Teoria de Números

M. Lurdes Teixeira
Dep. Matemática
Univ. Minho

2º semestre de 2019/2020

Teoria de Números é uma área da Matemática cujo objetivo é estudar propriedades dos números inteiros relacionadas com a divisibilidade, tais como: paridade, primalidade, fatorização, multiplicatividade, aditividade, etc..

Aplicações recentes ...

em computação e em tecnologias de informação.

Áreas atuais de aplicação:

Física, Química, Biologia, Computação, Criptografia, Comunicação Digital, Música, ...

Temas centrais

- Aritmética Modular
- Primalidade e Fatorização

Definição

Dados números inteiros a e b diz-se que b divide a se existe k inteiro tal que $a = b\,k$. Em tal caso escreve-se $b \mid a$, caso contrário escreve-se $b \nmid a$.

Teorema

Sejam $a, b, c, d \in \mathbb{Z}$. Então,

1. $1 \mid a, \qquad a \mid a \quad$ e $\quad a \mid 0$;
2. $a \mid 1$ sse $a = \pm 1 \quad$ e $\quad 0 \mid a$ sse $a = 0$;
3. $a \mid b$ e $b \mid c$ implica que $a \mid c$;
4. se $c \neq 0$, então $a \mid b$ sse $ac \mid bc$;
5. $a \mid b$ e $c \mid d$ implica que $ac \mid bd$;
6. $a \mid b$ e $b \mid a$ implica que $a = \pm b$;
7. $a \mid b$ e $b \neq 0$ implica que $|a| \leq |b|$;
8. $a \mid b$ e $a \mid c$ implica que $a \mid (bx + cy)$ para quaisquer $x, y \in \mathbb{Z}$;
9. $a \mid b$ e $a \mid b + c$ implica que $a \mid c$.

PROVA

Vamos provar algumas das alíneas do teorema anterior.

Sejam $a, b, c, d \in \mathbb{Z}$.

3. Se $a \,|\, b$ e $b \,|\, c$, então existem $k_1, k_2 \in \mathbb{Z}$ tais que $b = a\,k_1$ e $c = b\,k_2$, pelo que $c = a\,k_1 k_2$.

5. Se $a \,|\, b$ e $c \,|\, d$, então existem $k_1, k_2 \in \mathbb{Z}$ tais que $b = a\,k_1$ e $c = d\,k_2$, pelo que $bd = ac\,k_1 k_2$, ou seja, $ac \,|\, bd$.

6. Se $a \,|\, b$ e $b \,|\, a$, então existem $k_1, k_2 \in \mathbb{Z}$ tais que $b = a\,k_1$ e $b = a\,k_2$, pelo que $ab = ab\,k_1 k_2$, ou seja $k_1 k_2 = 1$. Então $k_1 = k_2 = 1$ ou $k_1 = k_2 = -1$.

7. Se $a \,|\, b$ e $b \neq 0$, então existe $k \in \mathbb{Z}$ tal que $b = a\,k$ e, como $|k| \geq 1$, resulta que $|b| = |a\,k| = |a|\,|k| \geq |a|$.

8. Se $a \,|\, b$ e $a \,|\, c$, então existem $k_1, k_2 \in \mathbb{Z}$ tais que $b = a\,k_1$ e $c = a\,k_2$, pelo que $bx + cy = a\,k_1 x + a\,k_2 y = a(k_1 x + k_2 y)$, pelo que $a \,|\, (bx + cy)$ para quaisquer $x, y \in \mathbb{Z}$.

Teorema - algoritmo da divisão (euclidiana)

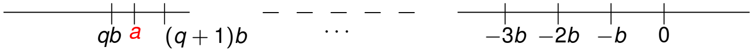
Dados números inteiros a e b com $b > 0$, existem e são únicos os inteiros q e r tais que $0 \leq r < b$ e

$$a = b\,q + r.$$

Graficamente ...

