Matemáticas Discretas

Oscar Bedoya

oscar.bedoya@correounivalle.edu.co

http://eisc.univalle.edu.co/~oscarbed/MD/

* Congruencias lineales
* Sistemas de congruencias lineales
* Teorema del residuo chino

Teoría de números

Encuentre un valor x tal que:

$3 \cdot x \equiv 4 \pmod 7$

$3x \bmod 7 = 4 \bmod 7$

Teoría de números

Encuentre un valor x tal que:

$$\mathbf{3 \cdot x \equiv 4 \pmod{7}}$$

un posible valor es x=6, porque

$$18 \equiv 4 \pmod{7}$$

18 mod 7 = 4

4 mod 7 = 4

Teoría de números

Encuentre un valor x tal que:

$$\mathbf{3 \cdot x \equiv 4 \pmod 7}$$

un posible valor es x=6, porque

$$18 \equiv 4 \pmod 7$$

- Otros valores de x que cumplen la congruencia son:
  - **x=13** ya que **$39 \equiv 4 \pmod 7$**
  - **x=-1** ya que **$-3 \equiv 4 \pmod 7$**
  - **x=20** ya que **$60 \equiv 4 \pmod 7$**

Congruencias lineales

- Una congruencia de la forma

$$\mathbf{a \cdot x \equiv b \pmod{m}}$$

donde m es un entero positivo, a y b son enteros y x es una variable, se llama **congruencia lineal**

Método para resolver $a \cdot x \equiv b \pmod{m}$

1) Encuentre el inverso de a mod m

2) Multiplique ambos lados de la congruencia por $\overline{a}$

$$\underbrace{\overline{a} \cdot a}_{1} \cdot x \equiv \overline{a} \cdot b \pmod{m}$$

$$x \equiv \overline{a} \cdot b \pmod{m}$$

3) Una vez que conozca el valor x, se tiene una solución

Resolver $\mathbf{3x \equiv 4 \pmod{7}}$

Teoría de números

Resolver $3x \equiv 4 \pmod{7}$

- Encuentre el inverso de 3 mod 7
- Multiplique a ambos lados de la congruencia por el inverso
- $x \equiv \overline{a} \cdot b \pmod{m}$ es una solución

$\text{mcd}(3, 7) = 1$

$1 = 3(\underline{s}) + 7(t)$

$\downarrow$

$\overline{a}$

Teoría de números

Resolver **3x ≡ 4 (mod 7)**

$a\bar{a} = 1$

- Encuentre el inverso de 3 mod 7

  El inverso es -2

$x \equiv \bar{a} b \mod m$

- Multiplique a ambos lados de la congruencia por el inverso

  $-2 \cdot 3 \cdot x \equiv -2 \cdot 4 \pmod 7$

  1

  $x \equiv -8 \pmod 7$

  $x = 6$

- **x=6** es una solución

Teoría de números

Resolver $\mathbf{5 \cdot x \equiv 2 \pmod{7}}$

- Encuentre el inverso de 5 mod 7
- Multiplique a ambos lados de la congruencia por el inverso
- $x \equiv \overline{a} \cdot b \pmod{m}$ es una solución

$5x \equiv 2 \bmod 7$

$5(6) \equiv 2 \bmod 7$

$5 \bmod 7$

$30 \equiv 2 \bmod 7$

$30 \bmod 7 = 2 \bmod 7$

$2 = 2$:)

$mcd(5, 7) = 1$:)

$5 \bmod 7 \left\{ 5 = 7 \times 0 + 5 \right.$

$7 \bmod 5 \left\{ \begin{array}{l} 7 = 5 + 2 \\ 2 = 7 - 5 \end{array} \right.$

$5 \bmod 2 \left\{ \begin{array}{l} 5 = 2 \times 2 + 1 \\ 1 = 5 - 2 \times 2 \end{array} \right.$

