

# Congruencias lineales

Clase 30

IIC 1253

Prof. Pedro Bahamondes

# Outline

**Inverso modular**

Congruencias

Teorema chino del resto

Epílogo



# Inversos modulares

## Definición

$b$  es **inverso** de  $a$  en módulo  $n$  si  $a \cdot b \equiv_n 1$ .

Podemos denotarlo como  $a^{-1}$ . Ojo: no es lo mismo que  $\frac{1}{a}$ .

## Ejemplo

¿Cuál es el inverso de 5 en módulo 3?

¿Existe siempre inverso para todo  $a$  y módulo  $n$ ?

# Inversos modulares

## Teorema

$a$  tiene inverso en módulo  $n$  si y sólo si  $MCD(a, n) = 1$ .

## Ejercicio

Demuestre el teorema.

Si  $MCD(a, n) = 1$ , decimos que  $a$  y  $n$  son **primos relativos** o **coprimos**

# Inversos modulares

## Teorema

$a$  tiene inverso en módulo  $n$  si y sólo si  $MCD(a, n) = 1$ .

( $\Rightarrow$ ) Supongamos que  $a$  tiene inverso en módulo  $n$ , digamos  $b$ . Por demostrar:  $MCD(a, n) = 1$ .

Como  $b$  es el inverso de  $a$  en módulo  $n$ , se cumple que  $a \cdot b \equiv_n 1$ , y por lo tanto  $(a \cdot b) \bmod n = 1$ . Entonces, tenemos que  $a \cdot b = k \cdot n + 1$ , y despejando 1 obtenemos que  $1 = a \cdot b - k \cdot n$ . Luego, necesariamente cualquier entero  $c$  tal que  $c \mid a$  y  $c \mid n$  debe cumplir que  $c \mid 1$ , por lo que la única posibilidad es que  $c$  sea 1, y por lo tanto necesariamente  $MCD(a, n) = 1$ .

# Inversos modulares

## Teorema

$a$  tiene inverso en módulo  $n$  si y sólo si  $MCD(a, n) = 1$ .

( $\Leftarrow$ ) Supongamos que  $MCD(a, n) = 1$ . Por demostrar:  $a$  tiene inverso en módulo  $n$ .

Si ejecutamos el algoritmo extendido del MCD obtenemos  $s, t$  tales que

$$1 = s \cdot a + t \cdot n$$

$$\Leftrightarrow a \cdot s = (-t) \cdot n + 1$$

$$\Leftrightarrow a \cdot s \bmod n = 1$$

$$\Leftrightarrow a \cdot s \equiv_n 1$$

Y entonces  $a$  tiene inverso en módulo  $n$ , específicamente  $s$ . □

¡Podemos calcular el inverso con el algoritmo extendido!  
En tal caso, el coeficiente  $s$  que acompaña a  $a$  es su inverso

# Objetivos de la clase

- Conocer la estructura de una congruencia lineal
- Resolver congruencias lineales
- Demostrar el teorema chino del resto
- Resolver sistemas de congruencias lineales



# Outline

Inverso modular

**Congruencias**

Teorema chino del resto

Epílogo

# Notación

Dados  $a, b, n \in \mathbb{Z}$ , si  $a \equiv_n b$  también podemos escribir:

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

Esta es la notación más usada en la literatura.

Ojo que no es lo mismo que  $(b \bmod n)$

# Ecuaciones de congruencia

## Definición

Una **congruencia lineal** es una ecuación de la forma

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

donde  $n \in \mathbb{N} - \{0\}$ ,  $a, b \in \mathbb{Z}$  y  $x$  es una variable.

## Ejemplos

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

$$4x \equiv 3 \pmod{6}$$

¿Cómo resolvemos estas ecuaciones?

# Inversos modulares

Definición (con nueva notación)

$b$  es **inverso** de  $a$  en módulo  $n$  si

$$ab \equiv 1 \pmod{n}$$

Podemos denotarlo como  $a^{-1}$ . Ojo: no es lo mismo que  $\frac{1}{a}$ .

¿Existe siempre inverso para todo  $a$  y módulo  $n$ ?

# Inversos modulares

## Teorema

$a$  tiene inverso en módulo  $n$  si y sólo si  $MCD(a, n) = 1$ .

