Divisibilidade: mdc e mmc

Vitória Aparecida Santos Ferreira - vitoriaaparecida94@gmail.com

26° Semana Olímpica - Janeiro 2023 - Nível 1

1 Definições iniciais

Serão apresentados alguns conceitos de Aritmética relacionados à divisibilidade.

1.1 Divisão euclidiana

Dados $a, b \in \mathbb{Z}_+, b > 0$, existem únicos inteiros q, r, chamados de *quociente* e *resto*, respectivamente, tais que

$$a = bq + r, 0 \leq r \leq b - 1.$$

Se $r = 0$, diz-se que b *divide* a e se escreve que $b|a$.

1.2 mdc e mmc: exemplos e propriedades

Sejam a, b inteiros positivos.

O **máximo divisor comum (mdc)** é o maior inteiro que divide os dois números originais simultaneamente. Se o mdc for 1, a, b são chamados de *coprimos* ou *primos entre si* ou *relativamente primos*.

O **mínimo múltiplo comum (mmc)** é o menor inteiro que é divisível por ambos os números originais.

Exemplos:

$\text{mdc}(12, 3) = 3$ $\text{mdc}(27, 45) = 9$ $\text{mmc}(31, 20) = 620$ $\text{mmc}(30, 72) = 360$.

Propriedades:

(i) Qualquer divisor comum desses números divide o $\text{mdc}(a, b)$.

> *Demonstração.* Denote $d := \text{mdc}(a, b)$. Usando a relação de Bézout, existem x, y inteiros tais que $d = ax + by$. Logo, dado c divisor comum dos números originais, ele pode ser colocado em evidência do lado direito da equação e, portanto, tem que dividir o lado esquerdo, isto é, d. □

(ii) Qualquer múltiplo comum desses números é divisível pelo $\text{mmc}(a, b)$.

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

> *Demonstração.* Considere $d := \text{mdc}(a, b)$ e $m := \text{mmc}(a, b)$. Por d dividir a, existe q inteiro com $a = qd \Rightarrow ab = (qd)b = d(qb)$. Note que qb é um múltiplo de b, mas também é um múltiplo e a, porque, pela equação acima,
>
> $$ab = d(qb) \Rightarrow \frac{(qb)}{a} = \frac{b}{d} \in \mathbb{Z}.$$

Por ser múltiplo comum de a, b, segue, de (ii), que existe c tal que $qb = mc$. Assim,

$$ab = d(qb) = d(mc).$$

Para encerrar a demonstração, é preciso ver que $c = 1$. Ocorre que

$$ab = dmc \Rightarrow \frac{a}{cd} = \frac{m}{b} \in \mathbb{Z}.$$

Portanto, cd divide a. De maneira semelhante, cd divide b. Por ser um divisor comum de a, b, tem-se, pela definição do mdc, que $cd \leq d$. Como $c \geq 1$, então $cd \geq d$ e a única forma de valer as duas desigualdades é que $cd = d$. Logo, $c = 1$ e

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

□

(iv) (Teorema de Euclides) Se $a = bq + r, 0 \leq r \leq b - 1$, então $\text{mdc}(a, b) = \text{mdc}(b, r)$.

Demonstração. Se mostrarmos que o conjunto $D(a, b)$ de divisores **comuns** de a, b coincide com o conjunto $D(b, r)$ de divisores **comuns** de b, r, então o resultado está provado, porque a busca pelo mdc chegará ao mesmo valor - o maior - percorrendo os dois conjuntos.

Seja d divisor de a, b. Com isso, d divide qualquer combinação linear de a, b, em particular $d|(a - bq = r)$. Portanto, d é divisor comum de b, r e, assim, $D(a, b) \subseteq D(b, r)$.

Tome, agora, $\tilde{d}$ divisor de b, r. Logo, $\tilde{d}|(bq + r = a)$ e segue que $\tilde{d}$ é divisor comum de a, b. Desse modo, $D(b, r) \subseteq D(a, b)$.

Pelas duas inclusões, $D(a, b) = D(b, r)$. □

1.3 Modos de calcular

Há alguns métodos para calcular cada uma das grandezas definidas acima.

Para o mdc:

- Fatoração em primos: a partir dela, toma-se o produto apenas dos primos **comuns** nas duas fatorações elevados aos **menores** expoentes.

