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

O Algoritmo de Euclides Estendido

Tópicos Adicionais

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

17 de agosto de 2022

1 O Algoritmo de Euclides

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**. Informalmente, esse método também é chamado **método do jogo da velha**.

Como exemplo, vamos calcular $\text{mdc}\,(270{,}168)$ utilizando divisões sucessivas. Iniciamos dividindo 270 por 168.

$$\begin{array}{r|l} 270 & 168 \\ \hline 102 & 1 \end{array}$$

Depois disso, dividimos 168 — que era o divisor na conta anterior — por 102 — que foi o resto encontrado na conta anterior.

$$\begin{array}{r|l} 168 & 102 \\ \hline 66 & 1 \end{array}$$

Seguimos com esse procedimento, sempre observando o resto. Enquanto não for encontrado um resto igual a 0, as divisões sucessivas do divisor pelo resto devem continuar. Desse modo, obtemos:

$$\begin{array}{r|l} 102 & 66 \\ \hline 36 & 1 \end{array} \qquad \begin{array}{r|l} 66 & 36 \\ \hline 30 & 1 \end{array} \qquad \begin{array}{r|l} 36 & 30 \\ \hline 6 & 1 \end{array} \qquad \begin{array}{r|l} 30 & 6 \\ \hline 0 & 5 \end{array}$$

O último resto diferente de 0 encontrado é o $\text{mdc}\,(270{,}168)$, ou seja, temos que $\text{mdc}\,(270{,}168) = 6$.

Esse método pode ser resumido no seguinte dispositivo prático:

	1	1	1	1	1	5
270	168	102	66	36	30	6
102	66	36	30	6	0	

Observe que o dispositivo é essencialmente a justaposição das várias divisões sucessivas realizadas; a única diferença é que os quocientes das divisões são colocados acima dos divisores — em vez de abaixo — a fim de que os restos possam ficar todos abaixo dos dividendos.

A partir de agora, nosso objetivo é dar uma demonstração da validade do Algoritmo de Euclides. Nosso ponto de partida é o Teorema de Eudoxius, que apresentamos a seguir.

Teorema 1 (Eudoxius). *Dados a e b inteiros, com $b > 0$, então a é múltiplo de b ou está localizado entre dois múltiplos consecutivos de b. De outro modo, dados a e b inteiros, com $b > 0$, então existe q inteiro tal que*

$$bq \leq a < b(q+1).$$

Prova. Suponha que $a \geq 0$ (o caso $a < 0$ pode ser tratado de forma análoga) e considere o número racional $\frac{a}{b}$.

O fato de o conjunto $\mathbb{N}$ dos números naturais ser ilimitado superiormente garante a existência de um natural maior que $\frac{a}{b}$. Dentre todos esses naturais, existe um que é o menor possível; chame-o de n. Então, $\frac{a}{b} < n$ é verdade, mas a minimalidade de n garante que $\frac{a}{b} < n-1$ é falso. Portanto, $\frac{a}{b} \geq n-1$, de modo que

$$n - 1 \leq \frac{a}{b} < n.$$

Chamando $n-1$ de q, temos $n = q+1$ e

$$q \leq \frac{a}{b} < q+1.$$

Multiplicando as desigualdades acima por b, segue finalmente que

$$bq \leq a < b(q+1),$$

conforme desejado. □

Agora, apresentamos uma demonstração para o Algoritmo da Divisão.