Si  $MCD(a, n) = 1$ , decimos que  $a$  y  $n$  son **primos relativos** o **coprimos**

# Ecuaciones de congruencia

Corolario (del teorema de los inversos)

Si  $a$  y  $n$  son primos relativos, entonces  $ax \equiv b \pmod{n}$  tiene solución en  $\mathbb{Z}_n$ .

Ejercicio

Demuestre el corolario.

Ejercicio

Resuelva las ecuaciones anteriores.

# Ecuaciones de congruencia

Corolario (del teorema de los inversos)

Si  $a$  y  $n$  son primos relativos, entonces  $ax \equiv b \pmod{n}$  tiene solución en  $\mathbb{Z}_n$ .

Como  $a$  y  $n$  son primos relativos,  $a$  tiene inverso en módulo  $n$ . Entonces:

$$\begin{aligned} ax \equiv b \pmod{n} &\Leftrightarrow (a^{-1} \cdot a)x \equiv (a^{-1} \cdot b) \pmod{n} \\ &\Leftrightarrow x \equiv (a^{-1} \cdot b) \pmod{n} \end{aligned}$$

# Ecuaciones de congruencia

## Ejercicio

Resuelva  $3x \equiv 2 \pmod{7}$ .

El inverso de 3 en módulo 7 es 5:  $3 \cdot 5 = 15 \equiv 1 \pmod{7}$ .

$$\begin{aligned}x &\equiv 5 \cdot 2 \pmod{7} \\ &\equiv 10 \pmod{7} \\ &\equiv 3 \pmod{7}\end{aligned}$$

$x = 3$  es solución en  $\mathbb{Z}_7$ .



# Outline

Inverso modular

Congruencias

**Teorema chino del resto**

Epílogo

# Teorema Chino del Resto

## Ejercicio

El General Tso se encontraba próximo a una nueva batalla, pero esta vez quería saber cuántos soldados de su ejército resultarían muertos, y para eso necesitaba contarlos.

Si los soldados se ordenaban en filas de 3, sobraban 2 soldados. Si se ordenaban en filas de 5, sobraban 3, y si se ordenaban en filas de 7, solo sobraban 2.

Si  $x$  es la cantidad de soldados en el ejército del General Tso:

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

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

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

¿Cómo resolvemos este sistema de ecuaciones?

# Teorema Chino del Resto

## Teorema

Sean  $m_1, m_2, \dots, m_n$  con  $m_i > 1$  tal que  $m_i, m_j$  son primos relativos con  $i \neq j$ . Para  $a_1, a_2, \dots, a_n \in \mathbb{Z}$ , el sistema de ecuaciones:

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

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

$$\vdots$$

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

tiene una única solución en  $\mathbb{Z}_m$  con  $m = \prod_{i=1}^n m_i$

La demostración es constructiva: ¡nos dará la solución!

# Teorema Chino del Resto

## Ejercicio

Demuestre el teorema.

## Ejercicio

¿Cuántos soldados tiene el ejército del General Tso?

# Teorema Chino del Resto

## Ejercicio

Demuestre el teorema.

Dividiremos la demostración en existencia (i) y unicidad (ii) de la solución al sistema de ecuaciones.

i) Sea  $m = m_1 \cdot m_2 \cdot \dots \cdot m_n$ . Para cada  $k \in \{1, \dots, n\}$  definimos

$$M_k = \frac{m}{m_k}$$

Dado que  $m_i, m_j$  son primos relativos para todo  $i \neq j$ , es claro que  $M_k$  y  $m_k$  son coprimos y por ende  $\text{MCD}(M_k, m_k) = 1$ . Por lo tanto,  $M_k$  tiene inverso  $M_k^{-1}$  en módulo  $m_k$ . Luego, definimos la solución  $x^*$  como:

$$x^* = a_1 \cdot M_1 \cdot M_1^{-1} + \dots + a_n \cdot M_n \cdot M_n^{-1}$$

# Teorema Chino del Resto

Definimos la solución  $x^*$  como:

$$x^* = a_1 \cdot M_1 \cdot M_1^{-1} + \dots + a_n \cdot M_n \cdot M_n^{-1}$$

¿Es  $x^*$  una solución para el sistema de ecuaciones?