- caso $a > 0$

- caso $a < 0$ (notar que $q < 0$)



PROVA

(Existência de q e r) Consideremos o conjunto

$$S = \{a - xb \in \mathbb{N}_0 \,|\, x \in \mathbb{Z}\}$$

Seja $x = -|a|$. Como $b \geq 1$, então

$$a - xb \;=\; a + |a|b \;\geq\; a + |a| \;=\; \begin{cases} 0 & \text{se } a < 0 \\ 2a & \text{se } a \geq 0 \end{cases}$$

Em qualquer caso, $a + |a|b \geq 0$, pelo que $S \neq \emptyset$. Então, ou $0 \in S$ e 0 é o elemento mínimo de S, ou $S \subseteq \mathbb{N}$ e, Pelo Princípio da Boa Ordenação de $\mathbb{N}$, S tem um elemento mínimo r. Então, existe $q \in \mathbb{Z}$, tal que

$$r = a - qb.$$

Suponhamos que $b \leq r$. Então, $r - b \geq 0$ e

$$r - b = a - qb - b = a - \underbrace{(q + 1)}_{x} b.$$

Assim, $r - b \in S$ e $r - b < r$, o que é absurdo. Logo, $r < b$.

PROVA - continuação

(Unicidade de q e r) Suponhamos que existem $q, q' \in \mathbb{Z}$ e $r, r' \in \mathbb{N}_0$ tais que

$$\begin{array}{ll} a = bq + r & \text{e } \ 0 \leq r < b, \\ a = bq' + r' & \text{e } \ 0 \leq r' < b. \end{array}$$

Então,

$$bq + r = bq' + r' \Longrightarrow b|q - q'| = |r' - r| \qquad \text{e}$$

$$\left\{ \begin{array}{l} 0 \leq r < b \\ 0 \leq r' < b \end{array} \right. \Longrightarrow \left\{ \begin{array}{l} -b < -r \leq 0 \\ 0 \leq r' < b \end{array} \right. \Longrightarrow -b < r' - r < b \Longrightarrow |r' - r| < b$$

Consequentemente, $b|q - q'| < b$, o que implica que $|q - q'| < 1$. Como $q - q' \in \mathbb{Z}$, então $q - q' = 0$.

Sendo $q = q'$ e $bq + r = bq' + r'$, então $r = r'$.

Corolário

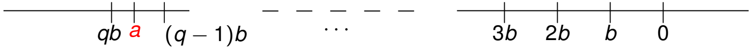
Dados números inteiros a e b com $b \neq 0$ existem e são únicos os inteiros q e r tais que $0 \leq r < |b|$ e

$$a = b \cdot q + r.$$

Graficamente no caso de $\mathbf{b} < \mathbf{0}$, tem-se:

- caso $a > 0$ (notar que $q \leq 0$)

- caso $a < 0$ (notar que $q > 0$)



PROVA

Pelo teorema anterior sabemos que existem e são únicos os inteiros q' e r' tais que

$$a = |b|q' + r' \text{ e } 0 \leq r' < |b|.$$

Se $b < 0$, então

$$a = |b|q' + r' \Leftrightarrow a = -bq' + r' \Leftrightarrow a = b(-q') + r'.$$

Neste caso, $q = -q'$ e $r = r'$.

Se $b > 0$, então

$$a = |b|q' + r' \Leftrightarrow a = bq' + r,$$

pelo que $q = q'$ e $r = r'$.

Dados $a, b \in \mathbb{Z}$ os números q e r dados pelo algoritmo da divisão dizem-se, respetivamente, o quociente e o resto da divisão de a por b.

Dividir a por b significa calcular o quociente e o resto da divisão de a por b.

EXEMPLO 1

$$\begin{array}{lllll}
a=2 & b=6 & 2=6\times 0+2 & q=0 & r=2\\
a=2 & b=-6 & 2=-6\times 0+2 & q=0 & r=2\\
a=-2 & b=6 & -2=6\times -1+4 & q=-1 & r=4\\
a=-2 & b=-6 & -2=-6\times 1+4 & q=1 & r=4\\
a=9 & b=6 & 9=6\times 1+3 & q=1 & r=3\\
a=9 & b=-6 & 9=-6\times (-1)+3 & q=-1 & r=3\\
a=-9 & b=6 & -9=6\times (-2)+3 & q=-2 & r=3\\
a=-9 & b=-6 & -9=-6\times 2+3 & q=2 & r=3
\end{array}$$

Proposição

Sejam $a, b \in \mathbb{Z}$. Então $b\,|\,a$ sse o resto da divisão de a por b é zero.

PROVA

$$b\,|\,a \quad\Leftrightarrow\quad \exists_{k\in\mathbb{Z}}\; a=bk \quad\Leftrightarrow\quad \exists_{k\in\mathbb{Z}}\; a=bk+0$$

Sejam $a, b \in \mathbb{Z}$ e D o conjunto dos divisores comuns de a e b, *i.e.*,

$$D = \{d \in \mathbb{Z} \mid d \,|\, a, d \,|\, b\}.$$

Como $1 \,|\, a$ e $1 \,|\, b$, então $1 \in D$. Se $a = b = 0$, então $D = \mathbb{N}$. Senão, se $d \in D$, então $|d| \leq \text{máx}\{|a|, |b|\}$ (pela alínea 6. do teorema anterior), pelo que D é um conjunto finito não vazio.

