Gabarito da primeira prova de Álgebra 1 turma B - 2017-2.

1. **Exercício 1 [4 pontos]**

   (a) (1 ponto) Encontre inteiros x, y tais que $31x + 24y = 1$.

   Aplicaremos o algoritmo de Euclides a 31 e 24.

31	24	
1	0	31
0	1	24
1	-1	7
-3	4	3
7	-9	1

   Logo $7 \cdot 31 + (-9) \cdot 24 = 1$. Temos $x = 7$ e $y = -9$.

   (b) (1 ponto) Resolva a equação $9x \equiv 3 \mod 12$.

   Dividindo por 3 obtemos $3x \equiv 1 \mod 4$ e multiplicando por 3 temos $x \equiv 3 \mod 4$ logo as soluções módulo 12 são 3, 7, 11.

   (c) (1 ponto) Resolva a equação $31x \equiv 6 \mod 24$.

   Pelo item 1 temos $31 \cdot 7 \equiv 1 \mod 24$ logo multiplicando a equação dada por 7 temos $x \equiv 6 \cdot 7 \mod 24$ ou seja $x \equiv 42 \mod 24$ ou seja $x \equiv 18 \mod 24$.

   (d) Mostre que se z é um número inteiro qualquer então existem dois inteiros a, b tais que $31a + 24b = z$.

   Sabemos pelo item (a) que $31 \cdot 7 + 24 \cdot (-9) = 1$. Multiplicando tal igualdade por z obtemos $31 \cdot 7z + 24 \cdot (-9z) = z$ logo basta escolher $a = 7z$ e $b = -9z$.

2. **Exercício 2 [1 ponto]**

   Para cada classe módulo 14 que admite inverso multiplicativo calcule o inverso multiplicativo de tal classe. Lembre-se que o inverso multiplicativo da classe $\overline{x}$ é uma classe $\overline{y}$ tal que $\overline{x} \cdot \overline{y} = \overline{1}$, ou seja $xy \equiv 1 \mod 14$.

   $\mathbb{Z}/14\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}\}$. As classes que admitem inverso são as classes $\overline{a}$ com a coprimo com 14 ou seja $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{9}$, $\overline{11}$, $\overline{13}$. O inverso de $\overline{1}$ é $\overline{1}$ e o inverso de $\overline{13}$ é $\overline{13}$ (sendo $\overline{13} = \overline{-1}$). Como $3 \cdot 5 \equiv 1$

mod 14 e $9 \cdot 11 \equiv 1 \mod 14$ temos que o inverso de $\overline{3}$ é $\overline{5}$, o inverso de $\overline{5}$ é $\overline{3}$, o inverso de $\overline{9}$ é $\overline{11}$ e o inverso de $\overline{11}$ é $\overline{9}$.

3. **Exercício 3 [3 pontos]**

   Seja $f : \mathbb{Z} \to \mathbb{Z}$ uma função, onde $\mathbb{Z}$ é o conjunto dos números inteiros.

   Defina uma operação de $\mathbb{Z}$ por

   $$x * y := f(x)f(y).$$

   (a) (1 ponto) Mostre que $*$ é uma operação comutativa.

   Como a multiplicação em $\mathbb{Z}$ é comutativa temos

   $$x * y = f(x)f(y) = f(y)f(x) = y * x.$$

   (b) Suponha que exista um elemento neutro $e \in \mathbb{Z}$, ou seja

   $$x * e = x = e * x$$

   para todo $x \in \mathbb{Z}$.

   i. (1 ponto) Mostre que f é injetiva.

   Suponha $f(a) = f(b)$, queremos mostrar que $a = b$. Temos

   $$a = a * e = f(a)f(e) = f(b)f(e) = b * e = b.$$

   ii. (1 ponto) Mostre que f é sobrejetiva.

   Seja $z \in \mathbb{Z}$, queremos encontrar $x \in \mathbb{Z}$ com $f(x) = z$. Temos $1 = 1 * e = f(1)f(e)$ e isso implica que $f(e) = \pm 1$ (sendo um inteiro). Se $f(e) = 1$ então temos $z = z * e = f(z)f(e) = f(z)$ logo $f(z) = z$ e podemos escolher $x = z$. Se $f(e) = -1$ então temos $-z = -z * e = f(-z)f(e) = -f(-z)$ logo $f(-z) = z$ e podemos escolher $x = -z$.

   Observe que o argumento acima mostra que se $*$ tem um elemento neutro então tem apenas duas possibilidades para f, que são $f(x) = x$ para todo x e $f(x) = -x$ para todo x.

4. **Exercício 4 [2 pontos]**

   Sejam A, B, C conjuntos. Lembre-se que $A - B = \{a \in A \ : \ a \notin B\}$. Mostre que

   $$A - (B - C) = (A - B) \cup (A \cap C).$$

   Cada inclusão vale um ponto.

Mostraremos a primeira inclusão, $A - (B - C) \subseteq (A - B) \cup (A \cap C)$. Se $x \in A - (B - C)$ temos $x \in A$ e $x \notin B - C$. Sendo $x \notin B - C$ tem dois casos: $x \notin B$ e $x \in B \cap C$. No primeiro caso $x \in A - B$ logo $x \in (A - B) \cup (A \cap C)$. No segundo caso $x \in A \cap C$ logo $x \in (A - B) \cup (A \cap C)$.

Mostraremos a segunda inclusão, $(A - B) \cup (A \cap C) \subseteq A - (B - C)$. Se $x \in (A - B) \cup (A \cap C)$ tem dois casos, $x \in A - B$ e $x \in A \cap C$. No primeiro caso $x \in A$ e $x \notin B$, logo $x \notin B - C$ logo $x \in A - (B - C)$. No segundo caso $x \in A$ e $x \in C$, logo $x \notin B - C$ logo $x \in A - (B - C)$.