Como  $M_j \equiv 0 \pmod{m_k}$  para todo  $j \neq k$ , entonces:

$$\begin{aligned} x^* &\equiv a_1 \cdot M_1 \cdot M_1^{-1} + \dots + a_n \cdot M_n \cdot M_n^{-1} \pmod{m_k} \\ &\equiv a_1 \cdot M_1 \cdot M_1^{-1} + \dots + a_k \cdot M_k \cdot M_k^{-1} + \dots + a_n \cdot M_n \cdot M_n^{-1} \pmod{m_k} \\ &\equiv a_k \cdot (M_k \cdot M_k^{-1}) \pmod{m_k} \\ &\equiv a_k \pmod{m_k} \end{aligned}$$

# Teorema Chino del Resto

## Ejercicio

Demuestre el teorema.

- ii) Por demostrar: si el sistema de ecuaciones tiene solución, entonces esta es única. Por contradicción, sean  $u, v$  soluciones distintas al sistema de congruencias. Para todo  $i \in \{1, \dots, n\}$  debe cumplirse que

$$u \equiv a_i \pmod{m_i}$$

$$v \equiv a_i \pmod{m_i}$$

y por transitividad de la equivalencia obtenemos que

$$u \equiv v \pmod{m_1}$$

$$u \equiv v \pmod{m_2}$$

$$\vdots$$

$$u \equiv v \pmod{m_n}$$

# Teorema Chino del Resto

## Lema

Sean  $m_1, m_2 > 1$  coprimos y  $u, v \in \mathbb{Z}$ . Si  $u \equiv v \pmod{m_1}$  y  $u \equiv v \pmod{m_2}$ , entonces  $u \equiv v \pmod{m_1 \cdot m_2}$ .

Supongamos que  $u \equiv v \pmod{m_1}$  y  $u \equiv v \pmod{m_2}$ . Por definición, sabemos que existen con  $k_1, k_2 \in \mathbb{Z}$  tales que:

$$u - v = k_1 \cdot m_1 \tag{1}$$

$$u - v = k_2 \cdot m_2 \tag{2}$$

por definición en (2):

$$m_2 \mid u - v \tag{3}$$

aplicando esto a (1):

$$m_2 \mid k_1 \cdot m_1 \tag{4}$$



# Teorema Chino del Resto

Como  $m_1$  y  $m_2$  son primos relativos, se debe tener que  $m_2 \mid k_1$ , por lo que existe  $k \in \mathbb{Z}$  tal que:

$$k_1 = k \cdot m_2 \quad (5)$$

y reemplazando en (1) obtenemos

$$\begin{aligned} u - v &= k_1 \cdot m_1 \\ u - v &= k \cdot m_2 \cdot m_1 \\ u &\equiv v \pmod{m_1 \cdot m_2} \end{aligned}$$

## Ejercicio

Generalice el lema para  $n$  equivalencias.

# Teorema Chino del Resto

ii) Anteriormente obtuvimos que

$$u \equiv v \pmod{m_1}$$

$$u \equiv v \pmod{m_2}$$

$$\vdots$$

$$u \equiv v \pmod{m_n}$$

Dado que  $m_1, m_2, \dots, m_n$  son primos relativos, por el lema se debe tener que:

$$u \equiv v \pmod{m_1 \cdot m_2 \cdot \dots \cdot m_n}$$

de donde se concluye que la solución es única en módulo  $m_1 \cdot m_2 \cdot \dots \cdot m_n$ .



# Teorema Chino del Resto

## Ejercicio

¿Cuántos soldados tiene el ejército del General Tso?

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

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

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

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

$$x = 2 \cdot 35 \cdot 35^{-1 \bmod 3} + 3 \cdot 21 \cdot 21^{-1 \bmod 5} + 2 \cdot 15 \cdot 15^{-1 \bmod 7}$$

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

$$x = 140 + 63 + 30$$

$$x = 233$$

$$x \equiv_{105} 23$$

# Outline

Inverso modular

Congruencias

Teorema chino del resto

**Epílogo**

# Objetivos de la clase

- Conocer la estructura de una congruencia lineal
- Resolver congruencias lineales
- Demostrar el teorema chino del resto
- Resolver sistemas de congruencias lineales