteiro *positivo* d ($d > 0$) que satisfaz às condições:

(1) $d \mid a$, $d \mid b$ e $d \mid c$

(2) se $e \mid a$, se $e \mid b$ e se $e \mid c$, então $e \leqslant d$

Assim, p.ex.:

mdc(39,42,54) = 3 e mdc(49,210,350) = 7

Importa notar que três inteiros $\underline{a}$, $\underline{b}$ e $\underline{c}$ podem ser *primos entre si*, isto é, o mdc(a,b,c) = 1, sem que sejam *primos entre si dois a dois*, que é o caso, p.ex., dos inteiros 6, 10 e 15.

<u>Teorema 5.6</u> O mdc(a,b,c) = mdc(mdc(a,b),c).

<u>Demonstração:</u>

Com efeito, seja mdc(a,b,c) = d e mdc(a,b) = e. Então, $d|a$, $d|b$ e $d|c$, e como existem inteiros $\underline{x}$ e $\underline{y}$ tais que $ax + by = e$, segue-se que $d|(ax + by)$ ou $d|e$, isto é, $\underline{d}$ é um *divisor comum* de $\underline{e}$ e $\underline{c}$ ($d|e$ e $d|c$).

Por outro lado, se $\underline{f}$ e um *divisor comum* qualquer de $\underline{e}$ e $\underline{c}$ ($f|e$ e $f|c$), então $f|a$, $f|b$ e $f|c$, o que implica $f \leqslant d$. Assim sendo, o mdc(e,c) = d, isto é, o

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

<u>Exemplo 5.5</u> Determinar o mdc(570, 810, 495).

Pelo teorema anterior, temos:

$$\text{mdc}(570,810,495) = \text{mdc}(\text{mdc}(570,810),495)$$

e como o mdc(570,810) = 30, segue-se que o

$$\text{mdc}(570,810,495) = \text{mdc}(30,495) = 15$$

EXERCÍCIOS

1. Determinar:

   (a) mdc(11, 99)

   (b) mdc(-21,14) (c) mdc(17,18)

2. Achar os elementos do conjunto $\{1,2,3,4,5\}$ que são *primos* com 8.

3. Seja o conjunto $A = \{1,2,3,4,5,6\}$. Enumerar os elementos do conjunto:

$$X = \{x \in A \mid \text{mdc}(x,6) = 1\}$$

4. Sabendo que o mdc(a,0) = 13, achar os valores do inteiro a.

5. Achar o *menor* inteiro positivo c da forma

$$c = 22x + 55y,$$

   onde x e y são dois inteiros.

6. Sendo n um inteiro qualquer, calcular o mdc(n, n+1).

7. Calcular:

   (a) mdc(n, n+2), sendo n um inteiro *par;*

   (b) mdc(n, n+2), sendo n um inteiro *ímpar.*

8. Sendo $\underline{n}$ um inteiro qualquer, achar os possíveis valores do máximo divisor comum dos inteiros $\underline{n}$ e $\underline{n+10}$.

9. Sendo $\underline{n}$ um inteiro qualquer, calcular o

$$\mathrm{mdc}(n-1,\ n^2 + n + 1).$$

10. Sendo $\underline{a}$ e $\underline{b}$ dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$), mostrar:

$$\mathrm{mdc}(a,b) = \mathrm{mdc}(-a,b) = \mathrm{mdc}(a,-b) = \mathrm{mdc}(-a,-b)$$

11. Sejam $\underline{a}$, $\underline{b}$ e $\underline{c}$ inteiros. Demonstrar:

(a) existem inteiros $\underline{x}$ e $\underline{y}$ tais que $c = ax + by$ se e somente se o $\mathrm{mdc}(a,b) \mid c$;

(b) se existem inteiros $\underline{x}$ e $\underline{y}$ tais que $ax+by=\mathrm{mdc}(a,b)$, então o $\mathrm{mdc}(x,y) = 1$.

12. Sejam $\underline{a}$, $\underline{b}$ e $\underline{c}$ inteiros. Demonstrar:

(a) Se o $\mathrm{mdc}(a,b) = 1$, então o $\mathrm{mdc}(ac,b) = \mathrm{mdc}(b,c)$.

(b) Se o $\mathrm{mdc}(a,b) = 1$ e se $c \mid (a+b)$, então o $\mathrm{mdc}(a,c) = 1$ e o $\mathrm{mdc}(b,c) = 1$.

(c) Se $b \mid c$, então o $\mathrm{mdc}(a,b) = \mathrm{mdc}(a + c,\ b)$.

(d) Se o $\mathrm{mdc}(a,b) = 1$, então o $\mathrm{mdc}(a^m,b^n) = 1$, onde $\underline{m}$ e $\underline{n}$ são inteiros positivos.

