MAT0120 - Álgebra I para Licenciatura

Lista 2 - Soluções

Professor: Kostiantyn Iusenko
Monitor: Douglas de Araujo Smigly

1º Semestre de 2021

1 Divisibilidade

(1) Mostre que um número inteiro a é par se e somente se a^2 for par.

Solução
$(\Rightarrow)$
Suponha que a é par. Então, existe um inteiro k tal que $a = 2k$. Dessa forma,

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

Logo, se a é par, então a^2 também é.
$(\Leftarrow)$
Para verificar que se a^2 é par, então a é par, podemos provar a contra-positiva: se a é ímpar, então a^2 é ímpar. De fato:

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

(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
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 $r \in \{0,1,2,3,4,5\}$.

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

Em todos os casos, concluímos que 6 divide o produto de três números inteiros consecutivos.

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 $\text{mdc}(3,8) = 1$, temos que $24 \mid y \Leftrightarrow 3 \mid y$ e $8 \mid y$.
Vamos provar que $8 \mid y$. Para isso, basta analisar o comportamento de y para os restos da divisão de n por 4.
Pelo algoritmo da divisão, temos que $n = 4k + r$ para $k \in \mathbb{Z}$ e $r \in \{0,1,2,3\}$.

- $n = 4k$. Nesse caso, temos que:

$$\begin{aligned} y = n(n+1)(n+2)(n+3) &= 4k(4k+1)(4k+2)(4k+3) \\ &= 8k(4k+1)(2k+1)(4k+3) \\ &= 8q, q \in \mathbb{Z} \end{aligned}$$

  Logo, $8 \mid x$ para $n = 4k$.

- $n = 4k+1$. Nesse caso,

$$\begin{aligned} y = n(n+1)(n+2)(n+3) &= (4k+1)(4k+2)(4k+3)(4k+4) \\ &= 8(4k+1)(2k+1)(4k+3)(k+1) \\ &= 8q, q \in \mathbb{Z} \end{aligned}$$

  Logo, $8 \mid x$ para $n = 4k+1$.

- $n = 4k+2$. Nesse caso, temos que:

$$\begin{aligned} y = n(n+1)(n+2)(n+3) &= (4k+2)(4k+3)(4k+4)(4k+5) \\ &= 8(2k+1)(4k+3)(k+1)(4k+5) \\ &= 8q, q \in \mathbb{Z} \end{aligned}$$

  Logo, $8 \mid x$ para $n = 4k+2$.

- $n = 4k+3$.Nesse caso, temos que:

$$\begin{aligned} y = n(n+1)(n+2)(n+3) &= (4k+3)(4k+4)(4k+5)(4k+6) \\ &= 8(4k+3)(k+1)(4k+5)(2k+3) \\ &= 8q, q \in \mathbb{Z} \end{aligned}$$

  Logo, $8 \mid x$ para $n = 4k+2$.

Em todos os casos, concluímos que 24 divide o produto de quatro números inteiros consecutivos.

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

Solução

Pelo algoritmo da divisão, $n = 2k + r; k \in \mathbb{Z}$ e $r \in \{0,1\}$. Testemos ambos os casos:

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

Assim, concluímos que $4 \nmid n^2 + 2$.

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

Solução

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

Para provar que $360 \mid x$, podemos verificar que $5 \mid x, 9 \mid x$ e $8 \mid x$, pois $\text{mdc}(5,8,9) = 1$ e $5 \cdot 8 \cdot 9 = 360$.

Analisemos x para cada caso:

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

  Logo, $5 \mid x$.
- $9 \mid x$: Novamente, pelo algoritmo da divisão, $a = 3k + r; k \in \mathbb{Z}$ e $r \in \{0,1,2\}$.
  - $a = 3k \Rightarrow a^2 = 9 \Rightarrow 9 \mid x$;
  - $a = 3k + 1 \Rightarrow (a-1)(a+2) = 9k(k+1) \Rightarrow 9 \mid x$;
  - $a = 3k + 2 \Rightarrow (a-2)(a+1) = 9k(k+1) \Rightarrow 9 \mid x$.

  Logo, $3 \mid x$.
- $8 \mid x$: Como pelo exercício 2 sabemos que 8 divide 4 números consecutivos, então $8 \mid x$.

Portanto, temos que

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

(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

(a) Seja $x = a^2 - a = a(a-1)$. Usando o algoritmo da divisão, podemos escrever $a = 2k + r; k \in \mathbb{Z}$ e $r \in \{0,1\}$. Temos então:

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

Em ambos os casos, concluímos que $a^2 - a$ é divisível por 2.

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

(c) Seja

$$\begin{aligned} x = a^5 - a &= a\left(a^4 - 1\right) \\ &= a\left(a^2 - 1\right)\left(a^2 + 1\right) \\ &= a\left(a^2 + 1\right)\left(a^2 - 1\right) \\ &= a\left(a^2 + 1\right)(a+1)(a-1) \\ &= (a-1)a(a+1)\left(a^2 + 1\right). \end{aligned}$$

Pelo exercício 2, sabemos que $6 \mid x$, pois um dos fatores de x é o produto de três números inteiros consecutivos. Como $6 \cdot 5 = 30$ e $\text{mdc}(5,6) = 1$, resta verificar que $5 \mid x$.

Pelo algoritmo da divisão, $a = 5k + r; k \in \mathbb{Z}$ e $r \in \{0,1,2,3,4\}$. Analisando cada uma das situações possíveis:

- $a = 5k \Rightarrow 5 \mid x$;
- $a = 5k+1 \Rightarrow (a-1) = 5k \Rightarrow 5 \mid x$;
- $a = 5k+2 \Rightarrow \left(a^2+1\right) = 5\left(5k^2 + 4k + 1\right) \Rightarrow 5 \mid x$;
- $a = 5k+3 \Rightarrow \left(a^2+1\right) = 5\left(5k^2 + 6k + 2\right) \Rightarrow 5 \mid x$;
- $a = 5k+4 \Rightarrow (a+1) = 5(k+1) \Rightarrow 5 \mid x$.

Assim:

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

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

Solução

Temos que

$$6k + 5 = 2 \cdot 3k + 3 + 2 = 3(2k+1) + 2 = 3k' + 2; k' \in \mathbb{Z}.$$

Vejamos um número da forma $3k + 2$ que não é da forma $6k + 5$. Um deles é $8 = 3 \cdot 2 + 2 = 6 \cdot 1 + 2$.

Na verdade, os números da forma $3k+2$ que não são da forma $6k+5$ são

$$2, 8, 14, 20, 26, 32, 38, 44, 50, 56, \ldots$$

que correspondem justamente aos números na forma $6k-2$.

(7) Usando o Algoritmo da Divisão, mostre que:

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

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

(c) o cubo de todo inteiro é da forma $9k$ ou $9k+1$ ou $9k+8$;

(d) o cubo de todo inteiro é da forma $7k$ ou $7k+1$ ou $7k+6$.

Solução

(a) Se n é um inteiro ímpar, então deve ser da forma $2p+1$. Pelo algoritmo da divisão, $p = 2k+r; k \in \mathbb{Z}$ e $r \in \{0,1\}$. Analisando os possíveis casos, temos:

- $p = 2k \Rightarrow n = 4k+1$;
- $p = 2k+1 \Rightarrow n = 4k+3$.

Logo, concluímos que n é da forma $4k+1$ ou $4k+3$.

(b) Pelo algoritmo da divisão, $n = 3p+r; p \in \mathbb{Z}$ e $r \in \{0,1,2\}$. Assim,

- $n = 3p \Rightarrow n^2 = 3 \cdot \left(3p^2\right) = 3k; k \in \mathbb{Z}$;
- $n = 3p+1 \Rightarrow n^2 = 3 \cdot \left(3p^2+2p\right) + 1 = 3k+1; k \in \mathbb{Z}$;
- $n = 3p+2 \Rightarrow n^2 = 3 \cdot \left(3p^2+4p+1\right) + 1 = 3k+1; k \in \mathbb{Z}$.

Logo, quadrado de todo inteiro é do forma ou $3k$ ou $3k+1$.

(c) Pelo algoritmo da divisão, $n = 3p+r; p \in \mathbb{Z}$ e $r \in \{0,1,2\}$.

- $n = 3p \Rightarrow n^3 = 9 \cdot \left(3p^3\right) = 9k; k \in \mathbb{Z}$;
- $n = 3p+1 \Rightarrow n^3 = 9 \cdot \left(3p^3+3p^2+p\right) + 1 = 9k+1; k \in \mathbb{Z}$;
- $n = 3p+2 \Rightarrow n^3 = 9 \cdot \left(3p^3+6p^2+4p\right) + 8 = 9k+8; k \in \mathbb{Z}$.

