O Teorema Chinês dos Restos

Teorema: Sejam $m_1, m_2, \cdots, m_k$ inteiros positivos primos dois a dois (ou seja, se $1 \leq i < j \leq k$ então $mdc(m_i, m_j) = 1$) e $M = \prod_{i=1}^{k} m_i$. Então, dados $a_1, a_2, \cdots, a_k$ quaisquer, o sistema de congruências

$$\begin{cases} x \equiv a_1 & \mod m_1 \\ x \equiv a_2 & \mod m_2 \\ \vdots & \\ x \equiv a_k & \mod m_k \end{cases}$$

tem solução que é única módulo M.

Aplicação à resolução de equações

$$327x \equiv 171 \mod 520$$

$$\Leftrightarrow$$

$$\begin{cases} 327x \equiv 171 \mod 5 \\ 327x \equiv 171 \mod 8 \\ 327x \equiv 171 \mod 13 \end{cases}$$

Aplicação à resolução de equações

$$327x \equiv 171 \mod 520$$

$\Leftrightarrow$

$$\begin{cases} 327x \equiv 171 \mod 5 \\ 327x \equiv 171 \mod 8 \\ 327x \equiv 171 \mod 13 \end{cases} \Leftrightarrow \begin{cases} 2x \equiv 1 \mod 5 \\ 7x \equiv 3 \mod 8 \\ 2x \equiv 2 \mod 13 \end{cases}$$

Aplicação à resolução de equações

$$327x \equiv 171 \mod 520$$

$$\Leftrightarrow$$

$$\begin{cases} 327x \equiv 171 \mod 5 \\ 327x \equiv 171 \mod 8 \\ 327x \equiv 171 \mod 13 \end{cases} \Leftrightarrow \begin{cases} 2x \equiv 1 \mod 5 \\ 7x \equiv 3 \mod 8 \\ 2x \equiv 2 \mod 13 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} x \equiv 3 \mod 5 \\ x \equiv 5 \mod 8 \\ x \equiv 1 \mod 13 \end{cases}$$

Teorema Chinês dos Restos

$$\begin{cases} x \equiv a_1 & \mod m_1 \\ x \equiv a_2 & \mod m_2 \\ \vdots & \\ x \equiv a_k & \mod m_k \end{cases}$$

Se, para cada $i \leq k$,

$$\frac{M}{m_i} b_i \equiv 1 \mod m_i$$

a solução do sistema é

$$x \equiv \sum_{i=1}^{k} \frac{M}{m_i} b_i a_i \mod M$$

Exemplo:

$$\begin{cases} x^2 \equiv 2 & \mod 7 \\ x^3 \equiv 1 & \mod 9 \\ x^4 \equiv 3 & \mod 11 \end{cases}$$

A primeira equação tem soluções 3 e 4 módulo 7,

A segunda equação tem soluções 1, 4 e 7 módulo 9,

A tereceira equação tem soluções 4 e 7 módulo 11,

Teríamos que resolver 12 sistemas de 3 equações

Exemplo (continuação)

$M = 7 \times 9 \times 11 = 693;$

$$\frac{M}{7} b_1 \equiv 1 \mod 7 \Leftrightarrow 99 b_1 \equiv 1 \mod 7$$

Exemplo (continuação)

$M = 7 \times 9 \times 11 = 693$;

$$\frac{M}{7} b_1 \equiv 1 \mod 7 \Leftrightarrow 99 b_1 \equiv 1 \mod 7 \Leftrightarrow b_1 \equiv 1 \mod 7$$

E, de modo semelhante,

$$b_2 \equiv 2 \mod 9, \qquad b_3 \equiv 7 \mod 11$$

Substituindo os valores dos a_i na expressão

$$\sum_{i=1}^{3} \frac{M}{m_i} b_i a_i = 99a_1 + 154a_2 + 441a_3$$

obtemos as 12 soluções

Teorema Chinês dos Restos

Se $M = m_1 \times \cdots \times m_k$ e $mdc(m_i, m_j) = 1$ se $i \neq j$, então a aplicação

$$\psi : \mathbb{Z}_{/M} \to \mathbb{Z}_{/m_1} \times \cdots \times \mathbb{Z}_{/m_k}$$

definida por

$$\psi(a) = (a \mod m_1, \cdots, a \mod m_k)$$

é uma bijecção.

A inversa de ψ é dada por

$$\psi^{-1}(a_1, \cdots, a_k) \equiv \sum_{i=1}^{k} \frac{M}{m_i} b_i a_i \mod M$$