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

Relação de Bézout e Aplicações - Parte 2

Tópicos Adicionais

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

23 de Outubro de 2022

Portal da Matemática
OBMEP

No final da primeira parte desta aula, demonstramos uma proposição que será bastante útil nessa continuação. Vamos enunciá-la mais uma vez.

Proposição 1. *Sejam a, b e c inteiros tais que a e b são primos entre si e $a \mid bc$. Então, $a \mid c$.*

Agora, vamos apresentar um lema que também será útil para demonstrar alguns resultados mais à frente.

Lema 2. *Sejam a, b e κ inteiros positivos. Então*

$$\operatorname{mmc}(\kappa a,\kappa b) = \kappa \operatorname{mmc}(a,b) \ \textit{e} \ \operatorname{mdc}(\kappa a,\kappa b) = \kappa \operatorname{mdc}(a,b).$$

Prova. Sejam $m = \operatorname{mmc}(a,b)$ e $m' = \operatorname{mmc}(\kappa a,\kappa b)$. Uma vez que m é múltiplo de a e de b, temos que κm é múltiplo de κa e de κb. Desse modo, $m' \leq \kappa m$, pois m' é o menor múltiplo positivo comum de κa e κb. Por outro lado, como m' é múltiplo de κa e de κb, temos que $\frac{m'}{\kappa}$ é múltiplo de a e de b. Como m é o menor múltiplo positivo comum de a e b, segue que $m \leq \frac{m'}{\kappa}$. Daí, obtemos $\kappa m \leq m'$. Comparando as duas desigualdades obtidas acima, concluímos que $m' = \kappa m$, ou seja,

$$\operatorname{mmc}(\kappa a,\kappa b) = \kappa \operatorname{mmc}(a,b).$$

Agora, sejam $d = \operatorname{mdc}(a,b)$ e $d' = \operatorname{mdc}(\kappa a,\kappa b)$. Como $d \mid a$ e $d \mid b$, temos que $\kappa d \mid \kappa a$ e $\kappa d \mid \kappa b$; logo, κd é um divisor comum de κa e κb. Como d' é o maior dos divisores comuns de κa e κb, concluímos que $\kappa d \leq d'$. Reciprocamente, sejam m e n inteiros tais que $am + bn = d$ — a existência de m e n é garantida pelo teorema de Bézout. Então, multiplicando ambos os lados dessa igualdade por κ, obtemos $\kappa am + \kappa bn = \kappa d$. Como $d' \mid \kappa a$ e $d' \mid \kappa b$, segue que $d' \mid \kappa d$ e, desse modo, obtemos $d' \leq \kappa d$. Assim, comparando as duas desigualdades obtidas acima, concluímos que $d' = \kappa d$, ou seja,

$$\operatorname{mdc}(\kappa a,\kappa b) = \kappa \operatorname{mdc}(a,b).$$

$\square$

Proposição 3. *Sejam a e b números inteiros positivos. Então, vale a igualdade*

$$\text{mdc}\,(a,b) \cdot \text{mmc}\,(a,b) = ab.$$

Prova. Inicialmente, vamos supor $\text{mdc}\,(a,b) = 1$. Seja $m = \text{mmc}\,(a,b)$. Como $b \mid m$, existe k inteiro tal que $m = kb$. Além disso, como $a \mid m = kb$ e $\text{mdc}\,(a,b) = 1$, concluímos que $a \mid k$. Logo, existe q inteiro tal que $k = qa$. Daí, $m = kb = qab$. Portanto, $ab \mid m$, o que acarreta $ab \leq m = \text{mmc}\,(a,b)$. Por outro lado, como m é o mínimo múltiplo comum de a e b, temos que $m \leq ab$. Então, segue que $m = ab$, conforme desejado.

Para o caso geral, sejam $d = \text{mdc}\,(a,b)$ e u,v inteiros tais que $a = du$ e $b = dv$. Então, $\text{mdc}\,(u,v) = 1$, de sorte que o caso especial discutido no parágrafo anterior dá $\text{mmc}\,(u,v) = uv$. Mas aí, aplicando os resultados do lema anterior, podemos escrever

$$\begin{aligned}
\text{mdc}\,(a,b) \cdot \text{mmc}\,(a,b) &= \text{mdc}\,(du,dv) \cdot \text{mmc}\,(du,dv) \\
&= d \cdot \text{mdc}\,(u,v) \cdot d \cdot \text{mmc}\,(u,v) \\
&= d^2 \cdot 1 \cdot uv \\
&= du \cdot dv \\
&= ab.
\end{aligned}$$

□

Exemplo 4. *Sejam a e b números inteiros positivos e $d = \text{mdc}\,(a,b)$. Então, na sequência*

$$(b, 2b, \ldots, ab),$$

há exatamente d múltiplos de a.

