Divisores

Definição. Diremos que um número inteiro d é um divisor de outro inteiro a, se a é múltiplo de d; ou seja, se $a = d \times c$, para algum inteiro c.

Quando a é múltiplo de d dizemos também que a é divisível por d ou que d divide a.

Representaremos o fato de um número d ser divisor de um número a, ou d dividir a, pelo símbolo $d \mid a$. Caso d não divida a, escrevemos $d \nmid a$.

Assim, por exemplo, temos que

$$1 \mid 6,\ 2 \mid 6,\ 3 \mid 6,\ 6 \mid 6,\ -6 \mid 6,\ -3 \mid 6,\ -2 \mid 6,\ -1 \mid 6.$$

Além disso, se $d \nmid -6, -3, -2, -1, 1, 2, 3, 6$, então $d \nmid 6$.

Temos também que $1 \mid a$ e $d \mid 0$, para todo d, inclusive quando $d = 0$ pois 0 é múltiplo de qualquer número.

Note também que se $d \mid a$, então $-d \mid a$, $d \mid -a$ e $-d \mid -a$.

Note que se a e d são números naturais, com $a \neq 0$, e se $d \mid a$, então $d \leqslant a$. De fato, sendo a um múltiplo natural não nulo do número natural d, sabemos que $a \geqslant d$.

Algoritmo do mdc de Euclides

O Lema de Euclides: Dados inteiros a e b, os divisores comuns de a e b são os mesmos que os divisores comuns de a e $b - c \times a$, para todo número inteiro c fixado.

Demonstração. Se d é um divisor comum de a e b, é claro que d é divisor comum de a e de $b - c \times a$.

Reciprocamente, suponha que d seja divisor comum de a e de $b - c \times a$. Logo, d é divisor comum de $b - c \times a$ e de $c \times a$ e, portanto, tem-se que d é divisor de b. Assim, d é divisor comum de a e b.

O Lema de Euclides nos diz que os divisores de comuns de a e b são os mesmos divisores comuns de a e $b - a \times c$, logo tomando o maior divisor comum em ambos os casos, obtemos a fórmula:

$$mdc(a, b) = mdc(a, b - a \times c),$$

o que permite ir diminuindo passo a passo a complexidade do problema, até torná-lo trivial.

Algoritmo de Euclides para o cálculo do mdc

Nada melhor do que um exemplo para entender o método.

Vamos calcular $mdc(a, b)$, onde $a = 162$ e $b = 372$.

Pelo Lema de Euclides, sabemos que o mdc de a e b é o mesmo que o de a e de b menos um múltiplo qualquer de a. Otimizamos os cálculos ao tomarmos o menor dos números da forma b menos um múltiplo de a e isto é realizado pelo algoritmo da divisão:

$$372 = 162 \times 2 + 48.$$

Assim,

$$mdc(372, 162) = mdc(372 - 162 \times 2, 162) = mdc(48, 162).$$

Apliquemos o mesmo argumento ao par $a_1 = 48$ e $b_1 = 162$:

$$162 = 48 \times 3 + 18.$$

Assim,

$$\begin{aligned} mdc(372, 162) &= mdc(162, 48) \\ &= mdc(162 - 48 \times 3, 48) \\ &= mdc(18, 48). \end{aligned}$$

Apliquemos novamente o mesmo argumento ao par $a_2 = 18$ e $b_2 = 48$:

$$48 = 18 \times 2 + 12.$$

Assim,

$$mdc(372, 162) = mdc(48, 18) = mdc(48 - 8 \times 2, 18) = mdc(12, 18).$$

Novamente, o mesmo argumento para o par $a_3 = 18$ e $b_3 = 12$ nos dá:

$$18 = 12 \times 1 + 6.$$

Assim,

$$mdc(372, 162) = mdc(18, 12) = mdc(18 - 12 \times 1, 12) = mdc(6, 12).$$

Finalmente, obtemos

$$mdc(372, 162) = mdc(12, 6) = mdc(12 - 6 \times 2, 6) = mdc(0, 6) = 6.$$

Logo,

$$mdc(372, 162) = 6.$$

O procedimento acima pode ser sistematizado como segue:

	2	3	2	1	2
372	162	48	18	12	6=mdc
48	18	12	6	0	

O Algoritmo de Euclides usado de trás para frente nos dá uma informação adicional fundamental.

Das igualdades acima podemos escrever:

$$6 = 18 - 12 \times 1$$
$$12 = 48 - 18 \times 2$$
$$18 = 162 - 48 \times 3$$
$$48 = 372 - 162 \times 2$$

Donde,

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

Assim, podemos escrever:

$$6 = mdc(372, 162) = 162 \times 23 + 372 \times (-10).$$

Este método sempre se aplica conduzindo ao seguinte importante resultado:

Teorema 3.3 (Relação de Bézout). Dados inteiros a e b, quaisquer, mas não ambos nulos, existem dois inteiros n e m tais que

$$mdc(a, b) = a \times n + b \times m.$$

Exemplo 1. Determine $mdc(a, b)$, $mmc(a, b)$ e inteiros n e m tais que $mdc(a, b) = a \times n + b \times m$ para os seguintes pares de números a e b.

