`Entregar para a monitora as soluções de 8 problemas a sua escolha.`

Problema 1. Prove que a soma de três números inteiros consecutivos é divisível por 3.

Problema 2. Mostre que o produto de quatro números inteiros consecutivos mais 1 é um quadrado perfeito.

Problema 3. Prove que para todo inteiro n, $n^3 - n$ é divisível por 6.

Problema 4. Mostre que se a soma dos dígitos de um número inteiro n é divisível por 3, então n também é divisível por 3.

Problema 5. Prove que todo número primo, com exceção do 2 e do 3, pode ser escrito na forma $6k + 1$ ou $6k + 5$, onde k é um número inteiro.

Problema 6. Para cada um dos pares de números abaixo a e b, calcule o máximo divisor comum $d = \text{mdc}(a, b)$ e determine inteiros x e y tais que $ax + by = d$.

(a) $a = 56$, $b = 15$

(b) $a = 345$, $b = 299$

(c) $a = 101$, $b = -23$

(d) $a = 1001$, $b = 77$

(e) $a = -34$, $b = 432$

(f) $a = 1422$, $b = 342$

(g) $a = 7919$, $b = 787$

(h) $a = 636$, $b = 96$

(i) $a = 462$, $b = 1071$

Problema 7. Seja a um inteiro. Prove que $2a + 1$ e $4a^2 + 1$ são primos entre si.

Problema 8. Prove que se a e b são números inteiros primos entre si, então $a + b$ e $a - b$ são primos entre si.

Problema 9. Prove que se a e b são números inteiros tais que $a + b$ e $a - b$ são primos entre si se, então $a^2 - b^2$ e ab são primos entre si.

Problema 10. Mostre que se a, b e c são números inteiros positivos tais que $\text{mdc}(a, b) = 1$ e $a|bc$, então $a|c$.

Problema 11. Prove que se a e b são números inteiros, então 2^a e $2^b - 1$ são primos entre si.

Problema 12. Prove que se a e b são números inteiros tais que $3a + 5b$ é divisível por 7, então a e b são primos entre si.

Problema 13. Sejam a e b elementos de $\mathbb{Z}_p$, com p primo. Prove que se $a \otimes b = 0$, então $a = 0$ ou $b = 0$.

Problema 14. Um número inteiro n é chamado de *número perfeito* se ele é igual à soma de seus divisores positivos próprios (excluindo ele mesmo). Por exemplo, 6 é um número perfeito, pois seus divisores próprios são 1, 2 e 3, e $1 + 2 + 3 = 6$. Prove que se $2^a - 1$ é um número primo, então $n = 2^{a-1}(2^a - 1)$ é um número perfeito.

Problema 15. Recorde que $\varphi(n)$ é a função totiente de Euler, que conta o número de inteiros positivos menores ou iguais a n que são primos com n. Prove que se p é um número primo e k é um inteiro positivo, então $\varphi(p^k) = p^k - p^{k-1}$.

Problema 16. Seja $(G, *)$ um grupo. O centro de G, denotado por $Z(G)$, é o conjunto de todos os elementos de G que comutam com todos os outros elementos de G; ou seja,

$$Z(G) = \{z \in G \mid z * g = g * z \text{ para todo } g \in G\}.$$

Prove que $Z(G)$ é um subgrupo de G.

Problema 17. Prove que o centro do grupo $(S_n, \circ)$ é trivial para $n \geq 3$, ou seja, $Z(S_n) = \{\iota\}$, onde ι é a permutação identidade.

Problema 18. Prove que se $(G, \circ)$ é um grupo finito de ordem par, então existe pelo menos um elemento $g \in G \setminus \{e\}$ tal que $g^2 = e$, onde e é o elemento identidade de G.

Problema 19. Seja G um grupo abeliano finito. Prove que o conjunto dos elementos de ordem 2 em G forma um subgrupo de G.

Problema 20. Prove que se G é um grupo finito de ordem n, então para qualquer elemento $g \in G$, $g^n = e$, onde e é o elemento identidade de G. Ademais, mostre que a ordem de qualquer elemento g divide n.

Problema 21. Dados dois subgrupos H e K de um grupo G, prove que a interseção $H \cap K$ também é um subgrupo de G.

Problema 22. Dados dois grupos $(G_1, *_1)$ e $(G_2, *_2)$, considere o produto cartesiano $G = G_1 \times G_2$ equipado com a operação $*$ definida por $(g_1, g_2) * (h_1, h_2) = (g_1 *_2 h_1, g_2 *_2 h_2)$. Mostre que $(G, *)$ é um grupo.

Problema 23. Considere o grupo $(\mathbb{Z}_2^3, +)$, onde $+$ é a adição componente a componente módulo 2. Liste todos os subgrupos deste grupo.

Problema 24. Mostre que todo grupo com 5 elementos é isomorfo ao grupo $(\mathbb{Z}_5, +)$.

Problema 25. Prove que todo grupo com 6 elementos é isomorfo ao grupo $(\mathbb{Z}_6, +)$ ou ao grupo $(S_3, \circ)$.

Problema 26. Seja p um número primo. Mostre que se $x^2 \equiv x \pmod{p}$, então $x \equiv 0 \pmod{p}$ ou $x \equiv 1 \pmod{p}$.

Problema 27. Seja p um número primo. Mostre que se $x^2 \equiv 1 \pmod{p}$, então $x \equiv 1 \pmod{p}$ ou $x \equiv -1 \pmod{p}$.

Problema 28. Seja p um número primo. Mostre que $(p-1)! \equiv -1 \pmod{p}$. (Dica: Use o exercício anterior para argumentar que os elementos de $\mathbb{Z}_p^*$ podem ser agrupados em pares de inversos, exceto pelos elementos 1 e $p-1$.)