Definição

Dados a e b inteiros não ambos nulos, chama-se máximo divisor comum de a e b ao maior inteiro d que divide a e divide b, o qual se representa por $\mathrm{m.d.c.}(a, b)$.

Proposição

Sejam $a, b \in \mathbb{Z}$ e $b \neq 0$.

1. $\mathrm{m.d.c.}(a, b) = \mathrm{m.d.c.}(|a|, |b|) = \mathrm{m.d.c.}(b, a)$.
2. se $b \,|\, a$, então $\mathrm{m.d.c.}(a, b) = |b|$.
3. $\mathrm{m.d.c.}(0, b) = |b|$.

Proposição - Igualdade de Bezout

Sejam a e b inteiros, não ambos nulos, e $d = \mathrm{m.d.c.}(a, b)$. Então existem $x, y \in \mathbb{Z}$ tais que $d = ax + by$.

PROVA

Suponhamos que $a \neq 0$. Seja
$$S = \{ax + by \mid x, y \in \mathbb{Z}, ax + by \in \mathbb{N}\}.$$
Notar que $S \neq \emptyset$ porque, por exemplo, $a^2 \in S$ ($a^2 = a\,a + b\,0$). Pelo Princípio da Boa Ordenação de $\mathbb{N}$, S tem elemento mínimo m. Como $m \in S$, existem $x, y \in \mathbb{Z}$ tais que
$$m = ax + by.$$

$m \mid a$ Como $m > 0$, existem inteiros q e r tais que $a = mq + r$ e $0 \leq r < m$. Então,
$$0 \leq r = a - mq = a - (ax + by)q = a(1 - x) + b(-yq).$$
Logo, se $r > 0$, $r \in S$, pelo que $m \leq r$, o que é impossível. Assim, $r = 0$.
Sendo $r = 0$, $a = mq$ pelo que $m \mid a$.

$m \mid b$ Análoga à prova anterior de que $m \mid a$.

$m = d$ Como $m \mid a$ e $m \mid b$, então $m \leq \mathrm{m.d.c.}(a, b) = d$. Como $d \mid (ax + by)$, então $d \leq m$.

Logo, $d = m = ax + by$.

Teorema

Sejam a e b inteiros não ambos nulos e $d \in \mathbb{N}$. Então $d = \mathrm{m.d.c.}(a, b)$ sse

1. $d \,|\, a$ e $d \,|\, b$,
2. se $c \in \mathbb{N}$ e $c \,|\, a$ e $c \,|\, b$, então $c \,|\, d$.

PROVA

Seja $d = \mathrm{m.d.c.}(a, b)$. Então, por definição, d verifica a condição 1.

Seja $c \in \mathbb{N}$ tal que $c \,|\, a$ e $c \,|\, b$. Então $c \,|\, ax + by$ para quaisquer $x, y \in \mathbb{Z}$. Logo $c \,|\, d$.

A prova da implicação recíproca é proposta como exercício.

O resultado deste teorema serve por vezes como definição do $\mathrm{m.d.c.}$ de dois inteiros.

Teorema

Sejam a e b inteiros não ambos nulos. Sendo $c \in \mathbb{N}$,

1. $\mathrm{m.d.c.}(ac, bc) = c\,\mathrm{m.d.c.}(a, b)$;
2. se $c \mid a$ e $c \mid b$, então $\mathrm{m.d.c.}\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c}\mathrm{m.d.c.}(a, b)$.

PROVA

Sejam a e b inteiros não ambos nulos e $d = \mathrm{m.d.c.}(a, b)$.