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

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

- $n = 7p \Rightarrow n^3 = 7 \cdot \left(49p^3\right) = 7k; k \in \mathbb{Z};$
- $n = 7p + 1 \Rightarrow n^3 = 7 \cdot \left(49p^3 + 21p^2 + 3p\right) + 1 = 7k + 1; k \in \mathbb{Z};$
- $n = 7p + 2 \Rightarrow n^3 = 7 \cdot \left(49p^3 + 42p^2 + 12p + 1\right) + 1 = 7k + 1; k \in \mathbb{Z}.$
- $n = 7p + 3 \Rightarrow n^3 = 7 \cdot \left(49p^3 + 63p^2 + 27p + 3\right) + 6 = 7k + 6; k \in \mathbb{Z}.$
- $n = 7p + 4 \Rightarrow n^3 = 7 \cdot \left(49p^3 + 84p^2 + 48p + 9\right) + 1 = 7k + 1; k \in \mathbb{Z}.$
- $n = 7p + 5 \Rightarrow n^3 = 7 \cdot \left(49p^3 + 105p^2 + 75p + 17\right) + 6 = 7k + 6; k \in \mathbb{Z}.$
- $n = 7p + 6 \Rightarrow n^3 = 7 \cdot \left(49p^3 + 126p^2 + 108p + 30\right) + 6 = 7k + 6; k \in \mathbb{Z}.$

Logo, o cubo de todo inteiro é do forma $7k$ ou $7k + 1$ ou $7k + 6$.

(8) Prove que nenhum inteiro da sequência $11, 111, 1111, \ldots$ é um quadrado perfeito.
[Dica:] Mostre que todo número quadrado perfeito é da forma $4k$ ou $4k + 1$.

Solução

Observe inicialmente que

$$\underbrace{11\ldots11}_{n \text{ números } 1} = \frac{10^n - 1}{9}$$

Agora, podemos escrever que

$$10^n - 1 = (10 - 1)(10^{n-1} + 10^{n-2} + \ldots + 10 + 1).$$

Logo,

$$\frac{10^n - 1}{9} = \frac{(10 - 1)(10^{n-1} + 10^{n-2} + \ldots + 10 + 1)}{9} = 10^{n-1} + 10^{n-2} \ldots + 10 + 1.$$

Vamos analisar os restos da divisão de um número da forma $1\ldots1$ por 4. Da expressão acima, observe que, como $10 = 2 \cdot 5$, então, se $\eta > 1$, temos que

$$10^\eta = (2 \cdot 5)^\eta = 2^\eta \cdot 5^\eta = 2^2 \cdot 2^{\eta-2} \cdot 5^\eta = 4 \cdot 2^{\eta-2} \cdot 5^\eta$$

Assim, concluímos que $4 \mid 10^\eta$ para todo $\eta > 1$. Dessa forma, temos

$$\begin{aligned}
10^{n-1} + 10^{n-2} \ldots 100 + 10 + 1 &= 4(2^{n-3} \cdot 5^{n-1}) + 4(2^{n-4} \cdot 5^{n-3}) + \ldots + 4(2^0 \cdot 5^2) + 10 + 1 \\
&= 4(2^{n-3} \cdot 5^{n-1} + 2^{n-4} \cdot 5^{n-3} + \ldots + 2^0 \cdot 5^2) + 11 \\
&= 4(2^{n-3} \cdot 5^{n-1} + 2^{n-4} \cdot 5^{n-3} + \ldots + 2^0 \cdot 5^2) + 8 + 3 \\
&= 4(2^{n-3} \cdot 5^{n-1} + 2^{n-4} \cdot 5^{n-3} + \ldots + 2^0 \cdot 5^2 + 2) + 3 \\
&= 4k + 3
\end{aligned}$$

Ou seja, qualquer número da sequência $11, 111, 1111, \ldots$ é da forma $4k + 3$. Vamos mostrar que um número quadrado perfeito não pode ser escrito nessa forma. Para isso, vamos utilizar o algoritmo da divisão.
Devemos ter $a = 4k + r; k \in \mathbb{Z}$ e $r \in \{0,1,2,3,4\}$. Analisando cada uma das situações possíveis:

- $a = 4k \Rightarrow a^2 = (4k)^2 = 16k^2 = 4(4k^2) = 4q$;
- $a = 4k+1 \Rightarrow a^2 = (4k+1)^2 = 16k^2 + 8k + 1 = 4(4k^2 + 2k) + 1 = 4q + 1$;
- $a = 4k+2 \Rightarrow a^2 = (4k+2)^2 = 16k^2 + 16k + 4 = 4(4k^2 + 4k + 1) = 4q$;
- $a = 4k+3 \Rightarrow a^2 = (4k+3)^2 = 16k^2 + 24k + 9 = 4(4k^2 + 6k + 2) + 1 = 4q + 1$.

Assim, os possíveis restos na divisão por 4 de um número quadrado perfeito são 0 e 1. Como o resto na divisão por 4 em um número na sequência é sempre 3, concluímos que nenhum desses termos pode ser um número quadrado perfeito.

Solução Alternativa: O Critério de Divisibilidade por 4 afirma que um número é divisível por 4 se, e somente se, os dois últimos algarismos formarem um número divisível por 4. Observe que cada termo da sequência pode ser escrito na forma

$$111\ldots11108 + 3$$

Como $4 \mid 08$, concluímos que qualquer número na sequência é da forma $4k+3$, e o quadrado de todo inteiro é da forma $4k$ ou $4k+1$, sendo impossível essa situação.

(9) Para $n \geq 1$, mostre que $\dfrac{n(n+1)(2n+1)}{6}$ é um inteiro.

[Dica:] Usando o Algoritmo da Divisão, n tem a forma $6k$ ou $6k+1$ ou $\cdots$ ou $6k+5$. Mostre o resultado em todos os casos.

Solução

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

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

Em todos os casos, concluímos que $\dfrac{n(n+1)(2n+1)}{6}$ é um inteiro.

Solução Alternativa: Na lista 1, provamos que

$$\sum_{k=1}^{n} k^2 = 1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Assim, sendo $\frac{n(n+1)(2n+1)}{6}$ uma soma de números quadrados perfeitos, segue que este valor é um inteiro.

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

Solução

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 $r \in \{0,1,2,3,4,5,6\}$. Analisando as situações:

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 $\{0,1,6\}$. Logo, se o número for simultaneamente quadrado e cubo perfeito, seu resto na divisão por 7 pertence ao conjunto $\{0,1,2,4\} \cap \{0,1,6\} = \{0,1\}$ Assim, x é do tipo $7k$ ou $7k+1$.

(11) Seja n um inteiro positivo. Prove por indução que:

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

Solução

(a) Nosso caso **base** será $n = 1$. Temos

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

Como **hipótese**, assuma que a afirmação é válida para $n = k > 1$, os seja,

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

Provemos que é válido como **passo indutivo** para $n = k+1$:

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

(*b*) Para o **caso base** $n = 1$,

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

Suponha por **hipótese** que para $n = k > 1$, tenhamos

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

Vejamos que a divisibilidade ocorre para $n = k + 1$, compreendendo o **passo indutivo**:

$$\begin{aligned} 3^{2(k+1)} + 7 &= 3^{2k} \cdot 3^2 + 7 \\ &= 9 \cdot 3^{2k} + 7 \\ &= 3^{2k} + 7 + 8 \cdot 3^{2k} \\ &= 8p + 8 \cdot 3^{2k} = 8\left(p + 3^{2k}\right) = 8q; \quad q \in \mathbb{Z}. \end{aligned}$$

(*c*) Para o **caso base** $n = 1$,

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

Suponha por **hipótese** que para $n = k > 1$, tenhamos

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

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

Vejamos que a divisibilidade ocorre para $n = k + 1$, compreendendo o **passo indutivo**:

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

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

Solução

Se um número é par mas não é divisível por 4, isso significa que ele deve ser da forma $4q + 2$, com q inteiro. Buscaremos então mostrar que $x^2 + y^2$ possui essa forma.
Sejam $x = 2k + 1; k \in \mathbb{Z}$ e $y = 2\ell + 1; \ell \in \mathbb{Z}$. Então

$$\begin{aligned} x^2+y^2 &= (2k+1)^2+(2\ell+1)^2 \\ &= 4k^2+4k+1+4\ell^2+4\ell+1 \\ &= 2\left(2k^2+2\ell^2+2k+2\ell+1\right) \\ &= 4\left(k^2+\ell^2+k+\ell\right)+2 \\ &= 4q+2. \end{aligned}$$

Assim, x^2+y^2 é par mas não é divisível por 4.

(13) Encontre todos os valores de n tais que n^2+1 é divisível por $n+1$.

Solução

Vamos primeiramente observar as relações existentes entre n^2+1 e $n+1$. Como estamos analisando a divisibilidade desses termos, utilizemo-nos do algoritmo da divisão de n^2+1 por $n+1$. Podemos escrever que $n^2+1=(n+1)q+r$, onde $q\in\mathbb{Z}$ e $r\in\{0,1,\ldots,n\}$. Vejamos agora as possibilidades para q e r. Para isso, observe que

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

Ou seja, $q=(n-1)$ e $r=2$. Assim, $n+1$ divide (n^2+1) se e somente se $n+1$ divide 2 (já que claramente $n+1$ divide $(n+1)(n-1)$), e portanto, como $D(2)=\{\pm1,\pm2\}$, temos 4 possibilidades:

- $n+1=2\Rightarrow n=1$;
- $n+1=-2\Rightarrow n=-3$;
- $n+1=1\Rightarrow n=0$;
- $n+1=-1\Rightarrow n=-2$.

