

Notas de Algebra I

Agustin
Hernandez

Algebra I

💡 Estas notas fueron tomadas por mí, **Agustín Hernández**, a partir de las teóricas dadas por Teresa en el **primer cuatrimestre del 2021 de Álgebra I**, las mismas **incluyen las clases prácticas** y la **bibliografía principal de la materia**. Además, muchas de las ecuaciones en Latex, y ciertos apartados fueron proporcionadas por los **apuntes de Maria Marino**.

Estas notas solo proporcionan los fundamentos teóricos de la materia, muy pocas veces esto solo alcanza para resolver las prácticas, es por eso que se recomienda ir a las clases prácticas y de consultas habitualmente. **Tip:** Llevar las prácticas de la mano de los resueltos de Joni 😊

Por cualquier error o sugerencia, envíenme un mail a: ahernandez@dc.uba.ar

- Versión online (Notion) de estas notas: <https://www.notion.so/Algebra-I-d28b8e5f2d524b379cae161d0e7222a2>

Links importantes

- Prácticas resueltas de Álgebra I por Joni: <https://drive.google.com/drive/u/0/folders/1cv5cDxSYgEZkNAYMbIQO->
- Página de la materia: <http://cms.dm.uba.ar/academico/materias/1ercuat2021/Algebra-I/>
- Apuntes de Maria Marino: <https://www.notion.so/marinomar/lgebra-I-62b6ddd7e47348679f4a4dcf04f91a2f>

Contenidos



Contenidos de la materia divididos por prácticas.

▼ Practica 1

Teórica 1 - Conjuntos: Pertenecía, inclusión, operaciones

Teórica 2 - Conjuntos: Tablas de verdad, producto cartesiano

Teórica 3 - Relaciones

Teórica 4 - Funciones

▼ Practica 2

Teórica 5 - Números naturales e inducción

Teórica 6 - Recurrencia, principio de inducción II, Fibonacci y Lucas

Teórica 7 (1) - Principio de inducción completa

▼ Practica 3

Teórica 7 (2) - Combinatoria de conjuntos

Teórica 8 - Cantidad de relaciones y funciones, factorial y número combinatorio

Teórica 9 - Triángulo de Pascal y binomio de Newton

▼ Practica 4

Teórica 10 - Números enteros, divisibilidad y congruencia

Teórica 11 - Algoritmo de división, restos y sistemas de numeración

Teórica 12 - MCD, Combinación lineal entera y coprimos

Teórica 13 - Los números primos

Teórica 14 - Divisores de un número y MCD, MCM y factorización

▼ Practica 5

Teórica 15 - Ecuaciones diofánticas

Teórica 16 - Sistemas de ecuaciones de congruencia y Teorema chino del resto

Teórica 17 - El pequeño teorema de Fermat

Teórica 18 - Sistema Criptográfico RSA y Teorema Euler-Fermat

▼ Practica 6

Teórica 19 - Números complejos

Teórica 20 - Raíces enésimas, grupo G_n y raíces primitivas de la unidad (1 y 2).

▼ Practica 7

Teórica 21 - El anillo de polinomios

Teórica 22 - Divisibilidad, Algoritmo de división, MCD y TFA

Teórica 23 - Evaluación y raíces múltiples

Teórica 24 - Cantidad de raíces y raíces en \mathbb{Q}

Teórica 25 - Factorización en $K[X]$ y $\mathbb{C}[X]$

Teórica 26 - Factorización en $\mathbb{R}[X]$

Teórica 1 - Conjuntos: Pertenecia, inclusion, operaciones

Conjuntos

Un conjunto es una colección no ordenada de objetos, llamados elementos del conjunto. Se dice que el conjunto contiene a estos elementos. Nosotros escribimos $a \in A$ para denotar que a es un elemento del conjunto A . Mientras que la notación $a \notin A$ denota que a no es un elemento del conjunto A .

Ejemplos:

$$\begin{aligned} A &= \{1, 2, 3\}, & B &= \{1, \{3\}, 2\}, & C &= \{\triangle, \circ, \star\} \\ \mathbb{N} &= \{1, 2, 3, 4, \dots\} & \mathbb{Z} &= \{\dots, -2, -1, 0, 1, 2, \dots\} \\ && \mathbb{R} & \text{ el conjunto de los numeros reales} \\ && \emptyset \text{ o } \{\} & \text{ el conjunto vacio} \end{aligned}$$

🗣️ **Observación:** El orden de los elementos no importa en un conjunto, y en un conjunto no se tiene en cuenta repeticiones de elementos.

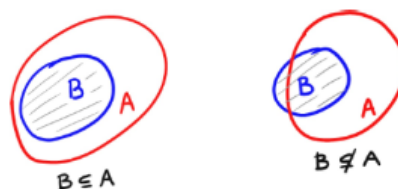
- Los conjuntos se suelen representar gráficamente por los llamados diagramas de Venn: simplemente se utiliza una circunferencia para representar el conjunto, y eventualmente en el interior sus elementos.

Subconjuntos e inclusion

Sea A un conjunto. Se dice que un conjunto B está contenido en A , y se nota $B \subset A$ (o también $B \subseteq A$), si todo elemento de B es un elemento de A . En ese caso decimos también que B está incluido en A , o que B es un subconjunto de A . Si B no es un subconjunto de A se nota $B \not\subset A$ (o $B \not\subseteq A$).

Ejemplos:

- Sea $A = \{1, 2, 3\}$: $\{1\} \subseteq A$, $\{2, 3\} \subseteq A$, $\emptyset \subseteq A$, $A \subseteq A$, $\{3, 4\} \not\subseteq A$.
- $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.
- $A \subseteq A$ y $\emptyset \subseteq A$ cualquiera sea el conjunto A .



O sea, B esta incluido en A si para todo x , se tiene que si x pertenece a B entonces x pertenece a A , y B no esta incluido en A si existe x perteneciendo a B tal que x no pertenece a A . Matemáticamente se escribe:

$$B \subseteq A \text{ si } \forall x, x \in B \Rightarrow x \in A, \quad B \not\subseteq A \text{ si } \exists x \in B : x \notin A.$$

Ejemplos de conjuntos dados por comprensión:

$$A = \{x \in \mathbb{R} : x \geq -2\}, B = \{k \in \mathbb{Z} : k > -2\}.$$

$$P = \{n \in \mathbb{N} : n \text{ es par}\}, I = \{k \in \mathbb{Z} : k \text{ es impar}\}.$$

Igualdad entre conjuntos

$$A = B \text{ si } A \subseteq B \text{ y } B \subseteq A$$

Es decir $A = B$ si tienen exactamente los mismos elementos.

Conjunto de partes

Dado un conjunto A , el conjunto de partes de A es el conjunto de todos los subconjuntos posibles de A .

El conjunto de partes de A es denotado por $\mathcal{P}(A)$

Ejemplos:

$$\mathcal{P}(\{0, 1, 2\}) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}$$
$$\mathcal{P}(\emptyset) = \{\emptyset\}$$

Operaciones entre conjuntos

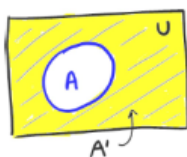
Complemento

Sea A subconjunto de un conjunto referencial U . El *complemento* de A (en U) es el conjunto de los elementos de U que no pertenecen a A , que se suele notar con A' o A^c . Es decir:

$$A^c = \{x \in U : x \notin A\}.$$

Ejemplos:

- Si $U = \{1, 2, 3\}$ y $A = \{2\}$, entonces $A^c = \{1, 3\}$.
- Si $U = \mathbb{N}$ y $A = \{2\}$, entonces $A^c = \{n \in \mathbb{N}, n \neq 2\}$.
- Si $(A^c)^c = A$



Union

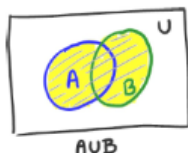
Sean A, B subconjuntos de un conjunto referencial U . La *unión* de A y B es el conjunto $A \cup B$ de los elementos de U que pertenecen a A o a B . Es decir:

$$A \cup B = \{x \in U : x \in A \text{ o } x \in B\}.$$

Notemos que este "o" involucrado en la definición de la union es no excluyente, es decir si un elemento esta en A y en B , esta en la union por estar en al menos alguno de los dos.

Ejemplos:

- Si $A = \{1, 2, 4\}$ y $B = \{3, 5\} \subseteq U = \{1, \dots, 10\}$, entonces $A \cup B = \{1, 2, 3, 4, 5\}$.
- Si $I = \{x \in \mathbb{R} : x \leq 2\} = (-\infty, 2]$ y $J = \{x \in \mathbb{R} : -10 \leq x < 10\} = [-10, 10) \subseteq U = \mathbb{R}$, entonces $I \cup J = \{x \in \mathbb{R} : x < 10\} = (-\infty, 10)$.
- Cualesquiera sean A y B , se tiene $A \cup B = B \cup A$ (conmutatividad), $A \cup \emptyset = A$, $A \cup U = U$, $A \cup A^c = U$.



