24ª Semana Olímpica
Nível 2
Profª. Kellem Corrêa Santos

Teorema Chinês dos Restos

Teorema de Bézout: Sejam *a* e *b* inteiros positivos. Então, existem inteiros *x* e *y* tais que

$$ax + by = mdc(a, b)$$

Teorema Chinês dos Restos (versão limitada): Sejam *m* e *n* dois inteiros maiores que 1 primos entre si e *a* e *b* dois outros inteiros quaisquer. Então, o sistema abaixo tem solução **única módulo *m.n***:

$$\begin{cases} x \equiv a \ (mod\ m) \\ x \equiv b \ (mod\ n) \end{cases}$$

Corolário: Sejam *m* e *n* dois inteiros maiores que 1 primos entre si e *a* e *b* dois outros inteiros quaisquer. Então, $x \equiv a \ (mod\ mn)$ se, e somente se, ambas as congruências abaixo são válidas:

$$\begin{cases} x \equiv a \ (mod\ m) \\ x \equiv b \ (mod\ n) \end{cases}$$

Aquecimento 1: Resolva o sistema

$$\begin{cases} x \equiv 1 \ (mod\ 2) \\ x \equiv 5 \ (mod\ 5) \end{cases}$$

Aquecimento 2: Resolva o sistema

$$\begin{cases} x \equiv 2 \ (mod\ 4) \\ x \equiv 3 \ (mod\ 6) \end{cases}$$

Aquecimento 3: Resolva o sistema

$$\begin{cases} x \equiv 0 \ (mod\ 4) \\ x \equiv 0 \ (mod\ 6) \end{cases}$$

Teorema Chinês dos Restos (versão completa): Sejam $m_1, m_2, \dots, m_k$ inteiros maiores que 1 dois a dois primos entre si e $a_1, a_2, \dots, a_k$ inteiros quaisquer. Então, o sistema abaixo tem solução **única módulo $\boldsymbol{m_1 m_2 \dots m_k}$:**

$$\begin{cases} x \equiv a_1 \ (mod\ m_1) \\ \dots \\ x \equiv a_k \ (mod\ m_k) \end{cases}$$

O Teorema Chinês dos Restos garante a existência e a unicidade da solução, porém, não ensina como encontrá-la. É possível provar que a solução é construída da seguinte forma:

$$x \equiv a_1 M_1 x_1 + \ a_2 M_2 x_2 + \dots + a_k M_k x_k (mod\ M)$$

onde
$M = m_1 m_2 \dots m_k$,
$M_i = \frac{M}{m_i}$,
x_i é tal que $M_i x_i \equiv 1 \ (mod\ m_i)$.

Exercícios:

1) Resolva $\begin{cases} x \equiv 2\ (mod\ 3) \\ x \equiv 3\ (mod\ 5) \\ x \equiv 2\ (mod\ 7) \end{cases}$

2) Resolva $\begin{cases} x \equiv 1 (mod\ 2) \\ x \equiv 1 (mod\ 3) \\ x \equiv 1 (mod\ 4) \\ x \equiv 1 (mod\ 5) \\ x \equiv 1 (mod\ 6) \\ x \equiv 0 (mod\ 7) \end{cases}$

3) Resolva $x^2 \equiv 11 (mod\ 35)$

4) Resolva $\begin{cases} x \equiv 1\ (mod\ 3) \\ x \equiv 4\ (mod\ 5) \\ x \equiv 1\ (mod\ 7) \end{cases}$

5) Resolva $\begin{cases} x \equiv 1\ (mod\ 4) \\ x \equiv 7\ (mod\ 9) \\ x \equiv 6\ (mod\ 11) \end{cases}$

6) (Estônia) Determine todos os restos possíveis da divisão do quadrado de um número primo com 120 por 120.

7) (USA) Existem 14 inteiros positivos consecutivos tais que cada um é divisível por um ou mais primos p do intervalo $2 \leq p \leq 11$?

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

9) (São Petesburgo) Dado um polinômio F(x) com coeficientes inteiros tal que, para cada inteiro n, o valor de F(n) é divisível por pelo menos um dos inteiros $a_1, a_2, \ldots, a_m$. Prove que podemos encontrar um índice k tal que F(n) é divisível por a_k para cada inteiro n.

10) (Olimpíada Nórdica) Para quais inteiros positivos n existe uma sequência $x_1, x_2, \ldots, x_n$ contendo cada um dos inteiros 1, 2, ..., n exatamente uma vez e tal que k divide $x_1 + x_2 + \cdots + x_k$ para k = 1, 2, ..., n?

11) (USA) Encontre o menor inteiro positivo *n* tal que $2^n + 5^n - n$ é múltiplo de 1000.

12) (Bulgária) Encontre o menor valor positivo para *x* tal que, quando dividido por 7, 9 e 11, deixa restos 3, 4 e 5, respectivamente.

13) (China) Suponha que p varia entre todos os primos maiores que 5. Quantos restos distintos possíveis existem na divisão de p^2 por 120?

14) (China) Seja N um número que, na base 6, é escrito como 531340. Já na base 8, N vale 124154. Na base 10, qual o resto de N na divisão por 210?