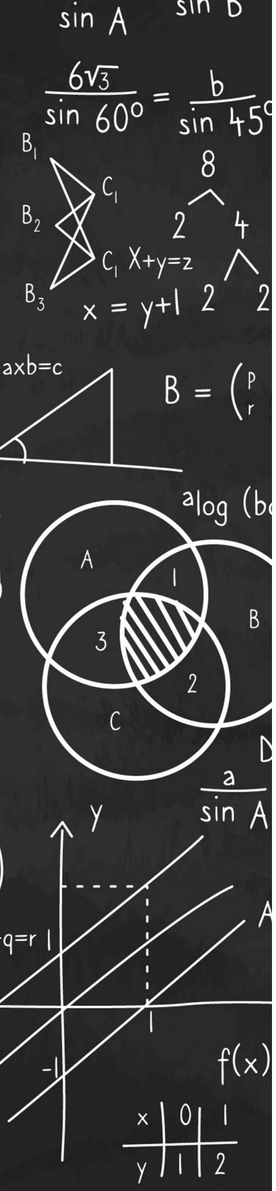


MATEMÁTICA DISCRETA 2

Aula 15

Congruência Linear

Cristiane Loesch

Brasília
2025

Congruência Linear

Dado $n \in \mathbb{N}$, uma congruência linear é uma congruência da forma:

$$\boxed{a\,x \equiv b\,(mod\,n)}$$

$\forall\, a, b, x \in \mathbb{Z}$

$x \rightarrow incognita$

* Dificuldade:

O problema de encontrar todos os números inteiros que satisfazem a congruência linear

$$a\,x \equiv b \bmod n$$

é idêntico ao da obtenção de todas as soluções da equação linear

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

chamada Equação Diofantina.

Congruência Linear

$$\boxed{ax \equiv b \pmod{n}}$$

$$n \in \mathbb{N}$$
$$\forall a, b, x \in \mathbb{Z}$$
$$x \rightarrow incognita$$

Congruência Linear

$$\boxed{ax \equiv b \pmod{n}}$$

$$n \in \mathbb{N}$$
$$\forall a, b, x \in \mathbb{Z}$$
$$x \rightarrow incognita$$

Ou seja, devemos encontrar qual o inteiro x satisfaz a relação.

Mas toda congruência linear tem solução?!

Congruência Linear

$$\boxed{a\,x \equiv b \,(mod\, n)}$$

$n \in \mathbb{N}$

$\forall\, a, b, x \in \mathbb{Z}$

$x \rightarrow incognita$

Não!
Vamos ver quando uma congruência linear tem solução

Mas toda congruência linear tem solução?!

QUANDO UMA CONGRUÊNCIA LINEAR POSSUI SOLUÇÃO?!

Dada

$$a \cdot x \equiv b \pmod{n}$$

QUANDO UMA CONGRUÊNCIA LINEAR POSSUI SOLUÇÃO?!

Dada

$$a \cdot x \equiv b \pmod{n}$$

por definição de congruência:

$$n / a \cdot x - b$$

QUANDO UMA CONGRUÊNCIA LINEAR POSSUI SOLUÇÃO?!

Dada

$$a \cdot x \equiv b \pmod{n}$$

por definição de congruência:

$$n / a \cdot x - b$$

ou seja,

$$a \cdot x - b = n \cdot k \qquad k \in \mathbb{Z}$$

QUANDO UMA CONGRUÊNCIA LINEAR POSSUI SOLUÇÃO?!

Dada

$$a \cdot x \equiv b \left(mod\, n \right)$$

por definição de congruência:

$$n / a \cdot x - b$$

ou seja,

$$a \cdot x - b = n \cdot k \qquad k \in \mathbb{Z}$$

reescrevendo:

$$a \cdot x - n \cdot k = b$$

Assim, a solução da congruência linear depende da solução da equação diofantina acima.

