Gabarito Lista 2, Álgebra I

Os seguintes dois Exercicio são muito uteis para mostrar os outros.

Exercicio 1. *Seja $k \in \mathbb{Z}$ positivo. Assim k divide o produto de q.q. k inteiros consecutivos.*

Demonstração: È facil ver (pelo o algoritmo da divisão) que um dos k inteiros consecutivos tem resto 0 quando dividimos por k. Assim k divide o produto deles.

Exercicio 2. *Se $a \mid c$, $b \mid c$ e mdc$(a, b) = 1$ assim $ab \mid c$.*

Demonstração:
Pelo T.de Bezout temos $1 = ax + by$ para algums $x, y \in \mathbb{Z}$. Assim $c = axc + byc$. Mas $c = a \cdot d_1$ e $c = b \cdot d_2$. Assim $axc = axbd_2$ e $byc = byad_1$. Portanto $c = axbd_2 + byad_1$ e ab divide c.

1. Se $a = 2k$ para algum $k \in \mathbb{Z}$, então $a^2 = 4k^2$ é par. Agora suponha, a^2 é par, observe que se a é ímpar, i.e., $a = 2k + 1$ para algum $k \in \mathbb{Z}$, então a^2 é impar também o qual contradiz o fato que a^2 é par.

2. Seja $m = n(n + 1)(n + 2)$. Assim usando o exercício [1] temos que m é divisivel por 2, similarmente, como m é produto de 3 número consecutivos usando o exercício 1 temos que m é divisivel por 3. Agora pelo exercício 2 m é divisível por 6.

   Se $m = n(n + 1)(n + 2)(n + 3)$. Assim $3|m$. Por outro lado $8|m$ (prove!). Assim pelo exercício 2 m é divisível por 24.

3. Suponha que existe um $n \in \mathbb{Z}$ tal que $4 \mid n^2 + 2$, logo $\exists k \in \mathbb{Z}$ tal que $n^2 + 2 = 4k$, dai

   $$n^2 = 4k - 2$$

   Agora, se $n = 2t$ for par, então

   $$4t^2 = 4k - 2$$

   logo

   $$2t^2 = 2k - 1$$

   observe que o lado esquerdo é par e o lado direito é ímpar o qual é absurdo. Se $n = 2t + 1$ for ímpar, então

   $$4t^2 + 4t + 1 = 4k - 2$$

   observe tambem que o lado esquerdo é ímpar e o lado direito é par o qual também é absurdo.

4. Observe que
$$a^2(a^2-1)(a^2-4) = (a-2)(a-1)aa(a+1)(a+2)$$
assim usando o exercício [1], obtemos que
$$5 \mid (a-2)(a-1)a(a+1)(a+2) \quad , \quad 3 \mid (a-2)(a-1)a \quad \text{e} \quad 3 \mid a(a+1)(a+2),$$
e usando o mesmo raciocinio do item 2 temos que
$$8 \mid (a-2)(a-1)a(a+1)$$
Portanto,
$$360 = 8 \cdot 3^2 \cdot 5 \mid (a-2)(a-1)aa(a+1)(a+2) = a^2(a^2-1)(a^2-4).$$

5. 1. Observe que $a^2 - a = (a-1)a$ e use o exercício 1.
   2. Observe que $a^3 - a = (a-1)a(a+1)$ e use o o exercício 1 ou o item 2.
   3. Observe que $a^3 - a = (a-1)a(a+1)(a^2+1)$ e use o exercício 1.

6. Notar primeiro que $6k+5 = 6k+3+2 = 3(2k+1)+2$ e que $6k+5$ é ímpar pois $6k+5 = 6k+4+1 = 2(3k+2)+1$ e $2 = 3(0)+2$.

7. a) Seja n um inteiro ímpar, logo pelo algoritmo da divisão $\exists q, r \in \mathbb{Z}$ tais que
$$n = 4q + r, \quad \text{onde} \quad 0 \le r < 4$$
   e como n é um inteiro ímpar, então $r \neq 0, 2$.

   b) Seja n um inteiro, logo pelo algoritmo da divisão $\exists q, r \in \mathbb{Z}$ tais que
$$n = 3k + r, \quad \text{onde} \quad 0 \le r < 3$$
   Observemos que
   Se $r = 0$, então $n^2 = 3(3k^2)$.
   Se $r = 1$, então $n^2 = (3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$.
   Se $r = 2$, então $n^2 = (3k+2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$.

   c) Seja n um inteiro, logo pelo algoritmo da divisão $\exists q, r \in \mathbb{Z}$ tais que
$$n = 3k + r, \quad \text{onde} \quad 0 \le r < 3$$
   Observemos que
   Se $r = 0$, então $n^3 = 9(3k^3)$.
   Se $r = 1$, então $n^3 = (3k+1)^3 = 27k^3 + 27k^2 + 9k + 1 = 9(3k^3 + 3k^2 + k) + 1$.
   Se $r = 2$, então $n^3 = (3k+2)^3 = 27k^3 + 54k^2 + 36k + 8 = 9(3k^3 + 6k^2 + 4k) + 8$.

