Material Teórico - Módulo de Divisibilidade

Conjunto e Quantidade de Divisores

Sexto Ano

Prof. Angelo Papa Neto

PORTAL DA MATEMÁTICA
OBMEP

1 Conjunto dos divisores

Para cada número natural n, o conjunto dos números naturais que dividem n é denotado por $D(n)$, ou seja,

$$D(n) = \{d \in \mathbb{N} \mid d \text{ é natural e divide } n\}. \tag{1}$$

Chamamos $D(n)$ de **conjunto dos divisores** de n.

Como qualquer número natural não nulo divide 0, temos

$$D(0) = \{1, 2, 3, \ldots\}.$$

Por outro lado, se $n \neq 0$ e d é um natural que divide n, então d é menor do que n. Assim, para $n \neq 0$, o conjunto $D(n)$ está contido no conjunto $\{1, 2, 3, \ldots, n\}$ e, sendo assim, $D(n)$ tem uma quantidade finita de elementos. Assim é que, por exemplo, $D(6) = \{1, 2, 3, 6\}$, $D(10) = \{1, 2, 5, 10\}$.

Observe que 1 e n sempre são elementos de $D(n)$. Portanto, a única maneira de $D(n)$ ter um único elemento é se tivermos $1 = n$; de outra forma, o único número natural para o qual o conjunto dos divisores tem apenas um elemento é o número 1: $D(1) = \{1\}$. Se n é maior do que 1 então $D(n)$ tem pelo menos dois elementos (1 e o próprio n), ou seja, $\{1, n\} \subset D(n)$, para todo n maior do que 1.

Também, é possível caracterizar um número primo usando seu conjuntos de divisores.

> O conjunto $D(n)$ tem *exatamente* dois elementos, isto é, $D(n) = \{1, n\}$ se, e somente se, n é primo.

Realmente, pela definição de número primo, se um natural $n > 1$ não é primo, então n possui um divisor d tal que $d \neq 1, n$. Logo, $\{1, d, n\} \subset D(n)$, de forma que $D(n)$ possui pelo menos três elementos.

Exemplo 1. *Os números* 12 *e* 15 *têm conjuntos de divisores respectivamente iguais a*

$$D(12) = \{1, 2, 3, 4, 6, 12\} \text{ e}$$

$$D(15) = \{1, 3, 5, 15\}.$$

A interseção $D(12) \cap D(15) = \{1, 3\}$ *é formada pelos números naturais que são divisores comuns de* 12 *e* 15. *O maior elemento de* $D(12) \cap D(15)$ *é, portanto, o maior divisor comum de* 12 *e* 15.

O argumento do exemplo 1 pode ser generalizado:

> Se a e b são números naturais não ambos nulos, então os elementos do conjunto $D(a) \cap D(b)$ são os divisores comuns de a e de b. Em particular,
>
> $$\text{mdc}\,(a, b) = \max(D(a) \cap D(b)),$$
>
> onde $\max(D(a) \cap D(b))$ denota o maior elemento do conjunto $D(a) \cap D(b)$.

Em particular, se $a = 0$ e $b > 0$, então $D(b) \subset \{1, 2, 3, \ldots\} = D(0)$, de forma que $D(0) \cap D(b) = D(b)$. Assim,

$$\text{mdc}\,(0, b) = \max D(b) = b.$$

Outro fato interessante sobre $D(n)$ é que, em geral, seus elementos podem ser agrupados, de uma maneira natural, *em pares*. Para entendermos como isso funciona, consideremos os casos particulares em que $n = 45$ e $n = 36$. No caso $n = 45$, podemos escrever

$$D(45) = \{1, 45\} \cup \{3, 15\} \cup \{5, 9\};$$

no caso $n = 36$, temos

$$D(36) = \{1, 36\} \cup \{2, 18\} \cup \{3, 12\} \cup \{6\}.$$

Observe que, em ambos os casos, tentamos sempre agrupar os elementos de $D(n)$ (isto é, os divisores de n) em pares d, d', com $dd' = n$. Isso funciona porque, se $d \in D(n)$, então d divide n, logo, n/d é inteiro; mas aí, chamando n/d de d', vemos que $dd' = d \times (n/d) = n$, ou seja, que n também é divisível por d'. Isto quer dizer que $d' \in D(n)$, de maneira que podemos juntar d e d', formando o subconjunto $\{d, d'\}$ de $D(n)$. Por exemplo, no caso em que $n = 45$, tomando $d = 3$, temos $d' = 45/3 = 15$, o que corresponde ao subconjunto $\{3, 15\}$ de $D(45)$.

