Lista de exercícios 02 - FMC

Andriel Vinicius de M. Fernandes

July 10, 2024

1 Congruência Modular

1. Demonstre:
   Sejam $a, b, c, d, n \in \mathbb{Z}$, com $n > 1$.
   Se $a \equiv c \pmod{n}$ e $b \equiv d \pmod{n}$, então:

   (a) $(a \cdot b) \equiv (c \cdot d) \pmod{n}$;
   Resolução.
   (1) Sejam $a, b, c, d, n \in \mathbb{Z}$, com $n > 1$, onde $a \equiv c \pmod{n}$ e $b \equiv d \pmod{n}$.
   (2) Por def., temos que $\exists k_1 \in \mathbb{Z}, k_1 \cdot n = a - c \implies a = k_1 n + c$.
   (3) Por def., temos que $\exists k_2 \in \mathbb{Z}, k_2 \cdot n = b - d \implies b = k_2 n + d$.
   Assim, temos:

$$
\begin{aligned}
(4) \quad a = k_1 n + c \quad & \text{(Por aritmética)} \\
(5) \quad ab = (k_1 n + c) \cdot b \quad & \text{(Por multiplicação por } b\text{)} \\
(6) \quad ab = bk_1 n + bc \quad & \text{(Por distributividade em 5)} \\
(7) \quad ab = (k_2 n + d)k_1 n + (k_2 n + d)c \quad & \text{(Por substituição em } b \text{ por 3)} \\
(8) \quad ab = k_1 n k_2 n + k_1 n d + k_2 n c + cd \quad & \text{(Por distributividade)} \\
(9) \quad ab = n(k_1 n k_2 + k_1 d + k_2 c) + cd \quad & \text{(Por evidência em } n\text{)} \\
(10) \quad ab = nk_3 + cd \quad & \text{(Para } k_3 = (k_1 n k_2 + k_1 d + k_2 c)\text{)} \\
(11) \quad ab - cd = nk_3 \quad & \text{(Por aritmética)} \\
(11) \quad n | ab - cd \quad & \text{(Por def. de divisibilidade)}
\end{aligned}
$$

   Portanto, $ab \equiv cd \pmod{n}$ pela def. de congruência.

(b) $a^m \equiv c^m \pmod{n}$, para qualquer $m \in \mathbb{Z}$.

2. Quantas soluções inteiras existem para x, com $0 \leq x < 150$ para a congruência linear $63x \equiv 30 \pmod{50}$? Quais são elas?

3. Qual o menor valor positivo que satisfaz esta congruência linear?

$$81x \equiv 12 \pmod{264}$$

4. Calcule $(8^{1}0 - 128^{1}796) \pmod{13}$. Mostre todos os resultados intermediários. Durante o processo nenhum número com mais de 3 dígitos deve ser gerado.