- Algoritmo de Euclides: por (iv),

$$\text{mdc}(a, b) = \text{mdc}(b, r),$$

onde r é o resto da divisão de a por b. Repetindo este procedimento, consegue-se, a cada etapa, diminuir os números para facilitar o cálculo, de forma que

$$a = bq + r, r < b \Rightarrow \text{mdc}(a, b) = \text{mdc}(b, r)$$

$$b = rq_1 + r_1, r_1 < r \Rightarrow \text{mdc}(b, r) = \text{mdc}(r, r_1)$$

$$r = r_1q_2 + r_2, r_2 < r_1 \Rightarrow \text{mdc}(r, r_1) = \text{mdc}(r_1, r_2)$$

$$r_1 = r_2q_3 + r_3, r_3 < r_2 \Rightarrow \text{mdc}(r_1, r_2) = \text{mdc}(r_2, r_3)$$

$$\vdots$$

$$r_{n-2} = r_{n-1}q_n + r_n, r_n < r_{n-1} \Rightarrow \text{mdc}(r_{n-2}, r_{n-1}) = \text{mdc}(r_{n-1}, r_n).$$

Para o mmc:

- Listagem: usando uma lista crescente para os múltiplos de a e outra para os múltiplos de b, toma-se o primeiro que se repetir.

- Fatoração em primos: usam-se **todos** os primos que aparecem em ambas as fatorações e, quando aparecerem nas duas, usam-se os **maiores** expoentes.

2 Exercícios

Em problemas de divisibilidade, pode ser útil manipular a condição original para uma outra, usando fatos simples, como

- Na divisão de números positivos, divisor é sempre menor ou igual ao dividendo.
- Se $a|b$, então $a|kb$, para qualquer k inteiro positivo.
- Se $a|b$ e $a|c$, então $a|mb + nc$, para quaisquer m, n inteiros positivos.

1. (São Petersburgo - 1996) Encontre todos os inteiros positivos n com
$$3^{n-1} + 5^{n-1} | 3^n + 5^n.$$

2. (IMO - 1998) Determine todos os pares (x, y) de inteiros positivos tais que x^2y+x+y seja divisível por $xy^2 + y + 7$.

3. (Irã - 2005) Sejam $n, p > 1$ inteiros, com p primo. Se $n|(p-1)$ e $p|(n^3-1)$, prove que $4p - 3$ é quadrado perfeito.

   (Dica: fatorar $n^3 - 1$ para aparecer $n - 1$.)

4. (HMMT - Harvard-MIT Math Tournament - 2002 - adaptado) Calcule mdc$(2022 + 2, 2022^2 + 2, 2022^3 + 2, \dots)$.

5. (OBM - 2019 - Nível 2) Sejam a, b, k inteiros positivos com $k > 1$ tais que
$$\text{mmc}(a, b) + \text{mdc}(a, b) = k(a + b).$$

   Prove que $a + b \geq 4k$.

   (Dica: pode ser útil usar que mdc$(a, b) \cdot$ mmc$(a, b) = a \cdot b$.)

6. Prove que mdc$(a^m - 1, a^n - 1) = a^{\text{mdc}(m,n)} - 1$.

7. Prove que dois termos consecutivos na sequência de Fibonacci são coprimos.

   Nota: a sequência de Fibonacci, $(1, 1, 3, 5, 8, 13, \dots)$, é dada por $F_1 = F_2 = 1$ e $F_n = F_{n-1} + F_{n-2}, \forall\ n \geq 3$.

   (Dica: usar indução em n.)

8. (AIME - 1985) Considere a sequência $101, 104, 109, 116, \dots$, cujos números são construídos por $a_n = 100 + n^2$, quando $n \in \{1, 2, 3, 4, \dots\}$. Seja $d_n := \text{mdc}(a_n, a_{n+1})$. Encontre o maior valor de d_n.

9. Durante uma liquidação a preço único, duas amigas fizeram compras, gastando R$ 375,00 e R$ 405,00. Qual a quantidade mínima de peças compradas ao todo?

10. (AIME - 1998) Para quais valores de k ocorre que $12^{12} = \text{mmc}(6^6, 8^8, k)$?

11. (AMC - 2020) Quantos inteiros positivos n são tais que n é múltiplo de 5 e mmc$(5!, n) = 5 \cdot$ mdc$(10!, n)$?

    (Dica: usar a fatoração em primos de $5!, 10!$.)

Referências

[1] D. Fomin, S. Genkin, and Itenberg I. *Círculos matemáticos: a experiência russa*. IMPA, 1st edition, 2012.

[2] A. Hefez. *Iniciação à Aritmética*. IMPA, 1st edition, 2016.

[3] F.B. Martinez, C.G. Moreira, N. Saldanha, and E. Tengan. *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro*. Projeto Euclides, 1st edition, 2011.

[4] Justin Stevens. *Olympiad number theory through challenging problems*. https://numbertheoryguy.com/publications/olympiad-number-theory-book/, 3rd edition, 2016.