Congruência Linear

TEOREMA: Sejam $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}$

a) $ax \equiv b \bmod n$ admite solução se, e somente se, $d = mdc(a, n) \mid b$

Congruência Linear

TEOREMA: Sejam $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}$

a) $ax \equiv b \bmod n$ admite solução se, e somente se, $d = mdc(a, n) \mid b$

b) se $d \mid b \Rightarrow ax \equiv b \bmod n$ possui exatamente d soluções incongruentes entre si $\bmod n$

Congruência Linear

TEOREMA: Sejam $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}$

a) $ax \equiv b \bmod n$ admite solução se, e somente se, $d = mdc(a,n) \mid b$

b) se $d \mid b \Rightarrow ax \equiv b \bmod n$ possui exatamente d soluções incongruentes entre si $\bmod n$

Se $x_0 \in \mathbb{Z}$ é uma solução particular → d soluções incongruentes entre si são obtidas por:

$$x_0 \ , \ x_0 + \frac{n}{d} \ , \ x_0 + \frac{2n}{d} \ , \ x_0 + \frac{(d-1)n}{d}$$

Congruência Linear

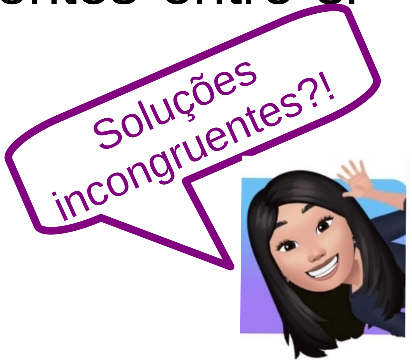
TEOREMA: Sejam $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}$

a) $ax \equiv b \bmod n$ admite solução se, e somente se, $d = mdc(a, n) \mid b$

b) se $d \mid b \Rightarrow ax \equiv b \bmod n$ possui exatamente d soluções incongruentes entre si $\bmod n$

Se $x_0 \in \mathbb{Z}$ é uma solução particular → d soluções incongruentes entre si são obtidas por:

$$x_0 \;,\; x_0 + \frac{n}{d} \;,\; x_0 + \frac{2n}{d} \;,\; x_0 + \frac{(d-1)n}{d}$$



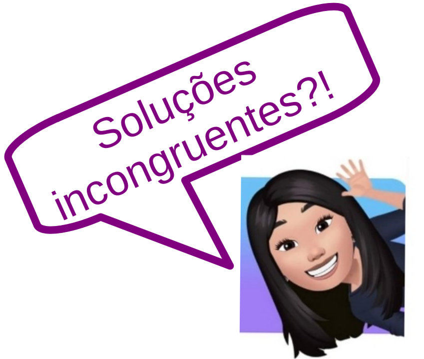
Congruência Linear

Se $x_0 \in \mathbb{Z}$ é uma solução particular $\rightarrow$ d soluções incongruentes entre si são obtidas por:

$$x_0 \;,\; x_0+\frac{n}{d} \;,\; x_0+\frac{2n}{d} \;,\; x_0+\frac{(d-1)n}{d}$$

As soluções incongruentes compõe a classe de congruência modulo n que satisfazem a equação.

Por exemplo:
Se x_0 é uma solução da CL e
$x_0 \equiv x_1 (\text{mod } n)$
logo x_1, também é solução da CL.



EXEMPLO: Verifique se as CL abaixo tem solução.

a) $2x \equiv 5 \, mod \, 6$

b) $4x \equiv 2 \, mod \, 6$

c) $8x \equiv 2 \, (mod \, 10)$

EXEMPLO: Verifique se as CL abaixo tem solução.

a) $2x \equiv 5 \, mod \, 6$ $\qquad mdc(2,6) = 2 \longrightarrow 2 \nmid 5 \qquad \nexists$ solução

b) $4x \equiv 2 \, mod \, 6$

c) $8x \equiv 2 (mod \, 10)$

EXEMPLO: Verifique se as CL abaixo tem solução.

