# Teorema Chinês dos Restos

Teorema Chinês dos Restos

## Tópicos Adicionais

**Tópicos Adicionais**
**Teorema Chinês dos Restos**

# 1 Exercícios Introdutórios

**Exercício 1.** Para cada um dos itens abaixo, encontre o menor inteiro positivo $a$ tal que:

(a) $2a \equiv 1 \pmod{11}$

(b) $3a \equiv 1 \pmod{13}$

(c) $5a \equiv 1 \pmod{17}$

**Exercício 2.** Encontre o menor inteiro positivo $x$ que satisfaz o seguinte sistema de congruências:

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 2 \pmod{5} \\ x &\equiv 3 \pmod{7} \end{aligned}$$

**Exercício 3.** Encontre todas as soluções do sistema:

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 2 \pmod{5} \\ x &\equiv 3 \pmod{11} \end{aligned}$$

**Exercício 4.** Encontre todas as soluções do sistema de congruências:

$$\begin{aligned} 4x &\equiv 2 \pmod{6} \\ 15x &\equiv 6 \pmod{21} \\ 12x &\equiv 4 \pmod{20} \end{aligned}$$

**Exercício 5.** Mostre que existem infinitos inteiros $x$ que satisfazem o sistema

$$\begin{aligned} x^2 &\equiv -1 \pmod{5}. \\ x^2 &\equiv -1 \pmod{17}. \\ x^2 &\equiv -1 \pmod{257}. \end{aligned}$$

**Exercício 6.** Determine se o sistema abaixo possui solução:

$$\begin{aligned} x &\equiv 2 \pmod{6} \\ x &\equiv 3 \pmod{8} \end{aligned}$$

**Exercício 7.** Determine se o sistema abaixo possui solução:

$$\begin{aligned} x &\equiv 1 \pmod{6} \\ x &\equiv 7 \pmod{8} \end{aligned}$$

**Exercício 8.** Determine $a$ de modo que o sistema abaixo possua solução:

$$\begin{aligned} x &\equiv 1 \pmod{6} \\ x &\equiv 7 \pmod{8} \\ x &\equiv a \pmod{15} \end{aligned}$$

**Exercício 9.** Encontre todos os inteiros positivos $x$ que satisfazem o seguinte sistema de congruências:

$$\begin{aligned} x &\equiv 2 \pmod{10} \\ x &\equiv 7 \pmod{11} \\ x &\equiv 5 \pmod{13} \end{aligned}$$

# 2 Exercícios de Fixação

**Exercício 10.** Encontre o menor inteiro positivo $x$ tal que $x \equiv 5 \pmod{7}$, $x \equiv 7 \pmod{11}$ e $x \equiv 3 \pmod{13}$.

**Exercício 11.** Resolva o sistema:

$$\begin{cases} 2x \equiv 2 \pmod{3} \\ 3x \equiv 2 \pmod{5} \\ 4x \equiv 3 \pmod{7} \end{cases}$$

**Exercício 12.** Para cada número natural $n$, existe uma sequência arbitrariamente longa de números naturais consecutivos, cada um deles sendo divisível por uma $s$-ésima potência de um número natural maior que 1.

# 3 Exercícios de Aprofundamento e de Exames

**Exercício 13.** Determine todos os restos possíveis da divisão do quadrado de um número primo com 120 por 120.

**Exercício 14.** (a) Existem 14 inteiros positivos consecutivos tais que, cada um é divisível por um ou mais primos $p$ do intervalo $2 \leq p \leq 11$?

(b) Existem 21 inteiros positivos consecutivos tais que, cada um é divisível por um ou mais primos $p$ do intervalo $2 \leq p \leq 13$?

**Exercício 15.** Sejam $a$ e $b$ inteiros positivos tais que, para qualquer $n$ natural, $a^n + n \mid b^n + n$. Prove que $a = b$.

