Teorema Chinês dos Restos

Sistema de Congruências

Tópicos Adicionais

Teorema Chinês dos Restos
Sistema de Congruências

1 Exercícios Introdutórios

Exercício 1. Para cada um dos itens abaixo, encontre todos os inteiros $a \in \{1, 2, 3, \ldots, 10\}$ de modo que:

(a) $2a \equiv 1 \pmod 3$

(b) $3a \equiv 1 \pmod 5$

(c) $5a \equiv 1 \pmod 7$

Exercício 2. Sabendo que $3 \cdot 7 - 4 \cdot 5 = 1$, encontre um inteiro a tal que:

(a) $7a \equiv 1 \pmod 5$

(b) $7a \equiv 2 \pmod 5$

Exercício 3. Encontre a e b tais que $141a + 17b = 1$ e, sem seguida, encontre um inteiro x que satisfaça

$$141x \equiv 1 \pmod{17}$$

Exercício 4. Resolva o sistema:

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

Exercício 5. Encontre uma solução inteira para o sistema:

$$\begin{cases} x \equiv 2 \pmod{11} \\ x \equiv 4 \pmod{12} \\ x \equiv 5 \pmod{13} \end{cases}$$

2 Exercícios de Fixação

Exercício 6. Resolva, quando possível, as congruências:

(a) $3x \equiv 5 \pmod 7$.

(b) $12x \equiv 38 \pmod{28}$.

Exercício 7. Encontre x inteiro tal que:

$$\begin{aligned} x &\equiv 1 \pmod{11}; \\ x &\equiv 2 \pmod 7. \end{aligned}$$

Exercício 8. Encontre x inteiro tal que:

$$\begin{aligned} x &\equiv 1 \pmod{11} \\ x &\equiv 2 \pmod 7 \\ x &\equiv 4 \pmod 5 \end{aligned}$$

Exercício 9. Encontre o menor inteiro positivo, maior que 1, que satisfaz o seguinte sistema de congruências:

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

Exercício 10. Encontre todas as soluções do sistema:

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

3 Exercícios de Aprofundamento e de Exames

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. Juca possui menos do que 800 bolinhas de gude. Ele gosta de separar as bolinhas em grupinhos com a mesma quantidade de bolinhas. Ele percebeu que se formar grupinhos com 3 bolinhas cada, sobram exatamente 2 bolinhas. Se ele formar grupinhos de 4 bolinhas, sobram 3 bolinhas. Se ele formar grupinhos de 5 bolinhas, sobram 4 bolinhas. E, finalmente, se ele formar grupinhos com 7 bolinhas cada, sobram 6 bolinhas.

(a) Se Juca formasse grupinhos com 20 bolinhas cada, quantas bolinhas sobrariam?

(b) Juca possui quantas bolinhas de gude?

Exercício 13. Sejam m e n dois inteiros positivos primos entre si. O Teorema Chinês dos Restos afirma que, dados inteiros i e j com $0 \leq i < m$ e $o \leq j < n$, existe exatamente um inteiro a, com $0 \leq a < mn$, tal que o resto da divisão de a por m é igual a i e o resto da divisão de a por n é igual a j. Por exemplo, para $m = 3$ e $n = 7$, temos que 19 é o único número que deixa restos 1 e 5 quando dividido por 3 e 7, respectivamente. Assim, na tabela a seguir, cada número de 0 a 20 aparecerá exatamente uma vez.

	0	1	2	3	4	5	6
0		A				B	
1				C			D
2		E			F		

Qual a soma dos números das casas com as letras A, B, C, D, E e F?

Exercício 14. Determine todos os restos possíveis da divisão do quadrado de um número primo com 120 por 120.

Exercício 15. Encontre todos os inteiros que deixam restos $1, 2$ e 3 quando divididos por $3, 4$ e 5, respectivamente.

Respostas e Soluções.

1. Testando os valores do conjunto dado, obtemos

(a) $a = 2, 5$ e 8.

(b) $a = 2$ e 7.

(c) $a = 3$ e 10

2.

(a) Em virtude da equação dada, $7 \cdot 3 \equiv 1 \pmod 5$, portanto $a = 3$ é uma solução possível

(b) Multiplicando a equação dada por 2, temos

$$6 \cdot 7 \equiv 8 \cdot 5 = 2$$

Daí, $7 \cdot 6 \equiv 2 \pmod 5$ e assim $a = 6$ é uma solução possível.

