Correcção Sumária

Grelha de correcção das respostas de escolha múltipla:

1.	2.	3.
a)	d)	c)

4. Comece-se que por notar que por $a \,|\, b$, $\frac{b}{a} \in \mathbb{Z}$, pelo que o problema está bem posto.

Uma vez que $p \,|\, b$, tem-se que $b = kp$ para um certo $k \in \mathbb{Z}$. Por outro lado, sendo p um número primo e $p \not| \, a$, $\text{mdc}(p, a) = 1$. Assim sendo, resulta da Proposição 1.9 do Texto sobre Divisibilidade que

$$a \,|\, b \ \wedge \ b = kp \implies a \,|\, k.$$

Tem-se então

$$\frac{b}{a} = \frac{k}{a} p$$

com $\frac{k}{a} \in \mathbb{Z}$, o que prova que $p \,|\, \frac{b}{a}$.

5.

5.1. Uma vez que por definição de máximo divisor comum tem-se que $\text{mdc}(a/2, b) \,|\, (a/2)$ e, naturalmente, $(a/2) \,|\, a$, resulta por transitividade que $\text{mdc}(a/2, b) \,|\, a$. Isto prova que $\text{mdc}(a/2, b)$ é um divisor comum a a e a b. Logo, resulta da definição de $\text{mdc}(a, b)$ que

$$\text{mdc}(a/2, b) \leq \text{mdc}(a, b). \tag{1}$$

Reciprocamente, uma vez que $\text{mdc}(a, b) \,|\, b$ em que b é um número ímpar, tem-se que $\text{mdc}(a, b)$ é um número ímpar. Logo, $2 \not| \, \text{mdc}(a, b)$, pelo que 2 e $\text{mdc}(a, b)$ são números primos entre si. Tal como na questão 4, resulta então que

$$\text{mdc}(a, b) \,|\, a \ \wedge \ a = 2\frac{a}{2} \implies \text{mdc}(a, b) \,|\, (a/2).$$

Consequentemente, $\text{mdc}(a, b)$ é um divisor comum a $a/2$ e a b, o que conduz pela definição de $\text{mdc}(a/2, b)$ à desigualdade

$$\text{mdc}(a, b) \leq \text{mdc}(a/2, b). \tag{2}$$

A igualdade pretendida deriva então de (1) e de (2).

5.2. Em termos de factorização em números primos, tem-se que $\text{mdc}(a^k, b^k)$ é igual ao produto dos factores comuns, cada um elevado ao menor expoente. Se a factorização em números primos de a^k e de b^k não têm factores comuns, então a factorização em números primos de a e de b também não têm factores comuns. Logo, $\text{mdc}(a, b) = 1$. (Note que se $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ para $p_1, \dots, p_r$ números primos, então $a^k = p_1^{k\alpha_1} \dots p_r^{k\alpha_r}$, sendo esta factorização de a^k em números primos única - Teorema Fundamental da Aritmética.)

6.

6.1. **Case Base: $\mathbf{n = 0}$**. Este caso é imediato, pois qualquer número não nulo divide o 0.

Hipótese de indução: Dado $n \in \mathbb{N}$, **qualquer**, suponhamos que

$$p \,|\, (n^p - n).$$

Tese de indução:

$$p \,|\, ((n+1)^p - (n+1)).$$

Pelo Binómio de Newton tem-se

$$\begin{aligned}(n+1)^p - (n+1) &= \sum_{k=0}^{p} \binom{p}{k} n^{p-k} - (n+1) \\ &= n^p + \binom{p}{1} n^{p-1} + \ldots + \binom{p}{p-1} n + 1 - (n+1) \\ &= (n^p - n) + \binom{p}{1} n^{p-1} + \ldots + \binom{p}{p-1} n,\end{aligned}$$

em que, pela hipótese de indução, $n^p - n$ é divisível por p, enquanto que os restantes termos são divisíveis por p pelo Exercício 9.1 da Actividade Formativa 2. Deste modo prova-se que p é divisor de $(n+1)^p - (n+1)$.

Pelo método de indução matemática, fica assim provado que

$$p \,|\, (n^p - n), \quad \forall\, n \in \mathbb{N}.$$

6.2. Se p não for primo, o resultado não é verdadeiro. Por exemplo, para $p = 4$, tem-se que p não é um divisor de $2^p - 2 = 14$.

7.

7.1. Tome-se, por exemplo, $a = 5, b = 2, k = 2$ e $n = 6$. Tem-se $2 \cdot 5 \equiv 2 \cdot 2 \,(\mathrm{mod}\, 6)$, mas $5 \not\equiv 2 \,(\mathrm{mod}\, 6)$.

7.2. Por exemplo, para $a = 2, b = 1, k = 3$ e $n = 7$, tem-se $2^3 \equiv 1^3 \,(\mathrm{mod}\, 7)$, mas $2 \not\equiv 1 \,(\mathrm{mod}\, 7)$.

Este exercício mostra que o recíproco das implicações estabelecidas no final das alíneas 4 e 5 da Proposição 1.24 do Texto sobre Congruências são ambos falsos.