5 - Congruências Lineares

Congruências lineares

Dados $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}$ com $a \neq 0$, queremos encontrar todos os inteiros $x \in \mathbb{Z}$ tais que:

$$a\,x \equiv_n b$$

Esta expressão diz-se uma congruência linear (ou do 1º grau) na incógnita x.

Exemplo : A congruência linear

$$3\,x \equiv_7 5$$

tem solução, por exemplo: $x = 4$

Note-se que todos os elementos de $[4]_7 = \{\cdots, -10, -3, 4, 11, 18, \cdots\}$ são também solução. Basta-nos portanto procurar as soluções num sistema completo de resíduos módulo 7, por exemplo: $\{0, 1, 2, 3, 4, 5, 6\}$.

Congruências lineares - existência de solução

Sabemos que

$$a\,x \equiv_n b \iff n | a\,x - b$$

ou seja existe $y \in \mathbb{Z}$ tal que

$$a\,x - b = n\,y \quad \iff \quad a\,x - n\,y = b$$

Logo

$$a\,x \equiv_n b \;\; \text{tem solução} \quad \iff \quad a\,x - n\,y = b \;\; \text{tem solução}$$

Teorema

Dados $n \in \mathbb{N}$ *e* $a, b \in \mathbb{Z}$ *com* $a \neq 0$,

$$a\,x \equiv_n b \;\; \textit{tem solução} \quad \iff \quad \textit{m.d.c.}(a, n) | b$$

Congruências lineares - unicidade da solução

Se a congruência linear

$$a\,x \equiv_n b$$

tem solução então m.d.c.$(a, n)|b$ e portanto

$$\text{m.d.c.}(a, n)|b \quad \wedge \quad \text{m.d.c.}(a, n)|a \quad \wedge \quad \text{m.d.c.}(a, n)|n$$

Logo podemos (e devemos!) dividir a, b, n por m.d.c.(a, n) de forma a obter uma congruência linear equivalente, onde o módulo e o coeficiente da incógnita são primos entre si.

Exemplo : A congruência

$$33\,x \equiv_{45} 18$$

tem solução pois m.d.c.$(33, 45) = 3|18$. Logo, dividindo por 3, temos:

$$33\,x \equiv_{45} 18 \quad \Leftrightarrow \quad 11\,x \equiv_{15} 6$$

Congruências lineares - unicidade da solução

Se m.d.c.$(a, n) = 1$ a congruência linear

$$a\, x \equiv_n b$$

tem solução e pela equação diofantina

$$a\, x - n\, y = b$$

sabemos que, dada uma solução x_0, a solução geral para a incógnita x, é dada por:

$$x = x_0 + n\, k \quad \text{com} \;\; k \in \mathbb{Z} \qquad \text{ou seja} \qquad x = [x_0]_n$$

Teorema

Seja $a\, x \equiv_n b$ uma congruência linear. Se m.d.c.$(a, n) = 1$ então a congruência linear tem exactamente uma classe de congrência módulo n como solução.

Congruências lineares - Exemplo

$$33\,x \equiv_{45} 18 \qquad \Leftrightarrow \qquad 11\,x \equiv_{15} 6$$

Como m.d.c.$(11, 15) = 1$ a congruência tem exactamente uma solução módulo 15 e portanto basta procurar a única solução num sistema completo de resíduos módulo 15, por exemplo:

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$$

Como $x_0 = 6$ é solução da congruência, a solução geral é dada por:

$$x = [6]_{15} = 6 + 15\,k \quad \text{com} \quad k \in \mathbb{Z}$$

Note-se que a congruência linear tem 3 soluções módulo 45:

$$x = [6]_{45} \qquad \vee \qquad x = [21]_{45} \qquad \vee \qquad x = [36]_{45}$$

Resolução de Congruências Lineares

Sabemos que se $a\, x \equiv_n b$ é uma congruência linear e m.d.c.$(a, n) = 1$ então a congruência linear tem exactamente uma classe de congruência módulo n como solução.