Intersección

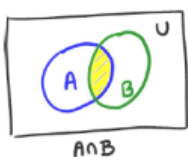
Sean A, B subconjuntos de un conjunto referencial U . La *intersección* de A y B es el conjunto $A \cap B$ de los elementos de U que pertenecen tanto a A como a B . Es decir:

$$A \cap B = \{x \in U : x \in A \text{ y } x \in B\}.$$

Ejemplos:

- Sean $A = \{1, 2, 3, 4\}$ y $B = \{1, 3, 5\} \subseteq U = \{1, \dots, 10\}$. Entonces $A \cap B = \{1, 3\}$
- Sean $I = \{x \in \mathbb{R} : x \leq 2\} = (-\infty, 2]$ y $J = \{x \in \mathbb{R} : -10 \leq x < 10\} = [-10, 10) \subseteq U = \mathbb{R}$, entonces $I \cap J = \{x \in \mathbb{R} : -10 \leq x \leq 2\} = [-10, 2]$.
- Cualesquiera sean A y B , se tiene $A \cap B = B \cap A$ (conmutatividad), $A \cap \emptyset = \emptyset$, $A \cap U = A$, $A \cap A^c = \emptyset$.

Cuando $A \cap B = \emptyset$, se dice que A y B son conjuntos disjuntos.



Leyes de De Morgan y distributivas

Sean A, B, C conjuntos dentro de un conjunto referencial U . Entonces:

Leyes de De Morgan

$$(A \cup B)^c = (A)^c \cap (B)^c \quad \text{y} \quad (A \cap B)^c = A^c \cup B^c.$$

Leyes distributivas

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad \text{y} \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

De las operaciones básicas se derivan las operaciones siguientes:

Diferencia

$A - B = A \cap B^c$, es decir:

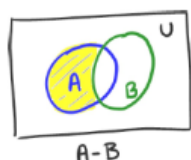
$$x \in A - B \Leftrightarrow x \in A \text{ y } x \in B^c \Leftrightarrow x \in A \text{ y } x \notin B.$$

Es decir, $A - B$ es el conjunto de los elementos de A que no son elementos de B :

$$A - B = \{a \in A : a \notin B\}$$

Ejemplos:

- Sean $A = \{1, 2, 3, 5, 8\}$ y $B = \{3, 4, 5, 10\} \subseteq U = \{1, \dots, 10\}$, entonces $A - B = \{1, 2, 8\}$ y $B - A = \{4, 10\}$
- Si $I = (-\infty, 2]$ y $J = [-10, 10) \subseteq U = \mathbb{R}$, entonces $I - J = (-\infty, -10)$ y $J - I = (2, 10]$.
- Siempre $A - \emptyset = A$, $A - U = \emptyset$, $A - A = \emptyset$, $A - A^c = A$. Pero $A - B \neq B - A$ en general.



Diferencia simétrica

$A \triangle B$ es el conjunto de los elementos de U que pertenecen a A o a B pero no a los dos a la vez. Es decir:

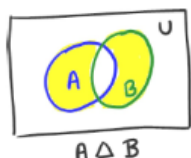
$$A \triangle B = \{c \in U : (c \in A \text{ y } c \notin B) \text{ o } (c \in B \text{ y } c \notin A)\}.$$

Vale:

$$A \triangle B = (A - B) \cup (B - A) = (A \cap B^c) \cup (B \cap A^c) = (A \cup B) - (A \cap B).$$

Ejemplos:

- Sean $A = \{1, 2, 3, 5, 8\}$ y $B = \{3, 4, 5, 10\} \subseteq U = \{1, \dots, 10\}$, entonces $A \triangle B = \{1, 2, 4, 8, 10\}$.
- Sean $I = (-\infty, 2]$ y $J = [-10, 10) \subseteq U = \mathbb{R}$, entonces $I \triangle J = (-\infty, -10) \cup (2, 10]$.
- Siempre $A \triangle B = B \triangle A$ (simetría), $A \triangle \emptyset = A$, $A \triangle U = A^c$, $A \triangle A = \emptyset$, $A \triangle A^c = U$.



Teórica 2 - Conjuntos: Tablas de verdad, producto cartesiano

Conjuntos - Tablas de verdad

- A^C : Negación \neg
- $A \cup B$: Disyunción no exclusiva \vee
- $A \cap B$: Conjunción \wedge
- $A \triangle B$: Disyunción exclusiva $\underline{\vee}$
- $A \subseteq B$: Implicación \implies
- $A = B$: Bi-implicación \iff

Tablas de verdad



Una proposición p o q es una afirmación que es o bien verdadera o bien falsa.

Negación:

p	$\neg p$
V	F
F	V

Conjunción:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Disyunción no excluyente:

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Disyunción excluyente:

p	q	$p \underline{\vee} q$
V	V	F
V	F	V
F	V	V
F	F	F

Implicación:

p	q	$p \Rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Bi-implicación:

p	q	$p \Leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Tipos de demostraciones



Existen otros tipos de demostraciones, estas son las más simples de entender y a veces de implementar.

Sean P y Q dos proposiciones.

Demostración directa

$$P \Rightarrow Q$$

Demostración por contra recíproca

$$\neg Q \Rightarrow (\neg P)$$

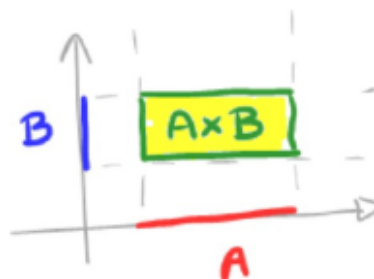
Demostración por el absurdo

$$\neg[P \wedge (\neg Q)]$$

Producto cartesiano

Sean A, B conjuntos. El producto cartesiano de A con B , que se nota $A \times B$, es el conjunto de pares ordenados

$$A \times B := \{(x, y) : x \in A, y \in B\}$$



- Al ser pares ordenados, importa el orden, de manera que si x es el primer elemento del par y pertenece a A , y es el segundo elemento del par y pertenece a B . Entonces:

$$A \times B \neq B \times A$$

Propiedades

Sea $A \subseteq \mathbb{U}$, $B \subseteq \mathbb{V}$

- $A \times \emptyset = \emptyset = B \times \emptyset$
- $A \times A = A^2$
- $A \times B \subseteq \mathbb{U} \times \mathbb{V}$
- $(A \times B)^C \neq A^C \times B^C$
- Si $A \neq B \neq \emptyset$ entonces $A \times B \neq B \times A$

🗣️ Observación:

Sean A_1, A_2, \dots, A_n conjuntos, entonces:

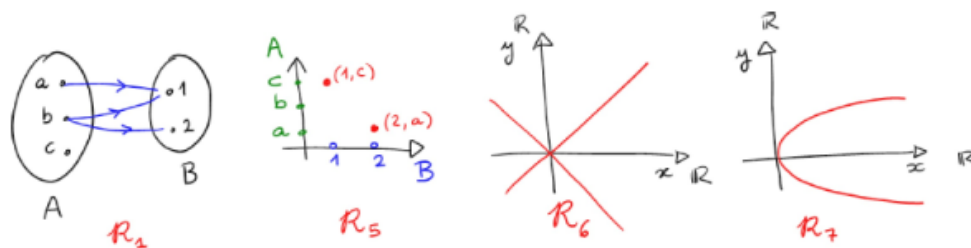
$$A_1 \times \dots \times A_n = \{(x_1, \dots, x_n) \in \mathbb{R}^n : x_1 \in A_1, \dots, x_n \in A_n\}$$

Teórica 3 - Relaciones

Sean A y B conjuntos. Una relación \mathcal{R} de A en B es un subconjunto cualquiera \mathcal{R} del producto cartesiano $A \times B$. Es decir \mathcal{R} es una relación de A en B si $\mathcal{R} \in \mathcal{P}(A \times B)$.

- \mathcal{R} es una relación de A en $B \iff \mathcal{R} \subseteq A \times B$
- Como $A \times B \neq B \times A$, el orden de los elementos de los pares importa. No son iguales las relaciones de A en B y las relaciones de B en A
- En vez de expresar: $(a, 1) \in \mathcal{R}_1$, se denota como: $a \mathcal{R}_1 1$ (se lee " a está relacionado con 1").
- El vacío, denotado \emptyset , siempre está contenido en $A \times B$, por lo que puede estar en \mathcal{R} .

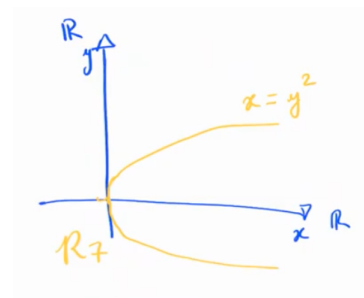
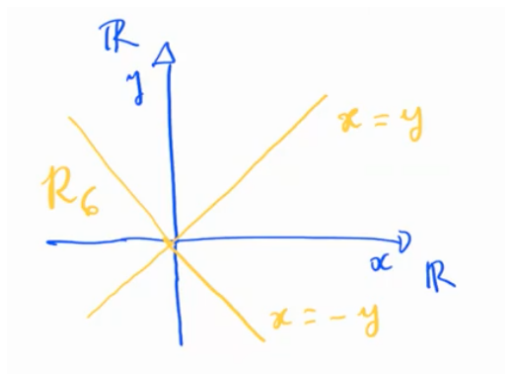
Posibles representaciones gráficas de las relaciones:



Ejemplos:

$$\mathcal{R}_6 = \{(x, y) \in \mathbb{R} : x^2 = y^2\}$$

$$\mathcal{R}_7 = \{(x, y) \in \mathbb{R} : x = y^2\}$$



Relación en un conjunto

Sea A un conjunto. Se dice que \mathcal{R} es una relación en A cuando $\mathcal{R} \subseteq A \times A$.

