Lista 2 com respostas

MAT0120 — 1° SEMESTRE DE 2020

Divisibilidade.

Exercício 1.
Mostre que um inteiro a é par se e somente se a^2 for par.

Solução 1.
$(\Rightarrow)$

$$a = 2k \Rightarrow a^2 = 4k^2 = 2\left(2k^2\right); k \in \mathbb{Z}.$$

Logo, se a é par, então a^2 também é.

$(\Leftarrow)$
Podemos provar a contrapositiva: se a é ímpar, então a^2 é ímpar. De fato:

$$a = 2k + 1 \Rightarrow a^2 = 4k^2 + 4k + 1 = 2\left(2k^2 + 2k\right) + 1 = 2k' + 1; k' \in \mathbb{Z}.$$

Exercício 2.
Mostre que o produto de três inteiros consecutivos é divisível por 6 e que o produto de quatro inteiros consecutivos é divisível por 24.

Solução 2.
Seja $x = n(n+1)(n+2)$ o produto de três números consecutivos. Precisamos provar que $6 \mid x$. De fato, em três números consecutivos, temos no mínimo um número par e apenas um número múltiplo de 3, logo, o produto é múltiplo de 6.

No entanto, vamos provar utilizando o algoritmo da divisão, onde $n = 6k + r$ para $k \in \mathbb{Z}$ e $r \in \{0, 1, 2, 3, 4, 5\}$.

- $n = 6k \Rightarrow x = 6k(6k+1)(6k+2) \Rightarrow 6 \mid x$;
- $n = 6k+1 \Rightarrow x = (6k+1)(6k+2)(6k+3) = 6(6k+1)(3k+1)(2k+1) \Rightarrow 6 \mid x$;
- $n = 6k+2 \Rightarrow x = (6k+2)(6k+3)(6k+4) = 6(3k+1)(2k+1)(6k+4) \Rightarrow 6 \mid x$;
- $n = 6k+3 \Rightarrow x = (6k+3)(6k+4)(6k+5) = 6(2k+1)(3k+2)(6k+5) \Rightarrow 6 \mid x$;
- $n = 6k+4 \Rightarrow x = (6k+4)(6k+5)(6k+6) = 6(6k+4)(6k+5)(k+1) \Rightarrow 6 \mid x$;
- $n = 6k+5 \Rightarrow x = (6k+5)(6k+6)(6k+7) = 6(6k+5)(k+1)(6k+7) \Rightarrow 6 \mid x$.

Seja $y = n\,(n+1)\,(n+2)\,(n+3)$ o produto de quatro números consecutivos. Precisamos provar que $24 \mid y$. De fato, em quatro números consecutivos, temos obrigatoriamente dois pares e dois ímpares. Dentre os pares, um deles é múltiplo de 2 enquanto o outro é múltiplo de 4, logo, o produto é múltiplo de 8 e, dentre os ímpares, um dos dois é obrigatoriamente múltiplo de 3.

Como, pelo item a), $6 \mid n\,(n+1)\,(n+2)$, então $6 \mid y$, logo $3 \mid y$. Além disso, como $\text{mdc}\,(3,8) = 1$, assim, $24 \mid y \Leftrightarrow 3 \mid y\ \text{ e }\ 8 \mid y$. Vamos provar que $8 \mid y$.

Pelo algoritmo da divisão, temos que $n = 4k + r$ para $k \in \mathbb{Z}$ e $r \in \{0, 1, 2, 3\}$.

- $n = 4k \Rightarrow y = 4k\,(4k+1)\,(4k+2)\,(4k+3) = 8k\,(4k+1)\,(2k+1)\,(4k+3) \Rightarrow 8 \mid y$;
- $n = 4k+1 \Rightarrow y = (4k+1)\,(4k+2)\,(4k+3)\,(4k+4) = 8\,(4k+1)\,(2k+1)\,(4k+3)\,(k+1) \Rightarrow 8 \mid y$;
- $n = 4k+2 \Rightarrow y = (4k+2)\,(4k+3)\,(4k+4)\,(4k+5) = 8\,(2k+1)\,(4k+3)\,(k+1)\,(4k+5) \Rightarrow 8 \mid y$;
- $n = 4k+3 \Rightarrow y = (4k+3)\,(4k+4)\,(4k+5)\,(4k+6) = 8\,(4k+3)\,(k+1)\,(4k+5)\,(2k+3) \Rightarrow 8 \mid y$.

Exercício 3.
Mostre que $4 \nmid n^2 + 2$ para qualquer inteiro n.

Solução 3.
Pelo algoritmo da divisão, $n = 2k + r; k \in \mathbb{Z}$ e $r \in \{0, 1\}$.

