Lista de exercícios 02 - FMC

Andriel Vinicius de M. Fernandes

July 21, 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:

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

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

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

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

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

2. Sejam $a, b, c, n \in \mathbb{Z}, n > 0$.
Demonstre que $ac \equiv bc \pmod{n} \iff a \equiv b \pmod{\frac{n}{mdc(c,n)}}$.
Resolução.
Demonstremos primeiro que $ac \equiv bc \pmod{n} \implies a \equiv b \pmod{\frac{n}{mdc(c,n)}}$.
(1) Assuma $ac \equiv bc \pmod{n}$, por hipótese.
(2) Logo, $n | ac - bc$, por def. de congruência.
(3) Então $\exists k_1 \in \mathbb{Z}, k_1 n = ac - bc$, por def. de divisibilidade em (2).
(4) Note que:

$$\begin{aligned} k_1 n = ac - bc &\implies k_1 n = (a - b)c && (\text{por aritmética}) \\ &\implies \frac{k_1 n}{mdc(c,n)} = (a - b)\frac{c}{mdc(c,n)} && (\text{por div. de } mdc(c,n)) \end{aligned}$$

(5) Note que $mdc(\frac{n}{mdc(c,n)}, \frac{c}{mdc(c,n)}) = 1$. Ou seja, eles são coprimos.
(6) Por reescrita em (4), note que:

$$\frac{n}{mdc(c,n)} | (a-b) \frac{c}{mdc(c,n)}$$

(7) Contudo, por (5), temos que:

$$\frac{n}{mdc(c,n)} | a-b \implies a \equiv b \pmod{\frac{n}{mdc(c,n)}} \quad \text{(por def. de congruência)}$$

Agora, demonstremos que $a \equiv b \pmod{\frac{n}{mdc(c,n)}} \implies ac \equiv bc \pmod{n}$.
(1) Assuma $a \equiv b \pmod{\frac{n}{mdc(c,n)}}$, por hipótese.
(2) Logo, $\frac{n}{mdc(c,n)} | a-b$, por def. de congruência.
(3) Então, $\exists k_1 \in \mathbb{Z}, \frac{n}{mdc(c,n)} k_1 = a-b$, por def. de divisibilidade em (2).
(4) Seja $d = mdc(c,n)$. Então, $d|c$ e $d|n$, por def. de mdc.
(5) Assim, $\exists k_2, k_3 \in \mathbb{Z}, k_2 d = c, k_3 d = n$, por def. de divisibilidade em (4).
Temos:

$$\begin{aligned}
\frac{n}{mdc(c,n)} k_1 = a-b &\implies \frac{n}{mdc(c,n)} k_1 c = (a-b)c && \text{(por multiplicação por } c\text{)} \\
&\implies \frac{n}{d} k_1 c = ac - bc && \text{(por substituição com } d\text{)} \\
&\implies \frac{n}{d} k_1 k_2 d = ac - bc && \text{(por (5))} \\
&\implies n k_1 k_2 = ac - bc && \text{(por aritmética)} \\
&\implies n k_4 = ac - bc && \text{(para } k_4 = k_1 k_2\text{)} \\
&\implies ac \equiv bc \pmod{n} && \text{(por def. de congruência)}
\end{aligned}$$

Portanto, está demonstrado que $ac \equiv bc \pmod{n} \iff a \equiv b \pmod{\frac{n}{mdc(c,n)}}$.

3. Demonstre que $mdc(2^a - 1, 2^b - 1) = 2^{mdc(a,b)} - 1$.
Resolução.
Sejam $a, b \in \mathbb{Z}, a, b \geq 0$. Seja $d = mdc(a,b)$.
(Provemos que $2^d - 1 \mid 2^a - 1 \wedge 2^b - 1$.)
(1) Note que $2^d - 1 | 2^d - 1$.
(2) Ou seja, $2^d \equiv 1 \pmod{2^d - 1}$, por def. de congruência modular.

(3) Por potenciação, temos $(2^d)^{\frac{a}{d}} \equiv 1^{\frac{a}{d}} \pmod{2^d - 1}$.
(4) Por aritmética, temos $2^a \equiv 1 \pmod{2^d - 1}$.
(5) Por congruência, temos $2^d - 1 | 2^a - 1$.
(6) Analogamente, pelos passos (3), (4) e (5), temos $2^d - 1 | 2^b - 1$.
(7) Portanto, $2^d - 1 | 2^a - 1 \text{e} 2^b - 1$.

[Agora, mostremos que $2^d - 1$ é o melhor divisor destes números.]
A concluir.

4. 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 $x = 10, x = 60, x = 110$.

5. 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.