Relación reflexiva, simétrica, antisimétrica y transitiva

Sea A un conjunto y \mathcal{R} una relación en A .

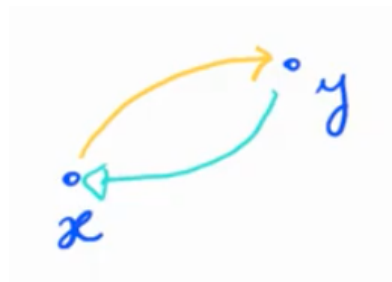
Reflexividad

Se dice que \mathcal{R} es reflexiva si $(x, x) \in \mathcal{R}, \forall x \in A$ se tiene $x \mathcal{R} x$.



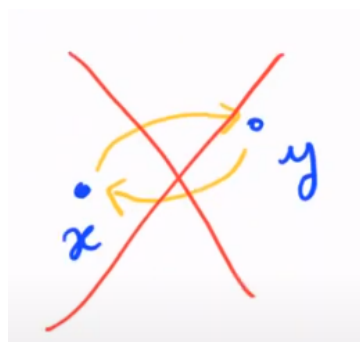
Simetría

Se dice que \mathcal{R} es simétrica si cada vez que un par $(x, y) \in \mathcal{R}$, entonces el par simétrico (y, x) también. Es decir $x \mathcal{R} y$ si y solo si $y \mathcal{R} x$.



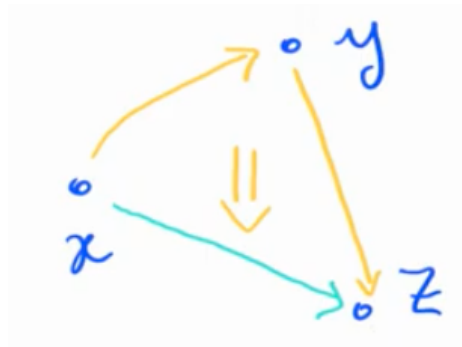
Antisimetría

Se dice que \mathcal{R} es antisimétrica si cada vez que un par $(x, y) \in \mathcal{R}$, con $x \neq y$, entonces el par $(y, x) \notin \mathcal{R}$. Es decir si se tiene $x \mathcal{R} y$ con $x \neq y$ entonces $y \not\mathcal{R} x$.



Transitividad

Se dice que \mathcal{R} es transitiva si $\forall x, y, z \in A$, tales que $(x, y) \in \mathcal{R}$ e $(y, z) \in \mathcal{R}$, se tiene que $(x, z) \in \mathcal{R}$. Es decir que si $x \mathcal{R} y$ e $y \mathcal{R} z$, entonces $x \mathcal{R} z$.



Relaciones de orden y equivalencia

Sea \mathcal{R} una relación en un conjunto X .

- Se dice que \mathcal{R} es una **relación de orden** si es reflexiva, antisimétrica y transitiva.
- Se dice que es una **relación de equivalencia** si es reflexiva, simétrica y transitiva.

🧐 **Observación:** La inclusión es una relación de orden

Clases de equivalencia

Sea \sim una relación de equivalencia en un conjunto X y sea $x \in X$.

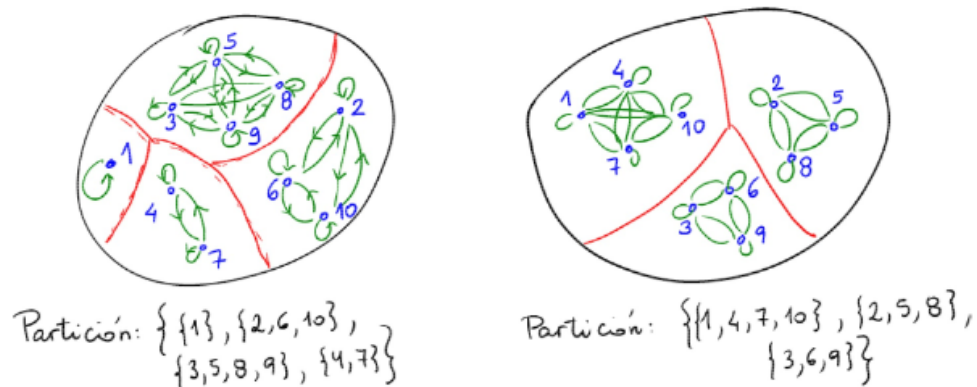
Entonces la **clase de** x es el conjunto

$$\bar{x} = \{y \in X : y \sim x\} \subseteq X$$

Cuando tenemos una relación de equivalencia partimos el conjunto en clases.

Propiedades

- $\bar{x} \neq \bar{y} \implies \bar{x} \cap \bar{y} = \emptyset$ (son disjuntas)
- $x \in \bar{x}$ (pues $x \sim x$)
- $X = \text{Unión de todas las clases}$



Teórica 4 - Funciones

Sean A y B conjuntos, y sea \mathcal{R} una relaciones de A en B . Se dice que \mathcal{R} es una función si para cada $x \in A$ existe un $y \in B$, y este elemento y es único. Es decir:

$$\forall x \in A, \exists! y \in B / x \mathcal{R} y$$

Dominio de una función

Se define el **dominio** de f como:

$$\text{Dom}(f) = \{x \in A : \exists y \in B \text{ con } f(x) = y\}$$

Imagen de una función

Sea $f : A \rightarrow B$ es una función. La **imagen** de f , que se nota $\text{Im}(f)$, es el subconjunto de elementos de B que están relacionados con algún elemento de A . Es decir

$$\text{Im}(f) = \{y \in B : \exists x \in A \text{ con } f(x) = y\}$$

Igualdad entre funciones

Sean $f, g : A \rightarrow B$ funciones. Se tiene:

$$f = g \iff f(x) = g(x), \forall x \in A$$

Funciones inyectivas, sobreyectivas y biyectivas

Sea $f : A \rightarrow B$ una función. Se dice que

- f es **inyectiva** si dos elementos distintos de A siempre van a parar a dos elementos distintos de B . Es decir:


$$x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$$

O equivalentemente:

$$f(x_1) = f(x_2) \implies x_1 = x_2$$

- f es **sobreyectiva** si $\text{Im}(f) = B$, es decir

$$\forall y \in B, \exists x \in A / f(x) = y$$

 **Observación:** Siempre es posible restringir el conjunto de llegada de la función para volverla sobreyectiva

- f es **biyectiva** si f es a la vez inyectiva y sobreyectiva. Es decir si f cumple que:

$$\forall y \in B, \exists! x \in A / f(x) = y$$

Composición de funciones

Sean A, B, C conjuntos, y $f : A \rightarrow B$ y $g : B \rightarrow C$ funciones, entonces la **composición** de f con g , que se nota $g \circ f$, donde $g \circ f : A \rightarrow C$ está dada por:

$$g \circ f(x) = g(f(x)) \quad , \forall x \in A$$

Función inversa

Si $f : A \rightarrow B$ es una función, quiere decir que:

$$\forall x \in A, \exists! y \in B / f(x) = y$$

y si además si f es biyectiva, quiere decir que:

$$\forall y \in B, \exists! x \in A / f(x) = y$$

Si defino $f^{-1} : B \rightarrow A$ como $f^{-1}(y) = x$, donde x es el único elemento de A tal que $y = f(x)$, f^{-1} es la **función inversa** de f .

Relación con la composición

Si f^{-1} es la inversa de f , entonces:

$$f^{-1} \circ f(x) = x, \forall x \in \text{Dom}(f) = \text{id}_{\text{Dom}(f)}$$

$$f \circ f^{-1}(x) = x, \forall x \in \text{Im}(f) = \text{id}_{\text{Im}(f)}$$

🗣️ **Observación:**

- Sea $f : A \rightarrow B$ una función biyectiva. Entonces:
 - $f^{-1} \circ f : A \rightarrow A$ satisface $f^{-1} \circ f = \text{id}_A$
 - $f \circ f^{-1} : B \rightarrow B$ satisface $f \circ f^{-1} = \text{id}_B$
- Sea $F : A \rightarrow B$ una función y supongamos que existe $g : B \rightarrow A$ que satisface que $g \circ f = \text{id}_A$ y $f \circ g = \text{id}_B$, entonces f es biyectiva y $g = f^{-1}$.

Teórica 5 - Números naturales e inducción

Los elementos del conjunto de los números naturales, notado \mathbb{N} , cumplen con las propiedades de

- Conmutatividad.
- Asociatividad.
- Distributividad del producto sobre la suma.

