Sistemas de congruências lineares

Definição Chama-se sistema de congruências lineares a um sistema do tipo

$$\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ \vdots \\ a_k x \equiv b_k \pmod{n_k} \end{cases} \qquad (S)$$

onde $k \in \mathbb{N} \setminus \{1\}$, $a_i, b_i \in \mathbb{Z}$, $n_i \in \mathbb{N}$ $(i = 1, 2, \ldots, k)$

Nota: Dois sistemas de congruências lineares dizem-se sistemas equivalentes se tiverem o mesmo conjunto de soluções

Proposição Sejam $n \in \mathbb{N}$ e $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ a decomposição de n em factores primos. Então a congruência linear $ax \equiv b \pmod{n}$

é equivalente ao sistema
$$\begin{cases} ax \equiv b \pmod{p_1^{m_1}} \\ ax \equiv b \pmod{p_2^{m_2}} \\ \vdots \\ ax \equiv b \pmod{p_k^{m_k}} \end{cases} \quad (*)$$

<u>Demonst:</u> Sup. que x_0 é solução de $ax \equiv b \pmod{n}$. Então $n \mid ax_0 - b$. Como $p_i^{m_i} \mid n$ então, por transitividade, $p_i^{m_i} \mid ax_0 - b$. Logo $ax_0 \equiv b \pmod{p_i^{m_i}}$, para todo o $i \in \{1, .., k\}$. Reciprocamente suponhamos que x_0 é solução de $(*)$. Então, para cada i, $p_i^{m_i} \mid ax_0 - b$. Como $m.d.c(p_i^{m_i}, p_j^{m_j}) = 1$, para $i \neq j$, então $p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} \mid ax_0 - b$, ou seja, x_0 é solução da congruência linear $ax \equiv b \pmod{n}$

$\square$

Exemplo Pretende-se resolver a congruência $17x \equiv 9 \pmod{276}$

Como m.d.c$(17, 276) = 1$ então $17x \equiv 9 \pmod{276}$ tem uma e uma só solução módulo 276. Temos $276 = 2^2 \times 3 \times 23$.

Pela prop. anterior $17x \equiv 9 \pmod{276}$ é equivalente ao sistema

$$\begin{cases} 17x \equiv 9 \pmod 4 \\ 17x \equiv 9 \pmod 3 \\ 17x \equiv 9 \pmod{23} \end{cases}$$

$17x \equiv 9 \pmod 4 \iff 17x \equiv 1 \pmod 4$ $\quad (4 \mid 9-1)$

$\iff 16x + x \equiv 1 \pmod 4$ $\quad$ (pois $4 \mid 16$)

$\iff x \equiv 1 \pmod 4$

$17x \equiv 9 \pmod 3 \iff 17x \equiv 0 \pmod 3$ $\quad$ (pois $3 \mid 9$)

$\iff x \equiv 0 \pmod 3$ $\quad$ (m.d.c$(3, 17) = 1$)

O sistema é equivalente a $\begin{cases} x \equiv 0 \pmod 3 \\ x \equiv 1 \pmod 4 \\ 17x \equiv 9 \pmod{23} \end{cases}$

$x \equiv 0 \pmod 3 \iff x = 3k$ com $k \in \mathbb{Z}$

$x \equiv 1 \pmod 4 \iff 3k \equiv 1 \pmod 4$

$\iff 9k \equiv 3 \pmod 4$

$\iff 8k + k \equiv 3 \pmod 4$

$\iff k \equiv 3 \pmod 4$ (pois $4 \mid 8$)

$\iff k = 3 + 4l, \quad l \in \mathbb{Z}$

Então $x = 3k \iff x = 3(3+4l) \iff x = 9 + 12l$

$17x \equiv 9 \pmod{23} \iff 17 \times (9 + 12l) \equiv 9 \pmod{23}$

$\iff 17 \times 12 \times l \equiv 9 - 17 \times 9 \pmod{23}$

$\Leftrightarrow \quad 17 \times 12 l \equiv (-16) \times 9 \pmod{23}$

$\Leftrightarrow \quad 17 l \equiv -4 \times 3 \pmod{23}$ (lei do corte)