Assim, os valores de n tais que n^2+1 é divisível por $n+1$ são $-2,-3,0$ e 1.

(14) Mostre que se $7\mid a^2+b^2$ então $7\mid a$ e $7\mid b$.

Solução

Vamos primeiramente observar quais são os possíveis restos da divisão de um número quadrado perfeito por 7.
Dado n, queremos analisar o comportamento de n^2 na divisão por 7. Pelo algoritmo da divisão, temos que $n=7p+r; p\in\mathbb{Z}$ e $r\in\{0,1,2,3,4,5,6\}$.
Dessa forma,

- $n=7p\Rightarrow n^2=49p^2=7\left(7p^2\right)=7k$;
- $n=7p+1\Rightarrow n^2=7\left(7p^2+2p\right)+1=7k+1$;
- $n=7p+2\Rightarrow n^2=7\left(7p^2+4p\right)+4=7k+4$;

- $n = 7p + 3 \Rightarrow n^2 = 7\left(7p^2 + 6p + 1\right) + 2 = 7k + 2$;
- $n = 7p + 4 \Rightarrow n^2 = 7\left(7p^2 + 8p + 2\right) + 2 = 7k + 2$;
- $n = 7p + 5 \Rightarrow n^2 = 7\left(7p^2 + 10p + 21\right) + 4 = 7k + 4$;
- $n = 7p + 6 \Rightarrow n^2 = 7\left(7p^2 + 12p + 35\right) + 1 = 7k + 1$;

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:

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

(15) Prove que $a^3 + b^3 + 4$ não é um cubo perfeito quaisquer que sejam os números naturais a e b.

Solução

Vamos analisar a equação pensando nos restos da divisão de a e b por 9. Pelo item (c) da questão 7, o cubo de todo inteiro é da forma $9k, 9k + 1$ ou $9k + 6$. Assim, a^3 e b^3 devem ter alguma dessas formas. A tabela abaixo mostra a forma de $a^3 + b^3 + 4$ para cada caso: Logo, os possíveis restos

a^3	b^3	$a^3 + b^3 + 4$
$9k$	$9k$	$9k + 9k + 4 = 9(2k) + 4$
$9k$	$9k + 1$	$9k + 9k + 1 + 4 = 9(2k) + 5$
$9k$	$9k + 8$	$9k + 9k + 8 + 4 = 9(2k + 1) + 3$
$9k + 1$	$9k$	$9k + 1 + 9k + 4 = 9(2k) + 5$
$9k + 1$	$9k + 1$	$9k + 1 + 9k + 1 + 4 = 9(2k) + 6$
$9k + 1$	$9k + 8$	$9k + 1 + 9k + 8 + 4 = 9(2k + 1) + 4$
$9k + 8$	$9k$	$9k + 8 + 9k + 4 = 9(2k + 1) + 3$
$9k + 8$	$9k + 1$	$9k + 8 + 9k + 1 + 4 = 9(2k + 1) + 4$
$9k + 8$	$9k + 8$	$9k + 8 + 9k + 8 + 4 = 9(2k + 2) + 2$

da divisão de $a^3 + b^3 + 4$ por 9 pertencem ao conjunto $\{2, 3, 4, 5, 6\}$. Como nenhum desses restos pode corresponder ao resto do cubo de um inteiro, concluímos que $a^3 + b^3 + 4$ não pode ser um cubo perfeito.

(16) Sejam a e b dois números inteiros tais que $78a = 179b$. Prove que $a + b$ possui mais do que 2 divisores positivos.

Solução

Adicionando $78b$ em ambos os lados, temos:

$$78b + 78a = 78a + 179b \Rightarrow 78(a + b) = 257b$$

Como $\text{mdc}(78, 257) = 1$, concluímos então que $257 \mid a + b$. Assim, os divisores de $a + b$ devem ser ao menos $1, 257$ e $a + b$. Logo, $a + b$ possui mais do que 2 divisores positivos.

(17) Seja a um número inteiro positivo tal que $a^{10}+1$ é divisível por 10.

(a) Mostre que a pode assumir infinitos valores.

(b) Se $a_1, a_2, \ldots, a_{2021}$ são 2021 inteiros positivos tais que $a_i^{10}+1$ é divisível por 10 para cada $i = 1, \ldots, 2021$, prove que

$$10 \nmid a_1 + a_2 + \ldots + a_{2021}$$

Solução

(a) Pelo algoritmo da divisão, podemos escrever $a = 10q + r$, onde $r \in \{0,1,2,3,4,5,6,7,8,9\}$ e $q \in \mathbb{Z}$. O resto da divisão de um número por 10 corresponde ao algarismo das unidades do número. Assim, $a^{10}+1$ será divisível por 10 se, e somente se, $r^{10}+1$ for divisível por 10. Para que isto ocorra, requere-se então que r^{10} tenha 9 como algarismo das unidades. Observe que isto é impossível de ocorrer se r for par ou igual a 5. Restam quatro casos a analisar:

- ♦ $r = 1$: Nesse caso, $1^{10}+1 = 2 \Rightarrow 10 \nmid 1^{10}+1$.
- ♣ $r = 3$: Nesse caso, $3^{10}+1 = 3^{8+2}+1 = 3^8 \cdot 3^2 + 1 = (3^4)^2 \cdot 9 + 1$. Como $3^4 = 81 = 10 \cdot 8 + 1$, o resto de 3^8 por 10 é 1, então $(3^4)^2 \cdot 9 + 1 = 10q + 1 \cdot 9 + 1 = 10 \cdot (9q) + 10 = 10(9q+1) \Rightarrow 10 \mid 3^{10}+1$.
- ♥ $r = 7$: Nesse caso, $7^{10}+1 = 7^{8+2}+1 = 7^8 \cdot 7^2 + 1 = (7^4)^2 \cdot 49 + 1$. Como $7^4 = 2401 = 10 \cdot 240 + 1$, o resto de 7^8 por 10 é 1, então $(7^4)^2 \cdot 49 + 1 = 10q + 1 \cdot 49 + 1 = 10 \cdot (49q) + 50 = 10(49q+5) \Rightarrow 10 \mid 7^{10}+1$.
- ♠ $r = 9$: Nesse caso, $9^{10}+1 = 9^{8+2}+1 = 9^8 \cdot 9^2 + 1 = (9^2)^4 \cdot 81 + 1$. Como $9^2 = 81 = 10 \cdot 8 + 1$, o resto de 9^8 por 10 é 1, então $(9^2)^4 \cdot 81 + 1 = 10q + 1 \cdot 81 + 1 = 10 \cdot (81q) + 82 = 10(81q+8) + 2 \Rightarrow 10 \nmid 9^{10}+1$

Assim, a pode ser qualquer número na forma $10k+3$ ou $10k+7$.

(b) Pelo item anterior, cada a_i deixa resto 3 ou 7 na divisão por 10. Como temos um número ímpar de parcelas, a soma desses restos não pode ser um número par. Assim, não pode ser um número divisível por 10.

(18) [Critério de divisibilidade por 7] Para verificar se um número é divisível por 7, devemos duplicar o algarismo das unidades e subtrair o resto do número. Se o resultado dessa operação for divisível por 7, então o número é divisível por 7.

(a) Verifique se os números 56735, 1563 e 1057 são divisíveis por 7.

(b) Prove a validade desse critério de divisibilidade.

Solução

(a) Pelo critério do enunciado, temos:

- ♥ $56735 \Rightarrow 5673 - 2 \cdot 5 = 5663 \Rightarrow 566 - 2 \cdot 3 = 560 \Rightarrow 56 - 2 \cdot 0 \Rightarrow 56 = 7 \cdot 8$
- ♣ $1563 \Rightarrow 156 - 2 \cdot 3 = 150 \Rightarrow 15 - 2 \cdot 0 = 15 = 7 \cdot 2 + 1$
- ♦ $1057 \Rightarrow 105 - 2 \cdot 7 = 91 \Rightarrow 9 - 2 \cdot 1 = 7 = 7 \cdot 1$.

Assim, 56735 e 1057 são divisíveis por 7, e 1563 não.

(b) Como $\text{mdc}(7,10) = 1$, pelo Teorema de Bézout, existem inteiros r e s tais que $7r + 10s = 1$. Logo,

$$7r + 10s = 1 \Rightarrow 10s - 1 = -7r \Rightarrow 10s - 1 = 7(-r) \Rightarrow 7 \mid 10s - 1 \Rightarrow 10s = 7k + 1, k \in \mathbb{Z}.$$

Vamos agora mostrar que, tomando $n = \overline{n_k n_{k-1} \dots n_1 n_0}$, e $m = \overline{n_k n_{k-1} \dots n_1} - sn_0$, $7 \mid n$, se e somente se $7 \mid m$.

