Ecuaciones lineales en cuerpos finitos

Silvio Reggiani

Álgebra y Geometría Analítica II (LCC)
FCEIA - UNR

25 de noviembre de 2016

Definición

Un **cuerpo** es un conjunto $\mathbb{F}$ dotado de dos operaciones, $+$ (suma) y $\cdot$ (producto), que satisfacen para todos $a, b, c \in \mathbb{F}$:

(S1) la suma es asociativa: $a + (b + c) = (a + b) + c$;

(S2) la suma es conmutativa: $a + b = b + a$;

(S3) la suma tiene un elemento nulo $0 \in \mathbb{F}$ tal que $a + 0 = a$;

(S4) existen los opuestos: para cada $a \in \mathbb{F}$ existe $-a \in \mathbb{F}$ tal que $a + (-a) = 0$;

(P1) el producto es asociativo: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

(P1) el producto es conmutativo: $a \cdot b = b \cdot a$;

(P3) el producto tiene un elemento neutro $1 \in \mathbb{F}$, $1 \neq 0$, tal que $a \cdot 1 = a$;

(P4) existen los inversos de los elementos no nulos: para cada $a \in \mathbb{F}$, $a \neq 0$, existe $a^{-1} \in \mathbb{F}$ tal que $a \cdot a^{-1} = 1$;

(D) propiedad distributiva: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Ejemplos conocidos

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ son cuerpos.
- $\mathbb{N}$, $\mathbb{Z}$ no son cuerpos.

Teorema

Cualquier resultado que hayamos probado para los números reales (o racionales o complejos) usando sólo los axiomas S1, ..., S4, P1, ..., P4, D será válido para cualquier cuerpo $\mathbb{F}$.

Ejemplo

$$\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

es un cuerpo (con las operaciones heredadas de $\mathbb{R}$).

Ejemplo (cont.)

- Primero debemos ver que las operaciones de suma y producto en $\mathbb{R}$ son *cerradas* en $\mathbb{Q}[\sqrt{2}]$.
- La suma es cerrada: si $a, b, c, d \in \mathbb{Q}$ entonces

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

- El producto es cerrado: si $a, b, c, d \in \mathbb{Q}$ entonces

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

- Con esto se ve fácilmente que se satisfacen todos los axiomas excepto P4 (existencia de inversos).

Ejemplo (cont.)

- Para ver que también vale P4, notemos que si $a + b\sqrt{2} \neq 0$ entonces

$$\begin{aligned} \frac{1}{a + b\sqrt{2}} &= \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} \\ &= \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2} \in \mathbb{Q}[\sqrt{2}] \end{aligned}$$

- Observar que $a + b\sqrt{2} \neq 0 \iff a \neq 0$ o $b \neq 0$, de lo contrario tendríamos que $\sqrt{2} \in \mathbb{Q}$. Además esto implica que $a^2 - 2b^2 \neq 0$ (completar detalles como ejercicio).

Comentario

- $\mathbb{Q}[\sqrt{2}]$ es el cuerpo que se obtiene *agregando* a $\mathbb{Q}$ la raíz del polinomio $x^2 - 2 = 0$.
- $\mathbb{C}$ es el cuerpo que se obtiene *agregando* a $\mathbb{R}$ la raíz del polinomio $x^2 + 1 = 0$.
- **Extensión de cuerpos:** es un procedimiento que consiste en construir un nuevo cuerpo a partir de uno dado agregando raíces de polinomios (con coeficientes en el cuerpo dado).
- En lo que sigue estudiaremos algo sobre cuerpos finitos, que en lugar de obtenerse agregando elementos se obtienen *quitando*, o mejor dicho, *identificando* ciertos elementos de $\mathbb{Z}$.

