Lista de exercícios 02 - FMC

Andriel Vinicius de M. Fernandes

July 13, 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)	$n \mid ab - cd$	(Por def. de divisibilidade)

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

(b) $a^m \equiv c^m \pmod{n}$, para qualquer $m \in \mathbb{Z}$.
Resolução.
Vamos demonstrar por indução em m.
(1) Suponha $a \equiv c \pmod{n}$.
(2) Seja $P(m) := a^m \equiv c^m \pmod{n}$.
(3) Passo base: $P(0)$.

$$\begin{aligned} P(0) :=& a^0 \equiv c^0 \pmod{n} \\ &\implies 1 \equiv 1 \pmod{n} \qquad (\text{por } x^0 = 1) \end{aligned}$$

Por reflexividade, $P(0)$ é válido.
(4) Hipótese Indutiva: seja um $k \in \mathbb{Z}$ arbitrário, tal que $P(k) := a^k \equiv c^k \pmod{n}$. Assim, $a = c + n \cdot w_0$, para $w_0 \in \mathbb{Z}$, por definição de congruência em (1).
(5) Logo:

$$\begin{aligned} (6) \quad a^k \cdot a &= (c + n \cdot w_0) \cdot a^k && (\text{por reescrita}) \\ (7) \quad &= c \cdot a^k + a^k \cdot n \cdot w_0 && (\text{por distributividade}) \\ (8) \quad &= c \cdot (c^k + n \cdot w_1) + (c^k + n \cdot w_1) \cdot (n \cdot w_0) && (\text{por H.I}) \\ (9) \quad &= cc^k + cnw_1 + c^k n + nw_1 nw_0 && (\text{por distributividade}) \\ (10) \quad &= cc^k + n(cw_1 + c^k + w_0 nw_1) && (\text{por evidência}) \\ (11) \quad &= cc^k + nw_2 && (\text{para } w_2 = (cw_1 + c^k + w_0 nw_1) \end{aligned}$$

Portanto, $a^{k+1} \equiv c^{k+1} \pmod{n}$.

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:

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

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?

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

Resolução.
Verifiquemos:

$$\begin{aligned} mdc(264, 81) : 264 &= 3 \cdot 81 + 21 && (21 = 264 - 3 \cdot 81) \\ 81 &= 3 \cdot 21 + 18 && (18 = 81 - 3 \cdot 21) \\ 21 &= 1 \cdot 18 + 3 && (3 = 21 - 18) \\ 18 &= 6 \cdot 3 + 0 \end{aligned}$$

Logo, $mdc(264, 81) = 3$.
Pela regra do cancelamento geral, temos que:

$$81x \equiv 12 \pmod{264} \implies 27x \cdot 3 \equiv 4 \cdot 3 \pmod{264} \iff 27x \equiv 4 \pmod{\frac{264}{3}}$$

Verifiquemos novamente o mdc entre 27 e 88:

$$\begin{aligned} mdc(88, 27) : 88 &= 3 \cdot 27 + 7 && (7 = 88 - 3 \cdot 27) \\ 27 &= 3 \cdot 7 + 6 && (6 = 27 - 3 \cdot 7) \\ 7 &= 1 \cdot 6 + 1 && (1 = 7 - 6) \\ 6 &= 6 \cdot 1 + 0 \end{aligned}$$

Logo, $mdc(88, 27) = 1$.
Assim, podemos calcular o inverso de 27 módulo 88 pelo algoritmo extendido de Euclides:

$$\begin{aligned} 1 &= 7 - 6 \\ &= 7 - (27 - 3 \cdot 7) \\ &= 7 - (27 - 3 \cdot (88 - 3 \cdot 27)) \\ &= 7 - (27 - 3 \cdot 88 + 9 \cdot 27) \\ &= 88 - 3 \cdot 27 - (27 - 3 \cdot 88 + 9 \cdot 27) \\ &= 4 \cdot 88 - 13 \cdot 27 \end{aligned}$$

Como $-13 \equiv 75 \pmod{88}$, temos que o inverso modular de 27 módulo 88 é 75.
Agora, note que:

$$\begin{aligned} & 75 \cdot 27x \equiv 4 \cdot 75 \pmod{88} \\ \implies & x \equiv 300 \pmod{88} \quad [\text{pois } 27 \cdot 75 \equiv 1 \pmod{88}] \\ \implies & x \equiv 300 \pmod{88} \\ \implies & x \equiv 36 \pmod{88} \quad [\text{pois } 300 \equiv 36 \pmod{88}] \end{aligned}$$

Logo, o menor inteiro que satisfaz a congruência é 36.