Como $7 \mid n$, então existe um inteiro q tal que $n = 7q$. Assim:

$$\overline{n_k n_{k-1} \dots n_1} + n_0 = 7q \Leftrightarrow$$

$$10 \cdot \overline{n_k n_{k-1} \dots n_1} + n_0 = 10 \cdot 7q \Leftrightarrow$$

$$10 \cdot \overline{n_k n_{k-1} \dots n_1} + n_0 = 7(10)q \Leftrightarrow$$

$$10 \cdot s \cdot \overline{n_k n_{k-1} \dots n_1} + s \cdot n_0 = s \cdot 7(10q) \Leftrightarrow$$

$$7k + 1 \cdot \overline{n_k n_{k-1} \dots n_1} + s \cdot n_0 = s \cdot 7(10q) \Leftrightarrow$$

$$7k \cdot \overline{n_k n_{k-1} \dots n_1} + \overline{n_k n_{k-1} \dots n_1} + s \cdot n_0 = s \cdot 7(10q) \Leftrightarrow$$

$$\overline{n_k n_{k-1} \dots n_1} + s \cdot n_0 = s \cdot 7(10q) - 7k \cdot \overline{n_k n_{k-1} \dots n_1} \Leftrightarrow$$

$$\overline{n_k n_{k-1} \dots n_1} + s \cdot n_0 = 7(10sq - k \cdot \overline{n_k n_{k-1} \dots n_1}) \Leftrightarrow$$

$$m = 7(10sq - k \cdot \overline{n_k n_{k-1} \dots n_1})$$

Logo, $7 \mid m$.

Para demonstrar o resultado agora, basta provar que $s = -2$ serve para o cálculo acima. De fato, $10 \cdot (-2) - 1 = -21 = 7 \cdot (-3)$. Assim, concluímos que $m = \overline{n_k n_{k-1} \dots n_1} - 2 \cdot n_0$ é um múltiplo de 7 se, e somente se, n o for.

(19) [Critérios de Divisibilidade por 3 e por 9] Seja a um número inteiro.

(a) Prove que a é divisível por 3 se, e somente se, a soma de seus dígitos for divisível por 3.

(b) Prove que um inteiro é divisível por 9 se, e somente se, a some de seus dígitos for divisível por 9.

(c) Mostre que o número

$$n = 2357111317192329313741434753596167 71,$$

formado pela concatenação dos números primos entre 2 e 71, é um múltiplo de 9.

Solução

Primeiramente, observe que, se

$$n = (a_n a_{n-1} \cdots a_1 a_0)_{10} = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10^1 + a_0 10^0$$

então

$$n = a_n \left(10^n - 1\right) + a_{n-1} \left(10^{n-1} - 1\right) + a_1 \left(10^1 - 1\right) + (a_n + a_{n-1} + \cdots + a_1 + a_0)$$

Agora, estamos aptos a resolver (a) e (b):

(a) Temos que

$$10 \equiv 1 \pmod 3 \Rightarrow 10^n \equiv 1 \pmod 3$$

Assim, $10^n - 1 \equiv 0 \pmod 3$. Portanto,

$$\begin{aligned} n &= a_n(10^n - 1) + a_{n-1}\left(10^{n-1} - 1\right) + \ldots + a_1\left(10^1 - 1\right) + (a_n + a_{n-1} + \cdots + a_1 + a_0) \\ &\equiv a_n(0) + a_{n-1}(0) + \ldots + a_1(0) + (a_n + a_{n-1} + \cdots + a_1 + a_0) \pmod 3 \\ &\equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 3 \end{aligned}$$

$$n \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 3$$

Logo, concluímos que n será divisível por 9 se, e somente se, $a_n + a_{n-1} + \cdots + a_1 + a_0$ o for, ou seja

$$3 \mid n \Leftrightarrow 3 \mid (a_n + a_{n-1} + \cdots + a_1 + a_0)$$

.

(b) Temos que

$$10 \equiv 1 \pmod 9 \Rightarrow 10^n \equiv 1 \pmod 9$$

Assim, $10^n - 1 \equiv 0 \pmod 9$. Portanto,

$$\begin{aligned} n &= a_n(10^n - 1) + a_{n-1}\left(10^{n-1} - 1\right) + \ldots + a_1\left(10^1 - 1\right) + (a_n + a_{n-1} + \cdots + a_1 + a_0) \\ &\equiv a_n(0) + a_{n-1}(0) + \ldots + a_1(0) + (a_n + a_{n-1} + \cdots + a_1 + a_0) \pmod 9 \\ &\equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 9 \end{aligned}$$

Logo, concluímos que n será divisível por 9 se, e somente se, $a_n + a_{n-1} + \cdots + a_1 + a_0$ o for, ou seja

$$9 \mid n \Leftrightarrow 9 \mid (a_n + a_{n-1} + \cdots + a_1 + a_0)$$

.

(c) Pelo item (b), basta verificar se a soma dos algarismos de n é divisível por 9. Como a soma dos algarismos de 235711131719232931374143475359616771 é 144 e $9 \mid 144$, concluímos que n é múltiplo de 9.

(20) [Critério de Divisibilidade por 11] Prove que um inteiro é divisível por 11 se, e somente se, a diferença entre a soma dos seus dígitos nas posições ímpares e a soma dos seus dígitos nas posições pares for divisível por 11.

Solução

Escrevendo

$$n = (a_n a_{n-1} \cdots a_1 a_0)_{10} = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10^1 + a_0 10^0,$$

Observe que

$$10 \equiv -1 (\mathrm{mod} 11) \Rightarrow \begin{cases} 10^n \equiv 1 (\mathrm{mod} 11), & \text{se n é par} \\ 10^n \equiv -1 (\mathrm{mod} 11), & \text{se n é ímpar} \end{cases}$$

Assim, temos que

$$\begin{aligned} n &\equiv a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10^1 + a_0 10^0 \pmod{11} \\ &\equiv a_n(-1)^n + a_{n-1}(-1)^{n-1} + \cdots + a_1(-1) + a_0 \cdot 1 \pmod{11} \\ &\equiv a_0 - a_1 + a_2 - a_3 + \cdots \pmod{11} \\ &\equiv (a_0 + a_2 + a_4 + \cdots) - (a_1 + a_3 + a_5 + \cdots) \pmod{11} \end{aligned}$$

$$11 \mid n \Leftrightarrow 11 \mid (a_0 + a_2 + a_4 + \cdots) - (a_1 + a_3 + a_5 + \cdots)$$

(21) * A soma dos algarismos de 2021! foi escrita na representação decimal. A soma dos algarismos do número resultante foi escrita na representação decimal, e assim por diante. Finalmente, o resultado é um número de um único algarismo. Encontre esse número.

Solução
Um número será divisível por 9 se e somente se a soma de seus algarismos o for. Logo, o último número obtido corresponderá ao resto da divisão de 2021! por 9. Como $9 \mid 2021!$, e $2021! \neq 0$, temos que o número procurado é o 9.

2 Máximo divisor comum e mínimo múltiplo comum

(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
Seja $d = \text{mdc}\,(a,0)$. Por definição, $d \mid 0$ e $d \mid a$. Vamos verificar que $d = |a|$. Para isso, note que $|a| \mid a$ e $|a| \mid 0, \forall a \in \mathbb{Z}$. Além disso, se $c \mid a$, $c \leq |a|$. Assim, $d = |a|$.
A prova que $\text{mdc}\,(a,a) = |a|$ é a mesma.
Por último, vejamos que $\text{mdc}(a,1) = 1$. Seja $d' = \text{mdc}\,(a,1)$. Por definição, $d' \mid 1$, o que implica que $d' = 1$, pois $d' > 0$.

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

Solução
Sejam $d = \text{mdc}\,(a,b)$ e $d' = \text{mdc}\,(|a|,|b|)$. Vamos provar que $d \mid d'$ e $d' \mid d$, acarretando $d = d'$. Temos que

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

o que termina a questão.

(3) Prove que o máximo divisor comum é uma operação associativa, ou seja, que

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

para todos $a, b, c \in \mathbb{Z}$.

Solução

Pelo exercício 2, basta provar o resultado para $a, b, c \in \mathbb{N}$.
Sejam

$$e = \text{mdc}(a, \text{mdc}(b, c)) \quad \text{e} \quad f = \text{mdc}(\text{mdc}(a, b), c).$$

Precisamos então provar que $e = f$. Para isso, vejamos que $e \mid f$ e $f \mid e$.

- $e \mid f$: Precisamos verificar que $e \mid \text{mdc}(a, b)$ e $e \mid c$, pois isso acarretará por definição de máximo divisor comum que $e \mid f$.

  Por definição, temos que $e \mid a$ e $e \mid \text{mdc}(b, c)$. Como $\text{mdc}(b, c) \mid b$ e $\text{mdc}(b, c) \mid c$, segue que $e \mid b$ e $e \mid c$.