3. Aplicando o Algoritmo de Euclides, obtemos a sequência de equações:

$$\begin{aligned} 141 &= 17 \cdot 8 + 5 \\ 17 &= 5 \cdot 3 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 1 \cdot 2 + 0. \end{aligned}$$

Daí,

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - (17 - 5 \cdot 3) \cdot 2 \\ &= 5 \cdot 7 - 17 \cdot 2 \\ &= (141 - 17 \cdot 8) \cdot 7 - 17 \cdot 2 \\ &= 141 \cdot 7 - 17 \cdot 58 \end{aligned}$$

Portanto,

$$141 \cdot 7 \equiv 1 \pmod{17}$$

e $a = 7$ é uma solução.

4. A primeira congruência nos permite concluir que $x = 5q + 3$. Daí

$$\begin{aligned} 5q + 3 &\equiv 4 \pmod 7 \\ 5q &\equiv 1 \pmod 7 \\ 15q &\equiv 3 \pmod 7 \\ q &\equiv 3 \pmod 7. \end{aligned}$$

Assim, $q = 3 + 7k$ e

$$\begin{aligned} x &= 5q + 3 \\ &= 5(3 + 7k) + 3 \\ &= 35k + 18, \end{aligned}$$

para algum inteiro k.

5. A primeira equação nos diz que $x = 11q + 2$. Substituindo este valor na segunda equação, encontramos:

$$11q + 2 \equiv 4 \pmod{12}$$

Daí, como $11 \cdot 11 \equiv 1 \pmod{12}$, podemos multiplicar a congruência anterior por 11 para obter

$$\begin{aligned} 11 \cdot 11q + 22 &\equiv 44 \pmod{12} \\ q + 22 &\equiv 8 \pmod{12} \end{aligned}$$

Daí, $q + 22 = 8 + 12k$. Isso implica

$$\begin{aligned} x &= 11(8 + 12k - 22) + 2 \\ &= 132k - 154 + 2 \\ &\equiv 5 \pmod{13} \end{aligned}$$

Daí,

$$\begin{aligned} 132k &\equiv 154 + 5 - 2 \pmod{13} \\ 2k &\equiv 1 \pmod{13} \\ 14k &\equiv 7 \pmod{13}. \\ k &\equiv 7. \end{aligned}$$

e assim $k = 9 + 13t$. Logo,

$$\begin{aligned} x &= 11q + 2 \\ &= 11(12k - 14) + 2 \\ &= 132k - 154 + 2 \\ &= 132(8 + 13t) - 154 + 2 \\ &= 1716t + 924 - 154 + 2 \\ &= 1716t + 772 \end{aligned}$$

e $x = 772$ é uma solução do sistema.

6.

(a) Multiplicando a primeira equação por 5, que é o inverso de 3 módulo 7, obtemos

$$\begin{aligned} 3x &\equiv 5 \pmod 7 \\ 15x &\equiv 25 \pmod 7 \\ x &\equiv 4 \pmod 7 \end{aligned}$$

Daí, $x = 7k + 4$ para algum inteiro k

(b) Se a congruência tivesse alguma solução, poderíamos escrever, para algum inteiro k,

$$\begin{aligned} 12x &= 38 + 28k \\ 4(3x - 7k) &= 38. \end{aligned}$$

Isso é impossível, pois 38 não é múltiplo de 4.

7. A primeira congruência nos diz que $x = 11k + 1$ para algum $k \in \mathbb{Z}$. Sejam q e r o quociente e o resto da divisão de k por 7, respectivamente. Assim, $k = 7q + r$ e $x = 77q + 11r + 1$. Para x satisfazer a segunda congruência, devemos encontrar $r \in \{0, 1, 2, 3, 4, 5, 6\}$ tal que $11r + 1 \equiv 2 \pmod 7$, ou seja, $4r \equiv 1 \pmod 7$. Como o inverso de $4 \pmod 7$ é 2, obtemos $r = 2$ e $x = 77q + 23$. Veja que para qualquer q inteiro, tal x é solução do sistema de congruências.

