Teoria Aritmética dos Números – Prova I

Critérios para avaliação: Clareza, corretude, rigor, e concisão (i) A redação das respostas deve ser clara. (ii) Todo o raciocínio desenvolvido na resposta deve estar correto. (iii) O nível de rigor nas respostas deve ser próximo ao usado na bibliografia básica. (iv) As respostas não devem ser mais longas que o necessário.

Atenção: não há uma pontuação "por questão". A nota da prova pretende aferir a compreensão, de forma ampla, do conteúdo.

Faça:

- duas questões dentre (1-4)
- uma questão dentre (5-7)
- uma questão dentre (8-9)

Ex. 1 — Prove que para todo n, $9 \mid (10^n - 1)$.
Comentário:

$$\begin{aligned} 10 &\equiv 1 \pmod 9 \\ 10^n &\equiv 1^n \pmod 9 \\ 9 &\mid (10^n - 1) \end{aligned}$$

Ex. 2 — Prove que $\operatorname{mdc}(a, 2+a)$ sempre é 1 ou 2, para todo inteiro a.
Comentário:
Usando o algoritmo de Euclides, se a é par:

$$\begin{aligned} 2 + a &= 1(a) + 2 \\ a &= k(2) + 0 \end{aligned}$$

Portanto $\operatorname{mdc}(a, 2+a) = 2$
Se a é ímpar,

$$\begin{aligned} 2 + a &= 1(a) + 2 \\ a &= k(2) + 1 \\ 2 &= 2(1) + 0 \end{aligned}$$

e $\operatorname{mdc}(a, 2a) = 1$.

Ex. 3 — Prove que $\mathrm{mdc}(a+b, a-b) \geq \mathrm{mdc}(a, b)$.
Comentário:
Sejam $d = \mathrm{mdc}(a, b)$ e $D = \mathrm{mdc}(a+b, a-b)$. Então

$$\begin{aligned} d &\mid a+b \\ d &\mid a-b, \end{aligned}$$

porque d divide tanto a como b.
Agora, d não pode ser maior que D, porque D é o *maior* divisor de $a+b$ e $a-b$. Logo, $d \leq D$.

Ex. 4 — Resolva a equação Diofantina $44x + 713y = 13$
Comentário:
44 e 713 são co-primos, logo $\mathrm{mdc}(44, 713) \mid 13$.
Resolvemos $44r + 713s = 1$:

$$\begin{aligned} 713 &= 16(44) + 9 \\ 44 &= 4(9) + 8 \\ 9 &= 1(8) + 1 \end{aligned}$$

$$\begin{aligned} 1 &= 9 - 1(8) \\ &= 713 - 16(44) - 1(44 - 4(9)) \\ &= 713 - 16(44) - 44 + 4(713 - 16(44)) \\ &= 5(713) - 81(44) \end{aligned}$$

Assim,

$$\begin{aligned} 5(713) - 81(44) &= 1 \\ (13 \cdot 5)(713) - (13 \cdot 81)(44) &= 13 && (\times 13) \\ 65(713) - 1053(44) &= 13 \end{aligned}$$

Ex. 5 — Mostre que $2^{67} + 3^{34}$ é múltiplo de 17. (Dica: Teorema de Fermat)
Comentário:
Pelo Teorema de Fermat, $a^{16} \equiv 1 \pmod 1)7$.

$$\begin{aligned} 2^{67} + 3^{34} &\equiv 2^{16(4)}2^3 + 3^{16(2)}3^2 && \pmod{17} \\ &\equiv 8 + 9 && \pmod{17} \\ &\equiv 17 && \pmod{17} \\ &\equiv 0 && \pmod{17} \end{aligned}$$

Ex. 6 — Quando é o resto da divisão de $(2016! - 2015!)$ por 2017? (Fato relevante: 2017 é primo)
Comentário: Usamos:

- Teorema de Wilson: $2016! \equiv -1 \pmod{2017}$.
- $2016! = (2015!)(2016)$, logo $2015! \equiv (2016!)(2016^{-1}) \pmod{2017}$.
- Como $2017 \equiv 0 \pmod{2017}$, então $2017 - 1 \equiv -1 \pmod{2017}$, logo $2016 \equiv -1 \pmod{2017}$.

$$\begin{aligned}
2016! - 2015! &\equiv (-1) - 2015! && \pmod{2017} \\
&\equiv -1 - \left[(2016!)(2016^{-1}\right] && \pmod{2017} \\
&\equiv -1 - \left[(-1)(2016^{-1})\right] && \pmod{2017} \\
&\equiv -1 - (-1)(2016) && \pmod{2017} && (2016 \equiv -1 \pmod{2017}) \\
&\equiv -1 + 2016 && \pmod{2017} \\
&\equiv 2015 && \pmod{2017}
\end{aligned}$$

Ex. 7 — Prove que $18! \equiv -1 \pmod{437}$. (Dica: $437 = (19)(23)$)
Comentário:

$$\begin{aligned}
18! &\equiv -1 \pmod{19} \\
&\equiv -1 \pmod{(19)(23)}
\end{aligned}$$

Ex. 8 — Diga se a afirmação é verdadeira ou falsa. Se for verdadeira, justifique. Se for falsa, mostre um contra-exemplo. “Se $x \in \mathbb{Z}$ é maior que zero e $4x \equiv 2 \pmod{5}$, então x não pode ser quadrado perfeito. (Dica, para começar: se x é quadrado perfeito, $x = y^2$, quais restos y pode deixar quando dividido por 5? E o que se pode concluir a respeito de x?)
Comentário:
Um número pode deixar restos $0, 1, 2, 3, 4$ módulo 5. Um quadrado pode deixar restos $0, 1, 4$ apenas:

$$\begin{aligned}
0^2 &\equiv 0 && \pmod{5} \\
1^2 &\equiv 1 && \pmod{5} \\
2^2 &\equiv 4 && \pmod{5} \\
3^2 &\equiv 4 && \pmod{5} \\
4^2 &\equiv 1 && \pmod{5}
\end{aligned}$$

Agora, do enunciado, $4x \equiv 2 \pmod{5}$, logo $4x$ não pode ser quadrado perfeito. Assim, não é possível que x seja quadrado módulo 5.

Ex. 9 — cancelado