- $n = 2k \Rightarrow n^2 + 2 = 4k^2 + 2 \Rightarrow 4 \nmid n^2 + 2$ pois $4 \mid 4k^2\ \text{ e }\ 4 \nmid 2$;
- $n = 2k+1 \Rightarrow n^2 + 2 = 4k^2 + 4k + 3 \Rightarrow 4 \nmid n^2 + 2$ pois $4 \mid \left(4k^2 + 4k\right)\ \text{ e }\ 4 \nmid 3$.

Exercício 4.
Prove que se $a \in \mathbb{Z}$, então $360 \mid a^2(a^2-1)(a^2-4)$.

Solução 4.
Seja $x = a^2\left(a^2-1\right)\left(a^2-4\right) = \underbrace{(a-2)\,(a-1)\,a\,(a+1)\,(a+2)}_{\text{cinco números consecutivos}}\,a$.

Pelo algoritmo da divisão, $a = 5k + r; k \in \mathbb{Z}$ e $r \in \{0, 1, 2, 3, 4\}$.

- $a = 5k \Rightarrow 5 \mid x$;
- $a = 5k+1 \Rightarrow (a-1) = 5k \Rightarrow 5 \mid x$;
- $a = 5k+2 \Rightarrow (a-2) = 5k \Rightarrow 5 \mid x$;
- $a = 5k+3 \Rightarrow (a+2) = 5k+5 = 5\,(k+1) \Rightarrow 5 \mid x$;
- $a = 5k+2 \Rightarrow (a-2) = 5k \Rightarrow 5 \mid x$.

Logo, $5 \mid x$.

Novamente, pelo algoritmo da divisão, $a = 3k + r; k \in \mathbb{Z}$ e $r \in \{0, 1, 2\}$.

- $a = 3k \Rightarrow a^2 = 9 \Rightarrow 9 \mid x$;
- $a = 3k + 1 \Rightarrow (a - 1)(a + 2) = 9k(k + 1) \Rightarrow 9 \mid x$;
- $a = 3k + 2 \Rightarrow (a - 2)(a + 1) = 9k(k + 1) \Rightarrow 9 \mid x$.

Como pelo exercício 2 sabemos que 8 divide 4 números consecutivos, então $8 \mid x$.

Assim:

$$5 \mid x \text{ e } 9 \mid x \ \text{ e } 8 \mid x \Rightarrow \text{mmc}(5, 9, 8) = 360 \mid x.$$

Exercício 5.
Seja a um inteiro. Mostre que:

a) $a^2 - a$ é divisível por 2;

b) $a^3 - a$ é divisível por 6;

c) $a^5 - a$ é divisível por 30.

Solução 5.

a) Seja $x = a^2 - a = a(a - 1)$, temos, pelo algoritmo da divisão, que $a = 2k + r; k \in \mathbb{Z}$ e $r \in \{0, 1\}$.
   - $n = 2k \Rightarrow a(a - 1) = 2k(2k - 1) \Rightarrow 2 \mid a^2 - a$;
   - $n = 2k + 1 \Rightarrow a(a - 1) = 2k(2k + 1) \Rightarrow 2 \mid a^2 - a$.

b) Seja $x = a^3 - a = (a - 1)a(a + 1)$. Provamos no exercício 2 que 6 divide três números consecutivos.

c) Seja $x = a^5 - a = a\left(a^4 - 1\right) = (a - 1)a(a + 1)\left(a^2 + 1\right)$. Pelo exercício 2, sabemos que $6 \mid x$. Vamos provar que $5 \mid x$.

   Pelo algoritmo da divisão, $a = 5k + r; k \in \mathbb{Z}$ e $r \in \{0, 1, 2, 3, 4\}$.
   - $a = 5k \Rightarrow 5 \mid x$;
   - $a = 5k + 1 \Rightarrow (a - 1) = 5k \Rightarrow 5 \mid x$;
   - $a = 5k + 2 \Rightarrow \left(a^2 + 1\right) = 5\left(5k^2 + 4k + 1\right) \Rightarrow 5 \mid x$;
   - $a = 5k + 3 \Rightarrow \left(a^2 + 1\right) = 5\left(5k^2 + 6k + 2\right) \Rightarrow 5 \mid x$;
   - $a = 5k + 4 \Rightarrow (a + 1) = 5(k + 1) \Rightarrow 5 \mid x$.

   Assim:

$$5 \mid x \ \text{ e } 6 \mid x \Rightarrow \text{mmc}(5, 6) = 30 \mid x.$$

Exercício 6.
Mostre que todo inteiro do forma $6k + 5$ é também da forma $3k + 2$, mas o contrario é falso.

