Matemática Finita | 21082

Proposta de Resolução Sumária

Grelha de correção das respostas de escolha múltipla:

1.	2.	3.
A)	C)	B)

4. Com vista a um absurdo, suponhamos que p não é um número primo. Logo, existem $n_1 \neq 1$, $n_2 \neq 1$, $n_1, n_2 \in \mathbb{N}$ tais que $p = n_1 n_2$. Sendo, em particular, n_1 e n_2 divisores de p, então $n_1, n_2 \notin \left[2, \sqrt{p}\right]$. Excluídos os casos $n_i = 0, 1$, $i = 1, 2$[1], isto significa que $n_1 > \sqrt{p}$ e $n_2 > \sqrt{p}$. Mas isto conduz a $p = n_1 n_2 > \sqrt{p}\sqrt{p} = p$, o que é um absurdo.

Como o absurdo resultou da hipótese de p não ser um número primo, conclui-se então que p é primo.

5. Suponhamos que $m \in \mathbb{N}$. Pelo Exercício 9.3 da Atividade Formativa 2, p é um divisor de $m^p - m = m(m^{p-1} - 1)$. Observe-se que por p ser um número primo, $p \geq 2$ e, por conseguinte, $m^{p-1} - 1 \in \mathbb{Z}$. Assim, atendendo a que $p \nmid m$, resulta do Lema 1.11 (alínea 1) e da Proposição 1.9 que

$$p \,|\, m(m^{p-1} - 1) \implies p \,|\, (m^{p-1} - 1).$$

Suponhamos agora que $m \in \mathbb{Z} \setminus \mathbb{N}$. Com exceção do caso $p = 2$, qualquer número primo $p > 2$ é ímpar e, portanto, $p - 1$ é par. Isto significa que

$$m^{p-1} = (-|m|)^{p-1} = (-1)^{p-1}|m|^{p-1} = |m|^{p-1},$$

com $|m| \in \mathbb{N}$, decorrendo então da primeira parte que p é um divisor de $|m|^{p-1} - 1 = m^{p-1} - 1$.

Se $p = 2$, então a hipótese $p \nmid m$ significa que $|m|$ é um número ímpar. Logo $|m| - 1$ é par e, consequentemente, $p \,|\, (|m| - 1)$.

[1] Note-se que, por hipótese, $p > 4$, pelo que $n_1 \neq 0$ e $n_2 \neq 0$.

6. Comece-se por observar que a existir um $k \in \mathbb{Z}$ tal que 41 é um divisor de $k^5 - 2$, tal k não pode ser um múltiplo de 41. Com efeito, se tal acontecesse, então 41 seria simultaneamente um divisor de k^5 e de $k^5 - 2$, o que, pela alínea (i) do Lema 1.1, significaria que 41 seria um divisor de $k^5 - (k^5 - 2) = 2$.

Com vista a um absurdo, suponhamos então que existe um $k \in \mathbb{Z}$ tal que $k^5 - 2$ é divisível por 41 e $41 \not| k$. Equivalentemente,

$$k^5 \equiv 2 \,(\mathrm{mod}\, 41).$$

Como 41 é um número primo e $41 \not| k$, resulta do exercício anterior que

$$k^{41-1} \equiv 1 \,(\mathrm{mod}\, 41).$$

Mas, pela parte final da alínea 5 da Proposição 1.24,

$$k^5 \equiv 2 \,(\mathrm{mod}\, 41) \implies k^{40} \equiv 2^8 \,(\mathrm{mod}\, 41)$$

Logo, por simetria e por transitividade (Proposição 1.24 alíneas 2 e 3),

$$k^{40} \equiv 1 \,(\mathrm{mod}\, 41),\ k^{40} \equiv 2^8 \,(\mathrm{mod}\, 41) \implies 2^8 \equiv 1 \,(\mathrm{mod}\, 41),$$

o que é um absurdo, pois 41 não é um divisor de $2^8 - 1$.

Conclusão: 41 não é divisor de nenhum número da forma $k^5 - 2$, $k \in \mathbb{Z}$.

7.1. Se p for um divisor de $u \in \mathbb{Z}$, então p é divisor de u^k e de u^m para quaisquer $k, m \in \mathbb{N}$, $k \neq 0 \neq m$. Ou seja,

$$u^k \equiv u^m \,(\mathrm{mod}\, p).$$

Suponhamos que p não é um divisor de $u \in \mathbb{Z}$. Logo, pelo Exercício 5,

$$u^{p-1} \equiv 1 \,(\mathrm{mod}\, p). \tag{1}$$

Dados k, m nas condições do enunciado, suponhamos que $k > m$. Da relação $k \equiv m \,(\mathrm{mod}\,(p-1))$ resulta então que

$$\exists\, a \in \mathbb{N} :\ k - m = a(p-1),$$

o que, por (1) e pela Proposição 1.24, parte final da alínea 5, implica que $u^{a(p-1)} \equiv 1 \,(\mathrm{mod}\, p)$. Por conseguinte, pelas alíneas 1 e 5 da Proposição 1.24,

$$u^k = u^{a(p-1)} u^m \equiv u^m \,(\mathrm{mod}\, p).$$

7.2. Novamente pela parte final da alínea 5 da Proposição 1.24 tem-se $u^m \equiv v^m \,(\mathrm{mod}\, p)$. Como $u^k \equiv u^m \,(\mathrm{mod}\, p)$ (cf. alínea anterior), por transitividade (Proposição 1.24 alínea 3) resulta então que

$$u^k \equiv v^m \,(\mathrm{mod}\, p).$$