La suma de Gauss y la serie geométrica

Se conoce como la [suma de Gauss](#) a la suma desde 1 hasta n y este proceso es generalizable mediante la sumatoria:

$$\sum_{k=1}^n k = \frac{n(n+1)}{2}, \forall n \in \mathbb{N}$$

Se conoce a la [serie geométrica](#) como la sumatoria:

$$\forall n \in \mathbb{N}: \quad 1 + q^2 + \dots + q^n = \sum_{k=0}^n q^k = \begin{cases} \frac{q^{n+1}-1}{q-1} & \text{si } q \neq 1 \\ n+1 & \text{si } q = 1 \end{cases},$$

Sumatoria y Productoria

Sea $n \in \mathbb{N}$. La notación $\sum_{i=1}^n a_i$, que se lee la [sumatoria](#) para i de 1 a n de a_i , representa la suma de los n primeros términos de la sucesión $(a_i)_{i \in \mathbb{N}}$:

$$\sum_{i=1}^n a_i = \sum_{i=1}^{n-1} a_i + a_n,$$

Propiedades:

$$\bullet \left(\sum_{k=1}^n a_k \right) + \left(\sum_{k=1}^n b_k \right) = \sum_{k=1}^n (a_k + b_k)$$

$$\bullet \sum_{k=1}^n (c \cdot a_k) = c \cdot \sum_{k=1}^n a_k$$

Productoria

Sea $n \in \mathbb{N}$. La notación $\prod_{i=1}^n a_i$, que se lee **la productoria** para i de 1 a n de a_i , representa el producto de los n primeros términos de la sucesión $(a_i)_{i \in \mathbb{N}}$:

$$\prod_{i=1}^n a_i = a_1 \cdot a_2 \cdot \dots \cdot a_n$$

Propiedades:

$$\bullet \prod_{i=1}^n i = 1 \cdot 2 \cdot \dots \cdot n = n!$$

$$\bullet \prod_{i=1}^n c = \underbrace{c \cdot c \cdot \dots \cdot c}_{n \text{ veces}} = c^n$$

$$\bullet \left(\prod_{k=1}^n a_k \right) \cdot \left(\prod_{k=1}^n b_k \right) = \prod_{k=1}^n (a_k \cdot b_k)$$

$$\bullet \prod_{k=1}^n (c \cdot a_k) = \left(\prod_{k=1}^n c \right) \cdot \left(\prod_{k=1}^n a_k \right) = c^n \cdot \prod_{k=1}^n a_k$$

El conjunto inductivo \mathbb{N} y el principio de Inducción

Sea $p(n)$ una proposición sobre \mathbb{N}

$$p(n) \text{ V, } \forall n \in \mathbb{N} \begin{cases} p(1) \text{ V} \implies p(2) \text{ V} \\ p(2) \text{ V} \implies p(3) \text{ V} \\ \vdots \\ p(h) \text{ V} \implies p(h+1) \text{ V} \end{cases}$$

Conjunto inductivo

Sea $H \subseteq \mathbb{R}$ se dice que H es **inductivo** si:

- $1 \in H$
- $\forall h \in \mathbb{R}$, si $h \in H$ entonces $h + 1 \in H$

Ejemplos:

- $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{N} \cup \{0\} = \mathbb{N}_0, \mathbb{Z}_{n_0} = \{k \in \mathbb{Z} : k \geq n_0\}$ son todos conjuntos inductivos.
- $\mathbb{N} \cup \{\frac{1}{2}\}$ no es **inductivo!** pues $\frac{1}{2}$ esta pero $\frac{1}{2} + 1 = \frac{3}{2}$ no!.

 **Observación:**

\mathbb{N} es el conjunto inductivo "más chico" que hay, es decir, si H es inductivo, entonces $\mathbb{N} \subseteq H$

Por lo tanto si $H \subseteq \mathbb{N}$ es inductivo entonces $H = \mathbb{N}$!

Sea $p(n)$ una proposición sobre \mathbb{N} .

Nos proponemos probar que $p(n)$ es Verdadero, $\forall n \in \mathbb{N}$

Método: Probar que $H : \{n \in \mathbb{N} : p(n) \text{ es Verdadero}\} \subseteq \mathbb{N}$ es un conjunto inductivo.

Si logramos probar que H es inductivo entonces $H = \mathbb{N}$ y se concluye que $p(n)$ es Verdadero $\forall n \in \mathbb{N}$

Principio de inducción

Sea $p(n)$ una proposición sobre \mathbb{N} . Si se cumple:

- Si $p(1)$ es Verdadera (Caso base)
- $\underbrace{p(h) \text{ es Verdadero}}_{\text{Hipótesis inductiva}} \implies p(h+1) \text{ es Verdadero}$, donde $p(h+1)$ es lo que quiero probar, $\forall h \geq 1$.

Entonces, $p(n)$ es Verdadero, $\forall n \in \mathbb{N}$

Principio de inducción corrido

Sea $n_0 \in \mathbb{Z}$ fijado y sea $p(n)$ una proposición sobre $\mathbb{Z}_{\geq n_0}$

Entonces si p satisface

1. Caso base: $p(n_0)$ es Verdadero
2. Paso inductivo: $\forall h \geq n_0, p(h) \text{ V} \implies p(h+1) \text{ V}$

Entonces $p(n)$ es verdadera, $\forall n \geq n_0$.

Teórica 6 - Recurrencia, principio de inducción II, Fibonacci y Lucas

! En la teórica se da una explicación de las Torres de Hanói, acá se opta por no hacerlo.

Sucesión definida por recurrencia

💡 Cuando decimos que algo está dado por recurrencia es cuando definimos un término siguiente en función del anterior. Por ejemplo:

Sea $a_1 = 1$ y $a_{n+1} = 2a_n + 1, \forall n \in \mathbb{N}$

Relación entre sucesión recurrente y sumatoria

💡 Recuerdo:

$$S_n = \sum_{i=1}^n a_i$$

$$S_1 = a_1 \quad y \quad S_{n+1} = S_n + a_{n+1} \quad \forall n \in \mathbb{N}$$

Principio de inducción II

Sea $p(n)$ una proposición, $n \in \mathbb{N}$, una proposición sobre \mathbb{N} .

Si se cumple que:

1. **Casos base:** $p(1)$ y $p(2)$ Verdaderos
2. **Paso inductivo:** $\forall h \geq 1$,

$\underbrace{p(h) \text{ y } p(h+1)}_{HI} \text{ Verdaderos} \implies p(h+2) \text{ Verdadero (donde } p(h+2) \text{ es lo que quiero probar).}$

Entonces $p(n)$ es Verdadero, $\forall n \in \mathbb{N}$.

Principio de inducción II "corrido"

Sea $n_0 \in \mathbb{Z}$ dado y sea $p(n)$, $n \geq n_0$, una proposición sobre $\mathbb{Z}_{\geq n_0}$

Si se cumple que:

1. **Casos base:** $p(n_0)$ y $p(n_0 + 1)$ Verdaderos
2. **Paso inductivo:** $\forall h \geq n_0$,

$p(h) \text{ y } p(h+1) \text{ Verdaderos} \implies p(h+2) \text{ Verdadero}$

Entonces $p(n)$ es Verdadero, $\forall n \geq n_0$.

Sucesión de Fibonacci

Nota para el lector: De acá en adelante estas notas surgen de los apuntes de Maria Marino.

$$F_n = \begin{cases} F_0 = 0 \\ F_1 = 1 \\ F_{n+2} = F_{n+1} + F_n \end{cases} \quad \forall n \geq 0$$

Polinomio asociado: $x^2 - x - 1 = 0$

Raíces:

$$\begin{cases} \phi = \frac{1+\sqrt{5}}{2} \\ \bar{\phi} = \frac{1-\sqrt{5}}{2} \end{cases} \implies \begin{cases} \phi^2 = \phi + 1 \\ \bar{\phi}^2 = \bar{\phi} + 1 \end{cases}$$

Sucesiones de Lucas

$$\begin{cases} a_0 = a \\ a_1 = b \\ a_{n+2} = c \cdot a_{n+1} + d \cdot a_n \end{cases} \quad \forall n \geq 0 \quad \text{donde } a, b, c, d \text{ son números dados.}$$

Se le asocia el polinomio $x^2 - c \cdot x - d = 0$. Asumamos que tiene 2 raíces **distintas**, r y \bar{r}

Tenemos que

$$\begin{cases} r^2 - cr - d = 0 \\ \bar{r}^2 - c\bar{r} - d = 0 \end{cases} \implies \begin{cases} r^2 = cr + d \\ \bar{r}^2 = c\bar{r} + d \end{cases}$$

Las sucesiones $(r^n)_{n \geq 0}$ y $(\bar{r}^n)_{n \geq 0}$ satisfacen ambas la recurrencia de la sucesión de Lucas: $a_{n+2} = c \cdot a_{n+1} + d \cdot a_n$, $\forall n \geq 0$, pues $r^{n+2} = r^n \cdot r^2 = r^n(cr + d) = cr^{n+1} + dr^n$ (y exactamente lo mismo para \bar{r}).