Solução 6.
Temos que $6k + 5 = 2 \cdot 3k + 3 + 2 = 3(2k + 1) + 2 = 3k' + 2; k' \in \mathbb{Z}$. Como contraexemplo: $8 = 3 \cdot 2 + 2 = 6 \cdot 1 + 2$.

Exercício 7.
Usando o Algoritmo da Divisão, mostre que:

a) todo inteiro impar é da forma $4k + 1$ ou $4k + 3$;

b) o quadrado de todo inteiro é do forma ou $3k$ ou $3k + 1$;

c) o cubo de todo inteiro é do forma $9k$ ou $9k + 1$ ou $9k + 8$.

Solução 7.

a) Pelo algoritmo da divisão, $p = 2k + r; k \in \mathbb{Z}$ e $r \in \{0, 1\}$.
   - $p = 2k \Rightarrow n = 4k + 1$;
   - $p = 2k + 1 \Rightarrow n = 4k + 3$.

b) Pelo algoritmo da divisão, $n = 3p + r; p \in \mathbb{Z}$ e $r \in \{0, 1, 2\}$.
   - $n = 3p \Rightarrow n^2 = 3 \cdot \left(3p^2\right) = 3k; k \in \mathbb{Z}$;
   - $n = 3p + 1 \Rightarrow n^2 = 3 \cdot \left(3p^2 + 2p\right) + 1 = 3k + 1; k \in \mathbb{Z}$;
   - $n = 3p + 2 \Rightarrow n^2 = 3 \cdot \left(3p^2 + 4p + 1\right) + 1 = 3k + 1; k \in \mathbb{Z}$.

c) Pelo algoritmo da divisão, $n = 3p + r; p \in \mathbb{Z}$ e $r \in \{0, 1, 2\}$.
   - $n = 3p \Rightarrow n^3 = 9 \cdot \left(3p^3\right) = 9k; k \in \mathbb{Z}$;
   - $n = 3p + 1 \Rightarrow n^3 = 9 \cdot \left(3p^3 + 3p^2 + p\right) + 1 = 9k + 1; k \in \mathbb{Z}$;
   - $n = 3p + 2 \Rightarrow n^3 = 9 \cdot \left(3p^3 + 6p^2 + 4p\right) + 8 = 9k + 8; k \in \mathbb{Z}$.

Exercício 8.
Para $n \geqslant 1$, mostre que $\dfrac{n(n+1)(2n+1)}{6}$ é um inteiro. (*Dica:* Usando o Algoritmo da Divisão, n tem forma $6k$ ou $6k + 1$ ou $\cdots$ ou $6k + 5$. Mostre o resulto em todos os casos).

Solução 8.
Seja $x = \dfrac{n(n+1)(2n+1)}{6}$. Pelo algoritmo da divisão, $n = 6p + r; p \in \mathbb{Z}$ e $r \in \{0, 1, 2, 3, 4, 5\}$.

- $n = 6p \Rightarrow x = k(6k + 1)(12k + 1) \in \mathbb{Z}$;
- $n = 6p + 1 \Rightarrow x = (6k + 1)(3k + 1)(4k + 1) \in \mathbb{Z}$;
- $n = 6p + 2 \Rightarrow x = (3k + 1)(2k + 1)(12k + 5) \in \mathbb{Z}$;

- $n = 6p + 3 \Rightarrow x = (2k + 1)(3k + 2)(12k + 7) \in \mathbb{Z}$;
- $n = 6p + 4 \Rightarrow x = (3k + 2)(6k + 5)(4k + 3) \in \mathbb{Z}$;
- $n = 6p + 5 \Rightarrow x = (6k + 5)(k + 1)(12k + 1) \in \mathbb{Z}$.

Exercício 9.
Verifique que se um inteiro n é um quadrado e um cubo simultaneamente (como no caso $64 = 8^2 = 4^3$), assim n é da forma $7k$ ou $7k + 1$.

Solução 9.
Seja n um número que é um quadrado e um cubo simultaneamente. Assim, $\exists a, b \in \mathbb{Z}$ tais que $n = a^2 = b^3$.

Pelo algoritmo da divisão, temos que $x = 7p + r; p \in Z$ e $r \in \{0, 1, 2, 3, 4, 5, 6\}$.

x	x^2	x^3
$7p$	$7(7p^2) = 7k$	$7(49p^3) = 7k$
$7p + 1$	$7(7p^2 + 2p) + 1 = 7k + 1$	$7(49p^3 + 21p^2 + 3p) + 1 = 7k + 1$
$7p + 2$	$7(7p^2 + 4p) + 4 = 7k + 4$	$7(49p^3 + 42p^2 + 12p + 1) + 1 = 7k + 1$
$7p + 3$	$7(7p^2 + 6p + 1) + 2 = 7k + 2$	$7(49p^3 + 63p^2 + 27p + 3) + 6 = 7k + 6$
$7p + 4$	$7(7p^2 + 8p + 2) + 2 = 7k + 2$	$7(49p^3 + 84p^2 + 48p + 9) + 1 = 7k + 1$
$7p + 5$	$7(7p^2 + 10p + 21) + 4 = 7k + 4$	$7(49p^3 + 105p^2 + 75p + 17) + 6 = 7k + 6$
$7p + 6$	$7(7p^2 + 12p + 35) + 1 = 7k + 1$	$7(49p^3 + 126p^2 + 108p + 30) + 6 = 7k + 6$