Teorema 2 (Algoritmo da Divisão). *Dados inteiros positivos a e b, existem, e são únicos, inteiros q e r tais que*

$$a = bq + r, \text{ com } 0 \leq r < b.$$

*Os números inteiros q e r são denominados **quociente** e **resto** da divisão de a por b, respectivamente.*

Prova. Pelo Teorema de Eudoxius, existe um número inteiro q tal que

$$bq \leq a < b(q+1).$$

Assim:

$$bq \leq a \Longrightarrow 0 \leq a - bq$$

e

$$a < b(q+1) \Longrightarrow a < bq + b \Longrightarrow a - bq < b.$$

Daí, fazendo $r = a - bq$, obtemos

$$a = bq + r,\ 0 \leq r < b.$$

Para provar a unicidade, suponha que q' e r' sejam inteiros tais que

$$a = bq' + r', \text{ com } 0 \leq r' < b.$$

Então

$$bq + r = a = bq' + r' \Longrightarrow b(q - q') = r' - r,$$

de sorte que

$$b|q' - q| = |r' - r|. \tag{1}$$

Logo, $|r' - r|$ é múltiplo de b. Mas veja que

$$r' < b \Longrightarrow r' - r < b - r < b$$

e

$$r < b \Longrightarrow r - r' < b - r' < b.$$

Assim, $|r' - r| < b$, de maneira que $|r' - r|$ é um múltiplo de b tal que $0 \leq |r' - r| < b$. Portanto, a única possibilidade é que $|r' - r| = 0$. Daí, $r' = r$ e, graças a (1), $q' = q$. Desse modo, quociente e resto da divisão de a por b são únicos. □

Agora, recordamos a seguinte propriedade da divisibilidade de números inteiros.

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

Prova. Como $d \mid a$ e $d \mid b$, existem inteiros q_1 e q_2 tais que $a = dq_1$ e $b = dq_2$. Assim, para quaisquer m e n inteiros, temos

$$ma + nb = mdq_1 + ndq_2 = d(mq_1 + nq_2).$$

Portanto, $d \mid (ma + nb)$. □

A seguir, provaremos um lema que é fundamental para a demonstração do Algoritmo de Euclides.

Lema 4. *Se a e b são inteiros tais que $a = bq + r$, então* $\text{mdc}\,(a,b) = \text{mdc}\,(b,r)$.

Prova. Seja d um inteiro tal que $d \mid a$ e $d \mid b$. Utilizando a proposição 3, obtemos

$$d \mid (1 \cdot a + (-q) \cdot b) \Longrightarrow d \mid (a - bq) \Longrightarrow d \mid r.$$

Por outro lado, se d é um inteiro tal que $d \mid b$ e $d \mid r$, então, utilizando outra vez a proposição 3, obtemos

$$d \mid (q \cdot b + 1 \cdot r) \Longrightarrow d \mid (bq + r) \Longrightarrow d \mid a.$$

Portanto, concluímos que os divisores comuns de a e b são os mesmos divisores comuns de b e r. Daí, segue que $\text{mdc}\,(a,b) = \text{mdc}\,(b,r)$. □

Voltando ao cálculo de $\text{mdc}\,(270,168)$ que fizemos no início deste material, veja que, como

$$\begin{array}{r|l} 270 & 168 \\ \hline 102 & 1 \end{array}$$

temos $270 = 1 \cdot 168 + 102$. Então, o lema anterior garante que

$$\text{mdc}\,(270,168) = \text{mdc}\,(168,102).$$

Prosseguindo com as divisões, obtivemos, sucessivamente,

$$\begin{aligned} 168 &= 1 \cdot 102 + 66 \\ 102 &= 1 \cdot 66 + 36 \\ 66 &= 1 \cdot 36 + 30 \\ 36 &= 1 \cdot 30 + 6 \\ 30 &= 5 \cdot 6 \end{aligned}$$

Então, várias aplicações do lema anterior dão

$$\begin{aligned}\text{mdc}\,(270{,}168) &= \text{mdc}\,(168{,}102)\\ &= \text{mdc}\,(102{,}66)\\ &= \text{mdc}\,(66{,}36)\\ &= \text{mdc}\,(36{,}30)\\ &= \text{mdc}\,(30{,}6) = 6.\end{aligned}$$

Repetindo a ideia utilizada para justificar $\text{mdc}\,(270{,}168) = 6$, vamos demonstrar o seguinte teorema.

