Correcção Sumária

Grelha de correcção das respostas de escolha múltipla:

1.	2.	3.
d)	d)	b)

4. Se $a \mid m$ e $b \mid m$, então e por definição de divisor, existem $k, l \in \mathbb{Z}$ tais que

$$m = ka, \quad m = lb.$$

Consequentemente, $ka = m = lb$. Isto implica, por transitividade,

$$b \mid (lb) \wedge (lb) \mid (ka) \implies b \mid (ka). \tag{1}$$

Mas, por hipótese, a e b são primos entre si. Logo, pela Proposição 1.9 do texto sobre Divisibilidade, resulta de (1) que

$$b \mid k,$$

ou seja, $k = rb$ para um certo $r \in \mathbb{Z}$. Assim sendo, tem-se

$$m = ka = (rb)a = r(ab),$$

o que prova que $(ab) \mid m$.

5.

5.1.1. Case Base: n = 0. Como $13 \mid (4 - (-9))$, tem-se, equivalentemente,

$$4^{0+1} \equiv -3^{0+2} \pmod{13},$$

o que prova o caso base.

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

$$4^{2n+1} \equiv -3^{n+2} \pmod{13}.$$

Tese de indução: $4^{2n+3} \equiv -3^{n+3} \pmod{13}$.

Atendendo à hipótese de indução, tem-se

$$4^{2n+1} \equiv -3^{n+2} \pmod{13}.$$

Por outro lado,

$$4^2 = 16 \equiv 3 \pmod{13}.$$

Logo, pela compatibilidade das congruências com o produto (Proposição 1.24 alínea 5 do texto sobre Congruências),

$$4^{2n+1} \cdot 4^2 \equiv -3^{n+2} \cdot 3 \pmod{13},$$

o que é equivalente ao pretendido:

$$4^{2n+3} \equiv -3^{n+3} \pmod{13}.$$

Pelo método de indução matemática, podemos assim concluir que para qualquer $n \in \mathbb{N}$ tem-se $4^{2n+1} \equiv -3^{n+2} \pmod{13}$.

5.1.2. De acordo com o Exercício 3 da Actividade Formativa 2 (ver resolução),

$$13\,|(16^n-3^n),\quad n\in\mathbb{N}.$$

Por linearidade (Lema 1.1 Propriedade (i) do texto sobre Divisibilidade), tem-se então

$$\left.\begin{array}{l} 13\,|(16^n-3^n) \\ \\ 13\,|\,13 \end{array}\right\} \implies 13\,|\,\underbrace{(4(16^n-3^n)+13\cdot 3^n)}_{=4^{2n+1}+3^{n+2}},$$

o que, equivalentemente, traduz-se por $4^{2n+1}\equiv -3^{n+2}\,(\mathrm{mod}\,13)$.

5.2. De acordo com o Lema 1.11 alínea 2 do texto sobre Divisibilidade,

$$\mathrm{mdc}(4^{2n+1}+3^{n+2},3^{n+2})=\mathrm{mdc}((4^{2n+1}+3^{n+2})-3^{n+2},3^{n+2})=\mathrm{mdc}(2^{4n+2},3^{n+2}).$$

Uma vez que 2 e 3 são números primos, 2^{4n+2} e 3^{n+2} são duas factorizações em números primos. Logo, tal como no Exercício 7 da Actividade Formativa 2 resulta que

$$\mathrm{mdc}(2^{4n+2},3^{n+2})=1.$$

6.

6.1. De modo equivalente, pretende-se provar que

$$p\,|\binom{p}{k},\quad k=1,2,\ldots,p-1.$$

Ora, para qualquer $k=1,2,\ldots,p-1$ tem-se que

$$p!=\binom{p}{k}(p-k)!k!$$

Como $p!=p(p-1)!$, $(p-1)!\in\mathbb{N}$, tem-se então $p\,|\,p!$ e, portanto,

$$p\,|\binom{p}{k}(p-k)!k! \tag{2}$$

O resto do exercício resume-se a provar que

$$p\not|\,(p-k)!k!,\quad k=1,2,\ldots,p-1. \tag{3}$$

Com efeito, provado (3), resulta do facto de p ser primo e do Lema 1.11 alínea 1 do texto sobre Divisibilidade que $\mathrm{mdc}(p,(p-k)!k!)=1$ e, portanto, por (2) e pela Proposição 1.9 do mesmo texto, $p\,|\,\binom{p}{k}$, $k=1,2,\ldots,p-1$.
Para provar (3) comece-se por notar que

$$k\equiv -(p-k)\,(\mathrm{mod}\,p)$$

ou, mais geralmente,

$$k-i\equiv -(p-k+i)\,(\mathrm{mod}\,p),\quad i=0,1,\ldots,k-1.$$

Assim sendo,

$$\begin{aligned} k!(p-k)! &\equiv (-1)^k(p-k)\underbrace{(p-k+1)\ldots(p-2)(p-1)(p-k)!}_{=(p-1)(p-2)\ldots(p-k+1)(p-k)!=(p-1)!}\,(\mathrm{mod}\,p)\\ &\equiv (-1)^k(p-k)(p-1)!\,(\mathrm{mod}\,p), \end{aligned}$$

onde, pelo Teorema 1.34 (Wilson),

$$(p-1)! \equiv -1 \,(\mathrm{mod}\, p)$$

por p ser primo. Consequentemente,

$$k!(p-k)! \equiv (-1)^{k+1}(p-k) \,(\mathrm{mod}\, p),$$

em que por $k = 1, 2, \ldots, p-1$ (ou seja, por $k \neq 0$, $k \neq p$), $(p-k) \not\equiv 0 \,(\mathrm{mod}\, p)$. Logo, $k!(p-k)! \not\equiv 0 \,(\mathrm{mod}\, p)$, o que equivale a (3).

6.2. Atendendo ao Binómio de Newton,

$$(1+m)^p = \sum_{k=0}^{p} \binom{p}{k} m^k = 1 + m^p + \sum_{k=1}^{p-1} \binom{p}{k}.$$

Mas, pela alínea anterior,

$$\binom{p}{k} \equiv 0 \,(\mathrm{mod}\, p),\ k = 1, \ldots, p-1 \implies \sum_{k=1}^{p-1} \binom{p}{k} \equiv 0 \,(\mathrm{mod}\, p).$$

Logo, pela reflexividade e pela compatibilidade das congruências com a soma (Proposição 1.24),

$$\underbrace{1 + m^p + \sum_{k=1}^{p-1} \binom{p}{k}}_{=(1+m)^p} \equiv 1 + m^p \,(\mathrm{mod}\, p).$$