6. 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:

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

7. Demonstre que para quaisquer inteiros $a, b, m_1, m, 2$, com $m_1, m_2 > 0$, se $a \equiv b \pmod{mmc(m_1, m_2)}$ então $a \equiv b \pmod{m_1}$.
Resolução. Sejam $a, b, m_1, m, 2 \in \mathbb{Z}$, com $m_1, m_2 > 0$.
(1) Suponha que $a \equiv b \pmod{mmc(m_1, m_2)}$, por hipótese.
(2) Temos $mmc(m_1, m_2) \mid a - b$, por def. de congruência.
(3) Temos $m_1 \mid mmc(m_1, m_2)$ por def. de mmc.
(4) Temos que, se $m_1 \mid mmc(m_1, m_2)$ e $mmc(m_1, m_2) \mid a - b$, então $m_1 \mid a - b$ por transitividade da div.
(5) Portanto, temos que $a \equiv b \pmod{m_1}$, por def. de congruência.

2 Teorema Chinês dos restos

1. Sobre o teorema chinês dos restos, responda:

   (a) Se p é um primo, qual o valor de $\Phi(p)$? Mostre que isso funciona para $p = 3, p = 5$.
   Resolução.
   Tomando um p primo, para todo $x < p$, temos que $mdc(x, p) = 1$. Portanto, temos que $\Phi(p) = p - 1$, pois é a quantidade de números menores que p. Podemos mostrar:

   - $p = 3$: $\Phi(3) = \#\{1, 2\} = 2$;
   - $p = 5$: $\Phi(5) = \#\{1, 2, 3, 4\} = 4$.

   (b) Considere o exemplo de representação de números por resíduos independentes, usando duas bases ($n = 2$): $m_1 = 3, m_2 = 5$. Calcule M_1 e M_2 conforme definidos acima, para este exemplo.
   Resolução.

Sejam $m_1, m_2, m_r \in \mathbb{Z}_+^*$, onde $m_1 = 3, m_2 = 5$.
Temos que m_1 e m_2 são coprimos. Assim temos:

$$m_r = m_1 \cdot m_2 = 3 \cdot 5 = 15$$

Podemos calcular M_i tal que:

- $M_1 = (\frac{m_r}{m_1})^{\Phi(m_1)} = (\frac{15}{3})^2 = 25$. Note que M_1 é resíduo independente, pois $25 \equiv 1 \pmod 3$ e $25 \equiv 0 \pmod 5$.
- $M_2 = (\frac{m_r}{m_2})^{\Phi(m_2)} = (\frac{15}{5})^4 = 81$. Note que M_2 é resíduo independente, pois $81 \equiv 1 \pmod 5$ e $81 \equiv 0 \pmod 3$.

2. Demonstre que, para $M_j = (\frac{m}{m_j})^{\Phi m_j}$, podemos concluir que $M_j \equiv 1 \pmod{m_j}$.
Resolução.
Seja m o produtório de todos os módulos de um sistema de congruências, ou seja, $m = m_1 \cdot m_2 \cdot \cdots \cdot m_j$, e $m_j \in \mathbb{Z}$.
Seja $M_j = (\frac{m}{m_j})^{\Phi m_j}$, com $M_j \in \mathbb{Z}$.
(1) Note que $m_j | m$, pois $\exists k \in \mathbb{Z}, k \cdot m_j = m$, onde $k = \frac{m}{m_j} = m_1 \cdot m_2 \cdots$.
(2) Então, temos que $mdc(k, m_j) = 1$, pois não há divisores em comum entre eles, visto que todos os módulos são coprimos entre si.
(3) Logo, temos que $k^{\Phi m_j} \equiv 1 \pmod{m_j}$, pelo teorema de Euler.
(4) Portanto, $M_j \equiv 1 \pmod{m_j}$ por substituição.

3. Considere um computador que representa números inteiros de 0 a $2^{10} - 1$, ou seja, de 10 bits. Para aumentar a capacidade de processamento deste computador, podemos utilizar o teorema chinês dos restos com os módulos $2^9 - 1, 2^7 - 1, 2^5 - 1$.

   (a) Como representar $2^{11}, 2^{13}$ nos módulos acima?
   Resolução.