Teorema 5 (Algoritmo de Euclides). *Sejam a e $b \neq 0$ inteiros não negativos. Aplicando o algoritmo da divisão sucessivas vezes, obtemos as sequências finitas de números inteiros q_1, q_2, ..., q_n e $a = r_0$, $b = r_1$, r_2, ..., r_{n-1} tais que*

$$\begin{aligned} r_0 &= q_1 r_1 + r_2,\ 0 \leq r_2 < r_1\\ r_1 &= q_2 r_2 + r_3,\ 0 \leq r_3 < r_2\\ &\vdots\\ r_{n-2} &= q_{n-1} r_{n-1} + r_n,,\ 0 \leq r_{n-1} < r_n\\ r_{n-1} &= q_n r_n.\end{aligned}$$

Além disso, para $0 \leq j \leq n-1$, temos

$$\text{mdc}\,(a{,}b) = \text{mdc}\,(r_j{,}r_{j+1}) = r_n.$$

Prova. A demonstracão é uma repetição da ideia aplicada anteriormente para calcular $\text{mdc}\,(270{,}168)$. De fato, podemos aplicar o algoritmo da divisão sucessivas vezes para obter uma sequência de restos e outra de quocientes, conforme prescrito pelo enunciado. O ponto fundamental a ser ressaltado aqui é que, em algum momento, chegaremos a uma divisão exata, ou seja, a um resto 0. De fato, como todos os restos são inteiros maiores ou iguais a 0 e $r_1 > r_2 > r_3 > \ldots$, depois de um número finito de divisões o resto será igual a 0. (Pois não há uma sequência decrescente e infinita de inteiros não

negativos.) Portanto, obtemos sequências finitas de números inteiros $q_1, q_2, \ldots, q_n$ e $a = r_0, b = r_1, r_2, \ldots, r_{n-1}$ tais que

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2,\ 0 \leq r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3,\ 0 \leq r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n,,\ 0 \leq r_{n-1} < r_n \\
r_{n-1} &= q_n r_n.
\end{aligned}$$

Daí, aplicando o lema 4 sucessivas vezes, obtemos $\text{mdc}\,(a,b) = \text{mdc}\,(r_0,r_1) = \text{mdc}\,(r_1,r_2) = \ldots = \text{mdc}\,(r_{n-1},r_n)$. Agora, veja que $\text{mdc}\,(r_{n-1},r_n) = r_n$, uma vez que $r_n \mid r_{n-1}$. □

Exemplo 6 (Olimpíada Internacional de Matemática - 1959)**.** *Prove que a fração* $\frac{21n+4}{14n+3}$ *é irredutível, para todo número natural* n*.*

Prova. Aplicando formalmente o Algoritmo de Euclides, temos

$$\begin{aligned}
21n + 4 &= (14n + 3) \cdot 1 + (7n + 1) \\
14n + 3 &= (7n + 1) \cdot 2 + 1 \\
7n + 1 &= 1 \cdot (7n + 1).
\end{aligned}$$

Portanto,

$$\begin{aligned}
\text{mdc}\,(21n + 4,14n + 3) &= \text{mdc}\,(14n + 3,7n + 1) \\
&= \text{mdc}\,(7n + 1,1) = 1.
\end{aligned}$$

□

Dicas para o Professor

Sugerimos que sejam utilizadas duas sessões de 50min para expor o conteúdo deste material. Recomendamos aos professores que calculem o mdc de outros pares de números inteiros

utilizando o lema 4 — seguindo o mesmo raciocínio utilizado para justificar $\text{mdc}\,(270{,}168) = 6$ —, antes de apresentar a demonstração do Algoritmo de Euclides. Isso contribuirá para um melhor entendimento do teorema.

Para saber mais sobre o mdc de inteiros, veja uma das referências a seguir.

Sugestões de Leitura Complementar

1. A. Caminha *Tópicos de Matemática Elementar, volume 5 - Teoria dos Números*. Rio de Janeiro, SBM, 2022.

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