Ejemplo

Consideramos en el conjunto $\mathbb{Z}_2 = \{0, 1\}$ las operaciones dadas por las siguientes tablas

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

- Es fácil verificar que $\mathbb{Z}_2$ con estas operaciones es un cuerpo (se obtiene identificando los enteros pares y los enteros impares).
- Observar que en $\mathbb{Z}_2$ se verifica la identidad $1 + 1 = 0$.
- Esto también puede expresarse como $1 = -1$, pero preferimos no utilizar esta notación.
- En $\mathbb{Z}_2$ no es posible definir un orden compatible con la suma y el producto. En efecto,
  - $0 < 1 \implies 1 = 0 + 1 < 1 + 1 = 0$, ABS
  - $1 < 0 \implies 0 = 1 + 1 < 0 + 1 = 1$, ABS

Característica de un cuerpo

- Todo cuerpo $\mathbb{F}$ tiene un elemento $1 \neq 0$.
- ¿Qué pasa si sumamos 1 sucesivas veces?

En $\mathbb{F} = \mathbb{R}$ obtenemos todos los números naturales:

$$\begin{aligned} 1 &= 1 \\ 1+1 &= 2 \\ 1+1+1 &= 3 \\ 1+1+1+1 &= 4 \\ 1+1+1+1+1 &= 5 \\ &\vdots \end{aligned}$$

En $\mathbb{Z}_2$ las sumas empiezan a repetirse:

$$\begin{aligned} 1 &= 1 \\ 1+1 &= 0 \\ 1+1+1 &= 1 \\ 1+1+1+1 &= 0 \\ 1+1+1+1+1 &= 1 \\ &\vdots \end{aligned}$$

- Si la suma sucesiva del 1 empieza a repetirse, entonces $1 + 1 + \cdots + 1 = 0$ eventualmente.

Definición

Sea $\mathbb{F}$ un cuerpo y sea $p \in \mathbb{N}$.

- Decimos que $\mathbb{F}$ tiene **característica** p si p es el menor natural tal que
$$\underbrace{1 + 1 + \cdots + 1}_{p \text{ veces}} = 0.$$
- Decimos que $\mathbb{F}$ tiene **característica** 0 si no existe p con esa propiedad (o sea, cualquier suma de unos en $\mathbb{F}$ es distinta de cero).

Ejemplo

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ son cuerpos de característica 0 (principio de inducción).
- $\mathbb{Z}_2$ es un cuerpo de característica 2.

Teorema

Si $\mathbb{F}$ es un cuerpo de característica $p \neq 0$, entonces p es un número primo.

Dem.

Razonamos por el absurdo.

- Si p no es primo, entonces $p = ab$ para ciertos naturales $a, b \geq 2$.
- $0 = \underbrace{1 + \cdots + 1}_{p \text{ veces}} = (\underbrace{1 + \cdots + 1}_{a \text{ veces}})(\underbrace{1 + \cdots + 1}_{b \text{ veces}})$.
- Como $\mathbb{F}$ es cuerpo, un producto igual a cero implica que alguno de los factores es igual a cero.
- Luego $\underbrace{1 + \cdots + 1}_{a \text{ veces}} = 0$ o bien $\underbrace{1 + \cdots + 1}_{b \text{ veces}} = 0$.
- Contradicción pues $a, b < p$ y p es el menor natural tal que sumar p veces el 1 da igual a 0. $\square$

Enteros módulo m

La *aritmética módulo* $m \geq 2$ es la aritmética de los restos de la división por m. Más precisamente:

- Dos enteros $x, y \in \mathbb{Z}$ se dicen **congruentes módulo** m si tienen el mismo resto al dividirlos por m. En símbolos,

$$x \equiv y \mod m \iff m \mid (y - x)$$

- La congruencia módulo m es una relación de equivalencia en $\mathbb{Z}$ (esto ya lo probamos cuando estudiamos divisibilidad, con otras palabras).
- Esta relación de equivalencia tiene m clases de equivalencia distintas (que corresponden a los posibles restos de la división por m).
- La suma y multiplicación en $\mathbb{Z}$ *bajan* al conjunto de clase de equivalencia. Esta es la llamada aritmética de los restos de la división por m, o aritmética módulo m.