$\Leftrightarrow \quad 17 l \equiv -12 \pmod{23}$

$\Leftrightarrow \quad 17 l \equiv -12 \pmod{23}$

$\Leftrightarrow \quad 23 l - 6 l \equiv -12 \pmod{23}$

$\Leftrightarrow \quad -6 l \equiv -12 \pmod{23}$

$\Leftrightarrow \quad l \equiv 2 \pmod{23}$ (m.d.c $(6, 23) = 1$)

$\Leftrightarrow \quad l = 2 + t\,23, \quad t \in \mathbb{Z}$

$x = 9 + 12 l \Leftrightarrow x = 9 + 12(2 + 23t) =$

$= 33 + 12 \times 23 t = 33 + 276 t$

Logo $x \equiv 33 \pmod{276}$ e 33 é a única solução de $17x \equiv 9 \pmod{276}$.

O Teorema Chinês dos restos permite-nos resolver este tipo de sistema de forma mais rápida e eficaz.

<u>Teorema</u> (teorema chinês dos restos)

Sejam $k \in \mathbb{N} \setminus \{1\}$, $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ e $n_1, n_2, \ldots, n_k \in \mathbb{N}$ tais que $(\forall i, j \in \{1, \ldots, k\},\ i \neq j \Rightarrow m.d.c(n_i, n_j) = 1)$

Então o sistema de congruências lineares

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

tem uma e uma só solução módulo $n = n_1 n_2 \cdots n_k$.

A solução $x_0 \pmod{n}$ é dada por:

$$x_0 = x_1 N_1 a_1 + x_2 N_2 a_2 + \dots + x_k N_k a_k$$

onde $N_i = \dfrac{n}{n_i}$ e x_i é solução de $N_i x \equiv 1 \pmod{n_i}$.

<u>Demonst:</u> Como, para $i \neq j$, n_i e n_j são primos entre si ou seja, $m.d.c(n_i, n_j) = 1$ então também se tem que $m.d.c\left(N_i, n_i\right) = 1$ e assim a congruência linear $N_i x \equiv 1 \pmod{n_i}$ tem uma e uma só solução módulo n_i. Seja ela x_i. Vamos provar que

$$x_0 = x_1 N_1 a_1 + x_2 N_2 a_2 + \dots + x_k N_k a_k$$

é solução do sistema.

Observamos que para $r, i \in \{1, 2, \dots, k\}$ com $r \neq i$ como $n_r \mid N_i$ então $N_i \equiv 0 \pmod{n_r}$ e portanto

$$x_0 = x_1 N_1 a_1 + x_2 N_2 a_2 + \dots + x_k N_k a_k$$

$$\equiv a_r N_r x_r \pmod{n_r}$$

Como x_r é tal que $N_r x \equiv 1 \pmod{n_r}$ então

$$x_0 \equiv a_r \pmod{n_r}.$$

Portanto x_0 é solução do sistema. Vejamos que é única módulo $n = n_1 n_2 \dots n_k$.

Suponhamos que x' é outra solução do sistema. Então

$$x_0 \equiv x' \pmod{n_r}$$

para todo o $r \in \{1, 2, \dots, k\}$. Logo $n_r \mid x_0 - x'$ como

$m.d.c(n_r, n_s) = 1$ com $r \neq s$ então $n \mid x_0 - x'$ e

$x' \equiv x_0 \pmod{n}$. $\square$

Teorema

Sejam $k \in \mathbb{N} \setminus \{1\}$, $a_1, a_2, \dots, a_k \in \mathbb{Z}$ e $n_1, n_2, \dots, n_k \in \mathbb{N}$.

Então
$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

tem solução sse $m.d.c(n_i, n_j) \mid (a_j - a_i)$ $\forall i, j \in \{1, \dots, k\}$

Além disso a solução é única módulo n onde n é o mínimo múltiplo comum de $n_1, n_2, \dots, n_k$.

Demonst: Ver sebenta $\square$

Nota: O Teorema chinês dos restos é um caso particular do teorema anterior.

Exemplo: Problema: encontrar um número inteiro que tem resto 2, 3 e 2 na divisão por 3, 5 e 7, respetivamente.

Queremos determinar x tal que
$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

Os números 3, 5 e 7 são primos logo primos entre si.

Podemos aplicar o teorema chinês dos restos.