a) $2x \equiv 5 \, mod \, 6$ $\quad mdc(2,6)=2 \longrightarrow 2 \nmid 5$ $\quad \nexists$ solução

b) $4x \equiv 2 \, mod \, 6$ $\quad mdc(4,6)=2 \longrightarrow 2 \mid 2$ $\quad \exists$ solução

SUA VEZ!

c) $8x \equiv 2 (mod \, 10)$

EXEMPLO: Verifique se as CL abaixo tem solução.

a) $2x \equiv 5 \, mod \, 6$ $\quad mdc(2,6)=2 \longrightarrow 2 \nmid 5$ $\quad \nexists$ solução

b) $4x \equiv 2 \, mod \, 6$ $\quad mdc(4,6)=2 \longrightarrow 2 \mid 2$ $\quad \exists$ solução

SUA VEZ!

c) $8x \equiv 2(mod \, 10)$ $\quad mdc(8,10)=2 \longrightarrow 2 \mid 2$ $\quad \exists$ solução

EXEMPLO: Encontre as soluções incongruentes de:

$$6x \equiv 3 \pmod{15}$$

EXEMPLO: Encontre as soluções incongruentes de:

$$6x \equiv 3 \pmod{15}$$

1º) encontrar uma solução $x = x_0$

$$15 / 6x - 3$$

$$6x - 3 = 15y \longrightarrow \begin{array}{l} x = ? \\ y = ? \end{array}$$

→ calcular o mdc utilizando o algoritmo de Euclides:

$$15 = 6 \cdot 2 + 3 \qquad r \neq 0 \qquad (1)$$

$$6 = 3 \cdot 2 + 0 \qquad r = 0 \qquad (2)$$

$$mdc(15, 6) = 3$$

$$d = 3$$

EXEMPLO:

$$6x \equiv 3 \pmod{15}$$

→ calcular o mdc utilizando o algoritmo de Euclides:

$$15 = 6 \cdot 2 + 3 \qquad r \neq 0 \qquad (1)$$

$$6 = 3 \cdot 2 + 0 \qquad r = 0 \qquad (2)$$

$$mdc(15, 6) = 3$$

$$d = 3$$

→ escrever $d = 3$ como combinação linear de 3 e 15 utilizando (1)

$$3 = -2 \cdot 6 + 1 \cdot 15$$

$$x_0 = -2 \qquad y_0 = 1$$

Congruência Linear

EXEMPLO:

$$6x \equiv 3 \pmod{15}$$

→ calcular o mdc utilizando o algoritmo de Euclides:

$$15 = 6 \cdot 2 + 3 \qquad r \neq 0 \qquad (1)$$

$$6 = 3 \cdot 2 + 0 \qquad r = 0 \qquad (2)$$

$$mdc(15, 6) = 3$$

$$d = 3$$

→ escrever $d = 3$ como combinação linear de 3 e 15 utilizando (1)

$$3 = -2 \cdot 6 + 1 \cdot 15$$

$$x_0 = -2 \qquad y_0 = 1$$

observe que

$$6(-2) = -12$$

$$-12 \equiv 3 \pmod{15}$$

$$-12 - 3 = -15$$

$$15 / -15$$

$$x_0 = -2$$

é uma solução da CL.

EXEMPLO:

$$6x \equiv 3 \pmod{15}$$

2º) considerar a forma geral da solução da equação diofantina

$$x = x_0 - \frac{b}{d}t \qquad y = y_0 + \frac{a}{d}t \qquad t \in \mathbb{Z}$$

para encontrar x.