1. Como $d \mid a$ e $d \mid b$, então $dc \mid ac$ e $dc \mid bc$, pelo que, $dc \mid \mathrm{m.d.c.}(ac, bc)$.
   Assim, $\mathrm{m.d.c.}(ac, bc) = kdc$, para algum $k \in \mathbb{N}$ e
   $$\left.\begin{array}{ll} kdc \mid ac & \Rightarrow kd \mid a \\ kdc \mid bc & \Rightarrow kd \mid b \end{array}\right\} \Rightarrow kd \mid d \Rightarrow k = 1.$$
2. $\mathrm{m.d.c.}(a, b) = \mathrm{m.d.c.}\left(c\frac{a}{c}, c\frac{b}{c}\right) = c \times \mathrm{m.d.c.}\left(\frac{a}{c}, \frac{b}{c}\right)$. Então,
   $$\frac{1}{c}\mathrm{m.d.c.}(a, b) = \mathrm{m.d.c.}\left(\frac{a}{c}, \frac{b}{c}\right).$$

Proposição

Dados a e b inteiros, se q e r são inteiros tais que $a = b \cdot q + r$, então $\mathrm{m.d.c.}(a, b) = \mathrm{m.d.c.}(b, r)$.

PROVA

Seja c um divisor comum de a e de b. Então,

$$c \,|\, (a - bq).$$

Logo, c é um dividor comum de b e de r.

Reciprocamente, se c um divisor comum de b e de r, então,

$$c \,|\, (a - bq).$$

Como $c \,|\, b$, conclui-se que $c \,|\, a$. Logo, c é um dividor comum de a e de b.

Em resumo, os divisores comuns de a e b são os divisores comuns de b e r. Então, $\mathrm{m.d.c.}(a, b) = \mathrm{m.d.c.}(b, r)$.

O algoritmo de Euclides tem por objetivo o cálculo do máximo divisor comum de dois inteiros e baseia-se nesta proposição.

EXEMPLO 2

$$\text{m.d.c.}(486, 218) = ?$$

$$\begin{aligned}
486 &= 218 \times 2 + 50 \\
218 &= 50 \times 4 + 18 \\
50 &= 18 \times 2 + 14 \\
18 &= 14 \times 1 + 4 \\
14 &= 4 \times 3 + 2 \\
4 &= 2 \times 2 + 0
\end{aligned}
\qquad
\begin{aligned}
\text{m.d.c.}(486, 218) &= \text{m.d.c.}(218, 50) \\
&= \text{m.d.c.}(50, 18) \\
&= \text{m.d.c.}(18, 14) \\
&= \text{m.d.c.}(14, 4) \\
&= \text{m.d.c.}(4, 2) \\
&= \text{m.d.c.}(2, 0) \\
&= 2
\end{aligned}$$

Teorema

Sejam a e b inteiros tais que $b \neq 0$. Aplicando sucessivamente o algoritmo da divisão, o processo termina ao fim de $n+2$ ($n \geq -1$) etapas, obtendo-se :

$$\begin{array}{lll}
a = b\,q_0 + r_0 & q_0, r_0 \in \mathbb{N}_0 & 0 < r_0 < |b| \\
b = r_0 q_1 + r_1 & q_1, r_1 \in \mathbb{N}_0 & 0 < r_1 < r_0 \\
r_0 = r_1 q_2 + r_2 & q_2, r_2 \in \mathbb{N}_0 & 0 < r_2 < r_1 \\
\vdots & \vdots & \vdots \\
r_{n-2} = r_{n-1} q_n + r_n & q_n, r_n \in \mathbb{N}_0 & 0 < r_n < r_{n-1} \\
r_{n-1} = r_n q_{n+1} + r_{n+1} & q_{n+1}, r_{n+1} \in \mathbb{N}_0 & 0 = r_{n+1} < r_n
\end{array}$$

em que $n+1 \geq 0$, considerando que $r_{-1} = b$. Assim, a sequência dos inteiros da forma r_i é uma sequência finita:

$$(r_{-1}, r_0, r_1, \ldots, r_n, 0),$$

e

$$r_n = \mathrm{m.d.c.}(a, b).$$

Algoritmo de Euclides

Entrada: a e b.

1. $x = a$, $y = b$.
2. Se $y = 0$, então $\mathrm{m.d.c.}(a, b) = x$ e terminar.
3. $r \leftarrow$ resto da divisão de x por y,
   $x \leftarrow y$,
   $y \leftarrow r$,

   voltar a 2.

Saída: $\mathrm{m.d.c.}(a, b)$.

Algoritmo de Euclides estendido

O algoritmo de Euclides estendido tem por objetivo o cálculo do $\mathrm{m.d.c.}$ de dois inteiros a e b, bem como de inteiros x e y referidos na igualdade de Bezout.