Assim, o resto da divisão de a^2 por 7 pertence ao conjunto $\{0, 1, 2, 4\}$ e o resto da divisão de b^3 por 7 pertence ao conjunto $\{0, 1, 6\}$. Assim, x é do tipo $7k$ ou $7k + 1$.

Exercício 10.
Seja n um inteiro positivo. Prove por indução que:

a) $7 \mid 2^{3n} - 1$ e $8 \mid 3^{2n} + 7$.

b) $3 \mid 2^n + (-1)^{n+1}$.

Solução 10.

a)

$$7 | 2^{3n} - 1$$

Base: $n = 1$

$$2^{3 \cdot 1} - 1 = 8 - 1 = 7 = 1 \cdot 7.$$

Hipótese: $n = k > 1$

$$2^{3k} - 1 = 7p; p \in \mathbb{Z}$$

Passo: $n = k + 1$

$$\begin{aligned} 2^{3(k+1)} - 1 &= 2^{3k} \cdot 2^3 - 1 \\ &= 2^{3k} - 1 + 7 \cdot 2^{3k} = 7p + 7 \cdot 2^{3k} \\ &= 7\left(p + 2^{3k}\right) = 7q; \quad q \in \mathbb{Z}. \end{aligned}$$

$$8 | 3^{2n} + 7$$

Base: $n = 1$

$$3^{2\cdot 1} + 7 = 9 + 7 = 16 = 2 \cdot 8$$

Hipótese: $n = k > 1$

$$3^{2k} + 7 = 8p; p \in \mathbb{Z}$$

Passo: $n = k + 1$

$$\begin{aligned} 3^{2(k+1)} + 7 &= 3^{2k} \cdot 3^2 + 7 \\ &= 3^{2k} + 7 + 8 \cdot 3^{2k} \\ &= 8p + 8 \cdot 3^{2k} = 8\left(p + 3^{2k}\right) = 8q; \quad q \in \mathbb{Z}. \end{aligned}$$

b) *Base*: $n = 1$

$$2^1 + (-1)^{1+1} = 2 + 1 = 3 = 1 \cdot 3$$

Hipótese: $n = k \geqslant 2$

$$2^k + (-1)^{k+1} = 3p; p \in \mathbb{Z}$$

$$2^{k-1} + (-1)^k = 3p'; p' \in \mathbb{Z}$$

Passo: $n = k + 1$

$$\begin{aligned} 2^{k+1} + (-1)^{k+2} &= 2^k \cdot 2^1 - (-1)^{k+1} \\ &= 2^k + (-1)^{k+1} + 2^k - 2(-1)^{k+1} \\ &= 3p + 2\left(2^{k-1} - (-1)^k\right) \\ &= 3p + 2 \cdot 3p' = 3(p + 2p') = 3q; \quad q \in \mathbb{Z} \end{aligned}$$

Exercício 11.
Sejam x, y inteiros ímpares. Mostre que $x^2 + y^2$ é par mas não é divisível por 4.

Solução 11.
Sejam $x = 2k + 1; k \in \mathbb{Z}$ e $y = 2k' + 1; k' \in \mathbb{Z}$ Assim:

$$x^2 + y^2 = 2\left(2k^2 + 2k'^2 + 2k + 2k' + 1\right) = 4\left(k^2 + k'^2 + k + k'\right) + 2.$$

Exercício 12.
Busque todos os valores de n tais que $n^2 + 1$ é divisível por $n + 1$.

Solução 12.

$$n^2 + 1 = (n^2 - 1) + 2 = (n + 1)(n - 1) + 2$$

Assim $n + 1$ divide $(n^2 + 1)$ se e somente se $n + 1$ divide 2, portanto

$$\begin{cases} n+1=2 \\ \text{ou} \\ n+1=-2 \\ \text{ou} \\ n+1=1 \\ \text{ou} \\ n+1=-1 \end{cases} \Rightarrow \begin{cases} n=1 \\ \text{ou} \\ n=-3 \\ \text{ou} \\ n=0 \\ \text{ou} \\ n=-2 \end{cases}$$

Exercício 13.
Mostre que se $7 \mid a^2 + b^2$ então $7 \mid a$ e $7 \mid b$.