$$x = x_0 - \frac{n}{d}t \longrightarrow d = mc(a,n) = 3$$

$$x = -2 - \frac{15}{3}t$$

$$x = -2 - 5t$$

3º) definir as classes de congruência módulo d para cada valor de t

$$d = 3 \longrightarrow t = 0, 1\, e\, 2$$

EXEMPLO:

$$6x \equiv 3 \pmod{15}$$

3º) definir as classes de congruência módulo d para cada valor de t

$$d = 3 \longrightarrow t = 0, 1\; e\; 2$$

$x = -2 - 5t$

$$x_0 = -2 - 5 \cdot 0 = -2 \equiv 13 \pmod{15}$$

$$x_1 = -2 - 5 \cdot 1 = -7 \equiv 8 \pmod{15}$$

$$x_2 = -2 - 5 \cdot 2 = -12 \equiv 3 \pmod{15}$$

Ou seja, todos os números inteiros que deixam resto 3 , 8 e 13 na divisão por 15 são soluções desta congruência linear.

$$\{\overline{3}, \overline{8}, \overline{13}\}$$

EXEMPLO: (OMBEP – adaptada) De quantas maneiras é possível comprar meias de $R\$10,00$ e $R\$14,00$ gastando $R\$100,00$?

EXEMPLO: (OMBEP – adaptada) De quantas maneiras é possível comprar meias de R\$10,00 e R\$14,00 gastando R\$100,00 ?

$$10\,x+14\,y=100$$

$$mdc(10,14)=2 \;\Rightarrow 2\,|\,100 \qquad \exists \quad \text{solução possível}$$

Simplificando:

$$5\,x+7\,y=50$$

$$mdc(5,7)=1$$

Vamos reescrever a equação em *mod 5* nas classes

$$\bar{0}\,\bar{x}+\bar{2}\,\bar{y}=\bar{0}\,mod\,5$$

$$\bar{2}\,\bar{y}=\bar{0}\,mod\,5$$

$$\bar{y}=?$$

Obs:

$7 \rightarrow classe\,2$

$7\,|\,5 \quad \text{tem resto} \quad 2$

Congruência Linear

EXEMPLO:

$$\bar{2}\,\bar{y} = \bar{0}\; mod\, 5 \qquad \bar{y} = ?$$

$mod\, 5 \longrightarrow$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$					
$\bar{1}$					
$\bar{2}$					
$\bar{3}$					
$\bar{4}$					

Congruência Linear

EXEMPLO:

$$\bar{2}\,\bar{y} = \bar{0}\ mod\ 5 \qquad \bar{y} = ?$$

$mod\ 5 \longrightarrow$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Congruência Linear

EXEMPLO:

$$\bar{2}\,\bar{y} = \bar{0} \; mod \, 5 \qquad \bar{y} = ?$$

$mod\,5$ →

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

→ olhar a linha do $\bar{2}$. único lugar em que $\bar{2} \cdot \bar{y} = \bar{0}$ é para $\bar{y} = \bar{0}$

↓

Y poderá assumir qualquer valor que quando dividido por 5 deixe resto zero, logo, múltiplos de 5

Congruência Linear

EXEMPLO:

$$\bar{2}\,\bar{y} = \bar{0}\, mod\, 5 \qquad \bar{y} = ?$$

$mod\, 5 \longrightarrow$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\longrightarrow$ olhar a linha do $\bar{2}$. único lugar em que $\bar{2} \cdot \bar{y} = \bar{0}$ é para $\bar{y} = \bar{0}$

$$y = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$$

Congruência Linear

EXEMPLO:

$$\bar{2}\,\bar{y} = \bar{0} \, mod\, 5 \qquad \bar{y} = ?$$

$mod\, 5 \rightarrow$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\rightarrow$ olhar a linha do $\bar{2}$. único lugar em que $\bar{2}\cdot\bar{y} = \bar{0}$ é para $\bar{y} = \bar{0}$

$$y = \{\ldots, \cancel{-10}, \cancel{-5}, 0, 5, 10, \ldots\}$$

y não pode ser negativo!

$$y = \{0, 5, 10, \ldots\}$$

Congruência Linear

EXEMPLO:

$$\bar{2}\,\bar{y} = \bar{0} \, mod \, 5 \qquad \bar{y} = ?$$

$$y = \{0, 5, 10, \ldots\}$$

como,

$$5x + 7y = 50$$

$$x = \{10, 3, \cancel{-4}, \cancel{-11}\}$$

x não pode ser negativo!