Entre todas las sucesiones de la forma $(\alpha \cdot r^n + \beta \cdot \bar{r}^n)_{n \geq 0}$ existe una sola que satisface las dos condiciones iniciales $a_0 = a$ y $a_1 = b$, y se calcula resolviendo

$$\begin{cases} \alpha \cdot r^0 + \beta \cdot \bar{r}^0 = a_0 = a \\ \alpha \cdot r^1 + \beta \cdot \bar{r}^1 = a_1 = b \end{cases} \iff \begin{cases} \alpha + \beta = a \\ \alpha \cdot r + \beta \cdot \bar{r} = b \end{cases}$$

el sistema tiene una única solución pues $r \neq \bar{r}$

$$\alpha = \frac{b - a \cdot \bar{r}}{r - \bar{r}} \\ \beta = \frac{a \cdot r - b}{r - \bar{r}}$$

Concluimos que para esos valores de α y β la sucesión $(\alpha \cdot r^n + \beta \cdot \bar{r}^n)_{n \geq 0}$ es la sucesión de Lucas definida por

$$\begin{cases} a_0 = a \\ a_1 = b \\ a_{n+2} = c \cdot a_{n+1} + d \cdot a_n \end{cases} \quad \forall n \geq 0$$

Teórica 7 (1) - Principio de inducción completa

Sea $p(n)$ una proposición sobre \mathbb{N} :

Si se cumple que:

1. **Caso base:** $p(1)$ Verdadero

2. **Paso inductivo:** $\forall h \in \mathbb{N}$

$$p(1)V, p(2)V, \dots, P(h)V \implies p(h+1) \text{ Verdadero.}$$

$$\text{Es lo mismo que decir: } p(k) V, \quad 1 \leq k \leq h \implies p(h+1)V$$

Entonces $p(n)$ es $\forall, \forall n \in \mathbb{N}$

Principio de inducción completa "corrido"

Sea $n_0 \in \mathbb{Z}$, y sea $p(n)$, $n \geq n_0$, una proposición enunciada sobre $\mathbb{Z}_{\geq n_0}$.

Entonces si se cumple que:

1. **Caso base:** $p(n_0)$ Verdadero

2. **Paso inductivo:** $\forall h \geq n_0$

$$p(k)V, n_0 \leq k \leq h \implies p(h+1) \text{ Verdadero.}$$

Entonces $p(n)$ es $\forall \forall n \geq n_0$.

Teórica 7 (2) - Combinatoria de conjuntos

💡 La combinatoria se llama al arte de contar.

Cardinal de un conjunto

1. Sea A un conjunto, y sea el cardinal, notado como $\#$, se define como $\#A$ = cantidad de elementos que tiene A .

Ejemplos:

- $A = \{2, 3, 7\} \Rightarrow \#A = 3$
- $A = \emptyset \Rightarrow \#A = 0$
- $A = \mathbb{N} \Rightarrow \#A = \infty$

Si A tiene finitos elementos decimos que A es un **conjunto finito**.

🧐 **Observación:** Sea A un conjunto finito, entonces $\#A = \mathbb{N}_0$ (un número natural ó 0).

Propiedades de operaciones sobre conjuntos

Sean A, B conjuntos finitos:

1. **Inclusión:** Si $B \subseteq A$, entonces $\#B \leq \#A$

2. **Unión:**

- Si A y B son **disjuntos**, entonces $\#(A \cup B) = \#A + \#B$
- Si A y B son conjuntos finitos cualesquiera, entonces

$$\#(A \cup B) = \#A + \#B - \#(A \cap B)$$

3. **Complemento:** Supongamos $A \subseteq U$ conjunto referencial finito:

$$\#A^C = \#U - \#A$$

4. **Diferencia:**

$$\begin{aligned}\#(A - B) &= \#(A - (A \cap B)) \\ &= \#((A \cap B)^C) \\ &= \#A - \#(A \cap B)\end{aligned}$$

5. **Diferencia simétrica:**

$$\begin{aligned}\#(A \Delta B) &= \#((A \cup B) - (A \cap B)) \\ &= \#(A \cup B) - \#(A \cap B) \\ &= \#A + \#B - 2\#(A \cap B)\end{aligned}$$

Cardinal del producto cartesiano

1. Sean A, B conjuntos finitos, entonces

$$\#(A \times B) = n \cdot m = \#A \cdot \#B$$

2. Sean A_1, \dots, A_n conjuntos finitos, entonces

»

3. Sea A un conjunto finito, entonces:

$$\#(A^n) = (\#A)^n$$

Cardinal de partes de un conjunto

Sea A un conjunto finito con $\#A = n$, entonces:

- $\#p(A) = 2^n$
- $A = \emptyset \Rightarrow \#p(A) = 1$

Teórica 8 - Cantidad de relaciones y funciones, factorial y número combinatorio

Cantidad de relaciones en un conjunto finito

Sea A un conjunto con $\#A = m$ y sea B un conjunto con $\#B = n$

Entonces la cantidad de relaciones que puedo formar de A en B es

$$\#p(A \times B) = 2^{\#(A \times B)} = 2^{m \cdot n}$$

! La cantidad de relaciones de B en A **es la misma** que la cantidad de relaciones de A en B

Consecuencia

Relaciones (de A) en A con $\#A = m$

$$\#p(A^2) = 2^{m^2}$$

Cantidad de funciones

Sean A, B conjuntos con $\#A = m$ y $\#B = n$.

Entonces

$$\#\{f : A \rightarrow B : f \text{ función}\} = \#B^{\#A} = n^m$$

$$\#\{f : B \rightarrow A : f \text{ función}\} = \#A^{\#B} = m^n$$

! La cantidad de funciones de B en A **NO es la misma** que la cantidad de funciones de A en B

🧐Observaciones:

Supongamos que A y B son conjuntos finitos y sea $f : A \rightarrow B$ una función

Entonces

1. Si f es **inyectiva**, entonces $\#A \leq \#B$
2. Si f es **sobreyectiva**, entonces $\#A \geq \#B$
3. Si f es **biyectiva**, entonces $\#A = \#B$

Cantidad de funciones biyectivas

Sean A, B conjuntos con el mismo cardinal $\#A = \#B = n$

Entonces

$$\#\{f : A \rightarrow B \text{ con } f \text{ función biyectiva}\} = n!$$



Se expande la definición de $n!$ para $n \in \mathbb{N}$: $0! = 1$

Esto coincide con la cantidad de permutaciones de elementos que hay posibles en un conjunto de n elementos.

Sea A con $\#A = n$,

Entonces $\#\{\text{Permutaciones de los elementos de } A\} = n!$



Permutaciones: cantidad de formas distintas en las que puedo ordenar los elementos de un conjunto. Dado un conjunto A tal que $\#A = n$, la cantidad de permutaciones posibles es $n!$

Cantidad de funciones inyectivas

Proposición

Sean A, B conjuntos con $\#A = m$ y $\#B = n$ y $m \leq n$

Entonces

$$\#\{f : A \rightarrow B \text{ con } f \text{ función inyectiva}\} = \frac{n!}{(n-m)!}$$

Número combinatorio

$\binom{n}{k}$ es la cantidad de subconjuntos de k elementos que tiene un conjunto con n elementos.

Sólo tiene sentido la expresión si $0 \leq k \leq n$, $n \in \mathbb{N}_0$.



Contar la cantidad de subconjuntos de k elementos en un conjunto de n elementos es lo mismo que contar las formas distintas que tengo de elegir k elementos en un conjunto de elementos (sin orden).

Propiedades

Sean $0 \leq k \leq n$ con $n \in \mathbb{N}_0$

- $\binom{n}{0} = 1 \implies \binom{0}{0} = 1$
- $\binom{n}{1} = n = \binom{n}{-1}$
- $\binom{n}{k} = \binom{n}{n-k}$
- La cantidad total de subconjuntos que tiene un conjunto con n elementos es $\#p(A) = 2^n$. Todos los subconjuntos puedo clasificarlos disjuntamente por su cardinal, conjuntos con 1 elemento, con 2 elementos, con 3 elementos, con n elementos, y así. Entonces el cardinal de partes de A es igual a la suma de los números combinatorios.

$$\#p(A) = 2^n = \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} = \sum_{k=0}^n \binom{n}{k}$$

Proposición

Sea $n \in \mathbb{N}_0$ y $0 \leq k \leq n$

Entonces

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$$

Pues $\frac{n!}{(n-k)!}$ = cantidad de k -uplas ordenadas de elementos distintos elegidos entre a_1, \dots, a_n (= cantidad de funciones inyectivas del $\{1, \dots, k\}$ en $A = \{a_1, \dots, a_n\}$)

Pero cada subconjunto con k elementos está contado en la fórmula $k!$ veces, que es la cantidad de permutaciones de un conjunto con k elementos.

$$k! \binom{n}{k} = \frac{n!}{(n-k)!} \implies \binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$$

Teórica 9 - Triángulo de Pascal y binomio de Newton

💡 **Recordo:** Dado $n \in \mathbb{N}_0, 0 \leq k \leq n$ se tiene las siguientes igualdades:

$$\binom{n}{k}$$

- Cantidad de subconjuntos con k elementos que tiene un conjunto con n elementos.
- Cantidad de formas de elegir k elementos en un conjunto con n elementos.
- $\frac{n!}{k!(n-k)!}$

Fórmula recursiva para el número combinatorio

Sea $n \in \mathbb{N}_0$. Entonces:

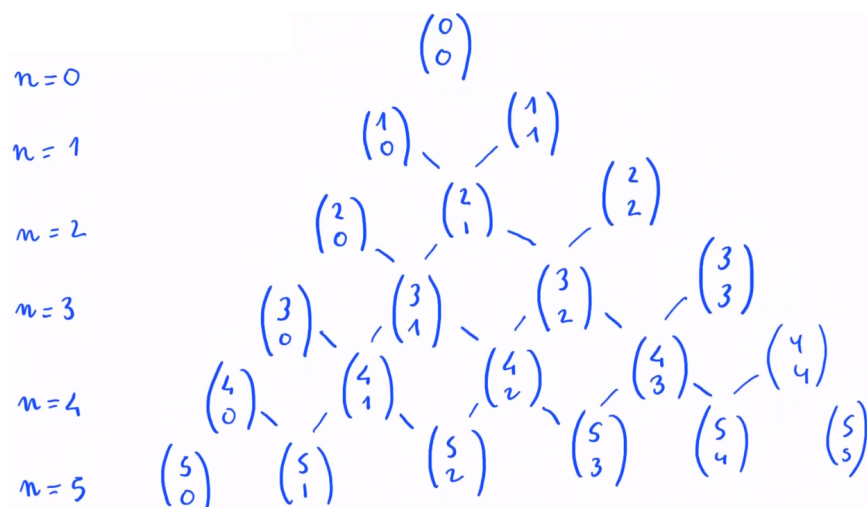
- $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$ para $1 \leq k \leq n$

El **primer termino** de la suma cuenta los subconjuntos con k elementos de $A_{n+1} = \{a_1, \dots, a_n, a_{n+1}\}$ que contienen al elemento a_{n+1} .

