Matemática Finita | 21082

Proposta de Resolução Sumária

Grelha de correção das respostas de escolha múltipla:

1.	2.	3.
C)	D)	D)

4.1. Suponhamos que $a, b \geq 2$. Sendo a, b dois números primos entre si, em termos de fatorização em números primos isto significa que a fatorização de cada um deles é da forma

$$a = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}, \quad b = q_1^{s_1} q_2^{s_2} \cdots q_m^{s_m},$$

onde $r_1, r_2, \cdots, r_n, s_1, s_2, \ldots, s_m$ são números inteiros positivos e $p_1, p_2, \ldots, p_n, q_1, q_2, \cdots, q_m$ são números primos todos distintos entre si. Como

$$a^k = p_1^{kr_1} p_2^{kr_2} \cdots p_n^{kr_n},$$

continuam a não existir números primos comuns à fatorização de a^k e de b, pelo que $\mathrm{mdc}(a^k, b) = 1$.

Se a ou b não forem maiores ou iguais a 2, cinco casos podem acontecer:

- $a = 0$ e $b \geq 1$: Nesta situação tem-se $\mathrm{mdc}(a^k, b) = \mathrm{mdc}(0, b) = b$ e $\mathrm{mdc}(a, b) = \mathrm{mdc}(0, b) = b$, pelo que se a e b forem números primos entre si, então a^k e b também são números primos entre si.
- $a \geq 1$ e $b = 0$: Neste caso tem-se $\mathrm{mdc}(a^k, b) = \mathrm{mdc}(a^k, 0) = a^k$ e $\mathrm{mdc}(a, b) = \mathrm{mdc}(a, 0) = a$, donde se a e b forem números primos entre si, então a^k e b também são números primos entre si.
- $a = 1$ e $b \geq 1$: Nesta situação $a^k = a$ e, por conseguinte, $\mathrm{mdc}(a^k, b) = \mathrm{mdc}(a, b) = \mathrm{mdc}(1, b) = 1$.
- $a \geq 1$ e $b = 1$: Neste caso $\mathrm{mdc}(a^k, 1) = 1 = \mathrm{mdc}(a, 1)$.

- $a < 0$ ou $b < 0$: O resultado segue dos casos anteriores, já que por definição de máximo divisor comum $\mathrm{mdc}(a, b) = \mathrm{mdc}(|a|, |b|)$ e $\mathrm{mdc}(a^k, b) = \mathrm{mdc}(|a|^k, |b|)$.

4.2. **Caso base:** $n = 1$. Provado na alínea 4.1.

Hipótese de indução: Escolhido e fixado um $1 \leq n \in \mathbb{N}$ arbitrário, suponhamos que $\mathrm{mdc}(a^k, b^n) = 1$.

Tese de indução: $\mathrm{mdc}(a^k, b^{n+1}) = 1$ (para o mesmo n fixado na hipótese de indução).

Passo de indução: Como $\mathrm{mdc}(a, b) = 1$, da alínea 4.1 resulta que $\mathrm{mdc}(a^k, b) = 1$. Pela hipótese de indução e por aplicação do Corolário 1.20 conclui-se então que

$$\mathrm{mdc}(a^k, b) = 1 \wedge \mathrm{mdc}(a^k, b^n) = 1 \implies \mathrm{mdc}(a^k, b^{n+1}) = 1.$$

Pelo princípio da indução matemática conclui-se que $\mathrm{mdc}(a^k, b^n) = 1$ para qualquer número natural $n > 0$.

4.3. Como $2006 = 2 \times 1003$, resulta da alínea 2 do Lema 1.11 que

$$\begin{aligned}
&\mathrm{mdc}((-9581)^{123} + (2006)^{12}, (1003)^{12}) \\
&= \mathrm{mdc}((-9581)^{123} + 2^{12} \times (1003)^{12}, (1003)^{12}) \\
&= \mathrm{mdc}((-9581)^{123}, (1003)^{12}),
\end{aligned}$$

em que, por definição de máximo divisor comum,

$$\begin{aligned}
\mathrm{mdc}((-9581)^{123}, (1003)^{12}) &= \mathrm{mdc}(-(9581)^{123}, (1003)^{12}) \\
&= \mathrm{mdc}((9581)^{123}, (1003)^{12}).
\end{aligned}$$

De seguida, calculemos $\mathrm{mdc}(9581, 1003)$. Por sucessivas aplicações do algoritmo de Euclides (Lema 1.4), tem-se

- $9581 = 1003 \times 9 + 554 \implies \mathrm{mdc}(9581, 1003) = \mathrm{mdc}(1003, 554)$
- $1003 = 554 \times 1 + 449 \implies \mathrm{mdc}(1003, 554) = \mathrm{mdc}(554, 449)$
- $554 = 449 \times 1 + 105 \implies \mathrm{mdc}(554, 449) = \mathrm{mdc}(449, 105)$
- $449 = 105 \times 4 + 29 \implies \mathrm{mdc}(449, 105) = \mathrm{mdc}(105, 29)$
- $105 = 29 \times 3 + 18 \implies \mathrm{mdc}(105, 29) = \mathrm{mdc}(29, 18)$

Como 29 é um número primo e $18 < 29$ (pelo que 29 não é divisor de 18), conclui-se pelo Lema 1.11, alínea 1, que

$$\mathrm{mdc}(9581, 1003) = \mathrm{mdc}(29, 18) = 1.$$

Consequentemente e pelo exercício anterior,

$$\mathrm{mdc}(9581, 1003) = 1 \implies \mathrm{mdc}((9581)^{123}, (1003)^{12}) = 1,$$

donde

$$\mathrm{mdc}((-9581)^{123} + (2006)^{12}, (1003)^{12}) = \mathrm{mdc}((9581)^{123}, (1003)^{12}) = 1.$$

5. Suponhamos que $a \equiv b \pmod{M}$, ou seja, $M \mid (a - b)$. Como $M = \mathrm{mmc}(n, m)$, tem-se que $n \mid M$ e $m \mid M$, donde, por transitividade (Lema 1.1), n e m são divisores de $a - b$, ou seja,

$$a \equiv b \pmod{n} \wedge a \equiv b \pmod{m}.$$

Reciprocamente, suponhamos que $a \equiv b \pmod{n}$ e que $a \equiv b \pmod{m}$, ou seja, $n \mid (a - b)$ e $m \mid (a - b)$. Seja $k = \mathrm{mdc}(M, a - b)$. Tem-se

$$n \mid (a - b) \wedge n \mid M \implies n \mid \underbrace{\mathrm{mdc}(M, a - b)}_{=k}$$

e, de modo semelhante,

$$m \mid (a - b) \wedge m \mid M \implies m \mid \underbrace{\mathrm{mdc}(M, a - b)}_{=k},$$

pelo que k é múltiplo de n e de m. Donde e por definição de mínimo múltiplo comum, $M = \mathrm{mmc}(n, m) \leq k$. Se $M \leq k = \mathrm{mdc}(M, a - b)$, então $M = \mathrm{mdc}(M, a - b)$, significando que M é divisor de $a - b$.