Assim,

$$y = \{0,5\}$$
$$x = \{10,3\}$$

Congruência Linear

EXEMPLO:

$$\bar{2}\,\bar{y} = \bar{0} \, mod \, 5 \qquad \bar{y} = ?$$

como,

$$y = \{0, 5, 10, \ldots\}$$

+5 +5

$$5x + 7y = 50$$

$$x = \{10, 3, \cancel{-4}, \cancel{-11}\}$$

-7 -7

Assim,

$$y = \{0, 5\}$$
$$x = \{10, 3\}$$

Sistemas de Congruência

EXEMPLO: (OBMEP) Em um cesto há uma quantidade N de ovos se os ovos forem agrupados de 3 em 3, sobram 2. Se forem agrupados de 4 em 4, sobra 1. Quantos ovos <u>podem haver</u> na cesta?

Sistemas de Congruência

EXEMPLO: (OBMEP) Em um cesto há uma quantidade N de ovos se os ovos forem agrupados de 3 em 3, sobram 2. Se forem agrupados de 4 em 4, sobra 1. Quantos ovos <u>podem haver</u> na cesta?

Considere:

$$N \equiv 2 \bmod 3$$
$$N \equiv 1 \bmod 4$$

Sistemas de Congruência

EXEMPLO: (OBMEP) Em um cesto há uma quantidade N de ovos se os ovos forem agrupados de 3 em 3, sobram 2. Se forem agrupados de 4 em 4, sobra 1. Quantos ovos podem haver na cesta?

Considere:

$$N \equiv 2 \mod 3$$

ou

$$N = 3\underbrace{a}_{\text{quociente}} + \underbrace{2}_{\text{resto}} \qquad a \in \mathbb{N}$$

Sistemas de Congruência

EXEMPLO: (OBMEP) Em um cesto há uma quantidade N de ovos se os ovos forem agrupados de 3 em 3, sobram 2. Se forem agrupados de 4 em 4, sobra 1. Quantos ovos podem haver na cesta?

Considere:

$$N \equiv 2 \mod 3$$

ou

$$N = 3a + 2 \quad (1) \qquad a \in \mathbb{N}$$

e

$$N \equiv 1 \mod 4 \quad (2)$$

Sistemas de Congruência

EXEMPLO: (OBMEP) Em um cesto há uma quantidade N de ovos se os ovos forem agrupados de 3 em 3, sobram 2. Se forem agrupados de 4 em 4, sobra 1. Quantos ovos podem haver na cesta?

Considere:

$$N \equiv 2 \bmod 3$$

ou

$$N = 3a + 2 \quad (1) \qquad a \in \mathbb{N}$$

e

$$N \equiv 1 \bmod 4 \quad (2)$$

de (1) e (2):

$$3a + 2 \equiv 1 \bmod 4$$

Sistemas de Congruência

EXEMPLO:

$$3a + 2 \equiv 1 \mod 4$$

Sistemas de Congruência

EXEMPLO:

$$3a+2\equiv 1 \, mod \, 4$$

$$3a+2-2\equiv 1-2 \, mod \, 4$$

$$3a\equiv -1 \, mod \, 4$$

como $-1\equiv 3 \, mod \, 4$

$$3a\equiv 3 \, mod \, 4$$

pela lei do cancelamento

$$a\equiv 1 \, mod \, 4$$

pelo algoritmo de Euclides:

$$a=4b+1$$

Substituindo em (1):

$$N=3(4b+1)+2$$

$$N=12b+3+2$$

$$N=12b+5$$

Sistemas de Congruência

EXEMPLO:

$$3a+2\equiv 1 \, mod\, 4$$

$$3a+2-2\equiv 1-2\, mod\, 4$$

$$3a\equiv -1\, mod\, 4$$

como $-1\equiv 3\, mod\, 4$

$$3a\equiv 3\, mod\, 4$$

pela lei do cancelamento

$$a\equiv 1\, mod\, 4$$

pelo algoritmo de Euclides:

$$a=4b+1$$

Substituindo em (1):

$$N=3(4b+1)+2$$

$$N=12b+3+2 \longrightarrow N\equiv 5\, mod\, 12$$

$$N=12b+5$$

Observe que a pergunta é "pode haver", logo vários números que satisfizerem a equação abaixo são soluções possíveis!