**Respostas e Soluções.**

**1.** Pelo Teorema de Fermat, se $p$ é primo e $mdc(a,p) = 1$, temos $a \cdot a^{p-2} \equiv 1 \pmod{p}$. Daí, $a^{p-2} \pmod{p}$ é o inverso de $a$ módulo $p$. Usando esta observação, podemos encontrar:

a) $a = 6$

b) $a = 9$

c) $a = 7$

**2.** Pelo Teorema Chinês dos Restos, a solução geral do sistema pode ser escrita como

$$x = 1 \cdot 35 \cdot m_{35} + 2 \cdot 21 \cdot m_{21} + 3 \cdot 15 \cdot m_{15} + 105q.$$

Os inteiros $m_{35}$, $m_{21}$ e $m_{15}$ são determinados como soluções das congruências:

$$\begin{aligned} 35 \cdot m_{35} &\equiv 1 \pmod{3} \\ 21 \cdot m_{21} &\equiv 1 \pmod{5} \\ 15 \cdot m_{15} &\equiv 1 \pmod{7} \end{aligned}$$

Resolvendo cada uma das congruências anteriores, podemos obter $m_{35} = 2$, $m_{21} = 1$ e $m_{15} = 1$. Daí,

$$\begin{aligned} x &\equiv 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 \pmod{105} \\ &\equiv 52 \pmod{105}. \end{aligned}$$

Portanto, o menor inteiro positivo é 52.

**3.** Pelo Teorema Chinês dos Restos, a solução geral do sistema pode ser escrita como

$$x = 1 \cdot 55 \cdot m_{55} + 2 \cdot 33 \cdot m_{33} + 3 \cdot 15 \cdot m_{15} + 165q.$$

Os inteiros $m_{55}$, $m_{33}$ e $m_{15}$ são determinados como soluções das congruências:

$$\begin{aligned} 55 \cdot m_{55} &\equiv 1 \pmod{3} \\ 33 \cdot m_{33} &\equiv 1 \pmod{5} \\ 15 \cdot m_{15} &\equiv 1 \pmod{11} \end{aligned}$$

Resolvendo cada uma das congruências anteriores, podemos obter $m_{55} = 1$, $m_{33} = 2$ e $m_{15} = 3$. Daí,

$$\begin{aligned} x &\equiv 1 \cdot 55 \cdot 1 + 2 \cdot 33 \cdot 2 + 3 \cdot 15 \cdot 3 \pmod{165} \\ &\equiv 157 \pmod{165}. \end{aligned}$$

**4.** Sabemos que

$$ak \equiv bk \pmod{m} \Leftrightarrow a \equiv b \pmod{m/d},$$

onde $d = mdc(k,m)$. Daí, o sistema anterior é equivalente a

$$\begin{aligned} 2x &\equiv 1 \pmod{3} \\ 5x &\equiv 2 \pmod{7} \\ 3x &\equiv 1 \pmod{5} \end{aligned}$$

Multiplicando cada equação pelo inverso do coeficiente que acompanha o $x$, temos

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 6 \pmod{7} \\ x &\equiv 2 \pmod{5} \end{aligned}$$

Pelo Teorema Chinês dos Restos, a solução geral do sistema pode ser escrita como

$$x = 2 \cdot 35 \cdot m_{35} + 6 \cdot 15 \cdot m_{15} + 2 \cdot 21 \cdot m_{21} + 105q.$$

Os inteiros $m_{35}$, $m_{15}$ e $m_{21}$ são determinados como soluções das congruências:

$$\begin{aligned} 35 \cdot m_{35} &\equiv 1 \pmod{3} \\ 15 \cdot m_{15} &\equiv 1 \pmod{7} \\ 21 \cdot m_{21} &\equiv 1 \pmod{5} \end{aligned}$$

Resolvendo cada uma das congruências anteriores, podemos obter $m_{35} = 2$, $m_{15} = 1$ e $m_{21} = 1$. Daí,

$$\begin{aligned} x &= 2 \cdot 35 \cdot 2 + 6 \cdot 15 \cdot 1 + 2 \cdot 21 \cdot 1 \pmod{105} \\ &\equiv 62 \pmod{105}. \end{aligned}$$

**5.** Podemos reduzir o sistema a um sistema linear encontrando soluções para cada uma das congruências. Por exemplo, se $x \equiv 2 \pmod{5}$, então $x^2 \equiv -1 \pmod{5}$. Daí, como queremos apenas encontrar infinitas soluções, iremos substituir a primeira congruência por $x \equiv 2 \pmod{5}$. Fazendo o mesmo com as outras duas, obtemos o seguinte sistema:

$$\begin{aligned} x &\equiv 2 \pmod{5}. \\ x &\equiv 4 \pmod{17}. \\ x &\equiv 16 \pmod{257}. \end{aligned}$$

É importante enfatizar que ele não é *equivalente* ao sistema anterior, pois $x \equiv -2 \pmod{5}$ também satisfaz $x^2 \equiv -1 \pmod{5}$. O relevante é que toda solução do último sistema também satisfaz o sistema inicial. Como o $mdc(5,17) = mdc(5,257) = mdc(17,257) = 1$, podemos usar o Teorema Chinês dos Restos para concluir que o sistema anterior possui infinitas soluções.