Prova. Seja $m = \text{mmc}\,(a,b)$. Veja que os d números m, $2m$, $\ldots$, dm são todos múltiplos de b, pois são múltiplos de m. Como $dm = ab$, tais números são menores ou iguais a ab, logo, fazem parte da sequência $(b, 2b, \ldots, ab)$. Dessa forma, encontramos pelo menos d múltiplos de a na sequência dada.

Agora, veja que qualquer múltiplo de a que faça parte da sequência $(b,2b,\ldots,ab)$ também será múltiplo de b (uma vez que todos os termos dessa sequência são múltiplos de b). Um tal múltiplo de a, sendo múltiplo de a e de b, será múltiplo de $m = \operatorname{mmc}(a,b)$. Daí, $m,2m,\ldots,dm = ab$ são os únicos múltiplos de a na sequência $(b,2b,\ldots,ab)$. $\square$

Exemplo 5. *Encontre todos os pares (a,b) de inteiros positivos tais que $a \geq b$ e*

$$\operatorname{mmc}(a,b) + \operatorname{mdc}(a,b) + a + b = ab.$$

Solução. Sejam $d = \operatorname{mdc}(a,b)$ e u,v inteiros positivos tais que $a = du$, $b = dv$. Então, $\operatorname{mdc}(u,v) = 1$ e

$$a \geq b \Leftrightarrow du \geq dv \Leftrightarrow u \geq v.$$

Além disso,

$$d \cdot \operatorname{mmc}(a,b) = ab = du \cdot dv = d^2uv,$$

o que implica

$$\operatorname{mmc}(a,b) = duv.$$

Substituindo $a = du$, $b = du$, $\operatorname{mdc}(a,b) = d$ e $\operatorname{mmc}(a,b) = duv$ na equação do enunciado, obtemos

$$duv + d + du + dv = d^2uv,$$

que é equivalente a

$$uv + u + v + 1 = duv,$$

ou, ainda, a

$$v + 1 = u(dv - v - 1).$$

Daí, concluímos que $u \mid (v + 1)$, logo, $u \leq v + 1$. Agora, como $u \geq v$, temos que $u = v$ ou $u = v + 1$. Analisemos esses dois casos separadamente:

- Se $u = v$, então $u = v = 1$, pois $\mathrm{mdc}\,(u,v) = 1$. Nesse caso,

  $$duv = uv+u+v+1 \Rightarrow d\cdot 1\cdot 1 = 1\cdot 1+1+1+1 \Rightarrow d = 4.$$

  Portanto, $a = 4$ e $b = 4$.

- Se $u = v + 1$, então

  $$\begin{aligned} & duv = uv + u + v + 1 \Leftrightarrow \\ \Leftrightarrow\ & d(v+1)v = (v+1)v + (v+1) + (v+1) \\ \Leftrightarrow\ & d\cancel{(v+1)}v = \cancel{(v+1)}(v+2) \\ \Leftrightarrow\ & d = \frac{v+2}{v} \\ \Leftrightarrow\ & d = 1 + \frac{2}{v}. \end{aligned}$$

  Como $\frac{2}{v}$ deve ser inteiro positivo, obtemos $v = 1$ ou $v = 2$. Caso $v = 1$, obtemos $u = v + 1 = 2$ e, daí,

  $$duv = uv+u+v+1 \Rightarrow d\cdot 2\cdot 1 = 2\cdot 1+2+1+1 \Rightarrow d = 3.$$

  Desse modo, $a = du = 3 \cdot 2 = 6$ e $b = dv = 3 \cdot 1 = 3$. Caso $v = 2$, temos que $u = v + 1 = 3$ e

  $$duv = uv+u+v+1 \Rightarrow d\cdot 3\cdot 2 = 3\cdot 2+3+2+1 \Rightarrow d = 2.$$

  Assim, $a = du = 2 \cdot 3 = 6$ e $b = dv = 2 \cdot 2 = 4$.

Portanto, $(a,b) = (4,4),(6,3)$ ou $(6,4)$. □

A seguir, apresentaremos uma sequência de proposições que nos auxiliarão na demonstração de um importante resultado de teoria elementar dos números, conhecido como Teorema Fundamental da Aritmética.