8. Use a dica da lista.

9. Sea $x \in \mathbb{Z}$ tal que $n^2 = x = m^3$ para alguns $m, n \in \mathbb{Z}$. Pelo algoritmo da divisão temos que

$$x = 7a + b, \;\; 0 \leq b \leq 6$$
$$n = 7c + d, \;\; 0 \leq d \leq 6$$
$$m = 7e + f, \;\; 0 \leq f \leq 6$$

observe que

$$n^2 = 7(7c^2) + 7(2cd) + d^2$$

assim

$$d^2 = -7(7c^2) - 7(2cd) + n^2 = -7(7c^2) - 7(2cd) + x = -7(7c^2) - 7(2cd) + 7a + b$$

$$d^2 = 7\left(a - 7c^2 - 2cd\right) + b$$

portanto b é um residuo de d^2 ao dividir por 7, mas como $0 \leq d \leq 6$, então é facil checar que os únicos residuos de d^2 ao divider por 7 são $0, 1, 2, 4$ assim

$$b \in \{0, 1, 2, 4\}$$

Similarmente temos que b também é um residuo de f^3 ao dividir por 7 e que como $0 \leq f \leq 6$ é facil checar que os únicos possiveis são $0, 1, 6$ logo

$$b \in \{0, 1, 6\}$$

Finalmente, temos que

$$b \in \{0, 1, 2, 4\} \cap \{0, 1, 6\} = \{0, 1\}.$$

10. a) Para $7 \mid 2^{3n} - 1$, não é dificil verificar o caso $n = 1$, e para o caso indutivo suponha que $2^{3k} - 1 = 7m$ para algum $m \in \mathbb{Z}$. Observe que

$$2^{3(k+1)} - 1 = 2^3 \cdot 2^{3k} - 1 = 2^3(2^{3k} - 1) + 2^3 - 1 = 2^3 \cdot 7m + 7 = 7(2^3m + 1).$$

Para $8 \mid 3^{2n} + 7$, não é dificil verificar o caso $n = 1$, e para o caso indutivo suponha que $3^{2k} + 7 = 8m$ para algum $m \in \mathbb{Z}$. Observe que

$$3^{2(k+1)} + 7 = 9(3^{2k} + 7) - 9 \cdot 7 + 7 = 9 \cdot 8m - 7 \cdot 8 = 8 \cdot (9m - 7).$$

b) Não é dificil verificar o caso $n = 1$, e para o caso indutivo suponha que $2^k + (-1)^{k+1} = 3m$ para algum $m \in \mathbb{Z}$. Observe que

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

11. Sejam $x = 2k + 1$ e $y = 2t + 1$, para alguns $k, t \in \mathbb{N}$, logo

$$x^2 + y^2 = (2k+1)^2 + (2t+1)^2 = 2(2k^2 + 2k + 2t^2 + 2t + 1)$$

assim, $2 \mid x^2 + y^2$, mas se $4 \mid x^2 + y^2$, então existe $m \in \mathbb{Z}$ tal que $x^2 + y^2 = 4m$, portanto,

$$4m = x^2 + y^2 = 2(2k^2 + 2k + 2t^2 + 2t + 1)$$

disso

$$2m = 2k^2 + 2k + 2t^2 + 2t + 1$$

$$2m = 2\left(k^2 + k + t^2 + t\right) + 1$$

o qual é absurdo, pois não existe um número que seja par e ímpar.

12. Considere $m = n + 1$ e achemos os $m \in \mathbb{Z}$ tais que $n^2 + 1 = (m-1)^2 + 1 = m^2 - 2m + 2$ é divisivel por $n + 1 = m$. Para isso, suponha que existe $k \in \mathbb{Z}$ tais que $m^2 - 2m + 2 = km$, logo

$$m(-m + 2 + k) = -m^2 + 2m + km = 2$$

o qual implica que

$$m \mid 2$$

assim

$$m = \pm 1 \text{ ou } m = \pm 2$$

Se $m = -1$, então $n = -2$ e claramente $-1 = -2 + 1$ divide $(-2)^2 + 1 = 5$.