Lema

Sean $x, x', y, y' \in \mathbb{Z}$ *tales que*

$$x \equiv x' \mod m \qquad\qquad y \equiv y' \mod m$$

Entonces,

1. $x + y \equiv x' + y' \mod m$
2. $xy \equiv x'y' \mod m$

En palabras, el resto de la división de $x + y$ *y* xy *entre* m *sólo depende de los restos de la división de* x *e* y *entre* m*.*

Dem.

Queda como ejercicio entender por qué esto ya fue probado. □

Para evitar trabajar con clases de equivalencia, usaremos la siguiente convención.

- $\mathbb{Z}_m := \{0, 1, \ldots, m-1\}$ (los restos de la división por m)
- La suma de $x, y, \in \mathbb{Z}_m$ es *el resto de la división por m de la suma de* x, y *en* $\mathbb{Z}$
- El producto de $x, y, \in \mathbb{Z}_m$ es *el resto de la división por m del producto* x, y *en* $\mathbb{Z}$

Lema

En $\mathbb{Z}_m$ *se verifican los axiomas*

- *S1, . . . , S4 (todos los axiomas de la suma)*
- *P1, P2, P3 (todos los axiomas del producto, salvo la existencia de inversos)*
- *D (ley distributiva)*

Dem.

Estos axiomas se verifican en $\mathbb{Z}$. $\square$

$\mathbb{Z}_2 = \{0, 1\}$

Las dos definiciones que vimos coinciden

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$\mathbb{Z}_3 = \{0, 1, 2\}$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Observar que los elementos no nulos tienen inverso: $1 = 1^{-1}$, $2 = 2^{-1}$. Luego en $\mathbb{Z}_3$ también se satisface P4.

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Observemos que $2 \in \mathbb{Z}_4$ no posee inverso multiplicativo (no hay ningún elemento que multiplicado por 2 dé 1). Luego $\mathbb{Z}_4$ no es un cuerpo.

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}_5$ es un cuerpo (el 1 aparece en todas las filas de la tabla de multiplicar excepto la primera, obviamente). Más precisamente,

$$1^{-1} = 1 \qquad 2^{-1} = 3$$
$$3^{-1} = 2 \qquad 4^{-1} = 4$$

Teorema

$\mathbb{Z}_p$ es un cuerpo $\iff$ p es primo.

Dem.

Sólo debemos ver que P4 $\iff$ p es primo (ya sabemos que las otras propiedades se cumplen).

Supongamos primero que p es primo

- Sea $x \in \mathbb{Z}_p - \{0\} = \{1, 2, \ldots, p-1\}$.
- x, p son coprimos en $\mathbb{Z}$.
- Existen $s, t \in \mathbb{Z}$ tales que $1 = sx + tp$ en $\mathbb{Z}$.
- $s = pq + r$, $0 \leq r < p$ (dividimos s por p).
- $1 = sx + tp = (pq + r)x + tp = rx + (q + t)p$ en $\mathbb{Z}$.
- $1 = rx$ en $\mathbb{Z}_p \implies r = x^{-1}$ en $\mathbb{Z}_p$,
- $\implies$ P4 $\implies$ $\mathbb{Z}_p$ cuerpo.

Dem. (cont.)

Supongamos que p no es primo

- $p = xy$ con $2 \leq x, y \leq p - 1$.
- $xy = 0$ en $\mathbb{Z}_p \implies \mathbb{Z}_p$ no es cuerpo. $\square$

Teorema (del binomio en caracterśitica p)

Sea $\mathbb{F}$ *un cuerpo de característica* $p \neq 0$, *entonces para todos* $a, b \in \mathbb{F}$ *vale*

$$(a+b)^p = a^p + b^p.$$

Lema

Para todo $1 \leq k \leq p-1$, $\displaystyle\binom{p}{k} = \frac{p!}{k!(p-k)!}$ *es divisible por* p

Dem.

Ejercicio. Dar una prueba algebraica y una prueba combinatoria.