  Vejamos que $e \mid \text{mdc}(a, b)$. Pelo Teorema de Bézout, temos que existem inteiros $r, s \in \mathbb{Z}$ tais $quear + bs = \text{mdc}(a, b)$. Como $e \mid a$ e $e \mid b$, então $e \mid ar$ e $e \mid bs$. Assim, $e \mid \text{mdc}(a, b)$. Portanto, concluímos que $e \mid \text{mdc}(\text{mdc}(a, b), c) \Rightarrow e \mid f$.

- $f \mid e$: Precisamos verificar que $f \mid a$ e $f \mid \text{mdc}(b, c)$, pois isso acarretará por definição de máximo divisor comum que $f \mid e$.

  Por definição, temos que $f \mid \text{mdc}(a, b)$ e $f \mid c$. Como $\text{mdc}(a, b) \mid a$ e $\text{mdc}(a, b) \mid b$, segue que $f \mid b$ e $f \mid c$.

  Vejamos que $f \mid \text{mdc}(b, c)$. Pelo Teorema de Bézout, temos que existem inteiros $r', s' \in \mathbb{Z}$ tais que $br' + cs' = \text{mdc}(b, c)$. Como $f \mid b$ e $f \mid c$, então $f \mid br'$ e $f \mid cs'$. Assim, $f \mid \text{mdc}(b, c)$. Portanto, concluímos que $f \mid \text{mdc}(a, \text{mdc}(b, c)) \Rightarrow f \mid e$.

(4) 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

Sejam $d = \text{mdc}(a, b)$ e $d' = \text{mdc}(na, nb)$. Pelo Teorema de Bézout, como $d = \text{mdc}(a, b)$, 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 $d \mid b$ pela definição de máximo divisor comum, então $nd \mid na$ e $nd \mid nb$, ou seja, $nd \mid d'$, pois $d' = \text{mdc}(na, nb)$.
Portanto, $nd = d'$.
Agora, para mostrar que $\text{mmc}(na, nb) = n\text{mmc}(a, b)$, usaremos que

$$mmc(\alpha, \beta)\text{mdc}(\alpha, \beta) = \alpha\beta,$$

para $\alpha, \beta \in \mathbb{N}^*$. Temos então:

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

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

(5) Determine $\text{mdc}(a,b)$ e $\text{mmc}(a,b)$ 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

(a) Usando o Algoritmo de Euclides, temos:

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

Agora, como $\text{mmc}(32,54)\cdot\text{mdc}(32,54) = 32\cdot 54$, temos:

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

Portanto,

$$\boxed{\text{mdc}(32,54) = 2 \text{ e } \text{mmc}(32,54) = 864}$$

(b) Usando o Algoritmo de Euclides, temos:

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

Agora, como $\text{mmc}(27,45)\cdot\text{mdc}(27,45) = 27\cdot 45$, temos:

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

Portanto,

$$\boxed{\text{mdc}(27,45) = 9 \text{ e } \text{mmc}(27,45) = 135}$$

(c) Usando o Algoritmo de Euclides, temos:

$$\begin{aligned}\text{mdc}\,(15,80) &= \text{mdc}\,(15, 80-5\cdot 15) = \text{mdc}\,(15,5)\\ &= \text{mdc}\,(15-3\cdot 5, 5) = \text{mdc}\,(0,5) = 5.\end{aligned}$$

Agora, como $\text{mmc}(15,80)\cdot\text{mdc}(15,80) = 15\cdot 80$, temos:

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

Portanto,

$$\boxed{\text{mdc}(15,80) = 5 \text{ e } \text{mmc}(15,80) = 240}$$

(d) Usando o Algoritmo de Euclides, temos:

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

Agora, como $\text{mmc}(8798,2314)\cdot\text{mdc}(8798,2314) = 8798\cdot 2314$, temos:

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

Portanto,

$$\boxed{\text{mdc}(8798,2314) = 2 \text{ e } \text{mmc}(8798,2314) = 10179286}$$

(e) Usando o Algoritmo de Euclides, temos:

$$\begin{aligned}\text{mdc}\,(1583890,3927) &= \text{mdc}\,(1583890-403\cdot 3927, 3927) = \text{mdc}\,(1309,3927)\\ &= \text{mdc}\,(1309, 3927-3\cdot 1309) = \text{mdc}\,(1309,0) = 1309.\end{aligned}$$

Agora, como $\text{mmc}(1583890,3927)\cdot\text{mdc}(1583890,3927) = 1583890\cdot 3927$, temos:

$$\text{mmc}\,(1583890,3927) = \frac{1583890\cdot 3927}{\text{mdc}\,(1583890,3927)} = 4751670.$$

Portanto,

$$\boxed{\text{mdc}(1583890,3927) = 1309 \text{ e } \text{mmc}(1583890,3927) = 4751670}$$

(6) 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

(a) Pelo Algoritmo de Euclides,

$$\begin{aligned} 72 &= 1 \cdot 56 + 16 \\ 56 &= 3 \cdot 16 + 8 \\ 16 &= 2 \cdot 8 \end{aligned}$$

Agora, como $\text{mdc}(56, 72) = 8$, vamos escrever 8 em função de uma combinação linear de 56 e 72 registrando em cada passo o resto como sendo a diferença do dividendo com o produto do quociente pelo divisor. Assim

$$\begin{aligned} 8 &= 56 - 3 \cdot 16 \\ &= 56 - 3 \cdot (72 - 1 \cdot 56) \\ &= 4 \cdot 56 - 3 \cdot 72 \end{aligned}$$

Assim, encontramos $r = 4$ e $s = -3$.

(b) Pelo Algoritmo de Euclides,

$$\begin{aligned} 138 &= 5 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 \end{aligned}$$

Agora, como $\text{mdc}(24, 138) = 6$, vamos escrever 6 em função de uma combinação linear de 24 e 138 registrando em cada passo o resto como sendo a diferença do dividendo com o produto do quociente pelo divisor. Assim

$$\begin{aligned} 6 &= 24 - 1 \cdot 18 \\ &= 24 - 1 \cdot (138 - 5 \cdot 24) \\ &= 6 \cdot 24 - 1 \cdot 138 \end{aligned}$$

Assim, encontramos $r = 6$ e $s = -1$.

(c) Pelo Algoritmo de Euclides,

$$\begin{aligned} 272 &= 2 \cdot 119 + 34 \\ 119 &= 3 \cdot 34 + 17 \\ 34 &= 2 \cdot 17 \end{aligned}$$

Agora, como $\text{mdc}(119, 272) = 17$, vamos escrever 17 em função de uma combinação linear de 119 e 272 registrando em cada passo o resto como sendo a diferença do dividendo com o produto do quociente pelo divisor. Assim

$$\begin{aligned} 17 &= 119 - 3 \cdot 34 \\ &= 119 - 3 \cdot (272 - 2 \cdot 119) \\ &= 7 \cdot 119 - 3 \cdot 272 \end{aligned}$$

Assim, encontramos $r = 7$ e $s = -3$.

(d) Pelo Algoritmo de Euclides,

$$\begin{aligned} 1128 &= 3 \cdot 336 + 120 \\ 336 &= 2 \cdot 120 + 96 \\ 120 &= 1 \cdot 96 + 24 \\ 96 &= 4 \cdot 24 \end{aligned}$$

Agora, como $\text{mdc}(1128, 336) = 24$, vamos escrever 24 em função de uma combinação linear de 1128 e 336 registrando em cada passo o resto como sendo a diferença do dividendo com o produto do quociente pelo divisor. Assim

$$\begin{aligned} 24 &= 120 - 1 \cdot 96 \\ &= 120 - 1 \cdot (336 - 2 \cdot 120) \\ &= 3 \cdot 120 - 1 \cdot 336 \\ &= 3 \cdot (1128 - 3 \cdot 336) - 1 \cdot 336 \\ &= 3 \cdot 1128 - 10 \cdot 336 \end{aligned}$$

Assim, encontramos $r = 3$ e $s = -10$.

(7) 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

Provemos cada uma das equivalências:
$((a) \Rightarrow (b))$ Suponha que $a \mid b$. Vamos mostrar que $\text{mdc}(a, b) = |a|$.
Se $a \mid b$, iss o significa que existe um $k \in \mathbb{Z}$ tal que $b = k \cdot a$. Assim, pela questão 4,

$$\begin{aligned} \text{mdc}(a, b) &= \text{mdc}(a, ka) \\ &= \text{mdc}(a \cdot 1, a \cdot k) \\ &= |a| \, \text{mdc}(1, k) \\ &= |a| \cdot 1 = |a| \end{aligned}$$

$((b) \Rightarrow (c))$ Suponha que $\text{mdc}(a, b) = |a|$. Vejamos que $\text{mmc}(a, b) = |b|$. Sabemos que, para $\alpha, \beta \in \mathbb{Z}$ temos

$$\text{mdc}(\alpha, \beta) \cdot \text{mmc}(\alpha, \beta) = |\alpha| \cdot |\beta| . \tag{1}$$

Utilizando esse fato, ao isolarmos $\text{mmc}(a, b)$, vem

$$\begin{aligned} \text{mmc}(a, b) &= \frac{|a||b|}{\text{mdc}(a, b)} \\ &= \frac{|a||b|}{|a|} \\ &= \frac{\cancel{|a|}|b|}{\cancel{|a|}} \\ &= |b| . \end{aligned}$$

$((c) \Rightarrow (a))$ Suponha que $\text{mmc}(a,b) = |b|$. Com esta hipótese em mãos, provemos que $a \mid b$. Novamente, pela relação (1),

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

Como $|a| = \text{mdc}(a,b)$, pela definição de máximo divisor comum, isso significa que $|a| \mid a$ e, em particular, que $|a| \mid b$. Logo, concluímos que $a \mid b$, como queríamos.

