Material Teórico - Módulo Algoritmo de Euclides Estendido, Relações de Bézout e Equações Diofantinas

Relação de Bézout e Aplicações

Tópicos Adicionais

Autor: Ulisses Lima Parente
Revisor: Prof. Antonio Caminha M. Neto

17 de Setembro de 2022

1 A relação de Bézout

Em aulas anteriores, aprendemos a calcular o máximo divisor comum de dois inteiros positivos utilizando o **Algoritmo de Euclides**, também conhecido como **método das divisões sucessivas**.

Agora, utilizaremos esse método para encontrar números inteiros m e n tais que

$$am + bn = \text{mdc}\,(a,b),$$

em que a e b são números inteiros — não simultaneamente nulos — dados. Iniciamos com o seguinte

Exemplo 1. *Calcule* $d = \text{mdc}\,(60,42)$. *Em seguida, encontre números inteiros* m *e* n *tais que*

$$60m + 42n = d.$$

Solução. Calculando $\text{mdc}\,(60,42)$ pelo método das divisões sucessivas, obtemos

	1	2	3
60	42	18	6
18	6	0	

Assim, $\text{mdc}\,(60,42) = 6$.

Agora, observando as divisões, podemos escrever

$$6 = 42 - 18 \cdot 2$$

e

$$18 = 60 - 42 \cdot 1.$$

Substituindo $18 = 60 - 42 \cdot 1$ na primeira igualdade, obtemos

$$\begin{aligned} 6 &= 42 - 18 \cdot 2 \\ &= 42 - (60 - 42 \cdot 1) \cdot 2 \\ &= 42 - 60 \cdot 2 + 42 \cdot 2 \\ &= 42 \cdot 3 - 60 \cdot 2 \\ &= 60 \cdot (-2) + 42 \cdot 3. \end{aligned}$$

Portanto, basta fazer $m = -2$ e $n = 3$. □

Observação 2. *Os números inteiros m e n encontrados no exemplo 1 não são únicos. De fato, temos*

$$\begin{aligned} 6 &= 60 \cdot (-2) + 42 \cdot 3 \\ &= 60 \cdot \left(-2 + \frac{42}{6}t\right) + 42 \cdot \left(3 - \frac{60}{6}t\right) \\ &= 60 \cdot (-2 + 7t) + 42 \cdot (3 - 10t)\,, \end{aligned}$$

em que t é um inteiro arbitrário. Então, fazendo $t = 1$, por exemplo, obtemos

$$6 = 60 \cdot 5 + 42 \cdot (-7).$$

Antes de apresentarmos o resultado principal deste material, vejamos a seguinte proposição, que utilizaremos não somente na demonstração do teorema, mas em muitos outros resultados.

Proposição 3. *Sejam a, b e d números inteiros tais que $d \mid a$ e $d \mid b$. Então, $d \mid (am + bn)$, quaisquer que sejam m e n inteiros.*

Prova. Como $d \mid a$ e $d \mid b$, existem inteiros c_1 e c_2 tais que

$$a = c_1 d \text{ e } b = c_2 d.$$

Assim, temos que

$$\begin{aligned} am + bn &= c_1 dm + c_2 dn \\ &= (c_1 m + c_2 n)d. \end{aligned}$$

Escrevendo $c = c_1 m + c_2 n \in \mathbb{Z}$, concluímos que existe um número inteiro c tal que $am + bn = cd$. Mas isso é o mesmo que dizer que d divide $am + bn$. □

Teorema 4 (Relação de Bézout)**.** *Sejam a e b inteiros não simultaneamente nulos. Então, existem inteiros m_0 e n_0 tais que*

$$\text{mdc}\,(a,b) = am_0 + bn_0.$$

Podemos dar uma demonstração bastante similar àquela que levou à solução do exemplo anterior, listando, a partir de a e b, as várias divisões sucessivas que levam ao $\text{mdc}\,(a,b)$ e, em seguida, trabalhando com tais divisões sucessivas na ordem reversa em que apareceram. No entanto, a fim de ilustrar a construção de uma argumentação *existencial* em Matemática[1], apresentaremos uma demonstração distinta.

Prova. Considere o conjunto

$$A = \{am + bn;\ m,n \in \mathbb{Z} \text{ e } am + bn > 0\}.$$

Fazendo $m = a$ e $n = b$, temos

$$am + bn = a \cdot a + b \cdot b = a^2 + b^2 > 0,$$

pois $a \neq 0$ ou $b \neq 0$, uma vez que a e b não são simultaneamente nulos. Logo, o conjunto A não é vazio.

Como A é um conjunto formado somente por números inteiros positivos, ele possui um elemento que é menor do que todos os demais. Denotando esse elemento por d_0, o fato de d_0 pertencer ao conjunto A garante que existem $m_0,n_0 \in \mathbb{Z}$ tais que

$$d_0 = am_0 + bn_0.$$

Afirmamos que $d_0 = \text{mdc}\,(a,b)$.