Para encontrarmos essa solução temos os seguintes métodos:

1º Método Por tentativas - procurando a solução num sistema completo de resíduos módulo n .

2º Método Equação diofantina - usando o algoritmo de Euclides para encontrar as soluções da equação diofantina:

$$a\, x - n\, y = b$$

Resolução de Congruências Lineares

3º Método Redução do coeficiente - tentando reduzir o coeficiente a da incónita x, a 1 (ou -1), à semelhança do que fazemos na resolução de equações. Para este método vamos usar o seguinte resultado:

Proposição

Seja $a\,x \equiv_n b$ uma congruência linear e $k \in \mathbb{Z}$ tal que:

$$\textit{m.d.c.}(n,k) = 1$$

Então:

$$\textit{(Regra 1)} \qquad a\,x \equiv_n b \iff k\,a\,x \equiv_n k\,b$$

e se $k|a$ *e* $k|b$

$$\textit{(Regra 2)} \qquad a\,x \equiv_n b \iff \frac{a}{k}\,x \equiv_n \frac{b}{k}$$

Resolução de Congruências Lineares - Exemplo 1

$$33\,x \equiv_{45} 18 \underset{/3}{\Leftrightarrow} 11\,x \equiv_{15} 6 \Leftrightarrow -4\,x \equiv_{15} 6 \underset{/(-2)}{\Leftrightarrow}$$

$$2\,x \equiv_{15} -3 \underset{\times 8}{\Leftrightarrow} 16\,x \equiv_{15} -24 \Leftrightarrow x \equiv_{15} 6$$

Logo a solução da congruência é dada por

$$x = [6]_{15} = 6 + 15\,k \quad k \in \mathbb{Z}$$

Em alternativa também podíamos ter feito o seguinte:

$$2\,x \equiv_{15} -3 \Leftrightarrow 2\,x \equiv_{15} 12 \underset{/2}{\Leftrightarrow} x \equiv_{15} 6$$

Resolução de Congruências Lineares - Exemplo 2

$$4\,x \equiv_{17} 15 \quad \Leftrightarrow \quad 4\,x \equiv_{17} -2 \quad \underset{\times 4}{\Leftrightarrow} \quad 16\,x \equiv_{17} -8 \quad \Leftrightarrow$$

$$-x \equiv_{17} -8 \quad \underset{\times(-1)}{\Leftrightarrow} \quad x \equiv_{17} 8$$

Logo a solução da congruência é dada por

$$x = [8]_{17} = 8 + 17\,k \quad k \in \mathbb{Z}$$

Em alternativa também podíamos ter feito o seguinte:

$$4\,x \equiv_{17} 15 \quad \Leftrightarrow \quad 4\,x \equiv_{17} 32 \quad \underset{/4}{\Leftrightarrow} \quad x \equiv_{17} 8$$

Resolução de Congruências Lineares - Exemplo 3

$$32\,x \equiv_{23} 21 \quad \Leftrightarrow \quad 9\,x \equiv_{23} 21 \quad \underset{/3}{\Leftrightarrow} \quad 3\,x \equiv_{23} 7 \quad \underset{\times 8}{\Leftrightarrow}$$

$$24\,x \equiv_{23} 56 \quad \Leftrightarrow \quad x \equiv_{23} 10$$

Logo a solução da congruência é dada por

$$x = [10]_{23} = 10 + 23\,k \quad k \in \mathbb{Z}$$

Em alternativa também podíamos ter feito o seguinte:

$$3\,x \equiv_{23} 7 \quad \Leftrightarrow \quad 3\,x \equiv_{23} 30 \quad \underset{/3}{\Leftrightarrow} \quad x \equiv_{23} 10$$

Resolução de Congruências Lineares - Exemplo 4

Vamos agora usar este método para resolver uma equação diofantina:

$$18\,x + 5\,y = 48 \quad \Rightarrow \quad 18\,x \equiv_5 48 \quad \Leftrightarrow \quad 3\,x \equiv_5 3 \quad \underset{/3}{\Leftrightarrow} \quad x \equiv_5 1$$