(8) 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

Para saber quando o Sol se alinha com Mercúrio e Vênus, precisamos encontrar o momento no qual ambos deram uma quantidade exata de voltas em torno do Sol, ou seja, um múltiplo comum do período de translação de ambos os planetas. Consequentemente, a resposta será $\text{mmc}(5393, 2111)$. Para calcular esse valor, atenhamo-nos inicialmente ao $\text{mdc}(5393, 2111)$. Pelo Algoritmo de Euclides,

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

Agora, como $\text{mmc}(5393, 2111)\cdot\text{mdc}(5393, 2111) = 5393\cdot 2111$, temos:

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

Portanto, Sol, Mercúrio e Vênus se alinham a cada 11384623 horas, ou seja, aproximadamente a cada 1300 anos (considerando que um ano tem $24\cdot 365 = 8760$ horas).

(9) Mostre que se a é um inteiro positivo então a e $a+1$ são primos entre si.

Solução

Para mostrar que dois números são primos entre si, basta mostrar que o mdc entre eles é 1. Assim, pelo Algoritmo de Euclides:

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

Assim, dois números consecutivos são sempre primos entre si.

(10) Escolhendo-se 51 números dentre os números naturais de 1 até 100, prove que existem ao menos 2 que devem ser primos entre si.

Solução

Pelo exercício anterior, sabemos que $\text{mdc}(a, a+1) = 1$. Vamos organizar os números de 1 a 100 em 50 pares:

$$\{1,2\}, \{3,4\}, \{5,6\}, \ldots, \{99,100\}.$$

Em cada um desses pares, temos números primos entre si. Como estamos escolhendo 51 números, ao menos 2 deles devem pertencer ao mesmo par, e portanto esses números serão primos entre si.

(11) 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, $d \leq \text{mdc}(2a, 2b) = 2\text{mdc}(a,b)$);

(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

(a) Seja $d = mdc\,(a+b, a-b)$. Pela definição de máximo divisor comum, temos que $d \mid a+b$ e $d \mid a-b$. Portanto:

$$d \mid (a-b) \Rightarrow d \mid (a-b)+(a+b) \Rightarrow d \mid a-b+a+b \Rightarrow d \mid 2a.$$

Analogamente,

$$d \mid (a+b) \Rightarrow d \mid (a+b)-(a-b) \Rightarrow d \mid a+b-a+b \Rightarrow d \mid 2b.$$

Como $d \mid 2a$ e $d \mid 2b$, então $d \mid \text{mdc}(2a, 2b)$. Pelo exercício 4, $\text{mdc}(2a, 2b) = 2\text{mdc}(a,b)$. Assim:

$$d \mid \text{mdc}(2a,2b) \Rightarrow d \mid 2 \cdot \text{mdc}(a,b) \Rightarrow d \mid 2 \cdot 1 \Rightarrow d \mid 2 \Rightarrow d = 2 \text{ ou } d = 1.$$

Consequentemente, segue que $d = 2$ ou $d = 1$.

(b) Seja $d = mdc\,(2a+b, a+2b)$. Pela definição de máximo divisor comum, temos que $d \mid 2a+b$ e $d \mid a+2b$. Portanto:

$$d \mid (2a+b) \Rightarrow d \mid (2a+b)-2(a+2b) \Rightarrow d \mid 2a+b-2a-4b \Rightarrow d \mid -3b \Rightarrow d \mid 3b$$

Analogamente,

$$d \mid (a+2b) \Rightarrow d \mid (a+2b)-2(2a+b) \Rightarrow d \mid a+2b-4a-2b \Rightarrow d \mid -3a \Rightarrow d \mid 3a.$$

Como $d \mid 3a$ e $d \mid 2b$, então $d \mid \text{mdc}(3a, 3b)$. Pelo exercício 4, $\text{mdc}(3a, 3b) = 3\text{mdc}(a,b)$. Assim:

$$d \mid \text{mdc}(3a,3b) \Rightarrow d \mid 3 \cdot \text{mdc}(a,b) \Rightarrow d \mid 3 \cdot 1 \Rightarrow d \mid 3 \Rightarrow d = 3 \text{ ou } d = 1.$$

Consequentemente, segue que $d = 3$ ou $d = 1$.

(c) Seja $d = mdc\left(a^2+b^2, a+b\right)$. Pelo Algoritmo de Euclides, temos

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

Assim, por definição de máximo divisor comum, temos que $d \mid 2b^2$ e $d \mid a+b$.

Analogamente,

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

Assim, por definição de máximo divisor comum, temos que $d \mid 2a^2$ e $d \mid a+b$.

Como $d \mid 2a^2$ e $d \mid 2b^2$, então $d \mid \text{mdc}(2a^2, 2b^2)$. Pelo exercício 4, $\text{mdc}(2a^2, 2b^2) = 2\text{mdc}(a^2, b^2)$. Assim:

$$d \mid \text{mdc}(2a^2, 2b^2) \Rightarrow d \mid 2 \cdot \text{mdc}(a^2, b^2) \Rightarrow d \mid 2 \cdot (\text{mdc}(a,b))^2 \Rightarrow d \mid 2 \cdot 1^2 \Rightarrow d = 2 \text{ ou } d = 1.$$

Portanto, segue que $d = 2$ ou $d = 1$.

(12) 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

Como $a \mid b$, então existe um $k \in \mathbb{Z}$ tal que $b = k \cdot a$. Se $\text{mdc}(b,c) = 1$, então, pelo Teorema de Bézout, existem $x, y \in \mathbb{Z}$, tais que:

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

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

$$d \mid kax + cy \Rightarrow d \mid 1.$$

Portanto, $d = 1$.

(13) Explique como definir o máximo divisor comum $\text{mdc}(a,b,c)$ de três números inteiros a, b, c. Em seguida, generalize sua definição para aplicar a qualquer quantidade de números inteiros.

Solução

Sabemos como resolver o máximo divisor comum no caso de dois elementos. Então, podemos pensar em calcular o máximo divisor comum de 3 números agrupando de dois em dois:

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

Observe que o valor de $\text{mdc}\,(a,b,c)$ independe da ordem na qual fazemos os agrupamentos (para uma demonstração desse fato, veja o exercício 3).
Generalizando com a mesma ideia, temos:

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

(14) Um empreiteiro deseja construir um prédio em um terreno retangular de dimensões 216 m por 414 m. Para isso deverá cercá-lo com estacas. Se ele colocar uma estaca em cada canto do terreno e utilizar sempre a mesma distância entre duas estacas consecutivas, qual será a quantidade mínima de estacas a serem utilizadas?

Solução

Precisamos dividir as estacas pelo terreno de modo que a distância entre elas seja sempre a mesma, independente de estar no lado que mede 216 m ou no lado que mede 414 m. Assim, essa distância corresponde a um divisor comum de 216 e 414, coo como queremos a menor quantidade de estacas possível, devemos procurar pelo máximo divisor comum entre 414 e 216.
Pelo Algoritmo de Euclides, temos:

$$\begin{aligned}\text{mdc}\,(414,216) &= \text{mdc}\,(414-1\cdot 216,216) = \text{mdc}\,(198,216)\\ &= \text{mdc}\,(198,216-1\cdot 198) = \text{mdc}\,(198,18)\\ &= \text{mdc}\,(198-11\cdot 18,18) = \text{mdc}\,(0,18) = 18.\end{aligned}$$

Portanto, como $\text{mdc}(216,414) = 18$, isso significa que as estacas ficarão a uma distância de 18 m uma das outras.
No total, o perímetro do terreno, por ser retangular, será de $2\cdot 216 + 2\cdot 414 = 1260$ m. Logo, serão necessárias no mínimo $\dfrac{1260}{18} = 70$ estacas para cercar o terreno.

(15) Dona Antônia possui um enfeite pisca-pisca, para árvores de Natal, que tem lâmpadas amarelas, vermelhas e azuis. As lâmpadas amarelas se acendem de 4 em 4 minutos; as vermelhas, de 3 em 3 minutos; e as azuis, de 6 em 6 minutos.