Dem. del Teorema

- $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$
- En $\mathbb{Z}_p$, $\binom{p}{k} a^k b^{p-k}$ significa sumar $\binom{p}{k}$ veces el término $a^k b^{p-k}$.
- Por el Lema, $\binom{p}{k} a^k b^{p-k} = 0$ para todo $1 \leq k \leq p-1$.
- Luego $(a+b)^p = a^p + b^p$. $\square$

Ecuaciones lineales en $\mathbb{Z}_p$

Estudiar ecuaciones lineales en $\mathbb{Z}_p$ es equivalente a estudiar el álgebra de matrices con coeficientes en $\mathbb{Z}_p$.

- Toda la teoría que desarrollamos sobre ecuaciones lineas vale para $\mathbb{Z}_p$ (nunca usamos los axiomas de orden).
- Toda la teoría que desarrollamos sobre determinantes vale para $\mathbb{Z}_p$ (tampoco usamos el orden aquí).
- Sin embargo, hay que tener algunas precauciones.

Ejemplo

Si $A \in \mathbb{Z}_p^{n\times n}$ y A' es la matriz que se obtiene de A intercambiando las filas $i \neq j$, entonces

$$\det A' = (p-1)\det A$$

(en $\mathbb{Z}_p$, el opuesto de 1 es $p-1$).

Ejemplo

1. Calcular el determinante de $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathbb{Z}_2^{2\times 2}$. Solución:

$$\begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} = (-1) \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1 \cdot \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1$$

2. Calcular el determinante de $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathbb{Z}_3^{2\times 2}$. Solución:

$$\begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} = (-1) \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 2 \cdot \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 2$$

En ambos casos la matriz es invertible.

Ejemplo

Sea la matriz $A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \in (\mathbb{Z}_2)^{3\times 3}$.

1. Decidir si A es invertible.
2. Resolver el sistema lineal $AX = 0$ sobre $\mathbb{Z}_2$.

Solución: Para resolver ambos problemas al mismo tiempo llevamos A a su forma ERF

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

$$\to \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} = R$$

Luego...

Ejemplo (cont.)

1. ... A no es invertible, pues es equivalente por filas a una matriz con una fila nula;
2. El sistema homogéneo

$$\begin{aligned} x_1 + x_2 &= 0 \\ x_1 + x_3 &= 0 \\ x_2 + x_3 &= 0 \end{aligned} \qquad (AX = 0)$$

es equivalente al sistema homogéneo

$$\begin{aligned} x_1 + x_3 &= 0 \\ x_2 + x_3 &= 0 \end{aligned} \qquad (RX = 0)$$

cuyo conjunto de soluciones es

$$\begin{aligned} \{(-x_3, -x_3, x_3) : x_3 \in \mathbb{Z}_2\} &= \{(x_3, x_3, x_3) : x_3 \in \mathbb{Z}_2\} \\ &= \{(0,0,0), (1,1,1)\} \text{ (cmpt. indet.)} \end{aligned}$$

Ejemplo

Sea la matriz $A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \in (\mathbb{Z}_3)^{3\times 3}$.

1. Decidir si A es invertible y encontrar su inversa en caso afirmativo.
2. Resolver el sistema $AX = Y$ sobre $\mathbb{Z}_3$ para $Y = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}$.

Solución: Hemos visto varias formas de resolver este problema. En este caso usaremos la matriz adjunta. Primero calculamos el determinante de A.

$$\det A = \begin{vmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{vmatrix} = 1 \cdot 2 \cdot 2 = 1$$

Luego, A es invertible. Más aún, su inversa esta dada por...

Ejemplo (cont.)

$$A^{-1} = \frac{1}{\det A} \operatorname{adj} A = \begin{pmatrix} -1 & -1 & 1 \\ -1 & 1 & -1 \\ 1 & -1 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 1 \\ 2 & 1 & 2 \\ 1 & 2 & 2 \end{pmatrix}$$

Finalmente, el sistema $AX = Y$ es compatible determinado y su (única) solución es

$$X = A^{-1}Y = \begin{pmatrix} 2 & 2 & 1 \\ 2 & 1 & 2 \\ 1 & 2 & 2 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2+2 \\ 1+2\cdot 2 \\ 2+2\cdot 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$$

Matrices de Hankel

Una **matriz de Hankel** es una matriz cuadrada con antidiagonales constantes. Es decir, A es una matriz de Hankel si

$$A_{i,j} = A_{(i+1),(j-1)}$$

(cuando los índices tengan sentido).