$2 \bmod 1 = 0$

$1 = 5 - 2 \times 2$

$1 = 5 - 2(7 - 5)$

$1 = (3)5 - (2)7$

$q = 3$

$x = 3 \times 2 \bmod 7$

$x = 6 \bmod 7$

$\boxed{x = 6}$

Teoría de números

Resolver $\mathbf{5 \cdot x \equiv 2 \pmod{7}}$

- Encuentre el inverso de 5 mod 7

  El inverso es 3

- Multiplique a ambos lados de la congruencia por el inverso

  $3 \cdot 5 \cdot x \equiv 3 \cdot 2 \pmod{7}$

  $x \equiv 6 \pmod{7}$

  $x = 6$

Teoría de números

Resolver **7·x ≡ 3 (mod 5)**

$7 \bmod 5$

$\text{mcd}(7, 5) = 1$

$7 \bmod 5$
$$\begin{cases} 7 = 5 \times 1 + 2 \\ 2 = 7 - 5 \times 1 \end{cases}$$

$5 \bmod 2$
$$\begin{cases} 5 = 2 \times 2 + 1 \\ 1 = 5 - 2 \times 2 \end{cases}$$

$2 \bmod 1 = 0$ ✗

$$\frac{7 \times 4 \bmod 5}{3} = \frac{3 \bmod 5}{3}$$

$1 = 5 - 2 \times 2$

$1 = 5 - 2(7 - 5)$

$1 = (3)5 + \underbrace{(-2)}\, 7$

$\bar{a} = -2$

$X = 3(-2) \bmod 5$

$$\begin{cases} -6 = 5(-2) + 4 \\ \boxed{X = 4} \end{cases}$$

Teoría de números

Resolver $\mathbf{7 \cdot x \equiv 3 \pmod{5}}$

- Encuentre el inverso de 7 mod 5

  El inverso es -2

- Multiplique a ambos lados de la congruencia por el inverso

  $-2 \cdot 7 \cdot x \equiv -2 \cdot 3 \pmod{5}$

  $x \equiv -6 \pmod{5}$

  $x = 4$

Teoría de números

$11 \bmod 6 = 5$

$5 \bmod 6 = 5$

$11 \equiv 5 \bmod 6$

Resolver 11·x ≡ 5 (mod 6)

1) inverso $11 \bmod 6$

$\mathrm{mcd}(11, 6) = 1 = 11(\underline{\quad}) + 6(\quad)$

$11 \bmod 6$ $\quad 11 = 6 + 5$

$5 = 11 - 6$

$6 \bmod 5$ $\quad 6 = 5 \times 1 + 1$

$1 = 6 - 5$

$5 \bmod 1 = 0$

$1 = 6 - 5$

$1 = 6 - 11 + 6$

$1 = 6(2) + 11(-1)$

$\boxed{\bar{a} = -1}$

$x = -5 \bmod 6$

$\boxed{x = 1}$

Teoría de números

Resolver $\mathbf{11 \cdot x \equiv 5 \pmod{6}}$

- Encuentre el inverso de 11 mod 6

    El inverso es -1

- Multiplique a ambos lados de la congruencia por el inverso

$$-1 \cdot 11 \cdot x \equiv -1 \cdot 5 \pmod{6}$$

$$x \equiv -5 \pmod{5}$$

$$x = 1$$

Método para resolver $a \cdot x \equiv b \pmod{m}$

- Encuentre el inverso de a mod m
- Multiplique ambos lados de la congruencia por $\overline{a}$

$$\overline{a} \cdot a \cdot x \equiv \overline{a} \cdot b \pmod{m}$$

$$x \equiv \overline{a} \cdot b \pmod{m}$$

- Una vez que conozca el valor x, se tiene una solución

Método para resolver $a \cdot x \equiv b \pmod{m}$

- Encuentre el inverso de a mod m
- Multiplique ambos lados de la congruencia por $\overline{a}$

$$\overline{a} \cdot a \cdot x \equiv \overline{a} \cdot b \pmod{m}$$

$$x \equiv \overline{a} \cdot b \pmod{m}$$

- Una vez que conozca el valor x, se tiene una solución
- Para encontrar todas las soluciones se expresa como:

$$x \equiv (\overline{a} \cdot b \pmod{m}) \bmod m$$

Teoría de números

Resolver $\mathbf{3x \equiv 4 \pmod 7}$

- Encuentre el inverso de 3 mod 7

  El inverso es -2

- Multiplique a ambos lados de la congruencia por el inverso

  $-2 \cdot 3 \cdot x \equiv -2 \cdot 4 \pmod 7$

  $x \equiv -8 \pmod 7$

  $x = 6$

- **$x=6$** es una solución

Teoría de números

Resolver **$3x \equiv 4 \pmod 7$**

- Encuentre el inverso de 3 mod 7 $\quad$ 3 mod 7

  El inverso es -2 $= \bar{a}$

- Multiplique a ambos lados de la congruencia por el inverso

  $-2 \cdot 3 \cdot x \equiv -2 \cdot 4 \pmod 7$

  $\boxed{x \equiv -8 \pmod 7}$

  $x = 6$

  $\boxed{x \equiv 6 \bmod 7}$

- **x=6** es una solución
- Todas las soluciones están dadas por $\boxed{\mathbf{x \equiv 6 \pmod 7}}$

  6

$\cancel{x} \bmod 7 = 6$

$$\boxed{x = 7 \times c + 6}$$

$c \in \mathbb{Z}$

$3x \equiv 4 \bmod 7$

$c = 0$

$x = 6$

$c = 1$

$x = 7 \times 1 + 6 = 13$

$c = 2$

$x = 7 \times 2 + 6 = 20$

$c = -1$

$x = -7 + 6 = -1$

$$\frac{39 \bmod 7}{4} = \frac{4 \bmod 7}{4}$$

$60 \bmod 7 = 4 \bmod 7$

$4 = 4$

$$-\frac{3 \bmod 7}{4} = \frac{4 \bmod 7}{4}$$

Teoría de números

Todas las soluciones están dadas por $\boxed{\mathbf{x \equiv 6 \pmod{7}}}$

- Se cumple que $7|(x-6)$, por lo tanto, $7 \cdot c = x-6$, es decir,

$$\mathbf{x = 6 + 7 \cdot c}$$

Teoría de números

Todas las soluciones están dadas por **$x \equiv 6 \pmod{7}$**

- Se cumple que $7|(x-6)$, por lo tanto, $7 \cdot c = x-6$, es decir,

$$x = 6 + 7 \cdot c$$

- Se asignan valores a c para conocer más soluciones:
    - Si **$c=0$**, se obtiene la solución **$x=6$**
    - Si **$c=-1$**, se obtiene la solución **$x=-1$**
    - Si **$c=1$**, se obtiene la solución **$x=13$**
    - Si **$c=2$**, se obtiene la solución **$x=20$**

Teoría de números

Resolver $\mathbf{5 \cdot x \equiv 2 \pmod{7}}$

- Encuentre el inverso de 5 mod 7

  El inverso es 3

- Multiplique a ambos lados de la congruencia por el inverso

$$3 \cdot 5 \cdot x \equiv 3 \cdot 2 \pmod{7}$$

$$x \equiv 6 \pmod{7}$$

$$x = 6$$

Encuentre 3 soluciones

$5x \equiv 2 \mod 7$

$\mathrm{mcd}(5, 7) = 1$

$5 \mod 7 \quad \left\{ 5 = 7 \times 0 + 5 \right.$

$7 \mod 5 \quad \left\{ \begin{array}{l} 7 = 5 \times 1 + 2 \\ 2 = 7 - 5 \times 1 \end{array} \right.$

$5 \mod 2 \quad \left\{ \begin{array}{l} 5 = 2 \times 2 + 1 \\ 1 = 5 - 2 \times 2 \end{array} \right.$

$1 = 5 - 2 \times 2$

$1 = 5 - 2(7 - 5)$

$1 = 5(3) + 7(-2)$

$\overline{a} = 3$

$x \equiv \overset{6}{6 \mod 7}$

6 $x \mod 7 = 6$

$x = 7 \times c + 6$

$x = 6$

Teoría de números

Resolver $\mathbf{5 \cdot x \equiv 2 \pmod{7}}$

- Encuentre el inverso de 5 mod 7

  El inverso es 3

- Multiplique a ambos lados de la congruencia por el inverso

  $$3 \cdot 5 \cdot x \equiv 3 \cdot 2 \pmod{7}$$

  $$x \equiv 6 \pmod{7}$$

  $$x = 6$$

- Solución general: $\mathbf{x \equiv 6 \bmod 7}$, $\mathbf{x = 6 + 7 \cdot c}$
- Soluciones: $x=6$, $x=13$, $x=-1$