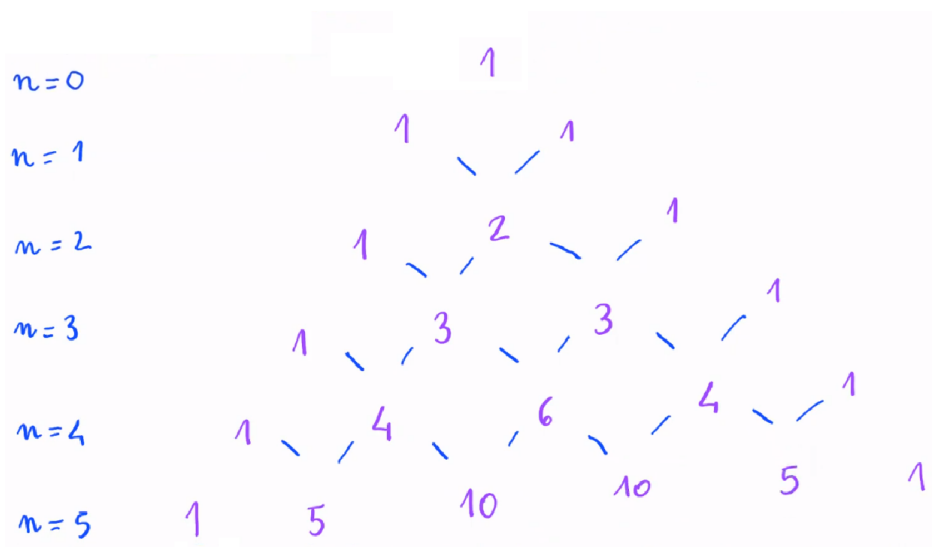
El **segundo termino** de la suma cuenta los subconjuntos con k elementos de A_{n+1} que **no** contienen al elemento a_{n+1} .

- Para $k = 0$ y $k = n + 1$, se tiene $\binom{n+1}{0} = \binom{n+1}{n+1} = 1$

Triángulo de Pascal



Estableciendo los primeros 3 términos de la cima del triángulo de pascal, y los laterales del triángulo (todos son iguales a 1), se puede implementar la fórmula recursiva de que cada número del triángulo de Pascal es la suma de dos sus respectivos números superiores (izquierda y derecha). De esta manera se tiene:



Observación: Efectivamente para $1 \leq k \leq n$ se tiene que, $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$ y también para $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

🧐 **Observación:** En la teórica se demuestra que esto es cierto por inducción, acá se opta por no hacerlo.

Binomio de Newton

$$(x + y)^n \text{ para } n \geq 0$$

Se define al Binomio de Newton, para $n \in \mathbb{N}_0$, como:

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$$

Teórica 10 - Números enteros, divisibilidad y congruencia

Números enteros

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\} \subseteq \mathbb{N}, \{0\}$$

Operaciones con los números enteros $(\mathbb{Z}, +, \cdot)$

Suma: Sean $a, b \in \mathbb{Z}$, entonces $a + b \in \mathbb{Z}$.

- Conmutatividad: $\forall a, b \in \mathbb{Z}, a + b = b + a$.
- Asociatividad: $\forall a, b, c \in \mathbb{Z}, (a + b) + c = a(b + c) = a + b + c$
- Existencia del elemento neutro: $0, \forall a \in \mathbb{Z}, a + 0 = a(0 + a)$
- Inverso aditivo (resta o opuesto): $\forall a \in \mathbb{Z}, \exists -a \in \mathbb{Z}$ que satisface $a + (-a) = 0$

Producto: $\forall a, b \in \mathbb{Z}, a \cdot b \in \mathbb{Z}$

- Conmutatividad: $\forall a, b \in \mathbb{Z}, a \cdot b = b \cdot a$.
- Asociatividad: $\forall a, b, c \in \mathbb{Z}, (a \cdot b) \cdot c = a \cdot (b \cdot c) = a \cdot b \cdot c$
- Existencia del elemento neutro: $1, \forall a \in \mathbb{Z}, a \cdot 1 = a$
- **NO EXISTE** inverso multiplicativo: $\forall a \in \mathbb{Z} - \{0\}, \exists a^{-1} \in \mathbb{Z}$ o sea que $a \cdot a^{-1} = 1$, por ejemplo $2^{-1} \cdot \frac{1}{2} = 1$ pero $\frac{1}{2} \notin \mathbb{Z}$.
- Distributividad: $a, b, c \in \mathbb{Z}, a(b + c) = ab + ac$

Propiedades especiales sobre el producto:

- $\forall a \in \mathbb{Z}$, se tiene que el 0 es **absorbente**: $0 \cdot a = 0$
- Sean $a, b \in \mathbb{Z}$ con $a \neq 0$ y $b \neq 0$, entonces $ab \neq 0$ (equivalentemente: $ab = 0 \implies a = 0 \vee b = 0$).

Observación de Teresa sobre tema que vamos a ver más adelante: Cuando tenemos un conjunto que cumple con las propiedades de Suma y Producto, se lo llama al mismo anillo conmutativo

Divisibilidad



Motivado porque en general si $a, d \in \mathbb{Z}$ con $d \neq 0$, entonces $\frac{a}{d} \notin \mathbb{Z}$.

Sean $a, d \in \mathbb{Z}$ con $d \neq 0$:

Se dice que d divide a a si $\exists k \in \mathbb{Z}$ tal que $a = kd$ (o sea $\frac{a}{d} \in \mathbb{Z}$, $\frac{a}{d} = k \in \mathbb{Z}$)

Observación: NO DIVIDIMOS NUNCA POR 0

Notación:

- Cuando d divide a a :

$$d \mid a \iff \exists k \in \mathbb{Z} : a = kd$$

- Cuando d **no** divide a a :

$$d \nmid a \iff \nexists k \in \mathbb{Z} : a = kd$$

- Dado $a \in \mathbb{Z}$

$$Div(a) = \{d \in \mathbb{Z} : d \mid a\} \subseteq \mathbb{Z} - \{0\}$$

$$Div_+(a) = \{d \in \mathbb{Z} : d \mid a\} \subseteq \mathbb{N}$$

Ejemplos:

- $6 \mid -24$ pues $-24 = (-4) \cdot 6$ ($\frac{-24}{6} = -4 \in \mathbb{Z}$).
- $8 \mid 32$ pues $32 = 4 \cdot 8$ ($\frac{32}{8} = 4 \in \mathbb{Z}$).
- $Div_+(24) = \{1, 2, 3, 4, 6, 8, 12, 24\}$.
- $Div(24) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24\}$.
- $6 \mid 0$ pues $0 = 0 \cdot 6$ ($\frac{0}{6} = 0 \in \mathbb{Z}$).

🧐 Observaciones:

Sean $a, d \in \mathbb{Z}$ con $d \neq 0$

- $\forall d \in \mathbb{Z}$ con $d \neq 0$, se tiene $d \mid 0 \implies Div_+(0) = \mathbb{N}, Div(0) = \mathbb{Z} - \{0\}$
- $d \mid a \iff \pm d \mid \pm a \iff |d| \mid |a|$
- Sea $a \neq 0$, entonces $d \mid a \implies |d| \leq |a|$
 \implies si $a \neq 0$, $Div_+(a) \subseteq \{1, 2, \dots, |a|\}$ y $Div(a) \subseteq \{-|a|, \dots, -1, 1, \dots, |a|\}$
Por lo tanto, $\forall a \neq 0$, a tiene **finitos** divisores en \mathbb{Z} .
- $Inv(\mathbb{Z}) = \{\pm 1\}$
- Si $d \mid a$ y $a \mid d$, entonces $|d| = |a|$
- Sea $a \in \mathbb{Z}$, entonces $\pm 1 \mid a$ y $\pm a \mid a$

Números primos y compuestos

- Sea $a \in \mathbb{Z}$. Se dice que a es un **número primo** si $a \neq 0, \pm 1$ y además a tiene únicamente esos 4 divisores garantizados (o esos 2 divisores positivos garantizados)
O sea $Div(a) = \{\pm 1, \pm a\}$, o $Div_+(a) = \{1, |a|\}$.
- Sea $a \in \mathbb{Z}$. Se dice que a es un **número compuesto** si $a \neq 0, \pm 1$ si tiene más divisores que esos 4 garantizados (o sea más que los 2 divisores positivos garantizados).
 a es compuesto si $a \neq 0, \pm 1$ y $\exists d$ con $1 < d < |a|$.

