Matemática Finita / Discreta

Exercícios Resolvidos 1 - Divisibilidade, Algoritmo de Euclides, Equação de Bézout

1. Determine o quociente e o resto, para a divisão inteira dos seguintes pares dividendo/divisor: (i) $D = 1745$, $d = 23$ (ii) $D = -1745$, $d = 23$.

   Resolução: (i) Pelo algoritmo usual obtemos $1745 = 23 \cdot 75 + 20$, donde o quociente é 75 e o resto é 20.
   (ii) A equação anterior permite escrever $-1745 = 23 \cdot (-75) - 20$. Uma vez que o resto é, por definição um inteiro entre 0 e 22, temos que fazer a seguinte modificação:

   $$-1745 = 23 \cdot (-75 - 1) + 23 - 20 = 23 \cdot (-76) + 3,$$

   pelo que, agora, o quociente é -76 e o resto 3.

2. Implemente o algoritmo de Euclides para determinar o máximo divisor comum d, entre os naturais 637 e 231. Verifique que $637/d$ e $231/d$ são números naturais.

   Resolução: Aplicando o algoritmo de divisão sucessivamente, obtemos:

   $$\begin{aligned} 637 &= 2 \cdot 231 + 175 \\ 231 &= 1 \cdot 175 + 56 \\ 175 &= 3 \cdot 56 + 7 \\ 56 &= 8 \cdot 7 \end{aligned}$$

   logo, $(637, 175) = 7$. Finalmente temos $637/7 = 91$ e $231/7 = 33$, como pretendido.

3. Considere os inteiros $a = 2406$ e $b = 654$.

   (a) Encontre $d = \text{mdc}(a, b)$, o máximo divisor comum entre a e b.
   (b) Encontre inteiros x e y, que satisfaçam a identidade de Bézout $ax + by = d$.

   Resolução: (a) Para determinar o mdc, usamos o algoritmo de Euclides, fazendo sucessivas divisões com resto:

   $$\begin{aligned} 2406 &= 3 \cdot 654 + 444 \\ 654 &= 1 \cdot 444 + 210 \\ 444 &= 2 \cdot 210 + 24 \\ 210 &= 8 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 + 0. \end{aligned}$$

Logo

$$\mathrm{mdc}(2406, 654) = \mathrm{mdc}(654, 444) = \cdots = \mathrm{mdc}(18, 6) = 6.$$

(b) Vamos usar o desenvolvimento do algoritmo de Euclides na alínea (a) para obter uma identidade da forma $ax + by = 6$. Assim, escrevemos:

$$\begin{aligned}
6 &= 24 + (-1) \cdot 18 = \\
&= 24 + (-1) \cdot (210 - 8 \cdot 24) = \\
&= (-1) \cdot 210 + 9 \cdot 24 = \\
&= (-1) \cdot 210 + 9 \cdot (444 - 2 \cdot 210) = \\
&= 9 \cdot 444 + (-19) \cdot 210 = \\
&= 9 \cdot 444 + (-19) \cdot (654 - 444) = \\
&= (-19) \cdot 654 + 28 \cdot 444 = \\
&= (-19) \cdot 654 + 28 \cdot (2406 - 3 \cdot 654) = \\
&= 28 \cdot 2406 + (-103) \cdot 654.
\end{aligned}$$

Assim, $(x, y) = (28, -103)$ é uma solução. Esta solução pode também ser obtida através da tabela:

d_i	$-q_i$	x_i	y_i
2406		1	0
654	-3	0	1
444	-1	1	-3
210	-2	-1	4
24	-8	3	-11
18	-1	-25	92
6		28	-103

4. Considere novamente os inteiros $a = 2406$ e $b = 654$.

   (a) Resolva a equação diofantina $ax + by = 102$, com x, y inteiros e $y > 0$.

   (b) É possível resolver a equação $ax + by = 184$ com x, y inteiros?