EXEMPLO 2- continuação

$$\mathrm{m.d.c.}(486, 218) = 2$$

$$\begin{array}{lcl}
\downarrow \qquad \quad \downarrow & & \\
486 = 218 \times 2 + 50 & \rightarrow & 2 = -218 \times 11 + (\underbrace{486 - 218 \times 2}) \times 48 \\
 & & \qquad = \mathbf{486} \times \mathbf{48} + \mathbf{218} \times (\mathbf{-107}) \\
218 = 50 \times 4 \ + 18 & \rightarrow & 2 = 50 \times 4 - (\underbrace{218 - 50 \times 4}) \times 11 = -218 \times 11 + \mathbf{50} \times 48 \\
50 = 18 \times 2 \ + 14 & \rightarrow & 2 = -18 \times 3 + (\underbrace{50 - 18 \times 2}) \times 4 = 50 \times 4 - \mathbf{18} \times 11 \\
18 = 14 \times 1 \ + 4 & \rightarrow & 2 = 14 - (\underbrace{18 - 14 \times 1}) \times 3 = -18 \times 3 + \mathbf{14} \times 4 \\
14 = 4 \times 3 \ + 2 & \rightarrow & 2 = 14 - \mathbf{4} \times 3 \\
4 = 2 \times 2 \ + 0 & & \\
 & & \uparrow \qquad \qquad \qquad \qquad \qquad \qquad \uparrow
\end{array}$$

$$x = 48 \qquad \qquad y = -107$$

EXEMPLO 3

Considere-se a equação linear $486x + 218y = 2$ nas incógnitas x e y.

Existem soluções inteiras para esta equação? Pelo exposto anteriormente, existe pelo menos uma solução que é

$$x = 48 \ \text{ e } \ y = -107.$$

Em geral, qualquer par do tipo

$$\left(48 + k\frac{218}{2}, \ -107 - k\frac{486}{2}\right)$$

com $k \in \mathbb{Z}$, é solução da equação, porque

$$\begin{aligned} & 486\left(48 + k\frac{218}{2}\right) + 218\left(-107 - k\frac{486}{2}\right) = 2 \\ & \Leftrightarrow 486 \times 48 + 486 \times k\frac{218}{2} - 218 \times 107 - 218 \times k\frac{486}{2} = 2 \\ & \Leftrightarrow (486 \times 48 - 218 \times 107) + \left(486 \times k\frac{218}{2} - 218 \times k\frac{486}{2}\right) = 2 \\ & \Leftrightarrow 2 + 0 = 2 \end{aligned}$$

Definição

Dois inteiros a e b não ambos nulos, dizem-se primos entre si se $\mathrm{m.d.c.}(a,b)=1$.

Teorema

Dados a e b inteiros não ambos nulos, então a e b são primos entre si sse existem inteiros x e y tais que $1 = ax + by$.

Proposição

Dados a e b inteiros não ambos nulos, se $d = \mathrm{m.d.c.}(a,b)$, então $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si.

Proposição

Sejam a e b são inteiros primos entre si. Se $c \in \mathbb{Z}$ é tal que $a \mid c$ e $b \mid c$, então $ab \mid c$.

Lema de Euclides

Sejam a e b inteiros primos entre si. Se $c \in \mathbb{Z}$ é tal que $a \mid bc$, então e $a \mid c$.

PROVA

Se a e b são inteiros primos entre si, então, existem $x, y \in \mathbb{Z}$ tais que $1 = ax + by$. Assim,

$$c = acx + bcy.$$

Como $a \mid ac$ e $a \mid bc$, então $a \mid (acx + bcy)$, ou seja, $a \mid c$.

EXEMPLO 4

- $15 \mid (2 \times 45)$ e $15 \mid 45$.
- $15 \mid 9 \times 10$ mas $15 \nmid 9$ e $15 \nmid 10$.

Proposição

Sejam $a, b, c \in \mathbb{Z} \setminus \{0\}$. Então $\text{m.d.c.}(a, c) = \text{m.d.c.}(b, c) = 1$ sse $\text{m.d.c.}(ab, c) = 1$.

PROVA

Resumidamente,

- $$\left.\begin{array}{ll} \text{m.d.c.}(a,c) = 1 & \Rightarrow 1 = ax + cy \\ \text{m.d.c.}(b,c) = 1 & \Rightarrow 1 = bx' + cy' \end{array}\right\}$$
  $$\Rightarrow 1 = (ax + cy)(bx' + cy') = ab\,(xx') + c\,(axy' + bx'y + cyy')$$
  $$\Rightarrow \text{m.d.c.}(ab, c) = 1$$
- $$\text{m.d.c.}(ab, c) = 1 \Rightarrow 1 = ab\,x + cy \Rightarrow \left\{\begin{array}{l} 1 = a\,(bx) + cy \Rightarrow \text{m.d.c.}(a,c) = 1 \\ 1 = b\,(ax) + cy \Rightarrow \text{m.d.c.}(b,c) = 1 \end{array}\right.$$

Dados a e b inteiros não nulos, o conjunto dos inteiros positivos múltiplos de a e b é

$$M = \{x \in \mathbb{N} : a \mid x, b \mid x\}$$

Notar que M é um subconjunto de $\mathbb{N}$ não vazio, pois $|ab| \in M$.