Proposição 6. *Sejam p um número primo e a um número inteiro positivo. Então, $\mathrm{mdc}\,(p,a) = 1$ ou $p \mid a$.*

Prova. Seja $d = \mathrm{mdc}\,(p,a)$. Como $d \mid p$ e p é primo, temos que $d = 1$ ou $d = p$. No primeiro caso, obtemos $\mathrm{mdc}\,(p,a) = 1$; no segundo, $p = d \mid a$. □

Proposição 7. *Sejam p um número primo e a,b inteiros positivos tais que $p \mid ab$. Então, $p \mid a$ ou $p \mid b$.*

Prova. Se $p \mid a$, não há nada a fazer. Assim, podemos supor que $p \nmid a$. Seja $d = \text{mdc}\,(p,a)$. Como $p \nmid a$, concluímos que $d = 1$. Portanto, temos que $p \mid ab$ e $\text{mdc}\,(p,a) = 1$. Pela proposição 1, concluímos que $p \mid b$. □

Corolário 8. *Sejam p, p_1, p_2, ..., p_r números primos. Se $p \mid p_1 p_2 \dots p_r$, então $p = p_i$, para algum $i \in \{1,2,\dots,r\}$.*

Prova. Suponha que $r = 2$. Uma vez que p é primo e $p \mid p_1 p_2$, podemos utilizar a proposição 7 para concluir que $p \mid p_1$ ou $p \mid p_2$. Como p_1 e p_2 também são números primos, concluímos que $p = p_1$ ou $p = p_2$. Agora, suponha que $r = 3$. Se $p \mid p_1 p_2 p_3$, então, mais uma vez aplicando a proposição 7 a $p \mid p_1(p_2 p_3)$, obtemos que $p \mid p_1$ ou $p \mid p_2 p_3$. Se $p \mid p_1$, então, como acima, $p = p_1$; se $p \mid p_2 p_3$, então, aplicando o caso $r = 2$, concluímos que $p = p_2$ ou $p = p_3$. Seguindo esse raciocínio, podemos utilizar o caso $r = 3$ para mostrar o caso $r = 4$, e assim por diante. Esse argumento pode ser formalizado utilizando o Princípio de Indução Finita. □

Lema 9 (Euclides). *Seja $n \geq 2$ um número inteiro. Então, n é primo ou pode ser escrito como o produto de uma quantidade finita de números primos, não necessariamente distintos.*

Prova. Façamos indução sobre $n \geq 2$. Se $n = 2$, não há nada a fazer. Suponha que $n > 2$ e que a propriedade do enunciado é verdadeira para todos os inteiros positivos maiores ou iguais a 2 e menores que n. Há duas possibilidades:

- n é primo: nesse caso, não há nada a fazer.
- n é composto: então, existem n_1 e n_2 inteiros tais que $n_1 \geq 2$, $n_2 \geq 2$ e $n = n_1 \cdot n_2$. Aplicando a hipótese de indução para n_1 e n_2 — note que ambos são menores que n —, obtemos que n_1 e n_2 podem ser escritos como produtos de quantidades finitas de números primos. Logo, $n = n_1 n_2$ também pode ser escrito como o produto de uma quantidade finita de primos.

$\square$

Chegamos finalmente ao resultado desejado.

Teorema 10 (Fundamental da Aritmética)**.** *Seja $n \geq 2$ um número inteiro. Então, existem números primos $p_1 < p_2 < \ldots < p_r$ e inteiros positivos a_1, a_2, $\ldots$, a_r, tais que n pode ser escrito da seguinte forma:*

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r}. \tag{1}$$

Além disso, se $q_1 < q_2 < \ldots < q_s$ são primos e b_1, b_2, $\ldots$, b_s são inteiros positivos tais que $n = q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_s^{b_s}$, então $r = s$ e $a_i = b_i$, $\forall i \in \{1,2,\ldots,r\}$.

Antes de passarmos à demonstração do Teorema Fundamental da Aritmética, vale a pena tecermos duas observações: primeiramente, note que, na primeira parte do enunciado (que se refere à *existência* de uma fatoração de n como um produto de potências de primos distintos), pode-se ter $r = 1$, isto é, $n = p_1^{a_1}$; escrevemos $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r}$ apenas para deixar claro um *padrão* de fatoração. Por outro lado, a segunda parte do enunciado diz que a decomposição de n como um produto de potências de números primos distintos é única, a menos da ordem dessas potências. Graças a essa unicidade de fatoração, (1) é conhecida como a **fatoração canônica** de n.