Solução 13.
Pelo algoritmo da divisão, temos que $n = 7p + r; p \in \mathbb{Z}$ e $r \in \{0, 1, 2, 3, 4, 5, 6\}$.

- $7\left(7p^2\right) = 7k;$
- $7\left(7p^2 + 2p\right) + 1 = 7k + 1;$
- $7\left(7p^2 + 4p\right) + 4 = 7k + 4;$
- $7\left(7p^2 + 6p + 1\right) + 2 = 7k + 2;$
- $7\left(7p^2 + 8p + 2\right) + 2 = 7k + 2;$
- $7\left(7p^2 + 10p + 21\right) + 4 = 7k + 4;$
- $7\left(7p^2 + 12p + 35\right) + 1 = 7k + 1;$

Note que o quadrado de um número, quando dividido por 7, deixa resto $0, 1, 2$ ou 4. De todas combinações possíveis para a soma de dois quadrados, a única que deixa resto múltiplo de 7 é se pegarmos dois números da forma $7k$. Assim:

$$7 \mid a^2 + b^2 \Leftrightarrow 7 \mid a \;\text{ e } 7 \mid b$$

Máximo divisor comum e mínimo múltiplo comum.

Exercício 1.
Para a não nulo mostre (usando somente a definição de mdc) que $\text{mdc}(a, 0) = \text{mdc}(a, a) = |a|$ e $\text{mdc}(a, 1) = 1$.

Solução 1.
Seja $d = \text{mdc}\,(a, 0)$. Por definição, $d \mid 0$ e $d \mid a$. Note que $|a| \mid a$ e $|a| \mid 0, \forall a \in \mathbb{Z}$. Além disso, se $c \mid a$, $c \leqslant |a|$. Assim, $d = |a|$.

A prova que $\text{mdc}\,(a, a) = |a|$ é a mesma.

Seja $d' = \text{mdc}\,(a, 1)$. Por definição, $d' \mid 1$, o que implica que $d' = 1$, pois $d' > 0$.

Exercício 2.
Mostre, usando somente a definição de mdc, que $\text{mdc}(a, b) = \text{mdc}(|a|, |b|)$.

Solução 2.
Sejam $d = \text{mdc}\,(a, b)$ e $d' = \text{mdc}\,(|a|, |b|)$. Assim:

$$\begin{matrix} d = \text{mdc}\,(a, b) \\ d' = \text{mdc}\,(|a|, |b|) \end{matrix} \Rightarrow \begin{matrix} d \mid a \ \text{ e } \ d|b \\ d' \mid |a| \ \text{ e } \ d' \mid |b| \end{matrix} \Rightarrow \begin{matrix} d \mid |a| \ \text{ e } \ d||b| \\ d' \mid a \ \text{ e } \ d' \mid b \end{matrix} \Rightarrow \begin{matrix} d \mid d' \\ d' \mid d \end{matrix} \Rightarrow d = d'$$

Exercício 3.
Sejam a, b dois inteiros não-nulos. Mostre que $\text{mdc}(na, nb) = n\text{mdc}(a, b)$ e $\text{mmc}(na, nb) = n\text{mmc}(a, b)$ se n é um inteiro positivo.

Solução 3.
Sejam $d = \text{mdc}\,(a, b)$ e $d' = \text{mdc}\,(na, nb)$. Assim, existem $x, y \in \mathbb{Z}$, tais que:

$$ax + by = d \Rightarrow nax + nby = nd.$$

Como $d' \mid na$ e $d' \mid nb$, então $d' \mid nd$.

Além disso, como $d \mid a$ e $d \mid b$, então $nd \mid na$ e $nd \mid nb$, ou seja, $nd \mid d'$.

Portanto, $nd = d'$.

$$\begin{aligned} \text{mmc}\,(na, nb) \cdot \text{mdc}\,(na, nb) &= (na) \cdot (nb) \\ \text{mmc}\,(na, nb) \cdot n \cdot \text{mdc}\,(a, b) &= (na) \cdot (nb) \\ \text{mmc}\,(na, nb) \cdot \frac{a \cdot b}{\text{mmc}\,(a, b)} &= a \cdot (nb) \\ \text{mmc}\,(na, nb) &= n \cdot \text{mmc}\,(a, b)\,. \end{aligned}$$

Exercício 4.
Determine $\mathrm{mdc}(a, b)$ e $\mathrm{mmc}(a, b)$ para os inteiros a e b dados abaixo:

a) $a = 32$ e $b = 54$;

b) $a = 27$ e $b = 45$;

c) $a = 15$ e $b = 80$;

d) $a = 8798$ e $b = 2314$;

e) $a = 1583890$ e $b = 3927$.