**6.** Supondo que o sistema possui solução, temos as seguintes equações:

$$\begin{aligned} x &= 6q_1 + 2 \\ x &= 8q_2 + 3. \end{aligned}$$

Daí, subtraindo uma equação da outra, obtemos $0 = 2(4q_2 - 3q_1) + 1$. Como o membro direito da equação é um número ímpar, temos uma contradição.

**7.** Supondo que o sistema possui solução, temos as seguintes equações:

$$\begin{aligned} x &= 6q_1 + 1 \\ x &= 8q_2 + 7. \end{aligned}$$

Daí, subtraindo uma equação da outra, obtemos $0 = 2(4q_2 - 3q_1 + 3)$. Basta que $4q_2 = 3(q_1 - 1) = 0$. Como $mdc(4,3) = 1$, devemos ter $q_2 = 3t$, ou seja, $q_1 = 4t + 1$. Assim,

$$\begin{aligned} x &= 6q_1 + 1 \\ &= 24t + 7 \\ x &= 8q_2 + 7 \\ &= 24(t+1) + 7 \end{aligned}$$

Assim, $x$ deixa resto 7 por 24 e é fácil verificar que quando isso ocorre as duas congruências anteriores são satisfeitas.

**8.** Pelo exercício anterior, as duas primeiras congruências podem ser substituídas por $x \equiv 7 \pmod{24}$. Portanto, basta decidir se o sistema:

$$\begin{aligned} x &\equiv 7 \pmod{24} \\ x &\equiv a \pmod{15} \end{aligned}$$

Possui solução. As duas congruências anteriores nos dizem que:

$$\begin{aligned} x &= 24q_1 + 7 \\ x &= 15q_2 + a. \end{aligned}$$

Daí, $0 = 3(8q_1 - 5q_2) + (7 - a)$. Essa equação possui solução se, e somente se, $3 \mid (7 - a)$. Um possível valor é $a = 1$. Neste caso, teremos

$$\begin{aligned} 0 &= 3(8q_1 - 5q_2) + (7 - a) \\ &= (8q_1 - 5q_2 + 2) \\ 5q_2 &= 2(4q_1 + 1). \end{aligned}$$

Assim, como $mdc(5,2) = 1$, segue que $4q_1 + 1 = 5t$ e $q_2 = 2t$. Como $5 \equiv 1 \pmod 4$, para que $4q_1 + 1 = 5t$, devemos ter $t = 4l + 1$, ou seja, $q_1 = 5l + 1$ e daí $x = 120l + 31$. É fácil verficiar que tal $x$ satisfaz as congruências:

$$\begin{aligned} x &\equiv 1 \pmod 6 \\ x &\equiv 7 \pmod 8 \\ x &\equiv 1 \pmod{15} \end{aligned}$$

**9.** Pelo Teorema Chinês dos Restos, a solução geral do sistema pode ser escrita como

$$x = 2 \cdot 143 \cdot m_{143} + 7 \cdot 130 \cdot m_{130} + 5 \cdot 110 \cdot m_{110} + 1430q.$$

Os inteiros $m_{143}$, $m_{130}$ e $m_{110}$ são determinados como soluções das congruências:

$$\begin{aligned} 143 \cdot m_{143} &\equiv 1 \pmod{10} \\ 130 \cdot m_{130} &\equiv 1 \pmod{11} \\ 110 \cdot m_{110} &\equiv 1 \pmod{13} \end{aligned}$$

Resolvendo cada uma das congruências anteriores, podemos obter $m_{143} = 7$, $m_{130} = 5$ e $m_{110} = 11$. Daí,

$$\begin{aligned} x &= 2 \cdot 143 \cdot 7 + 7 \cdot 130 \cdot 5 + 5 \cdot 110 \cdot 11 \pmod{1430} \\ &\equiv 1162 \pmod{1430}. \end{aligned}$$

**10.** Usando o teorema anterior com $m_1 = 5, m_2 = 7, m_3 = 11, a_1 = 5, a_2 = 7$ *e* $a_3 = 3$ podemos achar $x \equiv 887 \pmod{1001} = 7.11.13$. Como a solução é única módulo $m$, isso significa que, dentre os números $1, 2, \cdots, 1001$ a menor solução positiva é 887.