Prova. A parte da existência consiste simplesmente em *arrumar* a decomposição de n como o produto de uma quantidade finita de primos, dada pelo lema de Euclides. De fato, se juntarmos os primos iguais em potências e colocarmos esses primos em ordem crescente, poderemos escrever $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r}$, em que $p_1 < p_2 < \ldots < p_r$ são primos e a_1, a_2, $\ldots$, a_r são inteiros positivos.

Para a parte da unicidade, suponha que

$$p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r} = q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_s^{b_s},$$

com $p_1 < p_2 < \ldots < p_r$ e $q_1 < q_2 < \ldots < q_s$ primos, e a_1, a_2, $\ldots$, a_r, b_1, b_2, $\ldots$, b_r inteiros positivos. Então, $p_1 \mid$

$q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_s^{b_s}$, de sorte que a proposição 7 dá $p_1 = q_j$, para algum $j \in \{1,2,\ldots,s\}$. Analogamente, $q_1 \mid p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r}$, o que acarreta (novamente pela proposição 7) $q_1 = p_i$, para algum $i \in \{1,2,\ldots,r\}$. Assim, obtemos

$$p_1 = q_j \geq q_1 = p_i \geq p_1,$$

logo, $p_1 = q_1$.

Agora vamos mostrar que $a_1 = b_1$. Se fosse $a_1 > b_1$, poderíamos dividir ambos os membros da igualdade

$$q_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r} = q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_s^{b_s}$$

por $q_1^{b_1}$ para obter

$$q_1^{a_1-b_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r} = q_2^{b_2} \cdot \ldots \cdot q_s^{b_s}; \tag{2}$$

assim, um argumento análogo ao que fizemos acima garantiria que q_1 deveria ser igual a algum dos primos $q_2, \ldots, q_s$, o que não pode acontecer, pois, por hipótese, esses primos são dois a dois distintos. Da mesma forma, não é possível que seja $a_1 < b_1$. Portanto, $a_1 = b_1$, e há dois casos a considerar:

- Se $r = 1$ e $s = 1$, nada mais há a fazer.
- Se $r = 1$ e $s > 1$, então a igualdade (2) torna-se $1 = q_2^{b_2} \cdot \ldots \cdot q_s^{b_s}$, a qual é claramente impossível. Analogamente, não podemos ter $r > 1$ e $s = 1$.
- Se $r,s > 1$, então a igualdade (2) torna-se

  $$p_2^{a_2} \cdot \ldots \cdot p_r^{a_r} = q_2^{b_2} \cdot \ldots \cdot q_s^{b_s}.$$

  Repetindo novamente o argumento que levou a (2), concluímos que $p_2 = q_2$ e $a_2 = b_2$.

Prosseguindo várias vezes como acima, concluímos que $r = s$ e que $p_i = q_i$ e $a_i = b_i$, para todo $i \in \{1,2,\ldots,r\}$. Isso prova a unicidade da decomposição. $\square$

O próximo resultado caracteriza as fatorações canônicas dos divisores de n maiores que 1 em termos da fatoração canônica de n.

Corolário 11. *Sejam* $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r}$ *como no teorema anterior. Então, um inteiro positivo* d *é um divisor positivo de* n *se, e somente se, existirem inteiros* $c_1,c_2,\ldots,c_r$ *tais que* $0 \le c_1 \le a_1$, $0 \le c_2 \le a_2$, $\ldots$, $0 \le c_r \le a_r$ *e*

$$d = p_1^{c_1} \cdot p_2^{c_2} \cdot \ldots \cdot p_r^{c_r}.$$

Prova. Inicialmente, suponha que o inteiro positivo d seja um divisor positivo de n. Se $d = 1$, basta tomar todos os c_i iguais a 0. Senão, seja p^c uma potência de primo que aparece na decomposição canônica de d. Como $p \mid d$ e $d \mid n$, temos que $p \mid n$. Escrevendo a fatoração canônica de n como em (2), o corolário 8 garante que $p = p_i$ para algum $i \in \{1,2,\ldots,r\}$. Dessa forma, podemos escrever a fatoração canônica de d como

$$d = p_1^{c_1} \cdot p_2^{c_2} \ldots \cdot p_r^{c_r},$$

possivelmente com um ou mais dos c_j igual a 0 — caso p_j não seja um dos primos que divide d. Sendo $n = dq$, com $q \in \mathbb{N}$, temos igualmente que $q \mid n$. Argumentando como acima, podemos escrever