Congruência Simultânea

<u>Motivação:</u>

“ Que número será esse? Que :

quando dividido por 3, o resto é 2

quando dividido por 5, o resto é 3 e

quando dividido por 7, o resto é 2?”

Sun-Tsu (sec I)

matemático chinês

Congruência Simultânea

Motivação:

"Que número será esse? Que :
quando dividido por 3, o resto é 2
quando dividido por 5, o resto é 3 e
quando dividido por 7, o resto é 2?"

Sun-Tsu (sec I)
matemático chinês

Ou seja, que número é este que:

$$x \equiv 2 \bmod 3$$
$$x \equiv 3 \bmod 5$$
$$x \equiv 2 \bmod 7$$

para solucionar esta questão é necessário um sistema de congruências.

Congruência Simultânea

Solução: Suponha que os módulos m_k são em pares primos entre si.

Desta forma, o sistema admitirá soluções se cada congruência, individualmente, possuir solução. Ou seja,

$$d_k \mid b_k$$

para cada k, onde $d_k = mdc(a_k, m_k)$

Satisfeitas as condições, o fator d_k pode ser cancelado na k-ésima congruência para produzir um novo sistema, com o conjunto de soluções individuais, que assumem a forma

$$x_1 \equiv C_1 \, mod \, n_1$$
$$x_2 \equiv C_2 \, mod \, n_2$$
$$\dots$$
$$x \equiv C_k \, mod \, n_k$$

$$n_k = \frac{m_k}{d_k}$$
$$mdc(n_i, n_j) = 1$$
$$i \neq j$$

Chega-se ao: **TEOREMA CHINÊS DO RESTO**

Sejam $n_{1,} n_{2,} \ldots, n_r$ inteiros positivos tais que $mdc(n_i, n_j) = 1$, $i \neq j$. Então, o sistema de congruências lineares:

$$x_1 \equiv a_1 \, mod \, n_1$$
$$x_2 \equiv a_2 \, mod \, n_2$$
$$\ldots$$
$$x \equiv a_r \, mod \, n_r$$

Possui uma solução simultânea e quaisquer duas soluções congruentes módulo o produto $n_1 \cdot n_2 \cdot \ldots \cdot n_r$

A solução simultânea é dada por:

$$x = a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots + a_r N_r x_r$$

n_i : Números pares primos relativos ($mdc(n_k, N_k) = 1$) N_k : Produto de todos os n_i com fatores n_k omitido

Congruência Simultânea

RESUMINDO

TEOREMA CHINÊS DO RESTO

Dado o sistema

$$
\begin{aligned}
x_1 &\equiv a_1 \bmod n_1 \\
x_2 &\equiv a_2 \bmod n_2 \\
&\dots \\
x &\equiv a_r \bmod n_r
\end{aligned}
$$

$$mdc(n_i, n_j) = 1 \quad i \neq j$$

Define-se o sistema auxiliar

$$
\begin{aligned}
N_1 x_1 &\equiv 1 (\bmod n_1) \\
N_2 x_2 &\equiv 1 (\bmod n_1) \\
&\dots \\
N_r x_r &\equiv 1 (\bmod n_r)
\end{aligned}
$$

em que:

$$N_i = n_1 \cdot n_2 \cdot \ldots \cdot n_{i-1} \cdot n_{i+1} \ldots \cdot n_r$$

A solução do sistema é dada por

$$x = a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots + a_r N_r x_r \longrightarrow \begin{array}{c} x \equiv y (\bmod m) \\ m = n_1 \cdot n_2 \cdot \ldots \cdot n_r \end{array}$$