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.
Resolução.
Note que:

$$(8^{10} - 128^{1796}) \pmod{13} \implies (8^{10} \bmod 13) - (128^{1796} \bmod 13) \pmod{13}$$

A princípio calculemos $(8^{10} \bmod 13)$.
Note que $8^{10} = 8^2 \cdot 8^4 \cdot 8^4$. Vamos calcular cada:

- $8^2 \bmod 13 = 64 \bmod 13 = 12$
- $8^4 \bmod 13 = (8^2 \bmod 13)^2 \bmod 13 = 12^2 \bmod 13 = 1$

Portanto:

$$\begin{aligned} 8^{10} \bmod 13 &= (8^2 \bmod 13 \cdot 8^4 \bmod 13 \cdot 8^4 \bmod 13) \bmod 13 \\ &= (12 \cdot 1 \cdot 1) \bmod 13 \\ &= 12 \end{aligned}$$

Agora calculemos $(128^{1796}) \bmod 13$.
Note que $(128 \bmod 13)^{1796} \bmod 13 = 11^{1796} \bmod 13$.
Veja que $11^{1796} = 11^{1024} \cdot 11^{256} \cdot 11^{256} \cdot 11^{256} \cdot 11^4$. Vamos calcular cada:

- $11^4 \bmod 13 = (11^2 \bmod 13)^2 \bmod 13 = 4^2 \bmod 13 = 3$

- $11^{256} \bmod 13$:
  - Note que $256 = 21 \cdot 12 + 4$;
  - Pelo Pequeno Teorema de Fermat, tomando o primo 13 e o inteiro 11, sabemos que $11^{12} \equiv 1 \pmod{13}$;
  - Logo:

$$\begin{aligned} 11^{256} &\equiv (11^{12})^{21} \cdot 11^4 \pmod{13} \\ &\equiv 1^{21} \cdot 11^4 \pmod{13} \quad [\text{pois } 11^{12} \equiv 1 \pmod{13}] \\ &\equiv 11^4 \pmod{13} \\ &\equiv 3 \end{aligned}$$

- $11^{1024} \bmod 13 = (11^{256} \bmod 13)^4 \bmod 13 = 3^4 \bmod 13 = 3$

Desse modo, temos:

$$11^{1796} \bmod 13 = (3 \cdot 3 \cdot 3 \cdot 3 \cdot 3) \bmod 13 = 243 \bmod 13 = 9$$

Portanto, temos a operação final:

$$\begin{aligned} (8^{10} - 128^{1796}) \bmod 13 &= (8^{10} \bmod 13) - (128^{1796} \bmod 13) \bmod 13 \\ &= (12 - 9) \bmod 13 \\ &= 3 \end{aligned}$$

2 Teorema Chinês dos restos

1. Após muitos conflitos políticos no Brasil em 2030, os illuminatis decidem terceirizar uma intervenção militar e contratam um general chinês, que ficou encarregado de chefiar 500 soldados brasileiros antes de uma guerra civil, como para os chineses os ocidentais são todos muito parecidos, ele tinha uma certa dificuldade em contar os brasileiros. Seguindo uma intuição ancestral, após a guerra civil, o chinês alinhou os soldados em fileiras de 6 de forma que sobraram 3. Quando ele alinhou os soldados em fileiras de 7, também sobraram 3 soldados. Por fim, alinhou em fileiras de 11 e sobraram 5. Quantos soldados o general tinha no

final?
Resolução. Temos o seguinte sistema de congruências:

$$\begin{aligned} s &\equiv 3 \pmod 6 \\ s &\equiv 3 \pmod 7 \\ s &\equiv 5 \pmod{11} \end{aligned}$$

Pelos fato dos módulos serem coprimos, temos $m = m_1 \cdot m_2 \cdot m_3 = 6 \cdot 7 \cdot 11 = 462$.
Pelo teorema chinês dos restos, temos

$$s = s_1 \cdot M_1^{\Phi(m_1)} + s_2 \cdot M_2^{\Phi(m_2)} + s_3 \cdot M_3^{\Phi(m_3)} \pmod m$$

onde $M_i = \frac{m}{m_1}$, $s_i = a_i \bmod m_i$ e a_i é o resto em cada m_i.
Assim, temos os s:

- $s_1 = 3 \bmod 6 = 3$;
- $s_2 = 3 \bmod 7 = 3$;
- $s_3 = 5 \bmod 11 = 5$.

e os M:

- $M_1 = \frac{462}{6} = 77$;
- $M_2 = \frac{462}{7} = 66$;
- $M_3 = \frac{462}{11} = 42$.