Logo a solução da congruência é dada por

$$x = [1]_5 = 1 + 5\,k \qquad k \in \mathbb{Z}$$

Substituindo na equação diofantina a solução $x_0 = 1$ obtemos para y o valor $y_0 = 6$. Logo a solução geral da equação diofantina é dada por:

$$\begin{cases} x = 1 + 5\,k \\ y = 6 - 18\,k \qquad k \in \mathbb{Z} \end{cases}$$

Sistemas de congruências lineares

- Um sistema de congruências lineares terá solução se existir um valor $x \in \mathbb{Z}$ que satisfaça todas as congruências lineares do sistema.
- Obviamente, se uma das congruências lineares do sistema não tiver solução o sistema também não tem solução.
- No entanto é possível que todas as congruências lineares do sistema tenham solução mas o sistema seja impossível.

Sistemas de congruências lineares - Exemplo 1

Vejamos como podemos resolver um sistema de equações lineares usando o método de substituição :

$$\begin{cases} 7\,x \equiv_{11} 1 & \times 3 \\ 5\,x \equiv_{8} 3 & \\ 8\,x \equiv_{14} 6 & /2 \end{cases} \iff \begin{cases} 21\,x \equiv_{11} 3 \\ 5\,x \equiv_{8} 3 \\ 4\,x \equiv_{7} 3 \end{cases} \iff \begin{cases} -x \equiv_{11} 3 & \times(-1) \\ -3\,x \equiv_{8} 3 & /(-3) \\ -3\,x \equiv_{7} 3 & /(-3) \end{cases}$$

$$\begin{cases} x \equiv_{11} -3 \\ x \equiv_{8} -1 \\ x \equiv_{7} -1 \end{cases} \iff \begin{cases} \boxed{x = -3 + 11\,k} \\ -3 + 11\,k \equiv_{8} -1 \\ -3 + 11\,k \equiv_{7} -1 \end{cases} \iff (^*) \begin{cases} \cdots & \\ 3\,k \equiv_{8} 2 & \times(3) \\ 4\,k \equiv_{7} 2 & \times(2) \end{cases}$$

$$\begin{cases} \cdots \\ 9\,k \equiv_{8} 6 \\ 8\,k \equiv_{7} 4 \end{cases} \iff \begin{cases} \cdots \\ k \equiv_{8} -2 \\ k \equiv_{7} 4 \end{cases} \iff \begin{cases} \cdots \\ \boxed{k = -2 + 8\,u} \\ -2 + 8\,u \equiv_{7} 4 \end{cases}$$

$(*)$ Na resolução de uma congruência linear podemos passar qualquer termo de um membro para o outro, trocando-lhe o sinal (Propriedade 3).

Sistemas de congruências lineares -Exemplo 1

$$\begin{cases} \boxed{x = -3 + 11\,k} \\ \boxed{k = -2 + 8\,u} \\ u \equiv_7 6 \end{cases} \iff \begin{cases} \cdots \\ \cdots \\ u \equiv_7 -1 \end{cases} \iff \begin{cases} \boxed{x = -3 + 11\,k} \\ \boxed{k = -2 + 8\,u} \\ \boxed{u = -1 + 7\,t} \end{cases}$$

$x = -3 + 11\,k = -3 + 11(-2 + 8\,u) = -3 - 22 + 88\,u = -25 + 88(-1 + 7\,t) = -25 - 88 + 616\,t = -113 + 616\,t$

A solução geral do sistema é então:

$$x = [-113]_{616} = -113 + 616\,t \quad t \in \mathbb{Z}$$

- Note-se que existe uma única solução módulo $616 = 11 \times 8 \times 7$.
- Se na resolução do sistema pelo método de substituição obtivermos uma congruência linear impossível, isso significa que o sistema não tem solução.