$x_1, x_2, \ldots, x_r \rightarrow$ soluções do sistema de congruência linear auxiliar

EXEMPLO: resolvendo o problema proposto por Sun-Tsu

$$x \equiv 2 \, mod \, 3$$
$$x \equiv 3 \, mod \, 5$$
$$x \equiv 2 \, mod \, 7$$

Pelo teorema do resto chinês:

$$n = 3 \cdot 5 \cdot 7 = 105$$

$N_1 = 5 \cdot 7 = 35$ *omite posição 1

$N_2 = 3 \cdot 7 = 21$ *omite posição 2

$N_3 = 3 \cdot 5 = 15$ *omite posição 3

como:

$a_1 = 2$	$n_1 = 3$	$n = 105$	$N_1 = 35$
$a_2 = 3$	$n_2 = 5$		$N_2 = 21$
$a_3 = 2$	$n_3 = 7$		$N_3 = 15$

tem-se as congruências auxiliares:

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

são satisfeitas para:

$$x_1 = 2 \quad , \quad x_2 = 1 \quad , \quad x_3 = 1$$

logo, $x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$

e $x = 233 \equiv 23 \left(mod \, 105 \right)$

TEOREMA CHINÊS DO RESTO

VÍDEOS:

1) Demonstração do teorema e explicação

https://www.youtube.com/watch?v=uMhwa2SPi0w

https://www.youtube.com/watch?v=tcgi_4DRZM0&t=3s

2) Exemplo:

https://www.youtube.com/watch?v=Ra1HCGfrcoE&t=5s

Acesso em 28/05/2021

Exercícios

1)(OMBEP – adaptada) De quantas maneiras é possível comprar meias de R\$10,00 e R\$14,00 gastando R\$100,00 ?

OBS: No exemplo da aula fizemos mod 5. Agora faça com mod 7

2)(ENEM 2013) O ciclo de atividade magnética do Sol tem um período de 11 anos. O início deo 1º ciclo registrado se deu no começo de 1755 e s estendeu até o final de 1765. Desde então, todos os ciclos de atividade magnética do Sol tem sido registrados.

No ano de 2101, o Sol estará no ciclo de atividade magnética de número:

a) 32 b) 34 c) 33 d) 36 e) 31

Resolução dos Exercícios

1) $10x+14y=100$

$$mdc(10,14)=2 \;\Rightarrow 2\,|\,100$$

$$\div 2$$

$$5x+7y=50$$

$$(mdc(5,7)=1)$$

escrever mod 7 nas classe

$$\bar{5}\bar{x}+\bar{0}\bar{y}=\bar{1}\,mod\,7$$

$5\,|\,7$ tem resto 5
$50\,|\,7$ tem resto 1

$$\bar{5}\bar{x}=\bar{1}\,mod\,7$$

$$\bar{x}=?$$

$mod\,7$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

olhar a linha do $\bar{5}$, único lugar em que $\bar{5}\cdot\bar{x}=\bar{1}$ é para $\bar{x}=\bar{3}$. Logo, x pode assumir valores cuja divisão por 7 tenha resto 3

$$x=\{\ldots,10,3,\cancel{-4},\cancel{-11},\ldots\}$$

$$5x+7y=50$$

$$y=\{0,5\}$$

$$x=\{10,3\}$$

Resolução dos Exercícios

2)

Anos

1755	1756	1757	1758	1759	1760	1761	1762	1763	1764	1765
1766	1767	1768	1769	1770	1771	1772	1773	1774	1775	1776

.

.

.

restos $\div 11$

6	7	8	9	10	0	1	2	3	4	5

2101 = 191 cdot 11 → múltiplo de 11

logo

2101 equiv 0 mod 11

como

1760 equiv 0 mod11 → 6º ano do ciclo 1

2101 – 1760 = 341 = 31 cdot 11

2101 → 6º ano do ciclo 32