Com efeito, se d é um divisor positivo de a e b, então, pela proposição 3, temos que $d \mid (am_0 + bn_0)$, ou seja, $d \mid d_0$. Daí, uma vez que d e d_0 são ambos positivos, segue que $d \leq d_0$. Portanto, se mostrarmos que $d_0 \mid a$ e $d_0 \mid b$, concluiremos que d_0 é o maior divisor comum de a e b, isto é, $d_0 = \text{mdc}\,(a,b)$.

Para o que falta, raciocinando por contradição, suponhamos que $d_0 \nmid a$. Então, pelo Algoritmo da Divisão, existiriam q e r inteiros tais que

$$a = d_0q + r, \text{ com } 0 < r < d_0.$$

[1]Nas palavras do matemático americano L. C. Evans: "*nós, matemáticos, somos como teólogos, consideramos a existência como a atributo principal do que estudamos; mas, contrariamente aos teólogos, não nos apoiamos somente na fé*".

Mas aí,

$$\begin{aligned} a = d_0q + r &\Rightarrow a = (am_0 + bn_0)q + r \\ &\Rightarrow a = am_0q + bn_0q + r \\ &\Rightarrow r = a(1 - m_0q) + b(-n_0q); \end{aligned}$$

e, como $1 - m_0q \in \mathbb{Z}$ e $-n_0q \in \mathbb{Z}$, teríamos $r = a(1 - m_0q) + b(-n_0q) \in A$. No entanto, isso é uma contradição, pois d_0 é o menor elemento positivo de A e $0 < r < d_0$. Portanto, $d_0 \mid a$. A prova de que $d_0 \mid b$ é análoga.

Desse modo, concluímos que $d_0 = \text{mdc}\,(a,b)$. Assim, podemos escrever

$$am_0 + bn_0 = \text{mdc}\,(a,b).$$

□

Vejamos outro exemplo.

Exemplo 5. *Existe um par de números inteiros (x,y) tal que $65x + 91y = 39$? Em caso afirmativo, encontre um desses pares.*

Solução. Inicialmente, vamos utilizar o método das divisões sucessivas para calcular mdc (65,91). Assim fazendo, obtemos

	1	2	2
91	65	26	13
26	13	0	

Logo, mdc (65,91) = 13. Agora, o teorema 4 garante a existência de um par de inteiros (m,n) tal que

$$65m + 91n = 13.$$

Multiplicando ambos os membros da última igualdade por 3, obtemos $(65m + 91n) \cdot 3 = 13 \cdot 3$ ou, o que é o mesmo, $65 \cdot (3m) + 91 \cdot (3n) = 39$. Portanto, fazendo $x = 3m$ e $y = 3n$, concluímos que

$$65x + 91y = 39.$$

A fim de encontrar *efetivamente* um par de inteiros m e n tal que $65m + 91n = 13$, procedemos como no exemplo 1: utilizando as divisões sucessivas do Algoritmo de Euclides, temos

$$13 = 65 - 2 \cdot 26$$

e

$$26 = 91 - 1 \cdot 65.$$

Logo,

$$\begin{aligned} 13 &= 65 - 2 \cdot (91 - 1 \cdot 65) \\ &= 65 - 2 \cdot 91 + 2 \cdot 65 \\ &= 65 \cdot 3 + 91 \cdot (-2). \end{aligned}$$

Multiplicando a última igualdade por 3, obtemos

$$13 \cdot 3 = (65 \cdot 3 + 91 \cdot (-2)) \cdot 3,$$

ou seja,

$$39 = 65 \cdot 9 + 91 \cdot (-6).$$

Assim, $(x,y) = (9, -6)$ é uma solução de $65x + 91y = 39$. □

Observação 6. *Sejam a, b e c números inteiros tais que $d = \text{mdc}\,(a,b)$. O raciocínio empregado para encontrar uma solução para o exemplo anterior nos permite concluir que, se $d \mid c$, então existe pelo menos um par (x,y) de números inteiros, tal que $ax + by = c$, ou seja, que essa equação tem solução no conjunto dos inteiros.*

Uma equação do tipo $ax + by = c$, em que a, b e c são inteiros não nulos, é denominada ***equação diofantina linear****. Nas próximas aulas, voltaremos a estudar equações diofantinas lineares.*

A seguir, elaboraremos algumas consequências do Teorema de Bézout. Para a primeira delas, recorde que dois inteiros são ditos *primos entre si* se tiverem mdc igual a 1.

Corolário 7. *Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros m e n tais que $am + bn = 1$.*

Prova. Se a e b são primos entre si, então, por definição, $\text{mdc}\,(a,b) = 1$. Logo, pelo teorema 4, existem m e n inteiros tais que $am + bn = 1$.