Propiedades de la divisibilidad

Propiedades de la divisibilidad con $+$ y \cdot .

- Sean $a, b, d \in \mathbb{Z}$ con $d \neq 0$.

$$d \mid a \wedge d \mid b \implies d \mid a + b$$

- Ojo! $d \mid a + b \not\Rightarrow d \mid a$ y/o $d \mid b$

$$5 \mid 2 + 8 \text{ pero } 5 \nmid 2 \text{ y } 5 \nmid 8$$

- Pero si $d \mid a + b$ y $d \mid a$, entonces $d \mid b$

$$\text{Pues } b = (a + b) - a \wedge d \mid a + b \wedge d \mid a \implies d \mid (a + b) - a$$

- Si $d \mid a \implies d \mid ca, \forall c \in \mathbb{Z}$

- Ojo! $d \mid ca \not\Rightarrow d \mid c$ o $d \mid a$

$$6 \mid 12 = 4 \cdot 3 \quad \text{pero} \quad 6 \nmid 4 \wedge 6 \nmid 3$$

Sean $a_1, \dots, a_n, c_1, \dots, c_n \in \mathbb{Z}, d \in \mathbb{Z} - \{0\}$. Entonces:

$$\begin{cases} d \mid a_1 \\ \vdots \\ d \mid a_n \end{cases} \implies d \mid c_1 a_1 + \dots + c_n a_n$$

- $d \mid a$ y $d \mid b \implies d^2 \mid ab$
- $d \mid a \implies d^2 \mid a^2, d^3 \mid a^3$ y $d^n \mid a^n, \forall n \in \mathbb{N}$
- $d \mid a_1, d \mid a_2 \dots d \mid a_n \implies d^n \mid a_1 a_2 \dots a_n$

Ejemplo de aplicación de propiedades de la divisibilidad

Hallar todos los $a \in \mathbb{Z}$ con $a \neq 1$ tales que:

$$a - 1 \mid a^2 + 5$$

Se excluye el $a = 1$ debido a que cuando $a = 1 \implies a - 1 = 0$ que es absurdo, ya que 0 no puede dividir a ningún $k \in \mathbb{Z}$.

Tenemos que tratar de encontrar una expresión que no dependa de a a la derecha de la expresión, encontrar una constante por ejemplo.

Para ello podemos aplicar propiedades de la divisibilidad:

- $a - 1 \mid a - 1 \implies a - 1 \mid a(a - 1) = a^2 - a$, véase que se puede multiplicar el lado de la derecha de la expresión por a , ya que a pertenece a los enteros ($d \mid a \implies d \mid ka, k \in \mathbb{Z}$).

Sin embargo esta expresión sigue dependiendo de a hasta cierto punto, por lo que quizás me convendría probar multiplicar a $(a - 1)$ por algo que me de en el segundo termino una constante, probamos:

- $a - 1 \mid a - 1 \implies a - 1 \mid (a + 1)(a - 1) = a^2 - 1$.

Teniendo que $a - 1 \mid a^2 + 5$ y $a - 1 \mid a^2 - 1$, puedo aplicar la propiedad de que si $d \mid a$ y $d \mid b$, entonces $d \mid a \pm b$:

$$\begin{aligned} a - 1 \mid a^2 + 5 \wedge a - 1 \mid a^2 - 1 &\implies a - 1 \mid (a^2 + 5) - (a^2 - 1) \\ &\implies a - 1 \mid 6 \end{aligned}$$

Entonces, si $a - 1 \mid 6$, $a - 1 \in \text{Div}(6)$, donde $\text{Div}(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$ ($a \neq 1$), pero debo verificar los distintos valores de a ya que es una implicación y puede llegar a ocurrir que para algún $a \in \mathbb{Z}$, $a - 1 \nmid a^2 + 5$:

- $a - 1 = 1 \iff a = 2 \implies 2 - 1 \mid 2^2 + 5 \iff 1 \mid 7$ ✓
- $a - 1 = -1 \iff a = 0 \implies 0 - 1 \mid 0^2 + 5 \iff -1 \mid 5$ ✓
- $a - 1 = 2 \iff a = 3 \implies 3 - 1 \mid 3^2 + 5 \iff 2 \mid 14$ ✓
- $a - 1 = -2 \iff a = -1 \implies -1 - 1 \mid (-1)^2 + 5 \iff -2 \mid 6$ ✓
- $a - 1 = 3 \iff a = 4 \implies 4 - 1 \mid 4^2 + 5 \iff 3 \mid 21$ ✓
- $a - 1 = -3 \iff a = -2 \implies -2 - 1 \mid (-2)^2 + 5 \iff -3 \mid 9$ ✓
- $a - 1 = 6 \iff a = 7 \implies 7 - 1 \mid 7^2 + 5 \iff 6 \mid 54$ ✓
- $a - 1 = -6 \iff a = -5 \implies -5 - 1 \mid (-5)^2 + 5 \iff -6 \mid 30$ ✓

Sirven todos los valores de a : $a = 2, 0, 3, -1, 4, -2, 7, -5$.

Congruencia

Pequeño resumen de las propiedades de congruencia dado en las clases prácticas:


Proposición: Sean $a, b, c, d, e \in \mathbb{Z}$, $d \neq 0$

- \equiv es relación de equivalencia.
- $a \equiv b \pmod{d} \implies a + c \equiv b + c \pmod{d}$
- $a \equiv b \pmod{d} \wedge c \equiv e \pmod{d} \implies a + c \equiv b + e \pmod{d}$
- $a \equiv b \pmod{d} \implies ac \equiv bc \pmod{d}$
- $a \equiv b \pmod{d} \wedge c \equiv e \pmod{d} \implies a.c \equiv b.e \pmod{d}$
- $a \equiv b \pmod{d} \implies a^n \equiv b^n \pmod{d} \forall n \in \mathbb{N}$

Sea $d \in \mathbb{Z}$, $d \neq 0$. Sean $a, b \in \mathbb{Z}$, se dice que a es congruente a b módulo d si $d \mid a - b$.

Notación:

$$a \equiv b(d) \iff d \mid a - b$$

 **Observación:** Se lee como a congruente a b módulo d .

Ejemplos:

- $a \equiv 0(d) \iff d \mid a$.
- $a \equiv a(d)$ pues $d \mid a - a$.
- $18 \equiv 13(5)$ pues $5 \mid 18 - 13 \iff 5 \mid 5$
 $3 \equiv 18(5)$ pues $5 \mid 3 - 18 \iff 5 \mid -15$
- $\forall a \neq 1, a \equiv 1(a - 1)$ pues $a - 1 \mid a - 1$

Proposición: La congruencia módulo d es una relación de equivalencia en \mathbb{Z} :

$$aRb \iff a \equiv b(d)$$

Propiedades de la congruencia

- $a_1 \equiv b_1(d)$ y $a_2 \equiv b_2(d) \implies a_1 + a_2 \equiv b_1 + b_2(d)$
- $a \equiv b(d) \implies ca \equiv cb(d), \forall c \in \mathbb{Z}$

Resumen de estas dos propiedades:

$$\begin{cases} a_1 \equiv b_1(d) \\ \vdots \\ a_n \equiv b_n(d) \end{cases} \implies c_1 a_1 + \dots + c_n a_n \equiv c_1 b_1 + \dots + c_n b_n(d) \\ \forall c_1, \dots, c_n \in \mathbb{Z}$$

- $a_1 \equiv b_1(d)$ y $a_2 \equiv b_2(d) \implies a_1 a_2 \equiv b_1 b_2(d)$.

Además también vale que:

$$\begin{cases} a_1 \equiv b_1(d) \\ \vdots \\ a_n \equiv b_n(d) \end{cases} \implies a_1 \dots a_n \equiv b_1 \dots b_n(d)$$

- $a \equiv b(d) \implies a^n \equiv b^n(d), \forall n \in \mathbb{N}$

Teórica 11 - Algoritmo de división, restos y sistemas de numeración

Algoritmo de la división

Teorema (Algoritmo de división): Dados $a, d \in \mathbb{Z}$ con $d \neq 0$, existen $k, r \in \mathbb{Z}$ tales que:

$$a = k.d + r, \text{ con } 0 \leq r < |d|$$

Y además, estos k y r son únicos.

Donde a es el dividendo, k el cociente, d el divisor y r es el resto.


Notación del resto: $r_d(a)$ = resto de dividir a a por d

Ejemplo:

- $a = 1038 \wedge d = 14$ se tiene que $1038 = \underbrace{74}_k . 14 + \underbrace{2}_{r_{14}(1038)}$
- $a = 1038 \wedge d = -14$ se tiene que $1038 = \underbrace{(-74)}_k . (-14) + \underbrace{2}_{r_{14}(1038)}$
- $a = -1038 \wedge d = 14$ se tiene que $-1038 = \underbrace{-74}_k . 14 + \underbrace{-2}_{r_{14}(1038)}$.