   - $2^{11} \bmod 2^9 - 1 = 2^9 \cdot 2^2 \bmod 511 = 1 \cdot 4 \bmod 511 = 4$
   - $2^{11} \bmod 2^7 - 1 = 2^7 \cdot 2^4 \bmod 127 = 1 \cdot 16 \bmod 127 = 16$
   - $2^{11} \bmod 2^5 - 1 = 2^5 \cdot 2^6 \bmod 31 = 1 \cdot 64 \bmod 31 = 2$
   - $2^{13} \bmod 2^9 - 1 = 2^9 \cdot 2^4 \bmod 511 = 1 \cdot 16 \bmod 511 = 16$
   - $2^{13} \bmod 2^7 - 1 = 2^7 \cdot 2^6 \bmod 127 = 1 \cdot 64 \bmod 127 = 64$
   - $2^{13} \bmod 2^5 - 1 = 2^5 \cdot 2^8 \bmod 31 = 1 \cdot 256 \bmod 31 = 8$

(b) A partir das triplas de valores, determine a tripla da soma $2^{11}+2^{13}$.
Resolução. Para 2^{11} temos $(4, 16, 2)$, e para 2^{13} temos $(16, 64, 8)$. Portanto, temos:

$$\begin{aligned}(4, 16, 1) + (16, 64, 8) &= (4 + 16 \bmod 511, 16 + 64 \bmod 511, 8 + 2 \bmod 31) \\ &= (20, 80, 10)\end{aligned}$$

(c) Exiba o sistema de congruências da soma $2^{11} + 2^{13}$.
Resolução. A soma corresponde ao sistema abaixo:

$$x \equiv 20 \pmod{511} x \equiv 80 \pmod{127} x \equiv 10 \pmod{31}$$

(d) Com o esquema referenciado nesta questão, o computador conseguiria representar números até qual valor?
Resolução. Até o produto dos módulos, sendo este $m = 511 \cdot 127 \cdot 31 = 2011807$.

4. 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:

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

Pelo 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:

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

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:

$$\begin{aligned}
&(3 \cdot 77 \cdot 77 \bmod 462) + (3 \cdot (66^2 \bmod 462)^3 \bmod 462) + \\
&(5 \cdot 42^{10} \bmod 462) \pmod{462} \\
&\equiv (3 \cdot (77^2 \bmod 462) \bmod 462) + (3 \cdot 330 \bmod 462) + (5 \cdot 210) \pmod{462} \\
&\equiv (3 \cdot (5929 \bmod 462) \bmod 462) + (990 \bmod 462) + (1050 \bmod 462) \pmod{462} \\
&\equiv (3 \cdot 385 \bmod 462) + 66 + 126 \pmod{462} \\
&\equiv 231 + 66 + 126 \pmod{462} \\
&\equiv 423 \pmod{462}
\end{aligned}$$

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 modular de 17 módulo 20:

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (17 - 5 \cdot 3) \\ &= 3 - (17 - 5 \cdot (20 - 17)) \\ &= 3 - (17 - 5 \cdot 20 + 5 \cdot 17) \\ &= 3 - 17 + 5 \cdot 20 - 5 \cdot 17 \\ &= 20 - 17 - 17 + 5 \cdot 20 - 5 \cdot 17 \\ &= 6 \cdot 20 - 7 \cdot 17 \end{aligned}$$

vi. Como $-7 \equiv 13 \pmod{20}$, então temos o inverso modular $d = 13$.

vii. Portanto, temos que as chaves pública e privada são, respectivamente, $(17, 33)$ e 13.

(b) Desencripte o texto cifrado $c = 4$ para Alice.
Resolução.
Tomando o texto cifrado $c = 4$ de Beto e a chave privada $d = 13$ de Alice, vamos desencriptar em um texto claro m a partir da fórmula $m = c^d \bmod n$.
Temos:

$$\begin{aligned} m &= 4^{13} \bmod 33 \\ &= 4 \cdot 4^2 \cdot 4^2 \cdot 4^4 \cdot 4^4 \bmod 33 \end{aligned}$$

Vamos calcular cada potência em mod33:

i. $4 \bmod 33 = 4$;

ii. $4^2 \bmod 33 = 16 \bmod 33 = 16$;

iii. $4^4 \bmod 33 = (4^2 \bmod 33)^2 \bmod 33 = 16^2 \bmod 33 = 256 \bmod 33 = 25$.

Ou seja,

$$\begin{aligned} m &= 4 \cdot 4^2 \cdot 4^2 \cdot 4^4 \cdot 4^4 \bmod 33 \\ &= (4 \cdot 16 \cdot 16 \cdot 25 \cdot 25) \bmod 33 \\ &= (4 \cdot 16^2 \cdot 25^2) \bmod 33 \\ &= (1024 \cdot 625) \bmod 33 \\ &= (1024 \bmod 33) \cdot (625 \bmod 33) \bmod 33 \\ &= 1 \cdot 31 \bmod 33 \\ &= 31 \end{aligned}$$

Portanto, o texto claro para Alice é 31.