Sistemas de congruências lineares

Teorema

Seja $a\,x \equiv_n b$ *uma congruência linear e sejam* $n_1, n_2 \in \mathbb{Z}$ *tais que* $n = n_1 \times n_2$ *e* m.d.c.$(n_1, n_2) = 1$ *. Então:*

$$a\,x \equiv_n b \quad \Longleftrightarrow \quad \begin{cases} a\,x \equiv_{n_1} b \\ a\,x \equiv_{n_2} b \end{cases}$$

Corolário

Se $n = p_1^{\alpha_1}\, p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *é a decomposição de* n *em números primos:*

$$a\,x \equiv_n b \quad \Longleftrightarrow \quad \begin{cases} a\,x \equiv_{p_1^{\alpha_1}} b \\ a\,x \equiv_{p_2^{\alpha_2}} b \\ \dots \\ a\,x \equiv_{p_k^{\alpha_k}} b \end{cases}$$

Sistemas de congruências lineares - Exemplo 2

Vamos usar o Teorema para resolver a seguinte congruência linear:

$$17\,x \equiv_{276} 9$$

Como

$$276 = 280 - 4 = 4(70-1) = 4 \times 69 = 2^2 \times 3 \times 23$$

temos que:

$$17\,x \equiv_{276} 9 \quad \Longleftrightarrow \quad \begin{cases} 17\,x \equiv_{4} 9 \\ 17\,x \equiv_{3} 9 \\ 17\,x \equiv_{23} 9 \end{cases}$$

Sistemas de congruências lineares - Exemplo 2

$$\begin{cases} 17\,x \equiv_4 9 \\ 17\,x \equiv_3 9 \\ 17\,x \equiv_{23} 9 \end{cases} \iff \begin{cases} x \equiv_4 1 & \\ -x \equiv_3 0 & \times(-1) \\ -6\,x \equiv_{23} 9 & /(-3) \end{cases} \iff \begin{cases} x \equiv_4 1 & \\ x \equiv_3 0 & \\ 2\,x \equiv_{23} -3 & \times 12 \end{cases}$$

$$\begin{cases} x \equiv_4 1 \\ x \equiv_3 0 \\ 24\,x \equiv_{23} -36 \end{cases} \iff \begin{cases} x \equiv_4 1 \\ x \equiv_3 0 \\ x \equiv_{23} 10 \end{cases} \iff \begin{cases} 10 + 23\,k \equiv_4 1 \\ 10 + 23\,k \equiv_3 0 \\ \boxed{x = 10 + 23\,k} \end{cases}$$

$$\begin{cases} -k \equiv_4 -9 & \times(-1) \\ -k \equiv_3 -10 & \times(-1) \\ \ldots & \end{cases} \iff \begin{cases} k \equiv_4 9 \\ k \equiv_3 10 \\ \ldots \end{cases} \iff \begin{cases} k \equiv_4 1 \\ k \equiv_3 1 \\ \ldots \end{cases}$$

Sistemas de congruências lineares - Exemplo 2

$$\begin{cases} k \equiv_{12} 1 \\ \boxed{x = 10 + 23\,k} \end{cases} \iff \begin{cases} \boxed{k = 1 + 12\,t} \\ \boxed{x = 10 + 23\,k} \end{cases}$$

Logo

$$x = 10 + 23\,k = 10 + 23(1 + 12\,t) = 33 + 276\,t \qquad t \in \mathbb{Z}$$

Sistemas de congruências lineares - existência de solução

Teorema

Dados $n_1, n_2, \cdots, n_k \in \mathbb{N}$ *e* $b_1.b_2, \cdots, b_k \in \mathbb{Z}$*, o sistema*

$$\begin{cases} x \equiv_{n_1} b_1 \\ x \equiv_{n_2} b_2 \\ \cdots \\ x \equiv_{n_k} b_k \end{cases}$$

tem solução se e só se $\forall i, j$ *m.d.c.*$(n_i, n_j) \mid b_i - b_j$*.*

Além disso, se o sistema tiver solução ela é única módulo o inteiro n*, onde* n *é o mínimo múltiplo comum entre* $n_1, n_2, \cdots, n_k$