Reciprocamente, suponha que existam números inteiros m e n tais que $am + bn = 1$, e seja $d = \text{mdc}\,(a,b)$. Pela proposição 3

$$d \mid a \text{ e } d \mid b \Longrightarrow d \mid (\underbrace{am + bn}_{=1}) \Longrightarrow d \mid 1 \Longrightarrow d = 1.$$

Portanto, $\text{mdc}\,(a,b) = 1$. □

Exemplo 8. *Utilizando a identidade* $(n+1)\cdot 1 + n\cdot(-1) = 1$, *uma aplicação direta do corolário 7 nos permite concluir que* $\text{mdc}\,(n+1,n) = 1$, *qualquer que seja* n *inteiro, ou seja, quaisquer dois números inteiros consecutivos são primos entre si.*

Exemplo 9 (China). *Sejam* a, b, c *e* d *números inteiros tais que* $c + d \neq 0$ *e* $ad - bc = 1$. *Mostre que a fração* $\dfrac{a+b}{c+d}$ *é irredutível.*

Prova. Recordamos que uma fração é irredutível quando seus numerador e denominador são relativamente primos. Então, utilizando o corolário 7, mostraremos que existem inteiros m e n tais que

$$(a+b)m + (c+d)n = 1.$$

Para tanto, partindo da igualdade (dada) $ad - bc = 1$, somamos $bd - bd = 0$ ao primeiro membro para obter

$$\begin{aligned} ad - bc = 1 &\Longrightarrow ad + bd - bd - bc = 1 \\ &\Longrightarrow (ad + bd) - (bd + bc) = 1 \\ &\Longrightarrow (a+b)d - (c+d)b = 1 \\ &\Longrightarrow (a+b)d + (c+d)(-b) = 1. \end{aligned}$$

Assim, tomando $m = d$ e $n = -b$, obtemos

$$(a+b)m + (c+d)n = 1,$$

conforme desejado. □

O próximo corolário traz uma consequência muito útil do corolário 7.

Corolário 10. *Se* $\text{mdc}\,(a,b) = d$, *então* $\text{mdc}\,\left(\frac{a}{d},\frac{b}{d}\right) = 1$.

Prova. Como $\text{mdc}\,(a,b) = d$, utilizamos o teorema 4 para garantir a existência de inteiros m e n tais que $am + bn = d$. Dividindo os dois membros dessa igualdade por d, obtemos

$$\frac{am+bn}{d} = \frac{d}{d} \iff \frac{a}{d}\cdot m + \frac{b}{d}\cdot n = 1.$$

Graças à ultima igualdade acima, o corolário 7 assegura que

$$\text{mdc}\,\left(\frac{a}{d},\frac{b}{d}\right) = 1.$$

□

A seguir apresentamos outra consequência do corolário 7, a qual é extremamente útil para resolver problemas que envolvem divisibilidade de números inteiros.

Proposição 11. *Sejam a, b e c inteiros tais que a e b são primos entre si e $a \mid bc$. Então $a \mid c$.*

Prova. Como a e b são primos entre si, temos que $\text{mdc}\,(a,b) = 1$. Então, pelo teorema 4, existem m e n inteiros tais que $am + bn = 1$. Multiplicando os dois membros dessa igualdade por c, obtemos

$$\begin{aligned}(am+bn)\cdot c = 1\cdot c &\Longrightarrow amc + bnc = c\\ &\Longrightarrow a\cdot mc + bc\cdot n = c.\end{aligned}$$

Como $a \mid a$ e, por hipótese, $a \mid bc$, a proposição 3 garante que $a \mid (a\cdot mc + bc\cdot n)$, isto é, $a \mid c$. □

Observação 12. *Na proposição 11, a hipótese* $\text{mdc}\,(a,b) = 1$ *não pode ser relaxada. Por exemplo, veja que* $4 \mid 2\cdot 6$, *mas* $4 \nmid 2$ *e* $4 \nmid 6$. *Obviamente, isso não contraria a proposição 11, pois* $\text{mdc}\,(4,2) = \text{mdc}\,(4,6) = 2$.

Dicas para o Professor

Sugerimos que sejam utilizadas duas sessões de 50min para expor o conteúdo deste material. Recomendamos que os professores estimulem a utilização do raciocínio empregado na solução do exemplo 1 para encontrar pares de inteiros (m,n) que sejam soluções de outras equações do tipo $am + bn = \text{mdc}\,(a,b)$. Aproveite o exemplo 5 para comentar que, utilizando a mesma ideia, é possível apresentar uma solução para qualquer equação diofantina linear $ax + by = c$, desde que $\text{mdc}\,(a,b) \mid c$. É recomendável fazer outros exemplos como esse, sempre dando algum tempo para que os alunos tentem resolvê-los por meios próprios. Finalmente, ressalte a necessidade da hipótese $\text{mdc}\,(a,b) = 1$ na proposição 11.

O material aqui reunido pode ser utilizado para resolver um sem-número de problemas mais desafiadores de divisibilidade. Para o leitor interessado, sugerimos consultar a bibliografia a seguir.

Sugestões de Leitura Complementar

1. J. P. de Oliveira Santos. *Introdução à Teoria dos Números.* Rio de Janeiro, SBM, 2000.

2. A. C. Muniz Neto. *Tópicos de Matemática Elementar, Volume 5: Teoria dos Números*, 3ª edição. Rio de Janeiro, SBM, 2022.