$$q = p_1^{e_1} \cdot p_2^{e_2} \ldots \cdot p_r^{e_r},$$

também com um ou mais dos e_j igual a 0. Então, a igualdade $dq = n$ dá

$$p_1^{c_1+e_1} \cdot p_2^{c_2+e_2} \ldots \cdot p_r^{c_r+e_2} = p_1^{a_1} \cdot p_2^{a_2} \ldots \cdot p_r^{a_r},$$

e a parte de unicidade do Teorema Fundamental da Aritmética garante que

$$c_i + e_i = a_i, \; \forall \; i \in \{1,2,\ldots,r\}.$$

Em particular $0 \le c_i \le a_i$, para todo $i \in \{1,2,\ldots,r\}$.

Reciprocamente, seja d um inteiro positivo dado como no enunciado. Então, é imediato que $n = dq$, com

$$q = p_1^{a_1-c_1} \cdot p_2^{a_2-c_2} \ldots \cdot p_r^{a_r-c_r};$$

logo, $q \in \mathbb{N}$ e, daí, $d \mid n$. □

Corolário 12. *Sejam $n \geq 2$ inteiro e $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r}$ sua decomposição canônica. Então, a quantidade de divisores positivos de n é dada pela fórmula*

$$(a_1 + 1)(a_2 + 1) \ldots (a_r + 1).$$

Prova. Pelo corolário anterior, escolher um divisor de n é o mesmo que escolher uma sequência de números inteiros $(c_1, c_2, \ldots, c_r)$ tal que $0 \leq c_1 \leq a_1$, $0 \leq c_2 \leq a_2$, ..., $0 \leq c_r \leq a_r$. Mas, pelo Princípio Fundamental da contagem, essa última escolha pode ser feita de

$$(a_1 + 1)(a_2 + 1) \ldots (a_r + 1),$$

pois há $a_i + 1$ escolhas possíveis para cada c_i, uma vez que $c_i \in \{0,1,\ldots,a_i\}$. □

Exemplo 13. *Quantos divisores positivos tem o número $n = 12^{13} \cdot 13^{22} \cdot 22^{45} \cdot 45^{12}$?*

Solução. Inicialmente, observe que n não vem dado por sua fatoração canônica, uma vez que 12, 22 e 45 não são primos. Podemos remediar isso, substituindo $12 = 2^2 \cdot 3$, $22 = 2 \cdot 11$ e $45 = 3^2 \cdot 5$ nas bases das potências cujo produto define n, obtendo

$$\begin{aligned} n &= (2^2 \cdot 3)^{13} \cdot 13^{22} \cdot (2 \cdot 11)^{45} \cdot (3^2 \cdot 5)^{12} \\ &= 2^{26} \cdot 3^{13} \cdot 13^{22} \cdot 2^{45} \cdot 11^{45} \cdot 3^{24} \cdot 5^{12} \\ &= 2^{71} \cdot 3^{37} \cdot 11^{45} \cdot 13^{22} \cdot 5^{12}. \end{aligned}$$

Portanto, graças ao corolário anterior, n tem

$$(71 + 1)(37 + 1)(45 + 1)(22 + 1)(12 + 1) = 36.812.880$$

divisores positivos. □

Dicas para o Professor

Sugerimos que sejam utilizadas duas sessões de 50min para expor o conteúdo deste material. Recomendamos que os professores substituam alguns valores numéricos na proposição 3 e no exemplo 4 para que os alunos se convençam da validade das afirmações. Caracterizando o $\mathrm{mdc}\,(a,b)$ como o produto das potências dos fatores primos comuns a a e b, quando escolhemos os menores expoentes possíveis, e o mmc como o produto das potências de todos os fatores que aparecem nas decomposições de a e b, quando escolhemos os maiores expoentes possíveis, podemos dar outra demonstração para a proposição 3. É importante explicar esse procedimento aos alunos.

As referências a seguir contém grande quantidade adicional de resultados e problemas de teoria dos elementar dos números. Em particular, [2] traz vários problemas de competições de Matemática, todos eles resolvidos.

Sugestões de Leitura Complementar

1. J. P. de Oliveira Santos. *Introdução à Teoria dos Números.* Rio de Janeiro, Instituto de Matemática Pura e Aplicada, CNPq, 2000.

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

3. A. Hefez. *Aritmética.* Rio de Janeiro, SBM, 2014.