Seja $n = 3 \times 5 \times 7 = 105$. O sistema tem uma única solução módulo 105, construída da seguinte forma

$$x_0 = x_1 N_1 a_1 + x_2 N_2 a_2 + x_3 N_3 a_3$$

onde $N_1 = \frac{n}{n_1} = 5 \times 7$, $N_2 = \frac{n}{n_2} = 3 \times 7$ e $N_3 = \frac{n}{n_3} = 3 \times 5$

e x_i é tal que $N_i x_i \equiv 1 \pmod{n_i}$

$$35 x_1 \equiv 1 \pmod 3$$
$$21 x_2 \equiv 1 \pmod 5$$
$$15 x_3 \equiv 1 \pmod 7$$

$35 x_1 \equiv 1 \pmod 3 \iff 2 x_1 \equiv 1 \bmod 3 \Rightarrow x_1 = 2$

$21 x_2 \equiv 1 \pmod 5 \iff x_2 \equiv 1 \bmod 5 \Rightarrow x_2 = 1$

$15 x_3 \equiv 1 \pmod 7 \iff x_3 \equiv 1 \bmod 7 \Rightarrow x_3 = 1$

Temos assim que

$$x_0 = 2 \times 35 \times 2 + 1 \times 21 \times 3 + 1 \times 15 \times 2 = 233$$

é solução do sistema

Portanto $x_0 \equiv 233 \pmod{105} \Leftrightarrow x_0 \equiv 23 \pmod{105}$

Assim 23 é a única solução módulo 105.

Pequeno teorema de Fermat

Teorema: Se p é primo e $a \in \mathbb{Z}$ é tal que $p \nmid a$ então

$$a^{p-1} \equiv 1 \pmod{p}$$

Demonst: Ver sebenta

$\square$

Corolário Se p é primo então $a^p \equiv a \pmod{p}$, $\forall a \in \mathbb{Z}$.

Exemplos Queremos encontrar o resto da divisão de 5^{38} por 11.

Do pequeno teorema de Fermat: $5^{10} \equiv 1 \pmod{11}$

Logo $5^{30} \equiv 1^{3} \pmod{11}$. Portanto $5^{38} \equiv 5^{8} \pmod{11}$

$5^{2} \equiv 3 \pmod{11}$ logo $5^{8} \equiv 3^{4} \pmod{11}$

$5^{8} \equiv 81 \pmod{11} \iff 81 \equiv 4 \pmod{11}$

Conclusão:

$$\left.\begin{array}{l} 5^{38} \equiv 5^{8} \pmod{11} \\ 5^{8} \equiv 3^{4} \pmod{11} \\ 3^{4} \equiv 4 \pmod{11} \end{array}\right\} \Rightarrow 5^{38} \equiv 4 \pmod{11}$$

O resto da divisão de 5^{38} por 11 por 4.

Exemplo: O pequeno teorema de Fermat pode ser usado para mostrar que um número não é primo.

Vejamos que 117 não é primo. Tomamos $a = 2$ e vejamos que $2^{116} \not\equiv 1 \pmod{117}$.

Temos que $2^7 = 128$ e assim $2^7 \equiv 11 \pmod{117}$

Temos também $116 = 7 \times 16 + 4$ e assim

$$(2^7)^{16} \equiv 11^{16} \pmod{117}$$

$11^2 \equiv 4 \pmod{117}$ $\quad$ $11^{16} \equiv 4^8 \pmod{117}$

$$(2^7)^{16} \equiv 4^8 \pmod{117}$$

$$(2^7)^{16} \equiv 2^{16} \pmod{117}$$

$2^7 \equiv 11 \pmod{117}$ $\quad$ $2^{14} \equiv 11^2 \bmod 117$

$2^{14} \equiv 4 \bmod 117$

$2^{16} \equiv 16 \bmod 117$

$$(2^7)^{16} \equiv 16 \pmod{117}$$

$$2^{116} = (2^7)^{16} \times 2^2$$

$$2^{116} \equiv 16 \times 2^2 \pmod{117}$$

$$2^{116} \equiv 64 \pmod{117}$$

Logo $2^{116} \not\equiv 1 \pmod{117}$

Não se verifica o pequeno teorema de Fermat e, portanto, 117 não é primo.