(a) $a = 728$ e $b = 1496$

Solução: $8 = 728 \times 37 + 1496 \times (-1)$.

(b) $a = 108$ e $b = 294$.

Solução: $6 = 108 \times (-15) + 294 \times 7$.

Cálculo do mdc: algoritmo de Euclides - parte 1

O Algoritmo de Euclides para o cálculo do mdc baseia-se na seguinte propriedade dos números naturais.

Propriedade: Sejam a e b números naturais com $a < b$.

(a) Se d é um divisor comum de a e b, então d também é um divisor de $b - a$

(b) Reciprocamente, se d é um divisor de a e de $b-a$, então d é um divisor de b.

Exemplos:

- É fácil ver que 84 e 35 são múltiplos de 7. Então $84+35=119$ e $84-35=49$ são múltiplos de 7.

- O número $d=4$ é um divisor de $a=20$ e de $b=48$, pois $20=4\times 5$ e $48=4\times 12$. Daí $d=4$ é um divisor de $b-a=28$, pois $b-a=(4\times 12)-(4\times 5)=4\times(12-5)=4\times 7$.

- Para entender o item (b) vamos considerar que a e $b-a$ são múltiplos de d. Como $b=a+(b-a)$ é uma soma de múltiplos de d, segue que b também é um múltiplo de d.

É importante observar que a propriedade anterior implica que os divisores comuns de a e b são iguais aos divisores comuns de a e $b-a$.

Exercício 1: Se $a=18$ e $b=60$ calcule os conjuntos $D(a)$, $D(b)$ e $D(b-a)$ dos divisores de a, de b e de $b-a$. Em seguida verifique que $D(a)\cap D(b)=D(a)\cap D(b-a)$.
Solução. $D(a)=\{1,2,3,6,9,18\}$ $D(b)=\{1,2,3,4,5,6,10,12,15,20,30,60\}$ $D(b-a)=\{1,2,3,6,7,14,21,42\}$. Calculando os divisores comuns:

$$D(a)\cap D(b)=\{1,2,3,6\}=D(a)\cap D(b-a)$$

.
As propriedades que acabamos de verificar implicam que os divisores comuns de a e b são iguais aos divisores comuns de a e $b-a$. Em particular, o maior divisor comum de a e b é igual ao maior divisor comum de a e $b-a$. Ou seja, acabamos de verificar a seguinte propriedade.

Propriedade: Se a e b são números naturais com $a<b$, então $mdc(a,b)=mdc(a,b-a)$. Como veremos logo abaixo, esta propriedade permite ir reduzindo sucessivamente o cálculo do mdc de dois números ao cálculo do mdc de números cada vez menores. E como a única conta que deve ser feita é uma subtração, este método é mais fácil de ser aplicado do que os métodos anteriores, quando tínhamos que fatorar os números dados.

Exercício 2: Calcule $mdc(18,60)$.

Solução.

$$mdc(18,60)=mdc(18,60-18)=mdc(18,42)=$$

$$mdc(18,42)=mdc(18,42-18)=mdc(18,24)=$$
$$mdc(18,24)=mdc(18,24-18)=mdc(18,6)=6.$$

Exercício 3: Tente calcular o $mdc(1203, 3099)$ usando uma fatoração simultânea e depois calcule este mdc usando a propriedade $mdc(a, b) = mdc(a, b-a)$.

Solução. Como $1203 = 3 \times 401$, $3099 = 3 \times 1033$, 401 e 1033 são números primos, aparentemente pode ser difícil obter as fatorações destes dois números. E se alguém ainda não achar este exemplo difícil, podemos facilmente dificultar mais, propondo exemplos com números cada vez maiores até convencer de que o cálculo do mdc por meio da propriedade $mdc(a, b) = mdc(a, b - a)$ sempre permite o cálculo do mdc, enquanto que para calcular o mdc via uma fatoração simultânea precisamos descobrir divisores primos dos números dados, e isto realmente pode ser uma tarefa muito complicada.
Utilizando sucessivamente a igualdade $mdc(a, b) = mdc(a, b - a)$, o cálculo do mdc desejado pode ser efetuado do seguinte modo.

$$mdc(1203, 3099) = mdc(1203, 3099 - 1203) = mdc(1203, 1896) =$$

$$mdc(1203, 1896) = mdc(1203, 1896 - 1203) = mdc(1203, 693) =$$

$$mdc(693, 1203) = mdc(693, 1203 - 693) = mdc(693, 510) =$$

$$mdc(510, 693) = mdc(510, 693 - 510) = mdc(510, 183) =$$

$$mdc(183, 510) = mdc(183, 510 - 183) = mdc(183, 327) =$$

$$mdc(183, 327) = mdc(183, 327 - 183) = mdc(183, 144) =$$

$$mdc(144, 183) = mdc(144, 183 - 144) = mdc(144, 39) = 3.$$

Veja que a propriedade $mdc(a, b) = mdc(a, b - a)$ permite mostrar que dois números consecutivos sempre são relativamente primos.
De fato, $mdc(n, n + 1) = mdc(n, n + 1 - n) = mdc(n, 1) = 1$.