Solução 4.
a)

$$\begin{aligned} \mathrm{mdc}\,(32, 54) &= \mathrm{mdc}\,(32, 54 - 1 \cdot 32) = \mathrm{mdc}\,(32, 22) \\ &= \mathrm{mdc}\,(32 - 1 \cdot 22, 22) = \mathrm{mdc}\,(10, 22) \\ &= \mathrm{mdc}\,(10, 22 - 2 \cdot 10) = \mathrm{mdc}\,(10, 2) \\ &= \mathrm{mdc}\,(10 - 5 \cdot 2, 2) = \mathrm{mdc}\,(0, 2) = 2. \end{aligned}$$

$$\mathrm{mmc}\,(32, 54) = \frac{32 \cdot 54}{\mathrm{mdc}\,(32, 54)} = 864.$$

b)

$$\begin{aligned} \mathrm{mdc}\,(27, 45) &= \mathrm{mdc}\,(27, 45 - 1 \cdot 27) = \mathrm{mdc}\,(27, 18) \\ &= \mathrm{mdc}\,(27 - 1 \cdot 18, 18) = \mathrm{mdc}\,(9, 18) \\ &= \mathrm{mdc}\,(9, 18 - 2 \cdot 9) = \mathrm{mdc}\,(9, 0) = 9. \end{aligned}$$

$$\mathrm{mmc}\,(27, 45) = \frac{27 \cdot 45}{\mathrm{mdc}\,(27, 45)} = 135.$$

c)

$$\mathrm{mdc}\,(15, 80) = \mathrm{mdc}\,(15, 80 - 5 \cdot 15) = \mathrm{mdc}\,(15, 5) = \mathrm{mdc}\,(15 - 3 \cdot 5, 5) = \mathrm{mdc}\,(0, 5) = 5.$$

$$\mathrm{mmc}\,(15, 80) = \frac{15 \cdot 80}{\mathrm{mdc}\,(15, 80)} = 240.$$

d)

$$\begin{aligned} \mathrm{mdc}\,(8798, 2314) &= \mathrm{mdc}\,(8798 - 3 \cdot 2314, 2314) = \mathrm{mdc}\,(1856, 2314) \\ &= \mathrm{mdc}\,(1856, 2314 - 1 \cdot 1856) = \mathrm{mdc}\,(1856, 458) \\ &= \mathrm{mdc}\,(1856 - 4 \cdot 458, 458) = \mathrm{mdc}\,(24, 458) \\ &= \mathrm{mdc}\,(24, 458 - 19 \cdot 24) = \mathrm{mdc}\,(24, 2) \\ &= \mathrm{mdc}\,(2, 24 - 12 \cdot 2) = \mathrm{mdc}\,(2, 0) = 2. \end{aligned}$$

$$\text{mmc}\,(8798, 2314) = \frac{8798 \cdot 2314}{\text{mdc}\,(8798, 2314)} = 10179286.$$

Exercício 5.
Nos casos abaixo, utilize o Algoritmo de Euclides para determinar inteiros r e s tais que $\text{mdc}(a, b) = ar + bs$.

a) $a = 56$ e $b = 72$;

b) $a = 24$ e $b = 138$;

c) $a = 119$ e $b = 272$;

d) $a = 1128$ e $b = 336$.

Solução 5.

a)

$$\begin{array}{c} 72 = 1 \cdot 56 + 16 \\ 56 = 3 \cdot 16 + 8 \\ 16 = 2 \cdot 8 \end{array} \Rightarrow \begin{array}{c} 16 = 72 - 1 \cdot 56 \\ 8 = 56 - 3 \cdot 16 \end{array} \Rightarrow 8 = 56 - 3 \cdot (72 - 1 \cdot 56) = 4 \cdot 56 - 3 \cdot 72 \Rightarrow \begin{array}{c} r = 4 \\ s = -3 \end{array}$$

b)

$$\begin{array}{c} 138 = 5 \cdot 24 + 18 \\ 24 = 1 \cdot 18 + 6 \\ 18 = 3 \cdot 6 \end{array} \Rightarrow \begin{array}{c} 18 = 138 - 5 \cdot 24 \\ 6 = 24 - 1 \cdot 18 \end{array} \Rightarrow 6 = 24 - 1 \cdot (138 - 5 \cdot 24) = 6 \cdot 27 - 1 \cdot 138 \Rightarrow \begin{array}{c} r = 6 \\ s = -1 \end{array}$$

c)

$$\begin{array}{c} 272 = 2 \cdot 119 + 34 \\ 119 = 3 \cdot 34 + 17 \\ 32 = 2 \cdot 17 \end{array} \Rightarrow \begin{array}{c} 34 = 272 - 2 \cdot 119 \\ 17 = 119 - 3 \cdot 34 \end{array} \Rightarrow 17 = 119 - 3 \cdot (272 - 2 \cdot 119) = 7 \cdot 119 - 3 \cdot 272 \Rightarrow \begin{array}{c} r = 7 \\ s = -3 \end{array}$$