Pode ocorrer, contudo, que, ao realizarmos o emparelhamento descrito no parágrafo anterior, cheguemos à situação de um elemento $d \in D(n)$ que emparelha com ele mesmo, isto é, tal que $d' = d$. (Isso é o que ocorre no caso em que $n = 36$ e $d = 6$, quando $d' = 36/6 = 6$.) Nesses casos, temos $n = dd' = d^2$, um quadrado perfeito. Reciprocamente, supondo que n é um quadrado perfeito, digamos $n = d^2$, temos que o elemento $d \in D(n)$ emparelha com ele mesmo ($d' = d$), enquanto todos os outros elementos de $D(n)$ formam pares, da maneira descrita no parágrafo anterior. Assim, havendo k pares, a quantidade de elementos de $D(n)$ é, neste caso, igual a $2k + 1$, um número ímpar. Resumindo, temos:

> O conjunto $D(n)$ tem uma quantidade ímpar de elementos se, e somente se, n é um quadrado perfeito.

A seguir, exibimos mais dois exemplos, em um dos quais ocorre o emparelhamento de um elemento com ele mesmo.

Exemplo 2. *O emparelhamento dos elementos do conjunto* $D(20) = \{1, 2, 4, 5, 10, 20\}$ *é* $\{1, 20\}, \{2, 10\}$ *e* $\{4, 5\}$.

O emparelhamento dos elementos do conjunto

$$D(100) = \{1, 2, 4, 5, 10, 20, 25, 50, 100\}$$

é $\{1, 100\}, \{2, 50\}, \{4, 25\}, \{5, 20\}$ *e* $\{10, 10\}$. *O elemento* 10, *que emparelha com ele mesmo, é exatamente aquele cujo quadrado é igual a* 100.

2 Número de divisores

Nosso objetivo é, agora, contar a quantidade de elementos do conjunto $D(n)$, para $n \neq 0$, sem precisar listar todos esses elementos. Excluímos o número 0 pois, como vimos na seção anterior, $D(0)$ tem uma infinidade de elementos.

Vamos denotar por $d(n)$ o quantidade de elementos de $D(n)$, ou seja, $d(n)$ é a quantidade, ou **número de divisores** de n, para n natural não nulo.

Para valores pequenos de n é possível escrever explicitamente $D(n)$, como fizemos nos exemplos 1 e 2, e contar seus elementos. Se n é grande, essa tarefa se torna, em princípio, mais difícil. É necessário, portanto, um outro método para realizar essa contagem.

Para tal, vamos considerar a fatoração (única) de um número natural $n > 1$ como produto de potências de primos distintos:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}, \tag{2}$$

onde $p_1, p_2, \ldots, p_r$ são primos distintos e $\alpha_i \geq 1$, para cada i variando de 1 a r.

Exemplo 3. *O número 20 tem a seguinte fatoração como produto de potências de primos distintos:* $20 = 2^2 \cdot 5$. *Os divisores de 20, enumerados no exemplo 2, podem ser escritos como*

$$\begin{aligned}
1 &= 2^0 \cdot 5^0,\\
2 &= 2^1 \cdot 5^0,\\
4 &= 2^2 \cdot 5^0,\\
5 &= 2^0 \cdot 5^1,\\
10 &= 2^1 \cdot 5^1,\\
20 &= 2^2 \cdot 5^1.
\end{aligned}$$

A seguir, iremos mostrar que sempre é possível escrever os divisores de um número natural como fizemos no exemplo 3.

Suponhamos que d seja um divisor de n, diferente de 1. Se q é um primo que divide d, então q também divide n, logo q tem que ser um dos primos $p_1, \ldots, p_r$. Assim, os possíveis fatores primos de um divisor de n são também fatores primos de n. Podemos, então, escrever, para cada divisor d de n,

$$d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}, \tag{3}$$

onde $p_1, p_2, \ldots, p_r$ são os divisores primos distintos de n e, para cada i de 1 a r, temos $0 \leq \beta_i \leq \alpha_i$.

Conforme ilustramos já no exemplo 3, a inclusão do 0 como possibilidade para um ou mais dos β_i's permite que possamos representar todos os divisores de n. Realmente, no caso em que um primo p_i não aparece na decomposição de um divisor d, basta considerar que o expoente β_i de p_i em $d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$ é igual a 0. Note que, se todos os β_i's forem nulos, então $d = 1$.

