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:

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

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

$4 = 4$

$x = 6$

Teoría de números

Encuentre un valor x tal que:

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

un posible valor es x=6, porque

$18 \equiv 4 \pmod{7}$

Teoría de números

Encuentre un valor x tal que:

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

un posible valor es $x=6$, porque

$$18 \equiv 4 \pmod 7$$

- 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 $\overline{a}$

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

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

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

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

$3 \bmod 7$

$a \bmod m$

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

$\bar{a} = 1$

$\text{mcd}(a, m)$

$1 = (\bar{a})a + (s)m$

$1 = (1)7 - 3$

$3 \bmod 7 = 3$

$7 \bmod 3 = 1$

$3 \bmod 1 = 0$

$\bar{a} = -2$

$$\boxed{1 = 7 - 3(2)}$$

$3 = 3 - 7(0) = 3 = 3$

$$\overbrace{\bar{a}a}^{1}\, x \equiv b\bar{a} \bmod m$$

Multiplicando No va dar uno, pero lo deben asumir como 1

$$x \equiv 4(-2) \bmod 7$$

$$x \equiv -8 \bmod 7$$

x $$\boxed{x = 6}$$

$$3(6) \equiv 4 \bmod 7$$

$$18 \bmod 7 = 4 \bmod 7$$

$$4 = 4$$

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

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

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

  $x \equiv -8 \pmod 7$

  $x = 6$

- $\mathbf{x=6}$ es una solución

Teoría de números

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

- 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

a mod m

1) Inv 5 mod 7

mcd(5, 7) = 1

5 mod 7 = $\underline{5}$ → 5 = 5

7 mod 5 = 2 ← 2 = 7 − 5

$5 \bmod 2 = 1 \leftarrow 1 = 5 - 2(2)$

$2 \bmod 1 = 0$

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

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

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

$\bar{a} \quad a$

$x = 3(2) \bmod 7$

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

$30 \equiv 2 \bmod 7$

$30 \bmod 7 \equiv 2 \bmod 7$

$2 = 2$

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

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

$$x \equiv 6 \pmod 7$$

$$x = 6$$

Resolver $7 \cdot x \equiv 3 \pmod 5$

$ax \equiv b \bmod m$

$\mathrm{mcd}(a, m)$

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

Inv $a \bmod m$

$7 \bmod 5 = 2$

$5 \bmod 2 = \boxed{1}$

$2 \bmod 1 = 0$

$1 = 5 - 2(2)$

$2 = 7 - 5$

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

$\underline{1} = 5 - (2)7 + (2)5$

$1 = (3)5 + \underbrace{(-2)}_{\bar{q} = -2}7$

$x = \bar{q}\, b \bmod m$

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

$x = -6 \bmod 5 = 4$

$x = 4$

$7(4) = 3 \underbrace{\bmod}\, 5$

$28 \bmod 5 = 3$

$3 = 3$

Teoría de números

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

- 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

Resolver 11·x ≡ 5 (mod 6)

$ax \equiv b \bmod m \rightarrow$ 1.) Hallar $\underbrace{\text{inversa } a \bmod m}_{\bar{a}}$

2.) $x \equiv \bar{a}\, b \bmod m$

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

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

  $$x \equiv -8 \pmod 7$$

  $$x = 6$$

- $\mathbf{x=6}$ es una solución

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

$c \geq 1 \qquad 6/7c \qquad \sim \qquad 6/7$

Teoría de números

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

- 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,

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

- 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** -1 mod 7
  - Si **c=1**, se obtiene la solución **x=13** 13 mod 7
  - Si **c=2**, se obtiene la solución **x=20** 20 mod 7

Teoría de números

1) mcd(5, 7) = 1

$5(s) + 7(t) = 1$

Resolver **5·x ≡ 2 (mod 7)**

- Encuentre el inverso de 5 mod 7

  El inverso es 3

- Multiplique a ambos lados de la congruencia por el inverso

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

  $x \equiv 6 \pmod 7$

  $x = 6$

  $x = 6 + 7c$

Encuentre 3 soluciones

Teoría de números

Resolver **$5 \cdot x \equiv 2 \pmod 7$**

- 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: **$x \equiv 6 \bmod 7$, $x = 6 + 7 \cdot c$**
- Soluciones: $x=6$, $x=13$, $x=-1$

Teoría de números

Encuentre al menos 3 soluciones para la siguiente congruencia:

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

Teoría de números

Resolver $\mathbf{4 \cdot x \equiv 5 \ (mod\ 9)}$

- Encuentre el inverso de 4 mod 9

  El inverso es -2

- Multiplique a ambos lados de la congruencia por el inverso

  $-2 \cdot 4 \cdot x \equiv -2 \cdot 5 \ (mod\ 9)$

  $x \equiv -10 \ (mod\ 9)$

  $x = 8$

- Solución general: $\mathbf{x \equiv 8 \ mod\ 9,\ \ x = 8 + 9 \cdot c}$

- 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: $\mathbf{x \equiv 7 \bmod 16}$, $\mathbf{x = 7 + 16 \cdot c}$
- 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?

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?

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

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

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

Sistemas de congruencias lineales

Encontrar un valor de x que satisfaga las siguientes congruencias

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

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

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

Teorema del residuo Chino

Dado un sistema de congruencias de la forma:

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$x \equiv a_3 \pmod{m_3}$$

$$\vdots$$

$$x \equiv a_n \pmod{m_n}$$

Teoría de números

Teorema del residuo Chino

- Encuentre $m = m_1 \cdot m_2 \cdot m_3$, m_n
- Encuentre $M_1 = m/m_1$, $M_2 = m/m_2$ y $M_3 = m/m_3$ $\quad M_n = \frac{m}{m_n}$
- Encuentre

  y_1, el inverso de M_1 mod m_1

  y_2, el inverso de M_2 mod m_2 $\quad$ Yn = Mn mod mn

  y_3, el inverso de M_3 mod m_3
- La solución está dada por $x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$

  $+ a_n M_n y_n$

Teoría de números

Resolver

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

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

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

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

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

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

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

Teoría de números

Resolver

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

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

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

mcd(35, 11) = 1

(s)35 + (t)11 = 1

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

  35 mod 11, 77 mod 5, 55 mod 7

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

Resolver

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

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

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

Teoría de números

Resolver

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

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

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

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

  15 mod 11, 33 mod 5, 55 mod 3
- $y_1=3$, $y_2=2$, $y_3=1$
- $x = 4\cdot 15\cdot 3 + 3\cdot 33\cdot 2 + 1\cdot 55\cdot 1 = 433$

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

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

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

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

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

Resolver

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

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

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

- $m=5\cdot3\cdot2=30$
- $M_1=6$, $M_2=10$, $M_3=15$
- Se encuentran los inversos y_1, y_2, y_3 de:

  6 mod 5, 10 mod 3, 15 mod 2

- $y_1=1$, $y_2=1$, $y_3=1$
- $x = 2\cdot6\cdot1 + 2\cdot10\cdot1 + 1\cdot15\cdot1 = 47$