d)

$$\begin{array}{c} 1128 = 3 \cdot 336 + 120 \\ 336 = 2 \cdot 120 + 96 \\ 120 = 1 \cdot 96 + 24 \\ 96 = 4 \cdot 24 \end{array} \Rightarrow \begin{array}{c} 120 = 1128 - 3 \cdot 336 \\ 96 = 336 - 2 \cdot 120 \\ 24 = 120 - 1 \cdot 96 \end{array} \Rightarrow 24 = 120 - 1 \cdot (336 - 2 \cdot 120) =$$

$$= 3 \cdot 120 - 1 \cdot 33624 = 3 \cdot (1128 - 3 \cdot 336) - 1 \cdot 336 = 3 \cdot 1128 - 10 \cdot 336 \Rightarrow \begin{array}{c} r = 3 \\ s = -10 \end{array}$$

Exercício 6.
Para os inteiros não-nulos a e b, mostre que as seguintes condições são equivalentes

a) $a \mid b$;

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

c) $\text{mmc}(a, b) = |b|$.

Solução 6.

$$a \mid b \Rightarrow \text{mdc}\,(a, b) = |a|$$
$$a \mid b \Rightarrow b = k \cdot a; k \in \mathbb{Z} \Rightarrow \text{mdc}\,(a, b) = \text{mdc}\,(a, ka) = |a| \cdot \text{mdc}\,(1, k) = |a| \cdot 1 = |a|.$$

$$\begin{gathered}
\text{mdc}\,(a, b) = |a| \Rightarrow \text{mmc}\,(a, b) = |b| \\
\text{mdc}\,(a, b) \cdot \text{mmc}\,(a, b) = |a| \cdot |b| \\
|b| \cdot \text{mmc}\,(a, b) = |a| \cdot |b| \\
\text{mmc}\,(a, b) = |b|.
\end{gathered}$$

$$\begin{gathered}
\text{mmc}\,(a, b) = |b| \Rightarrow a \mid b \\
\text{mdc}\,(a, b) \cdot \text{mmc}\,(a, b) = |a| \cdot |b| \\
\text{mdc}\,(a, b) \cdot |b| = |a| \cdot |b| \Rightarrow \text{mdc}\,(a, b) = |a| \\
|a| \mid b \Rightarrow a \mid b.
\end{gathered}$$

Exercício 7.
Mercúrio leva 2111 horas para completar uma volta em torno do Sol, enquanto Vênus leva 5393 horas. Com que frequência Sol, Mercúrio e Vênus se alinham?

Solução 7.

$$\begin{aligned}
\text{mdc}\,(2111, 5393) &= \text{mdc}\,(2111, 5393 - 2 \cdot 2111) = \text{mdc}\,(2111, 1171) \\
&= \text{mdc}\,(2111 - 1 \cdot 1171, 1171) = \text{mdc}\,(940, 1171) \\
&= \text{mdc}\,(940, 1171 - 1 \cdot 940) = \text{mdc}\,(940, 231) \\
&= \text{mdc}\,(940 - 4 \cdot 231, 231) = \text{mdc}\,(16, 231) \\
&= \text{mdc}\,(16, 231 - 14 \cdot 16) = \text{mdc}\,(16, 7) \\
&= \text{mdc}\,(16 - 2 \cdot 7, 7) = \text{mdc}\,(2, 7) \\
&= \text{mdc}\,(2, 7 - 3 \cdot 2) = \text{mdc}\,(2, 1) \\
&= \text{mdc}\,(2 - 2 \cdot 1, 1) = \text{mdc}\,(0, 1) = 1.
\end{aligned}$$

$$\text{mmc}\,(2111, 5393) = \frac{2111 \cdot 5393}{\text{mdc}\,(2111, 5393)} = 11384623.$$

Eles se alinham em 11384623 horas, ou seja, aproximadamente 1300 anos.

Exercício 8.
Mostre que se a é um inteiro positive então a e $a+1$ são primos entre si.

Solução 8.
Para mostrar que dois números são primos entre si, basta mostrar que o mdc entre eles é 1.

$$\text{mdc}\,(a+1,a) = \text{mdc}\,(a+1-1\cdot a, a) = \text{mdc}\,(1,a) = \text{mdc}\,(1, a-a\cdot 1) = \text{mdc}\,(1,0) = 1.$$

Exercício 9.
Sejam a e b primos entre si não nulos. Determine $\text{mdc}(a^2+b^2, a+b)$.