- Las matrices de los ejemplos anteriores eran de Hankel.
- Las tablas de sumar en $\mathbb{Z}_p$ nos dan matrices de Hankel.

$$\underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{\in (\mathbb{Z}_2)^{2\times 2}} \qquad \underbrace{\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}}_{\in (\mathbb{Z}_3)^{3\times 3}} \qquad \underbrace{\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{pmatrix}}_{\in (\mathbb{Z}_5)^{5\times 5}}$$

Proposición

Sea p un número primo, $p \neq 2$, y sea $A \in (\mathbb{Z}_p)^{p \times p}$ la matriz de Hankel dada por $A_{ij} = (i-1) + (j-1)$. Entonces $\det A = 0$.

Dem.

- Aplicamos a A las OEF $e_i =$ "$\mathtt{f_p} \to \mathtt{f_p} + \mathtt{f_i}$".
- A es equivalente por filas a $B = e_{p-1}(\cdots e_2(e_1(A))\cdots)$.
- $\det A = \det B$, pues e_i es tipo II para todo i.
- $B_{pj} = 0 + 1 + 2 + \cdots + (p-1) = \dfrac{(p-1)p}{2} = 0.$
- La última fila de B es nula, luego
- $\det A = \det B = 0$ $\square$

Aplicaciones: reglas de divisibilidad

- **Problema:** dados $a \in \mathbb{Z}$ y $m \in \mathbb{N}$, ¿cuándo $m \mid a$?
- Podemos usar aritmética módulo m para resolver este problema:
$$m \mid a \iff a = 0 \text{ en } \mathbb{Z}_m$$
- OBS: $a \in \mathbb{Z}_m$ es el resultado de sumar a veces $1 \in \mathbb{Z}_m$

Divisibilidad por 2

- $a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$ (expr. en base 10).
- $10^i = 0$ en $\mathbb{Z}_2$ para todo $i \geq 1$.
- $a = 0$ en $\mathbb{Z}_2 \iff a_0 = 0$ en $\mathbb{Z}_2$.
- $2 \mid a \iff a_0$ es par (pero esto ya lo sabíamos ;-).

Divisibilidad por 4

- $a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$ (expr. en base 10).
- Hay dos maneras de trabajar este problema:
    1. $4 \mid a \iff a$ es par y $a/2 = 0$ en $\mathbb{Z}_2$.
    2. $a = 0$ en $\mathbb{Z}_4$ (aunque $\mathbb{Z}_4$ no es un cuerpo, es más *elegante* trabajar de esta manera).
- $10^i = 0$ en $\mathbb{Z}_4$ para todo $i \geq 2$.
- $a = a_1 10 + a_0$ en $\mathbb{Z}_4$.
- $4 \mid a \iff$ 4 divide al número que se forma con los dos últimos dígitos de a.

Ejemplo

- $4 \mid 8$, $4 \mid 12$, $4 \mid 120$, $4 \mid 1873246234988853242394624$
- $4 \nmid 123233210$, $4 \nmid 21387123765123651237651238712314$

Divisibilidad por 3

- $a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$ (expr. en base 10).
- Usamos el teorema del binomio en $\mathbb{Z}_3$: para $i \geq 1$

$$10^i = (9+1)^i = \sum_{k=0}^{i} \binom{i}{k} 9^i = \binom{i}{0} 9^0 = 1$$

  pues $9^i = 0$ en $\mathbb{Z}_3$.
- $a = 0$ en $\mathbb{Z}_3 \iff a_n + a_{n-1} + \cdots + a_1 + a_0 = 0$ en $\mathbb{Z}_3$.
- $3 \mid a$ (en $\mathbb{Z}$) $\iff$ la suma de sus cifras es divisible por 3 (en realidad, en esta suma se pueden omitir las cifras que sean múltiplo de 3).