13. Calcular o $\mathrm{mdc}(a+b,\ a-b)$, sabendo que $\underline{a}$ e $\underline{b}$ são inteiros *primos entre si*.

14. O mdc de dois inteiros positivos é 10 e o *maior* déles é 120. Determinar o outro inteiro.

15. Achar o *maior* inteiro positivo pelo qual se devem dividir os inteiros 160, 198 e 370 para que os *restos* sejam respectivamente 7, 11 e 13.

16. Determinar os inteiros positivos a e b sabendo:

(a) $a + b = 63$ e o $mdc(a,b) = 9$

(b) $ab = 756$ e o $mdc(a,b) = 6$

17. Os *restos* das divisões dos inteiros 4933 e 4435 por um inteiro positivo n são respectivamente 37 e 19. Achar o inteiro n.

18. Demonstrar que, se $n = abc + 1$, então o $mdc(n,a) = mdc(n,b) = mdc(n,c) = 1$.

19. Demonstrar que o $mdc(mdc(a,b),b) = mdc(a,b)$.

20. Demonstrar que o $mdc(n + k,k) = 1$ se e somente se o $mdc(n,k) = 1$.

21. Demonstrar que, se $a \mid bc$ e se o $mdc(a,b) = d$, então $a \mid cd$.

22. Demonstrar que, se $a \mid c$, se $b \mid c$ e se o $mdc(a,b) = d$, então $ab \mid cd$.

23. Demonstrar que, se o $mdc(a,b) = 1$ e se o $mdc(a,c) = d$, então $mdc(a,bc) = d$.

24. O inteiro ímpar d é um *divisor* de $a+b$ e de $a-b$. Demonstrar que d também é um *divisor* do $mdc(a,b)$.

25. Os inteiros positivos a, b e c são tais que o $mdc(a,b) = 1$, $a|c$ e $c|b$. Demonstrar que $a = 1$.

26. O $mdc(n,n + k) = 1$ para todo inteiro positivo n. Demonstrar que $k = 1$ ou $k = -1$.

27. Demonstrar que o $mdc(a,b) = mdc(a + kb,b)$ para todo inteiro k.

28. O $mdc(a,4) = 2 = mdc(b,4)$. Demonstrar que o $mdc(a + b,4) = 4$.

29. Os inteiros positivos m e n são tais que o $mdc(m,n) = d$. Mostrar que o $mdc(2^m - 1,2^n - 1) = 2^d - 1$.

30. Demonstrar que o $mdc(a,b) = mdc(a,b,a + b)$.

31. Demonstrar que o $mdc(a,b) = mdc(a,b,ax + by)$, quaisquer que sejam os inteiros x e y.

32. O $mdc(a,b) = p$, sendo p um *primo*. Achar os possíveis valores do:

(a) $mdc(a^2,b)$:

(b) $mdc(a^3,b)$; (c) $mdc(a^2,b^3)$.

33. Sabendo que o $mdc(a,p^2) = p$ e que o $mdc(b,p^3) = p^2$, onde p é um primo, calcular o $mdc(ab,p^4)$ e o $mdc(a + b,p^4)$.

34. Demonstrar que, se o $mdc(a,b) = d$, então o

$$mdc(a^2,b^2) = d^2.$$

35. Sejam $\underline{a}$ e $\underline{k}$ inteiros não conjuntamente nulos. Demonstrar que o $mdc(a, a+k) \mid k$.

36. Demonstrar que $mdc(a,b) = mdc(a,c)$ implica $mdc(a^2,b^2) = mdc(a^2,c^2)$.

37. Demonstrar que $mdc(a,b) = mdc(a,c)$ implica $mdc(a,b) = mdc(a,b,c)$.

38. Demonstrar que $mdc(a,b,c) = mdc(mdc(a,b), mdc(a,c))$.

39. Sejam $\underline{a}$ e $\underline{b}$ inteiros positivos tais que ab é um quadrado perfeito e o $mdc(a,b) = 1$. Demonstrar que $\underline{a}$ e $\underline{b}$ são quadrados perfeitos.

40. Demonstrar que o $mdc(a+b, a-b) \geqslant mdc(a,b)$.

41. Mostrar que o $mdc(5n+6, 5n+8) = 1$, onde $\underline{n}$ é um inteiro *ímpar*.

42. Sejam a, b, c, d $(b \neq d)$ inteiros tais que o $mdc(a,b) = mdc(c,d) = 1$. Mostrar que a soma $a/b + c/d$ não é um inteiro.

43. Determinar os inteiros positivos $\underline{a}$ e $\underline{b}$, sabendo:

$$a^2 - b^2 = 7344 \quad \text{e} \quad mdc(a,b) = 12.$$

44. Dividindo-se dois inteiros positivos pelo seu mdc, a soma dos quocientes obtidos é 8. Determinar os dois inteiros, sabendo que a sua soma é 384.