$-4 \equiv 5 \bmod 9$ Teoría de números

$248 \equiv 5 \bmod 9$

Encuentre al menos 3 soluciones para la siguiente congruencia:

- **$4 \cdot x \equiv 5 \pmod 9$**

$mcd(4, 9)$

$4 \bmod 9 \quad \{ 4 = 9 \times 0 + 4$

$9 \bmod 4 \quad \begin{cases} 9 = 4(2) + 1 \\ 1 = 9 - 4(2) \end{cases}$

$140 \bmod 9 = 5 \bmod 9$

$1 = 9(1) + 4(-2)$

$\bar{a} = -2$

$x \equiv -10 \bmod 9$

$x \equiv 8$

$\boxed{x \bmod 9 = 8}$

$x = 9 \times c + 8$

$c = 3$

$c = -1$

$c = 6$

$x = 35$

$x = -1$

$x = 62$

Teoría de números

Resolver $\mathbf{4 \cdot x \equiv 5 \pmod{9}}$

- Encuentre el inverso de 4 mod 9

  El inverso es -2

- Multiplique a ambos lados de la congruencia por el inverso

  $-2 \cdot 4 \cdot x \equiv -2 \cdot 5 \pmod{9}$

  $x \equiv -10 \pmod{9}$

  $x = 8$

- Solución general: $\mathbf{x \equiv 8 \bmod 9}$, $\mathbf{x = 8 + 9 \cdot c}$
- Soluciones: $x=8$, $x=17$, $x=-1$

Teoría de números

Encuentre al menos 3 soluciones para la siguiente congruencia:

- **$2 \cdot x \equiv 7 \pmod{17}$**

Teoría de números

Resolver $\mathbf{2 \cdot x \equiv 7 \pmod{17}}$

- Encuentre el inverso de 2 mod 17

  El inverso es -8

- Multiplique a ambos lados de la congruencia por el inverso

  $-8 \cdot 2 \cdot x \equiv -8 \cdot 7 \pmod{17}$

  $x \equiv -56 \pmod{17}$

  $x = 12$

- Solución general: $\mathbf{x \equiv 12 \bmod 17}$, $\mathbf{x = 12 + 17 \cdot c}$
- Soluciones: $x=12$, $x=29$, $x=-5$

Teoría de números

> Encuentre al menos 3 soluciones para las siguiente congruencia:

- **$3 \cdot x \equiv 5 \pmod{16}$**

Teoría de números

Resolver $\mathbf{3 \cdot x \equiv 5 \pmod{16}}$

- Encuentre el inverso de 3 mod 16

  El inverso es -5

- Multiplique a ambos lados de la congruencia por el inverso

  $-5 \cdot 3 \cdot x \equiv -5 \cdot 5 \pmod{16}$

  $x \equiv -25 \pmod{16}$

  $x = 7$

- Solución general: $\mathbf{x \equiv 7 \bmod 16,\ x = 7 + 16 \cdot c}$
- Soluciones: $x=7$, $x=23$, $x=-9$

Acertijo de Sun-Tsu

Existe un número que cuando se divide entre 3, el residuo es 2, cuando se divide entre 5, el residuo es 3, y cuando se divide entre 7 el residuo es 2. ¿Cuál es el número?

$$\begin{cases} x \bmod 3 = 2 \\ x \bmod 5 = 3 \\ x \bmod 7 = 2 \end{cases}$$

Acertijo de Sun-Tsu

Existe un número que cuando se divide entre 3, el residuo es 2, cuando se divide entre 5, el residuo es 3, y cuando se divide entre 7 el residuo es 2. ¿Cuál es el número?

