Universidade de Brasília

Faculdade do Gama

Matemática Discreta 2

Prof. Dr. Glauco Vitor Pedrosa

UnB Gama
O novo endereço da tecnologia

Classe Residual

- A **classe residual módulo m** de um inteiro a é o conjunto de todos os inteiros que são congruentes a a *módulo* m
- Este conjunto é representado pelo símbolo

a_m = { x ∈ Z | x ≡ a (mod m) }

ou seja,

a_m = { x ∈ Z | m | (x-a) } = { x ∈ Z | x = mk+a }

Exemplo:

10_{13} = { 10, 23, 36, 49, ...}

2_7 = { 2, 9, 16, 23, ...}

Sistemas de Congruências

- Resolva o seguinte sistema de congruências lineares:

$$\begin{cases} x \equiv 5 \pmod{7} \\ x \equiv 4 \pmod{9} \\ x \equiv 1 \pmod{10} \end{cases}$$

Podemos resolver um sistema de congruências lineares por 2 métodos:

- **Por substituição**
- **Pelo Teorema do Resto Chinês**

Sistemas de Congruências

$$\begin{cases} x \equiv 5 \bmod 7 \\ x \equiv 4 \bmod 9 \\ x \equiv 1 \bmod 10 \end{cases}$$

Da 1° equação temos que: $x = 7a+5$

Substituindo essa informação na 2° equação temos:

$x \equiv 4 \bmod 9$

$7a+5 \equiv 4 \bmod 9$

$7a \equiv -1 \bmod 9$

$7a \equiv 8 \bmod 9$ >> vamos multiplicar pelo inverso modular de 7 mod 9

$a \equiv 32 \bmod 9$

$a \equiv 5 \bmod 9$

Temos que, $a = 9b+5$, vamos substituir essa informação em $x = 7a+5$

Assim, $x = 7(9b+5)+5 = 63b+35+5 = 63b+40$

Sistemas de Congruências

$$\begin{cases} x \equiv 5 \bmod 7 \\ x \equiv 4 \bmod 9 \\ x \equiv 1 \bmod 10 \end{cases}$$

Substituindo 63b+40 na 3° equação temos :

$x \qquad\qquad \equiv 1 \bmod 10$

$63b+40 \equiv 1 \bmod 10$ => $3b$

$3b \qquad\quad \equiv 1 \bmod 10$ >> *vamos multiplicar pelo inverso modular de 3 mod 10 => 7*

$b \qquad\quad\; \equiv 7 \bmod 10$

Temos que, b = 10c+7. Vamos substituir essa informação 63b+40

Temos:

x = 63b+40

x = 63(10c+7)+40

x = 630c+441+40

x = 630c+481 ->>> nesse ponto eu consegui juntar as informações das 3 equações

Sistemas de Congruências

$$\begin{cases} x \equiv 5 \bmod 7 \\ x \equiv 4 \bmod 9 \\ x \equiv 1 \bmod 10 \end{cases}$$

Se **x = 630c+481**, então o sistema de congruências lineares acima pode ser simplificado pela seguinte congruência linear:

$$\mathbf{x \equiv 481 \bmod 630}$$

$$481_{630}$$

Sistemas de Congruências

- Resolva o seguinte sistema linear usando o método da substituição:

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

Resposta:

$\mathbf{x \equiv 52 \pmod{105}}$

$\mathbf{52_{105}}$

Teorema Chinês do Resto

- Dado um sistema de congruências lineares:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ x \equiv a_3 \pmod{m_3} \\ \quad \dots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

- Se mdc(m_i, m_j) = 1, para $i \neq j$, então a solução do sistema é dado por:

$$x = a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 + \dots + a_k M_k x_k$$

onde:

M_i = (o produto de todos os m) / m_i

x_i = o inverso modular de M_i (mod m_i)

Exercício

- Use o teorema do resto chinês para resolver o seguinte sistema de congruências lineares:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

Primeiro, vamos verificar se podemos resolver o sistema acima pelo Teorema Chinês do Resto:

$$mdc(3,5) = mdc(3,7) = mdc(5,7) = 1$$

Sim, o sistema tem solução.

Segundo, vamos calcular o produto 3.5.7 = **105**

Exercício

- Use o teorema do resto chinês para resolver o seguinte sistema de congruências lineares:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

<u>Terceiro</u>, vamos calcular

M_1 = (produto de todos os m) / 3 = 105/3 = 35

M_2 = (produto de todos os m) / 5 = 105/4 = 21

M_3 = (produto de todos os m) / 7 = 105/7 = 15

<u>Quarto,</u> vamos calcular as seguintes congruências:

$$\left.\begin{array}{l} 35x_1 \equiv 1 \pmod 3 \\ 21x_2 \equiv 1 \pmod 5 \\ 15x_3 \equiv 1 \pmod 7 \end{array}\right\} \Rightarrow \begin{array}{l} x_1 = 2 \\ x_2 = 1 \\ x_3 = 1 \end{array} \Rightarrow$$

x $\equiv$ 2.35.2+3.21.1+2.15.1=233

233 $\equiv$ 23 (mod 105)

Assim, a solução do sistema é:

$$23_{105}$$

Exercício

- Use o teorema do resto chinês para resolver o seguinte sistema de congruências lineares:

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{7} \end{cases}$$

Resposta:

$x \equiv 11 \pmod{42}$

Exercício

- Use o teorema do resto chinês para resolver o seguinte sistema de congruências lineares:

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 10 \pmod{7} \\ x \equiv 9 \pmod{11} \end{cases}$$

Resposta:

$x \equiv 108 \pmod{385}$