(*a*) Se às 20 horas e 15 minutos todas as lâmpadas se acenderem, a que horas elas voltarão a se acender novamente ao mesmo tempo?

(*b*) Dona Antônia quer deixar sua árvore de Natal mais colorida, e por isso vai comprar um pisca-pisca verde. De quanto em quanto tempo as lâmpadas verdes deverão acender para que todas as lâmpadas do ornamento decorativo de Dona Antônia acendam simultaneamente ao menos 87 vezes por dia?

Solução

(a) Como $\text{mmc}(4,3,6) = 12$, a próxima ocasião em que as lâmpadas acenderão simultaneamente será às 20 horas e 27 minutos.

(b) Seja m o tempo em que as lâmpadas verdes se acendem. Então, como o dia tem $24 \cdot 60 = 1440$ minutos, queremos que

$$\frac{1440}{\text{mmc}(4,3,6,m)} > 87 \Rightarrow x < \left\lfloor \frac{1440}{87} \right\rfloor \Rightarrow \text{mmc}(4,3,6,m) < 16$$

Como o máximo múltiplo comum é uma operação associativa, temos que

$$\text{mmc}(4,3,6,m) = \text{mmc}(\text{mmc}(4,3,6),m) = \text{mmc}(12,m).$$

Assim, devemos ter $\text{mmc}(12,m) < 16$. Como $16 < 2 \cdot 12$, m deve ser um divisor de 12. Assim, $m \in D(12)$. Logo, os possíveis valores para m são

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

(16) * Prove que, se a e b são números inteiros primos entre si com $a > b$, então para todo par de inteiros positivos m, n, temos que

$$\text{mdc}(a^m - b^m, a^n - b^n) = a^{\text{mdc}(m,n)} - b^{\text{mdc}(m,n)}.$$

[Dica:] Chamando $e = a^{\text{mdc}(m,n)} - b^{\text{mdc}(m,n)}$ e $f = \text{mdc}(a^m - b^m, a^n - b^n)$, mostre que $e \mid f$ e $f \mid e$, usando o Teorema de Bézout e o fato de que, se $\alpha \mid a^\beta - b^\beta$, então $\alpha \mid a^{\beta\gamma} - b^{\beta\gamma}$, para $\alpha, \beta, \gamma \in \mathbb{N}$.

Solução

Sejam $d = \text{mdc}(m,n)$, $e = a^d - b^d$ e $f = \text{mdc}(a^m - b^m, a^n - b^n)$. A afirmação do enunciado equivale a mostrar que $e = f$. Pela definição de máximo divisor comum, $d \mid m$. Logo, $m = dq, q \in \mathbb{Z}$. Assim,

$$\begin{aligned} a^m - b^m &= a^{dq} - b^{dq} \\ &= \left(a^d - b^d\right)\left(a^{(q-1)d} + a^{(q-2)d}b^d + a^{(q-3)d}b^{2d} + \ldots + a^d b^{(q-2)d} + b^{(q-1)d}\right) \\ &= \left(a^d - b^d\right)\left(\sum_{k=0}^{q-1} a^{kd} b^{((q-1)-k)d}\right) \\ &= e\left(\sum_{k=0}^{q-1} a^{kd} b^{((q-1)-k)d}\right) \end{aligned}$$

e portanto $e \mid a^m - b^m$. Analogamente, como $d \mid n$, temos que $e \mid a^n - b^n$. Assim, $e \mid f$.
Precisamos agora mostrar que $f \mid e$. Para isso, utilizando o Teorema de Bézout, escolhemos inteiros $x, y > 0$ tais que $mx - ny = d$. Então

$$a^{mx} = a^{d+ny} = a^{ny} \cdot a^d = a^{ny} \cdot (e + b^d)$$

Desse modo,

$$a^{mx} - b^{mx} = a^{ny}(e + b^d) - b^{d+ny} = a^{ny}e + a^{ny} \cdot b^d - b^d \cdot b^{ny} = b^d(a^{ny} - b^{ny}) + ea^{ny}$$

Por definição de máximo divisor comum, $f \mid a^m - b^m$, então $f \mid a^{mx} - b^{mx}$. Além disso, $f \mid a^n - b^n$, e portanto $f \mid a^{ny} - b^{ny}$. Assim, da equação acima concluímos que $f \mid ea^{ny}$. Mas $\text{mdc}(f, a) = 1$, pois qualquer divisor comum de a e f divide simultaneamente $a^m, a^m - b^m$, e consequentemente, b^m, mas $\text{mdc}(a, b) = 1$.
Como $f \mid ea^{ny}$ e $\text{mdc}(a, f) = 1$, segue que $f \mid e$.

(17) Para cada item, encontre o menor valor positivo de n para o qual a fração dada não é irredutível nem nula:

(a) $\dfrac{n-11}{3n+8}$

(b) $\dfrac{4n+17}{n-5}$

(c) $\dfrac{2n+5}{7n+1}$

(d) $\dfrac{n^3+2n^2-54n+34}{n^2+8n-7}$

Solução

(a) Para que a fração não seja irredutível, devemos ter $\text{mdc}(n-11, 3n+8) \neq 1$. Seja d um divisor comum de $n-11$ e $3n+8$. Então, pelo Algoritmo de Euclides, d deve ser um divisor de

$$3n + 8 - 3(n - 11) = 41$$

Dessa forma, devemos ter

$$\text{mdc}(n - 11, 3n + 8) = \text{mdc}(n - 11, 41).$$

Então, para que $d > 1$, $n - 11$ deve ser múltiplo de 41, e devemos ter

$$n - 11 = 41q \Rightarrow n = 41q + 11$$

Como $n - 11 > 0$, menor valor será obtido quando $q = 1$, ao passo que $n = 52$.

(b) Para que a fração não seja irredutível, devemos ter $\text{mdc}(4n+17, n-5) \neq 1$. Seja d um divisor comum de $4n+17$ e $n-5$. Então, pelo Algoritmo de Euclides, d deve ser um divisor de

$$4n + 17 - 4(n - 5) = 37$$

Dessa forma, devemos ter

$$\text{mdc}(n - 5, 4n + 17) = \text{mdc}(n - 5, 37).$$

Então, para que $d > 1$, $n - 5$ deve ser múltiplo de 37, e devemos ter

$$n - 5 = 37q \Rightarrow n = 37q + 5$$

Como $n - 5 > 0$, o menor valor será obtido quando $q = 1$, ao passo que $n = 42$.

(c) Para que a fração não seja irredutível, devemos ter $\text{mdc}(2n+5, 7n+1) \neq 1$. Seja d um divisor comum de $2n+5$ e $7n+1$. Então, pelo Algoritmo de Euclides, d deve ser um divisor de

$$7n+1-3(2n+5) = n-14$$

Dessa forma, devemos ter

$$\text{mdc}(2n+5, 7n+1) = \text{mdc}(2n+5, n-14).$$

Aplicando novamente o Algoritmo de Euclides,

$$2n+5-2(n-14) = 33$$

Logo,

$$\text{mdc}(2n+5, n-14) = \text{mdc}(n-14, 33).$$

Então, para que $d > 1$, $n-14$ deve ser múltiplo de um divisor de 33. Como $33 = 3 \cdot 11$, $n-14$ deve ser múltiplo de 3, e assim

$$n-14 = 3q \Rightarrow n = 3q+14$$

O menor valor será obtido quando $q = -4$, ao passo que $n = 2$.

(d) Para que a fração não seja irredutível, devemos ter $\text{mdc}(n^3+2n^2-54n+34, n^2+8n-7) \neq 1$. Seja d um divisor comum de $n^3+2n^2-54n+34$ e n^2+8n-7. Então, pelo Algoritmo de Euclides, d deve ser um divisor de

$$n^3+2n^2-54n+34-(n-6)(n^2+8n-7) = n-8$$

Dessa forma, devemos ter

$$\text{mdc}(n^3+2n^2-54n+34, n^2+8n-7) = \text{mdc}(n-8, n^2+8n-7).$$

Aplicando novamente o Algoritmo de Euclides,

$$n^2+8n-7-n(n-8) = 16n-7$$

Logo,

$$\text{mdc}(n-8, n^2+8n-7) = \text{mdc}(n-8, 16n-7).$$

Mais uma vez, por Euclides,

$$16n-7-16(n-8) = 121$$

Então, para que $d > 1$, $n-8$ deve ser múltiplo de um divisor de 121. Como $121 = 11^2$, $n-8$ deve ser múltiplo de 11, e assim

$$n-8 = 11q \Rightarrow n = 11q+8$$

O menor valor será obtido quando $q = 0$, ao passo que $n = 8$.

(18) * Sabe-se que, se F_m representa o m-ésimo número de Fibonacci, então

$$\text{mdc}(F_m, F_n) = F_{\text{mdc}(m,n)}, \quad \forall m, n \in \mathbb{N}.$$

Use este fato para provar que nenhum número de Fibonacci ímpar é divisível por 17.