$$\mathbf{x \equiv 2 \pmod{3}}$$

$$\mathbf{x \equiv 3 \pmod{5}}$$

$$\mathbf{x \equiv 2 \pmod{7}}$$

Sistemas de congruencias lineales

Encontrar un valor de x que satisfaga las siguientes congruencias

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

Teorema del residuo Chino

Dado un sistema de congruencias de la forma:

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

Teorema del residuo Chino

- Encuentre $m=m_1 \cdot m_2 \cdot m_3$
- Encuentre $M_1=m/m_1$, $M_2=m/m_2$ y $M_3=m/m_3$
- Encuentre

  y_1, el inverso de M_1 mod m_1

  y_2, el inverso de M_2 mod m_2

  y_3, el inverso de M_3 mod m_3
- La solución está dada por $x=a_1M_1y_1+a_2M_2y_2+a_3M_3y_3$

Teoría de números

Resolver

$x \equiv 2 \pmod{3}$

$x \equiv 3 \pmod{5}$

$x \equiv 2 \pmod{7}$

$m = 105$

$M_1 = \frac{105}{3} = 35$

$M_2 = \frac{105}{5} = 21$

$M_3 = \frac{105}{7} = 15$

$y_1 = \text{inv } 35 \bmod 3 \Rightarrow -1$

$y_2 = \text{inv } 21 \bmod 5 \Rightarrow 1$

$y_3 = \text{inv } 15 \bmod 7 \rightarrow 1$

$\boxed{x = 23}$

$x = 2(35)(-1) + 3(21)(1) + (15)(2)(1)$

$35 \bmod 3$

$35 \bmod 3$

$$\begin{cases} 35 = 3 \times 11 + 2 \\ 2 = 35 - 3 \times 11 \end{cases}$$

$3 \bmod 2$

$$\begin{cases} 3 = 2 \times 1 + 1 \\ 1 = 3 - 2 \times 1 \end{cases}$$

$2 \bmod 1 = 0$

$1 = 3 - 2 \times 1$

$1 = 3 - 1(35 - 3 \times 11)$

$1 = (12)\,3 + (-1)\,35$

$\bar{a} = -1$

$21 \bmod 5$

$\mathrm{mod}(21,5)$

$21 \bmod 5 \begin{cases} 21 = 5 \times 4 + 1 \\ 1 = \underline{21 - 5 \times 4} \end{cases}$

$1 = 21 + 5(-4)$

$\bar{a} = 1$

$15 \bmod 7$

$\begin{cases} 15 = 7 \times 2 + 1 \\ 1 = \underline{15} + 7(-2) \end{cases}$

$\bar{a} = 1$

Teoría de números

Resolver

$$\mathbf{x \equiv 2 \pmod{3}}$$

$$\mathbf{x \equiv 3 \pmod{5}}$$

$$\mathbf{x \equiv 2 \pmod{7}}$$

- $m=3 \cdot 5 \cdot 7=105$
- $M_1=35$, $M_2=21$, $M_3=15$
- Se encuentran los inversos y_1, y_2, y_3 de:

  35 mod 3, 21 mod 5, 15 mod 7
- $y_1=-1$, $y_2=1$, $y_3=1$
- $x = 2 \cdot 35 \cdot (-1) + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = \mathbf{23}$

Teoría de números

Resolver

$$x \equiv 4 \pmod{11}$$

$$x \equiv 2 \pmod{5}$$

$$x \equiv 3 \pmod{7}$$

$M = 385$

$m_1 = 35$ $m_3 = 55$

$m_2 = 77$

y_1 inv $35 \bmod 11$ $y_1 = -1$

y_2 inv $77 \bmod 5$ $y_2 = -2$

y_3 inv $55 \bmod 7$ $y_2 = -5$

$4 \times (-1) \times 35 + 2 \times (-2) \times 77 + 3 \times 55 \times (-5) = -1273$

$35 \bmod 11$

$mcd(11, 35) = 1$

$35 \bmod 11$ $\begin{cases} 35 = 3 \times 11 + 2 \\ 2 = 35 + 11(-3) \end{cases}$

$11 \bmod 2$ $\begin{cases} 11 = 2(5) + 1 \\ 1 = 11 + 2(-5) \end{cases}$

$1 = 11 + 2(-5)$

$1 = 11 + (35 + 11(-3))(-5)$

$1 = 11(16) + 35(-5)$

$a = -5$

$77 \bmod 5$:

