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:

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

   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 $63x \equiv 30 \pmod{150}$? Quais são elas?
Resolução.
Verifiquemos o $mdc(150, 63)$:

$$\begin{aligned} mdc(150,63): 150 &= 2 \cdot 63 + 24 & (24 = 63 \cdot 2 - 150) \\ 63 &= 2 \cdot 24 + 15 & (15 = 24 \cdot 2 - 63) \\ 24 &= 1 \cdot 15 + 9 & (9 = 24 - 1 \cdot 15) \\ 15 &= 1 \cdot 9 + 6 & (6 = 15 - 9) \\ 9 &= 3 \cdot 3 + 0 & \end{aligned}$$

Portanto, $mdc(150, 63) = 3$.
Note que, pela regra do cancelamento geral, temos:

$$63x \equiv 30 \pmod{150} \implies 21x * 3 \equiv 10 * 3 \pmod{150} \iff 21x \equiv 10 \pmod{\frac{150}{3}}$$

Logo, temos que resolver $21x \equiv 10 \pmod{\frac{150}{3}}$.
Verifiquemos:

$$\begin{aligned} mdc(50,21): 50 &= 2 \cdot 21 + 8 & (8 = 50 - 2 \cdot 21) \\ 21 &= 2 \cdot 8 + 5 & (5 = 21 - 2 \cdot 8) \\ 8 &= 1 \cdot 5 + 3 & (3 = 8 - 1 \cdot 5) \\ 5 &= 1 \cdot 3 + 2 & (2 = 5 - 1 \cdot 3) \\ 3 &= 1 \cdot 2 + 1 & (1 = 3 - 1 \cdot 2) \\ 2 &= 1 \cdot 2 + 0 & \end{aligned}$$

Portanto, $mdc(50, 21) = 1$.

Assim, vamos encontrar o inverso de 21 módulo 50:

$$\begin{aligned}
1 &= 3 - 2 \\
&= 3 - (5 - 3) \\
&= 2 \cdot 3 - 5 \\
&= 2 \cdot (8 - 5) - 5 \\
&= 2 \cdot 8 - 3 \cdot 5 \\
&= 2 \cdot 8 - 3 \cdot (21 - 2 \cdot 8) \\
&= 2 \cdot 8 - 3 \cdot 21 + 6 \cdot 8 \\
&= 8 \cdot 8 - 3 \cdot 21 \\
&= 8 \cdot (50 - 2 \cdot 21) - 3 \cdot 21 \\
&= 8 \cdot 50 - 16 \cdot 21 - 3 \cdot 21 \\
&= 8 \cdot 50 - 19 \cdot 21
\end{aligned}$$

Como $-19 \equiv 31 \pmod{50}$, temos que o inverso modular de 21 é 31.
Agora, note que:

$$\begin{aligned}
&31 \cdot 21x \equiv 10 \cdot 31 \pmod{50} \\
\Longrightarrow\ &651x \equiv 310 \pmod{50} \\
\Longrightarrow\ &x \equiv 10 \pmod{50} \quad \text{pois } (651 \equiv 1 \pmod{50}) \\
\Longrightarrow\ & \qquad x = 50 \cdot t + 10 \quad \text{(Por def.)}
\end{aligned}$$

para $0 \leq t \leq 2$.
Portanto, as 3 possíveis soluções para a congruência linear são $x = 10, x = 60, x = 110$.

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

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

4. Calcule $(8^10 - 128^1796) \pmod{13}$. Mostre todos os resultados intermediários. Durante o processo nenhum número com mais de 3 dígitos deve ser gerado.