Resolução: (a) Para resolver a equação $ax + by = 102$ primeiro verificamos que 6 é divisor de 102. De facto, $102 = 17 \cdot 6$. Como a, b e $c = 102$ são todos divisíveis por 6, a equação dada é equivalente a

$$\frac{2406}{6}x + \frac{654}{6}y = \frac{102}{6} \quad \Leftrightarrow 401x + 109y = 17.$$

A identidade do problema 3 mostra que $x' := 28$, $y' := -103$ é solução da equação $401x + 109y = 1$ (pois esta última equivale a $2406x + 654y = 6$). Assim, $(x_0, y_0) := (17 \cdot (28), 17 \cdot (-103))) = (476, -1751)$ é solução da equação pedida. No entanto, a coordenada y é negativa. Para encontrar uma outra solução com y positivo, usamos o facto de que *todas* as soluções de $401x + 109y = 17$ (note-se que 401 e 109 são primos entre si) são dadas por

$$(x_k, y_k) = (x_0 + 109k,\ y_0 - 401k)\,, \quad k \in \mathbb{Z}.$$

Assim, basta encontrar k inteiro de modo a ter $-1751-401k$ positivo. Temos que ter $k \leq -5$. Por exemplo, com $k = -5$, obtemos $(x_k, y_k) = (-69, 254)$. [Verificação: $401 \cdot (-69) + 109 \cdot 254 = 17$.]
(b) Como $184/6 = 30 + \frac{2}{3}$, 6 não é divisor de 184, pelo que a equação dada não tem soluções inteiras.

5. Encontre todas as soluções $x, y \in \mathbb{Z}$ da equação $\det A = 14$ onde

$$A = \begin{pmatrix} x & 70 \\ y & 343 \end{pmatrix}.$$

Resolução: A equação pretendida é

$$336x - 70y = 14,$$

cuja identidade de Bézout associada é:

$$336x' + 70y' = (336, 70).$$

Recorremos ao algoritmo de Euclides estendido através da tabela:

d_i	q_i	x_i	y_i
343		1	0
70	-4	0	1
63	-1	1	-4
7	-9	-1	5
0		10	-49

pelo que $343 \cdot (-1) + 70 \cdot 5 = 7$. Assim, temos

$$343(-2) - 70(-10) = 14$$

pelo que $x = -2$ e $y = -5$ é uma solução da equação pretendida. Para encontrar todas as soluções, vemos que $343/7 = 49$ e $70/7 = 10$ pelo que temos, finalmente:

$$x = -2 + 10k, \qquad y = -10 - 49k, \qquad k \in \mathbb{Z}.$$

6. Mostre as seguintes propriedades da relação de divisibilidade, com $a, b \in \mathbb{Z}$:

   (a) Para todos os inteiros a, k, temos $a \mid ka$;

   (b) Se $a \mid b$ para todo o $a \in \mathbb{Z}$, então $b = 0$; Se $a \mid b$ para todo o $b \in \mathbb{Z}$, então $a = \pm 1$;

   (c) Sejam $a, b \in \mathbb{Z}$. Se $a|b$ e $b|a$ então $|a| = |b|$;

Resolução: (a) Sejam $a, k \in \mathbb{Z}$. Por definição $a|ka \Leftrightarrow \exists q \in \mathbb{Z}$ tal que $ka = qa$. Esta afirmação é válida com $q := k$, pelo que $a|ka$ verifica-se sempre.
(b) A expressão "$a|b\ \forall a \in \mathbb{Z}$", significa, por definição, que "b é um inteiro tal que, para todo a inteiro, existe $q \in \mathbb{Z}$, tal que $b = qa$". Seja $a > b > 0$; Então $a|b$ é impossível (pois para isso teríamos $q = \frac{b}{a}$, que não é inteiro). Seja $0 > b > a$; então novamente, $a|b$ é impossível (pela mesma razão). Assim, b só pode ser 0. De facto, com $b = 0$ basta escolher $q = 0$ para termos $0 = 0 \cdot a$