$1 = 5 + (77 + 5(-15))(-2)$

$1 = (31)5 + 77(-2)$

$\boxed{a = -2}$

$77 \bmod 5 \begin{cases} 77 = 5 \times 15 + 2 \\ 2 = \end{cases}$

$5 \bmod 2 \begin{cases} 1 = 5 + 2(-2) \end{cases}$

$\underline{55 \bmod 7}$

$55 \bmod 7 \begin{cases} 55 = 7 \times 7 + 6 \\ 6 = 55 + 7(-7) \end{cases}$

$7 \bmod 6 \begin{cases} 7 = 6(1) + 1 \\ 1 = 7 + 6(-1) \end{cases}$

$1 = 7 + 6(-1)$

$1 = 7 + (55 + 7(-7))(-1)$

$1 = (8)(7) + 55(-1)$

$\bar{a} = \cancel{5}\,\underline{7}$

Teoría de números

$\lfloor -15.3 \rfloor = -16$

Resolver

$$x \equiv 4 \pmod{11}$$

$$x \equiv 2 \pmod{5}$$

$$x \equiv 3 \pmod{7}$$

$\frac{-1173}{11} = -107$

$11(-107) = -1177$

$\frac{-1173}{5} = -235$

$\left\lfloor \frac{-1173}{7} \right\rfloor = -168$

- $m = 11 \cdot 5 \cdot 7 = 385$
- $M_1 = 35$, $M_2 = 77$, $M_3 = 55$
- Se encuentran los inversos y_1, y_2, y_3 de:

  35 mod 11, 77 mod 5, 55 mod 7
- $y_1 = -5$, $y_2 = -2$, $y_3 = -1$
- $x = 4 \cdot 35 \cdot (-5) + 2 \cdot 77 \cdot (-2) + 3 \cdot 55 \cdot (-1) = -1173$

Teoría de números

Resolver

$$x \equiv 4 \pmod{11}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 1 \pmod{3}$$

Resolver

$$\mathbf{x \equiv 4 \pmod{11}}$$

$$\mathbf{x \equiv 3 \pmod{5}}$$

$$\mathbf{x \equiv 1 \pmod{3}}$$

- $m=11 \cdot 5 \cdot 3=165$
- $M_1=15$, $M_2=33$, $M_3=55$
- Se encuentran los inversos y_1, y_2, y_3 de:

  15 mod 11, 33 mod 5, 55 mod 3

- $y_1=3$, $y_2=2$, $y_3=1$
- $x = 4 \cdot 15 \cdot 3 + 3 \cdot 33 \cdot 2 + 1 \cdot 55 \cdot 1 = 433$

- **Resolver el acertijo:**

Se tiene un número que dividido entre 5 da como residuo 2, dividido entre 3 se obtiene como residuo 2 y al dividirlo entre 2 sobra 1. Encuentre el número usando el teorema del residuo chino

Teoría de números

- **Resolver el acertijo:**

Se tiene un número que dividido entre 5 da como residuo 2, dividido entre 3 se obtiene como residuo 2 y al dividirlo entre 2 sobra 1. Encuentre el número usando el teorema del residuo chino

$$\mathbf{x \equiv 2 \pmod{5}}$$

$$\mathbf{x \equiv 2 \pmod{3}}$$

$$\mathbf{x \equiv 1 \pmod{2}}$$

Teoría de números

Resolver

$$\mathbf{x \equiv 2 \pmod 5}$$

$$\mathbf{x \equiv 2 \pmod 3}$$

$$\mathbf{x \equiv 1 \pmod 2}$$

- $m=5\cdot 3\cdot 2=30$
- $M_1=6$, $M_2=10$, $M_3=15$
- Se encuentran los inversos y_1, y_2, y_3 de:

  6 mod 5, 10 mod 3, 15 mod 2

- $y_1=1$, $y_2=1$, $y_3=1$
- $x = 2\cdot 6\cdot 1 + 2\cdot 10\cdot 1 + 1\cdot 15\cdot 1 = 47$