**11.** Multiplicando as três equações pelos respectivos inversos de 2, 3, e 4 com respeito aos módulos 3, 5 e 7, obtemos

$$\begin{aligned} 2 \cdot 2x &\equiv 2 \cdot 2 \pmod 3 \\ x &\equiv 1 \pmod 3 \\ 2 \cdot 3x &\equiv 2 \cdot 2 \pmod 5 \\ x &\equiv 4 \pmod 5 \\ 2 \cdot 4x &\equiv 2 \cdot 3 \pmod 7 \\ x &\equiv 6 \pmod 7 \end{aligned}$$

Daí, $x + 1$ é múltiplo de 3, 5 e 7. Portanto, $x + 1 = 105k$, para algum $k$ inteiro.

**12.** Dado $m \in \mathbb{N}$, considere o conjunto $\{p_1, p_2, \ldots, p_m\}$ de primos distintos. Como $mdc(p_i^s, p_j^s) = 1$, então pelo teorema 3, existe $x$ tal que $x \equiv -i \pmod{p_i^s}$ para $i = 1, 2, \ldots m$. Cada um dos números do conjunto $\{x+1, x+2, \ldots, x+m\}$ é divisível por um número da forma $p_i^s$.

**13.** (Extraído da Olimpíada da Estônia) Seja $n$ tal que $mdc(n, 120) = 1$. Como $120 = 3 \cdot 5 \cdot 8$, temos que $n \not\equiv 0 \pmod 3$, $\pmod 5$ $\pmod 2$. Daí, $n^2 \equiv 1 \pmod 3$, $n^2 \equiv 1 \pmod 8$ e $n^2 \equiv 1$ ou $4 \pmod 5$. Sendo assim, $n^2$ satisfaz o sistema:

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 1 \pmod 8 \\ x &\equiv \pm 1 \pmod 5 \end{aligned}$$

cujas soluções são $x \equiv 1 \pmod{120}$ e $x \equiv 49 \pmod{120}$.

**14.** (Extraído da Olimpíada dos Estados Unidos) (a) Não. Suponha que existam tais inteiros. Da nossa lista de 14 inteiros consecutivos, 7 são números pares. Vamos observar os ímpares: $a, a+2, a+4, a+6, a+8, a+10$ *e* $a+12$. Podemos ter no máximo três deles divisíveis por 3, dois por 5, um por 7 e um por 11. Veja que 3 + 2 + 1 + 1 = 7. Pelo Princípio da Casa dos Pombos, cada um desses ímpares é divisível por exatamente um primo do conjunto $\{3, 5, 7, 11\}$. Além disso, note que os múltiplos de 3 só podem ser $\{a, a+6, a+12\}$. Dois dos números restantes em $(a+2, a+4, a+8,$ *e* $a+10)$ são divisíveis por 5. Mas isso é impossível. (b) Sim. Como os números $\{210, 11, 13\}$ são primos entre si, dois a dois, pelo teorema 3 existe um inteiro positivo $n > 10$ tal que:

$$n \equiv 0(\pmod{210} = 2 \cdot 3 \cdot 5 \cdot 7 \cdot)$$

$$n \equiv 1(\pmod{11})$$

$$n \equiv -1(\pmod{13})$$

Veja que o conjunto $\{n-10, n-9, \ldots, n+9, n+10\}$ satisfaz as condições do item (b).

**15.** Seja $p$ um primo maior que $a$ e $b$. Então $mdc(p,a) = mdc(p,b) = 1$. Como $mdc(p,p-1) = 1$, existe um inteiro positivo $n$ tal que $n \equiv 1 \pmod{p-1}$ e $n \equiv -a \pmod{p}$. Pelo teorema de Fermat, $a^n + n \equiv 0 \pmod{\ }$ e $b^n + n \equiv b - a \pmod{p}$. Assim, $p \mid |b-a|$. Como $|b-a| < p$, segue que $|b-a| = 0$ e $a = b$.

Produzido por Arquimedes Curso de Ensino
contato@cursoarquimedes.com