Propriedade: Se $a < b$ são números naturais e se r é o resto da divisão de b por a, então $mdc(a, b) = mdc(a, r)$.

De modo alternativo, pelas propriedades aritméticas do resto de uma divisão, observe que se d é um divisor comum de a e b, então d é um divisor comum de a e $r = b - aq$. Assim, de fato, é posível mostrar que o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de a e $r = b - aq$, em que r é o resto da divisão de b por a. Verifique esta propriedade na solução do seguinte exercício.

Exercício 4: Se $a = 84$ e $b = 330$ calcule o resto r da divisão de b por a, calcule os conjuntos $D(a)$, $D(b)$ e $D(r)$ dos divisores de a, de b e de r, e verifique que $D(a) \cap D(b) = D(a) \cap D(r)$.

Solução. Dividindo b por a obtemos $330 = 3 \times 84 + 78$, de modo que $r = 78$ é o resto da divisão de b por a.

$$D(a) = \{1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84\}$$

$$D(b) = \{1, 2, 3, 5, 6, 10, 11, 15, 22, 30, 33, 55, 66, 110, 165, 330\}$$

$$D(r) = \{1, 2, 3, 6, 13, 26, 39, 78\}$$

Calculando os divisores comuns:

$$D(a) \cap D(b) = \{1, 2, 3, 6\} = D(a) \cap D(r)$$

. Daí, como o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de a e r, tomando o maior dos elementos, concluímos que $mdc(a, b) = mdc(a, r)$.

Exercício 5: Calcule $mdc(162, 372)$.

Solução.

- Dividindo 372 por 162 obtemos $372 = 2 \times 162 + 48$. Assim $mdc(162, 372) = mdc(162, 48)$.

- Dividindo 162 por 48 obtemos $162 = 3 \times 48 + 18$. Daí $mdc(48, 162) = mdc(48, 18)$.

- Dividindo 48 por 18 obtemos $48 = 2 \times 18 + 12$ e portanto $mdc(18, 48) = mdc(18, 12)$.

- Dividindo 18 por 12 obtemos $18 = 1 \times 12 + 6$ e assim $mdc(12, 18) = mdc(12, 6)$.

- Portanto $mdc(162, 372) = mdc(6, 12) = 6$.

Quando aplicamos apenas a propriedade $mdc(a, b) = mdc(a, b - a)$.

$$mdc(162, 372) = mdc(162, 372 - 162) = mdc(162, 210) =$$
$$mdc(162, 210) = mdc(162, 210 - 162) = mdc(162, 48) =$$
$$mdc(48, 162) = mdc(48, 168 - 48) = mdc(48, 114) =$$
$$mdc(48, 114) = mdc(48, 114 - 48) = mdc(48, 66) =$$
$$mdc(48, 66) = mdc(48, 66 - 48) = mdc(48, 18) =$$
$$mdc(18, 48) = mdc(18, 48 - 18) = mdc(18, 30) =$$
$$mdc(18, 30) = mdc(18, 30 - 18) = mdc(18, 12) =$$

$$mdc(12, 18) = mdc(12, 18 - 12) = mdc(12, 6) = 6.$$

Exercício 6: Calcule $mdc(2282, 7063)$. *Solução.*

Dividindo 7063 por 2282 obtemos $7063 = 3\times2282+217$. Assim $mdc(2282, 7063) = mdc(2282, 217)$.

Dividindo 2282 por 217 obtemos $2282 = 10\times217+112$. Logo $mdc(217, 2282) = mdc(217, 112)$.

Dividindo 217 por 112 obtemos $217 = 1 \times 112 + 105$ e assim $mdc(112, 217) = mdc(112, 105)$.

Dividindo 112 por 105 obtemos $112 = 1\times105+7$ de modo que $mdc(105, 112) = mdc(105, 7)$.

Exercício 7: Encontre mdc $(2^{100} - 1, 2^{120} - 1)$
Solução: Observe inicialmente que $a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + ... + 1)$. Para o entendimento dessa igualdade basta efetivar as distributivas à direita que teremos a expressão à esquerda. Por outro lado, observando que $2^{120} - 1 = 2^{20}(2^{100} - 1) + (2^{20} - 1)$, então o resto da divisão de $2^{120} - 1$ por $(2^{100} - 1)$ é igual a $(2^{20} - 1)$. Assim, fazendo uso novamente da propriedade, segue que

$$mdc(2^{120} - 1, 2^{100} - 1) = mdc(2^{100} - 1, 2^{20} - 1).$$

Observe que, segundo a igualdade inicial, considerando $n = 5$, tem-se que $(2^{20} - 1)$ divide $(2^{100} - 1)$ pois $2^{100} - 1 = ((2^{20})^5 - 1) = (2^{20} - 1) \times ((2^{20})^4 + ((2^{20})^3 + ... + 1)$. Portanto, $mdc(2^{100} - 1, 2^{120} - 1) = 2^{20} - 1$.