Solução 9.
Seja $d = \text{mdc}\left(a^2+b^2, a+b\right)$. Então:

$$d = \text{mdc}\left(a^2+b^2, a+b\right) = \text{mdc}\left((a+b)(a-b)+2b^2, a+b\right) =$$
$$\text{mdc}\left((a+b)(a-b)+2b^2-(a-b)(a+b), a+b\right) = \text{mdc}\left(2b^2, a+b\right).$$

Analogamente:

$$d = \text{mdc}\left(a^2+b^2, a+b\right) = \text{mdc}\left((b+a)(b-a)+2a^2, a+b\right) =$$
$$\text{mdc}\left((b+a)(b-a)+2a^2-(b-a)(a+b), a+b\right) = \text{mdc}\left(2a^2, a+b\right).$$

Assim, $d \mid 2b^2$ e $d \mid 2a^2$. Logo:

$$d \mid \text{mdc}\left(2a^2, 2b^2\right) \Rightarrow d \mid 2\text{mdc}\left(a^2, b^2\right) \Rightarrow d \mid 2\left(\text{mdc}\,(a,b)\right)^2 \Rightarrow d \mid 2\cdot 1$$

Logo, $d = 1$ ou $d = 2$.

Exercício 10.
Assumido que $\text{mdc}(a,b) = 1$, mostre o seguinte:

a) $\text{mdc}(a+b, a-b) = 1$ ou 2. (*Dica:* Seja $d = \text{mdc}(a+b, a-b)$ e mostre que $d \mid 2a$, $d \mid 2b$; assim, $d \leqslant \text{mdc}(2a, 2b) = 2\text{mdc}(a,b)$);

b) $\text{mdc}(2a+b, a+2b) = 1$ ou 3;

c) $\text{mdc}(a+b, a^2+b^2) = 1$ ou 2. (*Dica:* $a^2+b^2 = (a+b)(a-b)+2b^2$.)

Solução 10.

a) Seja $d = \text{mdc}\,(a+b, a-b)$. Logo:

$$\begin{matrix} d \mid a+b \\ d \mid a-b \end{matrix} \Rightarrow \begin{matrix} d \mid a+b+(a-b) \\ d \mid a-b-(a+b) \end{matrix} \Rightarrow \begin{matrix} d \mid 2a \\ d \mid -2b \end{matrix} \Rightarrow \begin{matrix} d \mid 2a \\ d \mid 2b \end{matrix} \Rightarrow d \mid \text{mdc}\,(2a, 2b) \Rightarrow d \mid 2\text{mdc}\,(a,b) \Rightarrow d \mid 2{\cdot}1.$$

Logo, $d = 1$ ou $d = 2$.

b) Seja $d = \text{mdc}\,(2a+b, a+2b)$. Logo:

$$\begin{matrix} d \mid 2a+b \\ d \mid a+2b \end{matrix} \Rightarrow \begin{matrix} d \mid 2a+b-2\,(a+2b) \\ d \mid a+2b-2\,(2a+b) \end{matrix} \Rightarrow \begin{matrix} d \mid -3b \\ d \mid -3a \end{matrix} \Rightarrow \begin{matrix} d \mid 3a \\ d \mid 3b \end{matrix} \Rightarrow d \mid \text{mdc}\,(3a,3b) \Rightarrow d \mid 3\text{mdc}\,(a,b) \Rightarrow d \mid 3{\cdot}1.$$

Logo, $d = 1$ ou $d = 3$.

c) Igual ao exercício 9.

Exercício 11.
Sejam $a, b, c \in \mathbb{Z}$ tais que $a \mid b$ e $\text{mdc}(b, c) = 1$. Mostre que $\text{mdc}(a, c) = 1$.

Solução 11.
$a \mid b \Rightarrow b = k \cdot a; k \in \mathbb{Z}$. Se $\text{mdc}\,(b, c) = 1$, então, por Bezout, existem $x, y \in \mathbb{Z}$, tais que:

$$bx + cy = 1 \Rightarrow kac + cy = 1.$$

Seja $d = \text{mdc}\,(a, c)$. Como $d \mid a$, então $d \mid kac$; como $d \mid c$, então $d \mid cy$. Logo, $d \mid 1$. Portanto,$d = 1$.

Exercício 12.
Explique como definir o maximo divisor comum $\text{mdc}(a, b, c)$ de três números inteiros a, b, c. Em seguida, generalize sua definição para aplicar a qualquer número dos inteiros.

Solução 12.
É só agrupar de dois em dois.

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

Generalizando:

$$\text{mdc}\,(a_1, a_2, \cdots, a_{n-1}, a_n) = \text{mdc}\,(a_1, a_2, \cdots, \text{mdc}\,(a_{n-1}, a_n)).$$