Ejemplo

- $3 \mid 51234897$. En efecto,

$$\begin{aligned} 3 \mid 51234897 &\iff 3 \mid 5+1+2+3+4+8+9+7 \\ &\iff 3 \mid 5+1+2+4+8+7 = 27 \end{aligned}$$

  Luego, $3 \mid 51234897$.

- Decidir si $a = 2850794330094087974062$ es múltiplo de 3.

$$\begin{aligned} 3 \mid a &\iff 3 \mid 2+8+5+0+7+9+4+3+3+0+0+9 \\ &\qquad\qquad +4+0+8+7+9+7+4+0+6+2 \\ &\iff 3 \mid 2+8+5+7+4+4+8+7+7+4+2 = 58 \\ &\iff 3 \mid 5+8 = 13 \end{aligned}$$

  Luego, a **no** es múltiplo de 3.

Divisibilidad por 11

- En $\mathbb{Z}_{11}$, $10 = -1 \implies 10^i = (-1)^i$.
- $a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0 = 0$ en $\mathbb{Z}_{11} \iff a_0 - a_1 + \cdots + (-1)^n a_n = 0$ en $\mathbb{Z}_{11}$.
- Por tanto, un entero a es divisible por 11 si la suma alternada de sus cifras en un múltiplo de 11.

Ejemplo

- 1111 es divisible por 11.
- 11111 no es divisible por 11.
- Un número capicúa con una cantidad par de cifras es divisible por 11.

Ejercicio

Escribir reglas de divisibilidad por 5, 6, 7, 8 y 9.

Aritmética del calendario

Ejemplo

Determinar qué día de la semana fue el 23 de noviembre de 2015.

$$
\begin{array}{llll}
0 = \text{dom} & 1 = \text{lun} & 2 = \text{mar} & 3 = \text{mié} \\
4 = \text{jue} & 5 = \text{vie} & 6 = \text{sáb} &
\end{array}
$$

- 23 nov 2016 $= 3$, 23 nov 2015 $= x$.
- $x + 366 = 3$ (2016 es bisiesto).
- En $\mathbb{Z}_7$, $366 = 350 + 16 = 7 \cdot 50 + 7 \cdot 2 + 2 = 2$.
- Luego, $x = 3 - 366 = 3 - 2 = 1 =$ lun.

Ejemplo

Determinar qué día de la semana fue el 23 de noviembre de 1810.

- Calendario Gregoriano: desde 1582.
- Tiene años comunes (365 días) y años bisiestos (366 días).
- Años seculares: múltiplos de 100, e.g. 1600, 1700, 1800, ...
- Un año secular es bisiesto $\iff$ es múltiplo de 400, e.g. 1600 es bisiesto pero 1700 no es bisiesto.
- Si al 23 nov 1810 le corresponde el día x, entonces

$$\begin{aligned} 3 &= x + (2016 - 1810) \cdot 365 + N \\ &= x + 206 \cdot 365 + N \qquad (365 = 1) \\ &= x + 210 - 4 + N = x - 4 + N \\ \implies 0 &= x + N \end{aligned}$$

  donde N es la cantidad de años bisiestos entre 1810 y 2016.

Ejemplo (cont.)

- ¿Cómo encontramos N?
- El último año bisiesto antes de 1810 es 1808.
- El año 2016 es bisiesto.
- Entre 1810 y 2016 hay un solo año secular: 1900.
- $N = \dfrac{2016 - 1808}{4} - 1 = 51.$
- Luego, $x = -N = -51 = -49 - 2 = -2 = 5 =$ vie.

Aplicación a funciones polinomiales

Definición

Sea $\mathbb{F}$ un cuerpo. Una función $Q : \mathbb{F} \to \mathbb{F}$ se dice una **función polinomial** (a veces llamada simplemente un polinomio) si tiene la forma

$$Q(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

para algún $n \geq 0$ y ciertos $a_0, a_1, \ldots, a_n \in \mathbb{F}$.

Ejemplo

La función $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = 2^x$ no es polinomial.
Solución: usamos un poco de análisis matemático:

- $f(x) = e^{x \log 2}$;
- $f^{(n)}(x) = (\log 2)^n f(x) \neq 0$ (derivada n-ésima);
- Las funciones polinomiales en $\mathbb{R}$ tienen derivada nula para n suficientemente grande.