Então, pelo Princípio de Boa Ordenação de $\mathbb{N}$, M tem elemento mínimo.

Definição

Dados a e b inteiros não nulos, chama-se mínimo múltiplo comum de a e b ao menor inteiro positivo que é divisível por a e por b.

O mínimo múltiplo comum de a e b representa-se por $\mathrm{m.m.c.}(a, b)$.

Proposição

Sejam $a, b \in \mathbb{Z} \setminus \{0\}$.

1. $\mathrm{m.m.c.}(a, b) = \mathrm{m.m.c.}(|a|, |b|) = \mathrm{m.m.c.}(b, a)$.
2. $\mathrm{m.m.c.}(a, a) = |a|$.
3. se $b \mid a$, então $\mathrm{m.m.c.}(a, b) = |a|$.
4. $\mathrm{m.d.c.}(a, b) \mid \mathrm{m.m.c.}(a, b)$.
5. $\mathrm{m.m.c.}(ka, kb) = |k| \, \mathrm{m.m.c.}(a, b)$ para qualquer $k \in \mathbb{Z} \setminus \{0\}$.

Teorema

Sejam $a, b \in \mathbb{Z} \setminus \{0\}$. Então, $m = \mathrm{m.m.c.}(a, b)$ sse

1. $a \mid m$ e $b \mid m$,
2. se $c \in \mathbb{N}$ e $a \mid c$ e $b \mid c$, então $m \mid c$.

PROVA

Seja $m = \mathrm{m.m.c.}(a, b)$. Pela definição de mínimo múltiplo comum, a condição 1. é válida.

Pelo algoritmo da divisão, existem inteiros q e r, com $0 \leq r < m$, tais que

$$c = mq + r.$$

Como $a \mid m$, $a \mid c$ e $b \mid m$, $b \mid c$, então $a \mid r$ e $b \mid r$, respetivamente. Consequentemente, $r = 0$ ou $m = \mathrm{m.m.c.}(a, b) \leq r$. Logo $r = 0$ e $m \mid c$.

Reciprocamente, a condição 1. implica que m é um múltiplo comum de a e b, e a condição 2. implica que $m \leq c$, para qualquer múltiplo comum de a e b.

O resultado deste teorema serve por vezes como definição do $\mathrm{m.m.c.}$ de dois inteiros.

Teorema

Sejam $a, b \in \mathbb{Z} \setminus \{0\}$. Então

$$m = \text{m.m.c.}(a, b) = \frac{|ab|}{\text{m.d.c.}(a, b)}.$$

PROVA Sem perda de generalidade, suponhamos que $a, b > 0$.

- **Caso $\text{m.d.c.}(a, b) = 1$**

  Como ab é múltiplo de a e b, então $m \mid ab$, pelo teorema anterior. Mas, se $\text{m.d.c.}(a, b) = 1$, $a \mid m$ e $b \mid m$, então $ab \mid m$. Logo $m = ab = \frac{|ab|}{\text{m.d.c.}(a,b)}$.

- **Caso $\text{m.d.c.}(a, b) = d \in \mathbb{N}$**

  Sabemos que $\text{m.d.c.}(\frac{a}{d}, \frac{b}{d}) = 1$, o que implica que $\text{m.m.c.}(\frac{a}{d}, \frac{b}{d}) = \frac{(\frac{a}{d} \cdot \frac{b}{d})}{\text{m.d.c.}(\frac{a}{d}, \frac{b}{d})}$.

  Por outro lado, $\text{m.m.c.}(a, b) = d\, \text{m.m.c.}(\frac{a}{d}, \frac{b}{d})$, donde se conclui que

$$\text{m.m.c.}(a, b) = d \frac{\left| \frac{a}{d} \; \frac{b}{d} \right|}{1} = d \frac{|ab|}{d^2} = \frac{|ab|}{d} = \frac{|ab|}{\text{m.d.c.}(a, b)}.$$