Logo, temos:

$$\begin{aligned} s &\equiv s_1 \cdot M_1^{\Phi(m_1)} + s_2 \cdot M_2^{\Phi(m_2)} + s_3 \cdot M_3^{\Phi(m_3)} \pmod m \\ &\equiv 3 \cdot 77^3 + 3 \cdot 66^6 + 5 \cdot 42^{10} \pmod{462} \\ &\equiv (3 \cdot 77^3 \bmod 462) + (3 \cdot 66^6 \bmod 462) + (5 \cdot 42^{10} \bmod 462) \pmod{462} \\ &\equiv (3 \cdot 77 \cdot (77^2 \bmod 462) \bmod 462) + (3 \cdot (66^2 \bmod 462)^3 \bmod 462) + (5 \cdot 42^{10} \bmod 462) \quad (\text{m} \\ &= (3 \cdot 77 \cdot (77^2 \bmod 462) \bmod 462) + (3 \cdot (66^2 \bmod 462)^3 \bmod 462) + \\ &(5 \cdot 42^{10} \bmod 462) \pmod{462} \end{aligned}$$

Resolvamos $(66^2 \bmod 462)^3$:

$$\begin{aligned}(66^2 \bmod 462)^3 &= (4356 \bmod 462)^3 \bmod 462 \\ &= 198^3 \bmod 462 \\ &= (198 \bmod 462) \cdot (198^2 \bmod 462) \bmod 462 \\ &= 198 \cdot (39204 \bmod 462) \bmod 462 \\ &= 198 \cdot 396 \bmod 462 \\ &= 78408 \bmod 462 \\ &= 330\end{aligned}$$

Resolvamos também $(42^{10} \bmod 462)$. Note que $42^{10} = 42^2 \cdot 42^4 \cdot 42^4$. Vejamos cada um deles em módulo 462:

- $(42^2 \bmod 462) = 1764 \bmod 462 = 378$;
- $(42^4 \bmod 462) = (42^2 \bmod 462)^2 \bmod 462 = 378^2 \bmod 462 = 142884 \bmod 462 = 126$;

Logo:

$$42^{10} = (378 \cdot 126 \cdot 126) \bmod 462 = 6001128 \bmod 462 = 210$$

Retomando:

$$\begin{aligned}&(3 \cdot 77 \cdot (77^2 \bmod 462) \bmod 462) + (3 \cdot (66^2 \bmod 462)^3 \bmod 462) + \\ &(5 \cdot 42^{10} \bmod 462) \pmod{462} \\ &\equiv (3 \cdot 77 \cdot 385 \bmod 462) + (3 \cdot 330 \bmod 462) + (5 \cdot 210) \pmod{462} \\ &\equiv (88935 \bmod 462) + (990 \bmod 462) + (1050 \bmod 462) \pmod{462} \\ &\equiv 231 + 66 + 126 \pmod{462} \\ &\equiv 423 \pmod{462}\end{aligned}$$

Portanto, o número final de soldados do general chinês é de 423.

3 Criptografia

1. Considere o sistema RSA com os seguintes parâmetros: $p = 3, q = 11, e = 17$.

(a) Determine as chaves pública e privada dos usuários.
Resolução.
Vamos criar as chaves privada e pública de Alice e Beto.

i. Tome $p = 3, q = 11$.
ii. Então, tome $n = 3 \cdot 11 = 33$.
iii. Seja Φ o produto de $\phi(p)$ e $\phi(q)$.
Ou seja, $\Phi = (3-1) \cdot (11-1) = 20$.
iv. Tome $e = 17$ tal que $mdc(17, \Phi) = 1$ e $1 < e < \Phi$. Verifiquemos:

$$\begin{aligned} mdc(20, 17) : 20 &= 1 \cdot 17 + 3 && (3 = 20 - 17) \\ 17 &= 5 \cdot 3 + 2 && (2 = 17 - 5 \cdot 3) \\ 3 &= 1 \cdot 2 + 1 && (1 = 3 - 2) \\ 2 &= 2 \cdot 10 \end{aligned}$$

v. Vamos calcular o inverso de 17 módulo 20:

(b) Desencripte o texto cifrado $c = 4$ para Alice.
Resolução.