En $\mathbb{Z}_p$ la situación es muy diferente

Teorema

Toda función $f : \mathbb{Z}_p \to \mathbb{Z}_p$ es una función polinomial.

Lema

Sea $\mathbb{F}$ *un cuerpo y sean* $a_1, \ldots, a_n \in \mathbb{F}$. *Consideremos la* **matriz de Vandermonde** $V \in \mathbb{F}^{n \times n}$ *dada por*

$$V = \begin{pmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{pmatrix}.$$

Entonces

$$\det V = \prod_{i<j} (a_j - a_i).$$

En particular, si $a_1, \ldots, a_n$ *son todos distintos en* $\mathbb{F}$, *entonces* V *es invertible.*

Dem.

Ejercicio. □

Dem. del Teorema

Buscamos

$$Q(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{p-1} x^{p-1}$$

tal que $Q(x) = f(x)$ para todo $x \in \mathbb{Z}_p$. Este problema lleva a un sistema de p ecuaciones lineales con p incógnitas $a_0, a_1, \ldots, a_{p-1}$

$$\begin{aligned}
a_0 + a_1 0 + a_2 0^2 + \cdots + a_{p-1} 0^{p-1} &= f(0) \\
a_0 + a_1 1 + a_2 1^2 + \cdots + a_{p-1} 1^{p-1} &= f(1) \\
a_0 + a_1 2 + a_2 2^2 + \cdots + a_{p-1} 2^{p-1} &= f(2) \\
&\vdots \\
a_0 + a_1 (p-1) + a_2 (p-1)^2 + \cdots + a_{p-1} (p-1)^{p-1} &= f(p-1)
\end{aligned}$$

Dem. del Teorema (cont.)

Observemos que la matriz de coeficientes del sistema anterior es la matriz de Vandermonde asociada a los elementos $0, 1, 2, \ldots, p-1$ (todos distintos en $\mathbb{Z}_p$):

$$V = \begin{pmatrix} 1 & 0 & 0^2 & \cdots & 0^{p-1} \\ 1 & 1 & 1^2 & \cdots & 1^{p-1} \\ 1 & 2 & 2^2 & \cdots & 2^{p-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & p-1 & (p-1)^2 & \cdots & (p-1)^{p-1} \end{pmatrix}$$

Por el lema previo, V es invertible y por ende el sistema tiene solución única. $\square$

Observación

El teorema nos dice que existe un único polinomio $Q(x)$ de grado a lo sumo $p-1$ tal que $f(x) = Q(x)$. En particular, todo polinomio con coeficientes en $\mathbb{Z}_p$ de grado mayor que p, puede reescribirse como un polinomio de grado a lo sumo $p-1$.

Ejemplo

Encontrar un polinomio $Q(x)$ de grado a lo sumo 2 sobre $\mathbb{Z}_3$ tal que $Q(x) = 2^x$ para todo $x \in \mathbb{Z}_3$. Solución: si $Q(x) = ax^2 + bx + c$, debemos resolver el sistema

$$\begin{aligned} Q(0) &= c = 2^0 = 1 \\ Q(1) &= a + b + c = 2^1 = 2 \\ Q(2) &= a + 2b + c = 2^2 = 1 \end{aligned}$$

Matricialmente,

$$\left(\begin{array}{ccc|c} 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 2 \\ 1 & 2 & 1 & 1 \end{array}\right) \to \left(\begin{array}{ccc|c} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 2 & 0 & 0 \end{array}\right) \to \left(\begin{array}{ccc|c} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 2 \end{array}\right)$$

$$\to \left(\begin{array}{ccc|c} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 2 \\ 1 & 0 & 0 & 2 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \end{array}\right)$$

Ejemplo (cont.)

Luego

$$a = 2 \qquad\qquad b = 2 \qquad\qquad c = 1$$

$$Q(x) = 2x^2 + 2x + 1 = 2^x.$$