Agora, a terefa de contar os divisores de n é relativamente simples: para cada potência $p_i^{\beta_i}$, temos $\alpha_i + 1$ possibilidades de escolha para o expoente β_i, que são os números naturais de 0 a α_i. Assim, cada fator $p_i^{\beta_i}$ de $p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$ contribui com $\alpha_i + 1$ possibilidades para a quantidade total de divisores. Pelo princípio fundamental da contagem, a quantidade total de divisores é o produto $(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_r + 1)$. Resumindo:

> Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ é a fatoração do número natural n como produto de potências de primos distintos, então a quantidade de divisores de n é
>
> $$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_r + 1).$$

Exemplo 4. *Determine a quantidade de divisores do número 1348.*

Solução. A fatoração de 1348 como produto de potâncias de primos é $1348 = 2^2 \cdot 337$. Dessa forma, $d(1348) = (2 + 1) \cdot (1 + 1) = 6$. □

Exemplo 5. *Determine a quantidade de divisores pares e ímpares do número* $n = 3^{12} - 1$.

Solução. Podemos fatorar o número n da seguinte maneira:

$$\begin{aligned}
n &= 3^{12} - 1 = (3^6 + 1)(3^6 - 1)\\
&= (3^6 + 1)(3^3 + 1)(3^3 - 1)\\
&= 730 \cdot 28 \cdot 26\\
&= 2^4 \cdot 5 \cdot 7 \cdot 13 \cdot 73.
\end{aligned}$$

Os divisores ímpares de n são aqueles que não possuem o fator 2, ou seja, são do tipo $5^a \cdot 7^b \cdot 13^c \cdot 73^d$, onde $a, b, c, d \in \{0, 1\}$. Logo, a quantidade de divisores ímpares de n é $2 \cdot 2 \cdot 2 \cdot 2 = 16$.

O total de divisores de n é

$$d(n) = (4 + 1) \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 5 \cdot 16 = 80.$$

Assim, a quantidade de divisores pares de n é $80 - 16 = 64$. □

Exemplo 6. *Encontre todos os números naturais menores do que 100 e que têm exatamente 12 divisores naturais.*

Solução. Queremos encontrar $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ de modo que $(\alpha_1 + 1) \ldots (\alpha_r + 1) = 12$. Devemos, então, estudar as diversas maneiras de escrever 12 como produto de números naturais.

Fatorando 12 como $3 \cdot 4$, obtemos $\alpha_1 = 2$ e $\alpha_2 = 3$, logo $n = p_1^2 p_2^3$. Como $n < 100$, a única possibilidade nesse caso é $n = 3^2 2^3 = 72$. Se $12 = 2 \cdot 2 \cdot 3$, então $n = p_1 p_2 p_3^2$ e a restrição $n < 100$ implica que os únicos valores possíveis são $3 \cdot 5 \cdot 2^2 = 60$, $7 \cdot 3 \cdot 2^2 = 84$ e $2 \cdot 5 \cdot 3^2 = 90$. A fatoração $12 = 6 \cdot 2$ fornece $n = p_1^5 p_2$ e a restrição $n < 100$ nos diz que o único valor possível para n é $2^5 \cdot 3 = 96$. A fatoração $12 = 12 \cdot 1$ fornece $n = p_1^{11} \geq 2^{11} > 100$. Logo, nesse caso não há valores de n satifazendo a restrição do enunciado. Portanto, os únicos naturais menores do que 100 e que têm exatamente 12 divisores são $60, 72, 84, 90$ e 96.

□

Dicas para o Professor

O conteúdo dessa aula pode ser visto em dois encontros de 50 minutos cada. A fórmula que fornece a quantidade de divisores de um número dado usa a fatoração única de um número natural maior do que 1 como produto de primos. Esse é um bom momento para relembrar esse importante resultado. Vale ressaltar que a unicidade, que é de vital importância aqui, não foi discutida explicitamente até o final do século XVIII, quando K. F. Gauss (1777 - 1855) estabeleceu rigorosamente esse resultado no seu tratado *Disquisitiones Arithmeticæ* (Investigações Aritméticas), publicado em 1801.

A justificativa da fórmula para $d(n)$ usa o princípio fundamental da contagem. Caso os alunos não tenham familiaridade com Combinatória, você pode explicar esse princípio com alguns exemplos simples (por exemplo, contando o número de cadeiras da sala multiplicando o número de filas pelo o número de cadeiras em cada fila).

Mais exemplos podem ser explorados. Eles podem ser encontrados nas referências ou na página da OBMEP, `www.obmep.org.br`.

Sugestões de Leitura Complementar

1. A. Caminha. *Tópicos de Matemática Elementar, Volume 5: Teoria dos Números.* Rio de Janeiro, Editora S.B.M., 2012.

2. E. de Alencar Filho. *Teoria Elementar dos Números.* São Paulo, Nobel, 1989.

3. J. P. de Oliveira Santos. *Introdução à Teoria dos Números.* Rio de Janeiro, Editora IMPA, 1998.