Inversos y congruencias lineales

Clase 29

IIC 1253

Prof. Sebastián Bugedo

Outline

¿Cómo están?

Tercer Acto: Aplicaciones

Algoritmos, grafos y números

Playlist Tercer Acto

DiscretiWawos #3

Además sigan en instagram:
@orquesta_tamen

Máximo común divisor

Teorema

Si $a, b \in \mathbb{Z} \setminus \{0\}$, entonces $MCD(a, b) = MCD(b,\ a \bmod b)$.

Ejercicio

Demuestre el teorema.

Algoritmo de Euclides extendido

Algoritmo extendido del MCD

Sea $a \geq b$.

1. Definimos una sucesión $\{r_i\}$ como:

$$r_0 = a,\ r_1 = b,\ r_{i+1} = r_{i-1} \bmod r_i$$

2. Definimos sucesiones $\{s_i\}$, $\{t_i\}$ tales que:

$$s_0 = 1, \quad t_0 = 0$$

$$s_1 = 0, \quad t_1 = 1$$

$$s_{i+1} = s_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot s_i, \quad t_{i+1} = t_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot t_i$$

3. Calculamos estas sucesiones hasta un k tal que $r_k = 0$.
4. Entonces, $MCD(a, b) = r_{k-1} = s_{k-1} \cdot a + t_{k-1} \cdot b$.

Tenemos todo para calcular el MCD y los pesos que lo expresan como combinación lineal de a y b

Algoritmo de Euclides extendido

Ejercicio

Dados $a = 8$ y $b = 5$, use el algoritmo para calcular $MCD(a, b)$ y $s, t \in \mathbb{Z}$ tales que $MCD(a, b) = s \cdot a + t \cdot b$.

Algoritmo de Euclides extendido

Usamos el algoritmo extendido sobre $a = 8$ y $b = 5$

i	r_i	s_i	t_i	combinación
0	8	1	0	$8 = 1 \cdot 8 + 0 \cdot 5$
1	5	0	1	$5 = 0 \cdot 8 + 1 \cdot 5$
2	$8 \bmod 5$	$1 - \lfloor 8/5 \rfloor \cdot 0$	$0 - \lfloor 8/5 \rfloor \cdot 1$	
	3	1	-1	$3 = 1 \cdot 8 - (-1) \cdot 5$
3	$5 \bmod 3$	$0 - \lfloor 5/3 \rfloor \cdot 1$	$1 - \lfloor 5/3 \rfloor \cdot (-1)$	
	2	-1	2	$2 = (-1) \cdot 8 + 2 \cdot 5$
4	$3 \bmod 2$	$1 - \lfloor 3/2 \rfloor \cdot (-1)$	$-1 - \lfloor 3/2 \rfloor \cdot 2$	
	1	2	-3	$1 = 2 \cdot 8 + (-3) \cdot 5$
5	$2 \bmod 1$	—	—	
	0	—	—	

Concluimos que $MCD(8, 5) = 1 = 2 \cdot 8 + (-3) \cdot 5$, con $s = 2$ y $t = -3$.

Identidad de Bézout

El desarrollo algorítmico anterior muestra el siguiente resultado en acción

Identidad de Bézout

Para todo $a, b \in \mathbb{N} \setminus \{0\}$, existen $s, t \in \mathbb{Z}$ tales que

$$MCD(a, b) = sa + tb$$

Este es un resultado elemental en teoría de números

Objetivos de la clase

- Conocer el concepto de inverso en $\mathbb{Z}_n$
- Conocer la estructura de una congruencia lineal
- Resolver congruencias lineales

Outline

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

$$\begin{aligned} & 1 = s \cdot a + t \cdot n \\ \Leftrightarrow \quad & a \cdot s = (-t) \cdot n + 1 \\ \Leftrightarrow \quad & a \cdot s \bmod n = 1 \\ \Leftrightarrow \quad & a \cdot s \equiv_n 1 \end{aligned}$$

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

Outline

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?

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:

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

Ecuaciones de congruencia

Ejercicio

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

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

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

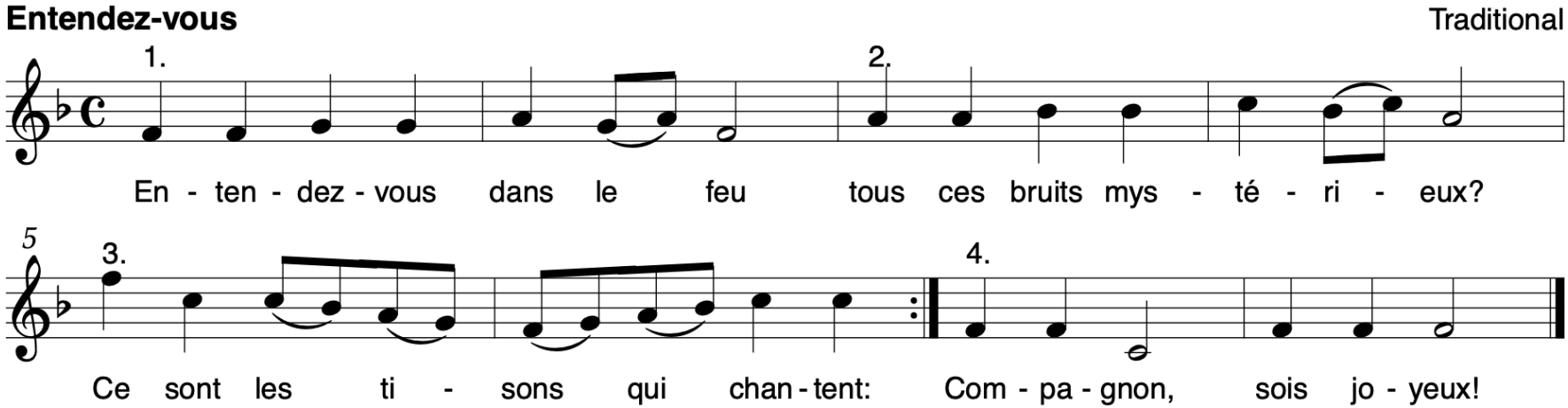
$x = 3$ es solución en $\mathbb{Z}_7$.

Outline

Objetivos de la clase

- Conocer el concepto de inverso en $\mathbb{Z}_n$
- Conocer la estructura de una congruencia lineal
- Resolver congruencias lineales

Última vocalización



Entendez-vous dans le feu
tous ces bruits mystérieux?

Ce sont les tisons qui chantent:
Compagnon, sois joyeux!