para todo o $a \in \mathbb{Z}$.
A expressão "$a|b\ \forall b \in \mathbb{Z}$", significa, por definição, que "a é um inteiro tal que, para todo b inteiro, existe $q \in \mathbb{Z}$, tal que $b = qa$". Seja a um número natural maior que 1. Então $a + 1 \in \mathbb{N}$ e a não divide $a + 1$, pois o resto da divisão de $a + 1$ por a é 1. Se $a = 0$ não há forma de encontrar q para resolver a equação $b = q \cdot 0$ com $b \neq 0$. Mas se $a = 1$, dado $b \in \mathbb{Z}$ temos sempre $1|b$ pois existe $q \in \mathbb{Z}$ (de facto, $q := b$) tal que $b = q \cdot 1$. Assim, se $a \in \mathbb{N}$, a única hipótese é $a = 1$. Do mesmo modo, se $a \in -\mathbb{N}$, verifica-se que a única hipótese é $a = -1$.
(c) Sejam a, b positivos. Então $a|b$ e $b|a$ implica que $a \leq b$ e $b \leq a$ respectivamente. Logo $a = b$. Se a é positivo e b negativo, seja $c = -b$. Aplicando o raciocínio anterior, temos $a = -b$. Os outros casos são análogos, pelo que se sempre se conclui que $|a| = |b|$.

7. Mostre ou indique um contra-exemplo para as seguintes afirmações:

   (a) Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid bc$ então $a \mid b$ ou $a \mid c$;

   (b) Sejam $a, b, q, r \in \mathbb{Z}$ tais que $a = bq + r$. Então $(a, b) = (b, r)$;

   (c) Sejam $a, b \in \mathbb{Z}$. Se $(a, b) = d$ então $(\frac{a}{d}, \frac{b}{d}) = 1$.

   (d) Para $a, b \in \mathbb{Z}$, e $k \in \mathbb{N}$, temos $(ka, kb) = k \cdot (a, b)$.

   Resolução: (a) A afirmação é falsa em geral. Por exemplo, se $a = 6$, $b = 3$ e $c = 4$ temos que $a|bc$ pois $6|12$. No entanto, 6 não divide nem 3, nem 4. A afirmação é verdadeira nos casos em que a é primo (visto nas aulas), ou em que $(b, c) = 1$ (ver o problema seguinte).
   (b) Seja $d = (a, b)$. Então $d \mid a$ e $d \mid b$. Logo, $d \mid (a - bq)$ pelo que $d \mid r$. Logo d é um divisor comum a r e a b. Seja c um outro inteiro que divide b e r simultaneamente. Então também divide $a = bq + r$. Como c divide a e b, então divide d (por definição de $d = (a, b)$). Assim, qualquer divisor comum a b e r divide d. Conclui-se então que d é o mdc de b e r.
   (c) Se $(a, b) = d$ então, pela aplicação do algoritmo de Euclides, existe solução inteira de $ax + by = d$. Mas a/d e b/d são também inteiros e aquela equação é equivalente a

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

   Seja $(\frac{a}{d}, \frac{b}{d}) = c$. Então temos $c|\frac{a}{d}$ e $c|\frac{b}{d}$, e esta equação implica $c|1$. Mas isto quer dizer que $c = 1$.
   (d) Seja $d = (a, b)$. Então $kd \mid ka$ e $kd \mid kb$, porque $d|a$ e $d|b$. Logo kd é um divisor comum a ka e kb. Por outro lado, pela identidade de Bézout, é possível resolver a equação $d = ax + by$, com $x, y \in \mathbb{Z}$, equação que equivale a $kd = kax + kby$. Consideremos $c \in \mathbb{Z}$ tal que $c|ka$ e $c|kb$. Pela última equação $c|kd$. Assim, por definição, kd é o máximo divisor comum entre ka e kb.