Se $m = 1$, então $n = 0$ e claramente $1 = 0 + 1$ divide $0^2 + 1 = 1$.

Se $m = -2$, então $n = -3$ e claramente $-2 = -3 + 1$ divide $(-3)^2 + 1 = 10$.

Se $m = 2$, então $n = 1$ e claramente $2 = 1 + 1$ divide $1^2 + 1 = 2$.

Portanto,

$$n \in \{-3, -2, 0, 1\}.$$

13. Use item[9.].

Maximo divisor comum e minimo multiplo comum

1. É claro que $|a|$ divide 0 e a e se existir $d \in \mathbb{Z}$ tal que

$$d \mid a$$

então $d \mid \ |a|$.

Por outro lado, se $d \mid 1$, então $d = \pm 1$, portanto $\text{mdc}(a, 1) = 1$.

2. Seja $d = \text{mdc}(a, b)$ e $t = \text{mdc}(na, nb)$, logo exitem $x_0, y_0 \in \mathbb{Z}$ tais que

$$ax_0 + by_0 = d$$

assim

$$d \mid a \;\; e \;\; d \mid b \implies dn \mid na \;\; e \;\; dn \mid nb \implies dn \mid t$$
$$t \mid na \;\; e \;\; t \mid nb \implies t \mid nax_0 + nby_0 = nd$$

Portanto $t = nd$.

Por outro lado,

$$\text{mmc}(na, nb) = \frac{nanb}{\text{mdc}(na, nb)} = \frac{n^2ab}{\text{mdc}(a, b)n} = \frac{nab}{\text{mdc}(a, b)} = n\frac{ab}{\text{mdc}(a, b)} = \text{mmc}(a, b)n$$

3. (a) $a = 2^5$ e $b = 2 \cdot 3^3$, logo $2 = \text{mdc}(a, b)$ e portanto

$$\text{mmc}(a, b) = \frac{ab}{\text{mdc}(a, b)} = \frac{2^6 \cdot 3^3}{2} = 2^5 \cdot 3^3$$

   (b) Ver item (a).

   (c) Ver item (a).

   (d) Ver item (a).

4. (a)

$$72 = 56 + 16 \implies 72 - 56 = 16 \;\; \text{e} \;\; \text{mdc}(72, 56) = \text{mdc}(56, 16)$$
$$56 = 16 \times 3 + 8 \implies 56 = (72 - 56) \times 3 + 8 \;\; \text{e} \;\; \text{mdc}(72, 56) = \text{mdc}(56, 16) = \text{mdc}(16, 8) = 8$$

   logo

$$56 \times 4 - 72 \times 3 = 8$$

   .

   (b)

$$138 = 24 \times 5 + 18 \implies 138 - 5 \times 24 = 18 \;\; \text{e} \;\; \text{mdc}(138, 24) = \text{mdc}(24, 18)$$
$$24 = 18 + 6 \implies 24 = (138 - 5 \times 24) + 6 \;\; \text{e} \;\; \text{mdc}(138, 24) = \text{mdc}(24, 18) = \text{mdc}(18, 6) = 6$$

   logo

$$6 \times 24 - 138 = 6$$

   (c) ver itens (a) e (b)

   (d) ver itens (a) e (b)

5.

"a ⇒ b" Claramente $|a|$ divide a e b e se existir $d \in \mathbb{Z}$ talque $d \mid a$ e $d \mid b$, então d divide $|a|$.

"b ⇒ c"

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

"c ⇒ a" Como $\text{mmc}(a, b) = |b|$, então a divide $|b|$ e portanto $a \mid b$.

6. Como $\text{mdc}(2111, 5393) = 1$, assim $\text{mmc}(2111, 5393) = 2111 \cdot 5393 = 11384623$ ou seja o Sol, Mercúrio e Vênus alinham cada 11384623 horas.

7. (a) Usar dica.

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

$$d \mid 2a + b \ \text{ e } \ d \mid a + 2b$$

   isto implica

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

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

   disso

$$d \mid \text{mdc}(3a, 3b) = 3\text{mdc}(ab) = 3$$

   (c) Use a dica

8. Seja $d = \text{mdc}(a, c)$. Primeiramente, exitem $x_0, y_0 \in \mathbb{Z}$ tais que

$$bx_0 + cy_0 = 1$$

   Agora, como $d \mid a$ e $d \mid c$ e $\dfrac{b}{a} \in \mathbb{Z}$, então

$$d \mid a\left(\frac{b}{a}\right)x_0 + cy_0 = 1$$

   portanto $d = 1$.