Solução

Seja F_n um número de Fibonacci ímpar, e considere $d = \text{mdc}(17, F_n)$. Se $17 \mid F_n$, e F_n é ímpar, então d deve ser ímpar. Mas

$$d = \text{mdc}(17, F_n) = \text{mdc}(34, F_n) = \text{mdc}(F_9, F_n) = F_{\text{mdc}(9,n)}.$$

Como $\text{mdc}(9, n) \in \{1, 3, 9\}$, os possíveis valores para d são $F_1 = 1$, $F_3 = 2$ e $F_3 = 34$. Como d é ímpar, segue que $d = 1$, ou seja, $17 \nmid F_n$.

(19) * Sejam a_n e b_n inteiros satisfazendo a relação

$$a_n + b_n\sqrt{2} = (1 + \sqrt{2})^n,$$

para todo inteiro positivo n. Prove que $\text{mdc}(a_n, b_n) = 1$.
[Dica:] Aplique indução em n.

Solução

Vamos usar indução em n. Para o **caso base**, vamos considerar $n = 1$. Note que

$$\left(1 + \sqrt{2}\right)^1 = 1 + \sqrt{2} \Rightarrow a_1 = 1 \text{ e } b_1 = 1.$$

E claramente $\text{mdc}(a_1, a_1) = \text{mdc}(1, 1) = 1$. Para a **hipótese de indução**, considere que, para algum $n = k \geq 1$, tenhamos que, se

$$a_k + b_k\sqrt{2} = \left(1 + \sqrt{2}\right)^k,$$

então $\text{mdc}(a_k, b_k) = 1$. Para o **passo indutivo**, precisamos mostrar que se

$$a_{k+1} + b_{k+1}\sqrt{2} = \left(1 + \sqrt{2}\right)^{k+1},$$

então $\text{mdc}(a_{k+1}, b_{k+1})$. Observe que

$$\begin{aligned} a_{k+1} + b_{k+1} &= \left(1 + \sqrt{2}\right)^{k+1} \\ &= \left(1 + \sqrt{2}\right)\left(1 + \sqrt{2}\right)^k \\ &= \left(1 + \sqrt{2}\right)\left(a_k + b_k\sqrt{2}\right) \\ &= (a_k + 2b_k) + (a_k + b_k)\sqrt{2} \end{aligned}$$

Portanto, $a_{k+1} = a_k + 2b_k$ e $b_{k+1} = a_k + b_k$.
Vejamos agora que $\text{mdc}(a_{k+1}, b_{k+1}) = 1$. Pelo Algoritmo de Euclides,

$$\text{mdc}(a_{k+1}, b_{k+1}) = \text{mdc}(a_k + 2b_k, a_k + b_k) = \text{mdc}(b_k, a_k + b_k) = \text{mdc}(b_k, a_k) = 1.$$

(20) * Sejam m e n dois números inteiros positivos primos entre si. Encontre os possíveis valores de

$$\text{mdc}(5^m + 7^m, 5^n + 7^n).$$

[Dica:] Escreva $5^m + 7^m = (5^n + 7^n)(5^{m-n} + 7^{m-n}) - 5^n 7^{m-n} - 5^{m-n} 7^n$, e analise o que ocorre com esta expressão para $m < 2n$ e $m > 2n$ para utilizá-la no Algoritmo de Euclides. Em seguida, verifique os possíveis valores de $\text{mdc}(5^m + 7^m, 5^n + 7^n)$ conforme as paridades de m e n.

Solução

Como $\text{mdc}(m,n) = 1$, então $m \neq n$. Suponha sem perda de generalidade que $m > n$. Observe que

$$5^m + 7^m = (5^n + 7^n)(5^{m-n} + 7^{m-n}) - 5^n 7^{m-n} - 5^{m-n}7^n$$

Vamos agora considerar dois casos:

- Se $m < 2n$, podemos escrever

  $$5^n 7^{m-n} + 5^{m-n}7^n = 5^{m-n} \cdot 7^{m-n}(5^{2n-m} + 7^{2n-m}).$$

  Assim,

  $$\begin{aligned} 5^m + 7^m &= (5^n + 7^n)(5^{m-n} + 7^{m-n}) - 5^n 7^{m-n} - 5^{m-n}7^n \\ &= (5^n + 7^n)(5^{m-n} + 7^{m-n}) - 5^{m-n} \cdot 7^{m-n}(5^{2n-m} + 7^{2n-m}) \end{aligned}$$

  Portanto, pelo Algoritmo de Euclides

  $$\begin{aligned} \text{mdc}(5^m + 7^m, 5^n + 7^n) &= \text{mdc}(5^{m-n} \cdot 7^{m-n}(5^{2n-m} + 7^{2n-m}, 5^n + 7^n) \\ &= \text{mdc}(5^{2n-m} + 7^{2n-m}, 5^n + 7^n), \end{aligned}$$

  pois 5 e 7 não dividem $5^n + 7^n$, acarretando $5^{m-n} \cdot 7^{m-n} \nmid 5^n + 7^n$.

- Se $m > 2n$, podemos escrever

  $$5^n 7^{m-n} + 5^{m-n}7^n = 5^n \cdot 7^n(5^{m-2n} + 7^{m-2n}).$$

  Assim,

  $$\begin{aligned} 5^m + 7^m &= (5^n + 7^n)(5^{m-n} + 7^{m-n}) - 5^n 7^{m-n} - 5^{m-n}7^n \\ &= (5^n + 7^n)(5^{m-n} + 7^{m-n}) - 5^n \cdot 7^n(5^{m-2n} + 7^{m-2n}) \end{aligned}$$

  Portanto, pelo Algoritmo de Euclides

  $$\begin{aligned} \text{mdc}(5^m + 7^m, 5^n + 7^n) &= \text{mdc}(5^n \cdot 7^n(5^{m-2n} + 7^{m-2n}) \\ &= \text{mdc}(5^{m-2n} + 7^{m-2n}, 5^n + 7^n), \end{aligned}$$

  pois 5 e 7 não dividem $5^n + 7^n$, acarretando $5^n \cdot 7^n \nmid 5^n + 7^n$.

Chamando $S(m,n) = \text{mdc}(5^m + 7^m, 5^n + 7^n)$, observe que, dos cálculos acima, temos

$$S(m,n) = \begin{cases} S(n, 2n-m), & \text{se } m < 2n \\ S(n, m-2n), & \text{se } m > 2n \end{cases} \tag{2}$$

Como o processo do Algoritmo de Euclides é finito, eventualmente obteremos $S(0,-)$. Vamos analisar o que ocorre com as paridades de m e n :

- Se m e n possuem paridades diferentes, isso significa que $m+n$ é ímpar. Em particular, $2n-m$ deverá ser 1 em algum momento, e teremos ao final

  $$S(m,n) = S(1,0) = \text{mdc}(5^1 + 7^1, 5^0 + 7^0) = \text{mdc}(12,2) = 2.$$

  Vejamos alguns exemplos que corroboram a argumentação acima:

– Se $m = 18$ e $n = 7$, $m > 2n$, então aplicando 2 sucessivas vezes, obtemos

$$\begin{aligned} S(18,7) &= S(7, 18 - 2 \cdot 7) \\ &= S(7,4) = S(4, 2 \cdot 4 - 7) \\ &= S(4,1) = S(1, 4 - 2 \cdot 1) \\ &= S(1,2) = S(1, 2 - 2 \cdot 1) \\ &= S(1,0) = 2 \end{aligned}$$

– Se $m = 11$ e $n = 8$, $m < 2n$,então aplicando 2 sucessivas vezes, obtemos

$$\begin{aligned} S(11,8) &= S(8, 2 \cdot 8 - 11) \\ &= S(8,5) = S(5, 2 \cdot 5 - 8) \\ &= S(5,2) = S(2, 5 - 2 \cdot 2) \\ &= S(2,1) = S(1, 2 - 2 \cdot 1) \\ &= S(1,0) = 2 \end{aligned}$$

- Se m e n têm a mesma paridade, isso significa que $m + n$ é par e, mais ainda, que m e n são ímpares, pois caso contrário, $\text{mdc}(m,n) \neq 1$. Então ao final teremos

$$S(m,n) = S(1,1) = \text{mdc}(5^1 + 7^1, 5^1 + 7^1) = \text{mdc}(12,12) = 12.$$

Vejamos um exemplo:

– Se $m = 11$ e $n = 7$, então aplicando 2 sucessivas vezes, obtemos

$$\begin{aligned} S(11,7) &= S(7, 2 \cdot 7 - 11) \\ &= S(7,3) = S(3, 7 - 2 \cdot 3) \\ &= S(3,1) = S(1, 3 - 2 \cdot 1) \\ &= S(1,1) = S(0,0) = 12 \end{aligned}$$

Assim, concluímos que

$$\text{mdc}(5^m + 7^m, 5^n + 7^n) = \begin{cases} 12, & \text{se } 2 \mid m+n \\ 2, & \text{se } 2 \nmid m+n \end{cases}.$$

Observação: Exercícios marcados com * são extras.