8. Pelo exemplo anterior, para x satisfazer as duas primeiras equações, devemos ter $x = 77q + 23$. Dividindo q por 5, obtemos $q = 5l + s$ com $0 \leq s < 5$. Daí, $x = 385l + 77s + 23$. Para satisfazer a última congruência, devemos ter $77s + 23 \equiv 4 \pmod 5$, ou seja, $2s \equiv 1 \pmod 5$. Como 3 é o inverso de 2 (mod 5), $s = 3$ e consequentemente $x = 385l + 254$.

9. Veja que $x - 1$ deve ser um múltiplo positivo de $3, 5$ e 7. O menor múltiplo positivo desses números é $3 \cdot 5 \cdot 7 = 105$. Logo, $x = 105 + 1 = 106$.

10. A primeira congruência nos diz que $x = 3k + 2$, para algum inteiro k. Daí,

$$\begin{aligned} 3k + 2 &\equiv 3 \pmod 5 \\ 3k &\equiv 1 \pmod 5 \\ 6k &\equiv 2 \pmod 5 \\ k &\equiv 2 \pmod 5. \end{aligned}$$

Isso nos permite escrever $k = 5t + 2$, para algum inteiro t. Substituindo na última equação, temos

$$\begin{aligned} x &= 3k + 2 \\ &= 3(5t + 2) + 2 \\ &= 15t + 8 \\ &\equiv 5 \pmod 2 \end{aligned}$$

Assim

$$\begin{aligned} 15t + 8 &\equiv 5 \pmod 2 \\ t &\equiv 1 \pmod 2 \end{aligned}$$

Finalmente, isso nos permite escrever $t = 2l + 1$, para algum inteiro l, e

$$\begin{aligned} x &= 15t + 8 \\ &= 15(2l + 1) + 8 \\ &= 30l + 23. \end{aligned}$$

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. (Extraído do Banco de Problema da OBMEP)

(a) Seja B o número de bolinhas de Juca. Veja que o número de bolinhas que sobram ao formar um grupinho é igual ao resto da divisão de B pelo tamanho dos grupinhos. Para determinar o resto na divisão por 20, deve-se utilizar os restos na divisão por 4 e por 5, já que $20 = 4 \cdot 5$. Suponha que seja dada uma bola a mais para Juca. Sabendo que com com grupinhos de 5 bolinhas sobram 4 bolinhas e em grupinhos de 4 sobram 3, então Juca pode dividir as $B + 1$ bolas em grupinhos de 4 bolas e em grupinhos de 5 bolas sem sobrar nenhuma, logo $B + 1$ é múltiplo de $4 \cdot 5 = 20$, já que este é o Mínimo Múltiplo Comum entre 4 e 5. Portanto, B deixa resto 19 na divisão por 20. Assim, sobrariam 19 bolinhas.

(b) Para cada um dos números do conjunto $\{3, 4, 5, 7\}$, o resto na divisão é uma unidade a menos que o tamanho dos grupinhos. Deste modo, se adicionarmos uma bola a mais na coleção de Juca, teremos um número $B + 1$ que é múltiplo de 3, 4, 5 e 7, consequentemente, $B + 1$ é múltiplo do Mínimo Múltiplo Comum destes quatro números, ou seja, múltiplo de $3 \cdot 4 \cdot 5 \cdot 7 = 420$. Como Juca possui menos que 800 bolinhas, então $B + 1 = 420$ e assim concluímos que $B = 419$.

13. (Extraído da OBM 2009) Resolvendo os sistemas de congruências correspondentes, podemos encontrar $A = 15, B = 12, C = 10, D = 13, E = 8$ e $F = 11$. Assim, $A + B + C + D + E + F = 69$.

14. (Extraído da Olimpíada da Estônia) Seja n tal que $mdc(n, 120) = 1$. Como $120 = 3 \cdot 5 \cdot 8$, temos que $n \not\equiv 0$ (mod 3), (mod 5) (mod 2). Daí, $n^2 \equiv 1 \pmod 3$, $n^2 \equiv 1$ (mod 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 $x \equiv 49 \pmod{120}$.

15. Se x é o inteiro procurado, devemos ter:

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 1 \pmod 4 \\ x &\equiv 1 \pmod 5. \end{aligned}$$

Daí, $x + 2$ é múltiplo de $3, 4$ e 5, ou seja, $x + 2 = 100q$m para algum inteiro q.

Produzido por Arquimedes Curso de Ensino
contato@cursoarquimedes.com