Pero como $-2 < 0$: no cumple la condición del resto, entonces se suma y resta el divisor, se saca factor común y se logra un resto mayor que 0 que cumpla.

$$-1038 = -74.14 - \underbrace{14 + 14}_{\pm d} - 2 \iff -1038 = -75.14 + 12 \text{ con } 0 \leq 12 < 14.$$

 **Observación:** En la teórica se realiza la demostración del teorema, acá se opta por omitirla.

Restos

Recordando que (Algoritmo de división) dados $a, d \in \mathbb{Z}$ con $d \neq 0$, existen $k, r \in \mathbb{Z}$ tales que:

$$a = k.d + r, \text{ con } 0 \leq r < |d|$$

 **Observaciones:**

1. Suponiendo que $0 \leq a < |d|$, entonces $a = r_d(a)$

2. $r_d(a) = 0 \iff d \mid a \iff a \equiv 0 \pmod{d}$

3. Congruencia y restos:

$$\bullet a \equiv r_d(a) \pmod{d}$$

$$\bullet a \equiv r \pmod{d} \text{ con } 0 \leq r < |d| \implies r = r_d(a)$$

$d \mid a - r \implies \exists k \in \mathbb{Z} : a - r = kd \implies a = kd + r \text{ con } 0 \leq r < |d| \implies r = r_d(a)$, es decir que el resto de dividir a por d .

$$\bullet r_1 \equiv r_2 \pmod{d} \text{ con } 0 \leq r_1, r_2 < |d| \implies r_1 = r_2.$$

$$\bullet \boxed{a \equiv b \pmod{d} \iff r_d(a) = r_d(b).}$$

Tablas de restos

Relación de resto con suma y producto

- $r_d(a + b) = r_d(r_d(a) + r_d(b))$ pues $a + b \equiv r_d(a) + r_d(b) \pmod{d}$
- $r_d(ab) \equiv r_d(r_d(a) \cdot r_d(b))$
- $r_d(a^n) = r_d(r_d(a)^n)$
- **Tablas de restos:**

$r_7(a)$	0	1	2	3	4	5	6
$r_7(a^2)$	0	1	4	2	2	4	1
$r_7(a^3)$	0	1	1	6	1	6	6

Nota para el lector: Estas notas de tablas de restos fueron copiados de los apuntes de Maria Marino.

Sistemas de numeración

Desarrollo en base d

Sea $d \in \mathbb{N}, d \geq 2$. Entonces $\forall a \in \mathbb{N}_0$ se puede escribir en la forma

$$a = r_n d^n + r_{n-1} d^{n-1} + \dots + r_1 d + r_0$$

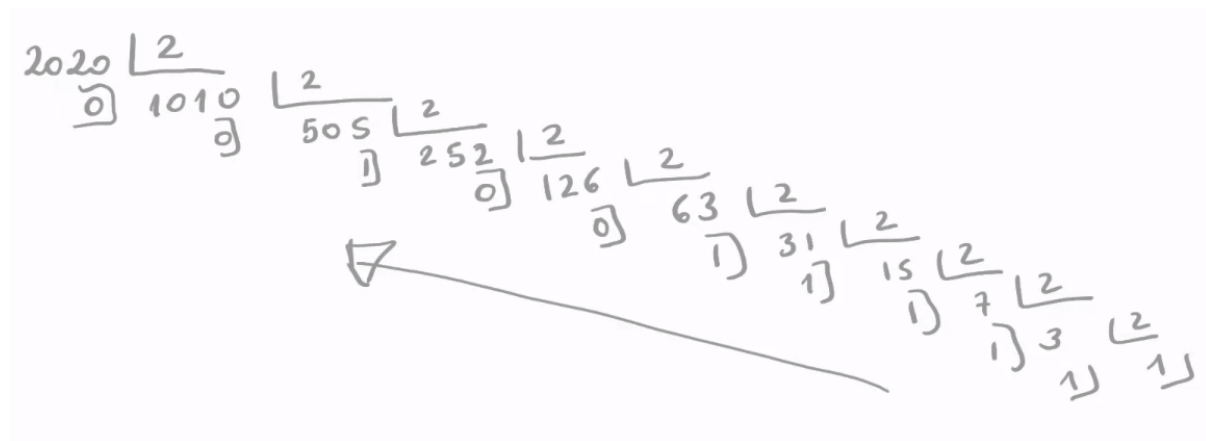
Con $0 \leq r_i < d$ para $0 \leq i \leq n$ con $r_n \neq 0$ si $a \neq 0$.

Y este desarrollo es único, es decir r_n, \dots, r_0 son únicos en esas condiciones.

Notación: $a = (r_n r_{n-1} \dots r_1 r_0)_d$.

Convención: $2020 = (2020)_{10}$

- $2020 = (5614)_7$
- $2020 = (11111100100)_2 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^2$



Observaciones:

1. $d^n = (\underbrace{10\dots 0}_n)_d$ tiene $n + 1$ cifras

2. **¿Cuál es el número más grande que puedo escribir usando n cifras en base d ?**

$$\underbrace{((d-1)(d-1)\dots(d-1))}_n = \sum_{i=0}^{n-1} (d-1)d^i$$

Otra forma de pensarlo es: d^n es el número más chico que puedo escribir usando $n + 1$ cifras, por lo tanto, el número más grande que puedo escribir usando n cifras es $d^n - 1$.

3. **¿Cuántos números hay con $\leq n$ cifras en base d ?**

Del 0 al $d^n - 1$, o sea hay d^n .

4. **¿Cuál es la forma más rápida de calcular 2^{16} ?**

Forma "*dividir y conquistar*", usa cuatro productos.

$$2 \mapsto 2 \cdot 2 = 4 \mapsto 4 \cdot 4 = 2^4 \mapsto 2^4 \cdot 2^4 = 2^8 \mapsto 2^8 \cdot 2^8 = 2^{16}$$

Para calcular a^n genérico, escribo n en base 2. Por ejemplo, si $n = 2^4 + 2^2 + 1$, entonces

$$\rightsquigarrow a^n = a^{2^4} + a^{2^2} + a$$

Nota para el lector: Estas observaciones fueron copiadas de los apuntes de Maria Marino.

Teórica 12 - MCD, Combinación lineal entera y coprimos

Sean $a, b \in \mathbb{Z}$, **no ambos nulos**. El MCD entre a y b es el mayor de los divisores común entre a y b y se nota $(a : b)$.

Algoritmo de Euclides

Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Entonces $\forall k \in \mathbb{Z}$ se tiene:

$$(a : b) = (b : a - kb)$$

En particular, como $r_b(a) = a - kb$, con k el cociente (para $b \neq 0$), se tiene

$$(a : b) = (b : r_b(a))$$

Ejemplo:

Calcular $(-120 : 84) = (120 : 84)$

1. Divido a 120 por 84:

$$120 = 84 + 36 \implies (120 : 84) = (84 : 36)$$

2. Divido a 84 por 36:

$$84 = 2 \cdot 36 + 12 \implies (84 : 36) = (36 : 12)$$

3. Divido a 36 por 12:

$$36 = 3 \cdot 12 + 0 \implies (36 : 12) = (12 : 0) = 12$$

En conclusión:

$$(120 : 84) = (84 : 36) = (36 : 12) = (12 : 0) = 12$$

Nota para el lector: Este ejemplo se da en la teórica, pero fue copiado de las notas de Maria Marino.

Máximo común divisor y combinación entera

El máximo común divisor es combinación entera. Sean $a, b \in \mathbb{Z}$ no ambos nulos, entonces:

$$\exists s, t \in \mathbb{Z} : (a : b) = sa + tb$$

Ejemplo:

$(324 : 120)$ usando el algoritmo de Euclides:

$$\begin{aligned} & (324 : 120) \\ & 324 = 2 \cdot 120 + 84 \\ & \quad \vdots \\ \implies & 12 = (324 : 120) \end{aligned}$$

Mirándolo "de abajo para arriba":

$$\begin{aligned}
 12 &= 84 - 2 \cdot 36 \\
 &= 84 - 2(120 - 84) \\
 &= 3 \cdot 84 - 2 \cdot 120 \\
 &= 3(324 - 2 \cdot 120) - 2 \cdot 120 \\
 12 &= \underbrace{3}_s \cdot 324 + \underbrace{-8}_t \cdot 120
 \end{aligned}$$

Consecuencias:

1. El máximo común divisor satisface que todo divisor común lo divide.

Sean $a, b \in \mathbb{Z}$ no ambos nulos, y $d \in \mathbb{Z} - \{0\}$. Si

$$d|a \text{ y } d|b \implies d|(a : b)$$

2. Sea $c \in \mathbb{Z}$. Entonces

$$\exists s', t' \in \mathbb{Z} \text{ con } c = s'a + t'b \iff (a : b)|c$$

3. Sea $a, b \in \mathbb{Z}$ no ambos nulos, y sea $k \in \mathbb{N}$

»

Coprimos


Dados $a, b \in \mathbb{Z}$ no ambos nulos, se dice que son números coprimos si $(a : b) = 1$.

Notación: $a \perp b \iff (a : b) = 1$

 **Observación:**

$$a \perp b \iff \exists s, t \in \mathbb{Z} \text{ tal que } 1 = sa + tb$$

Coprimizar

 No existe la palabra coprimizar, básicamente la invento Teresa y se va a usar en toda la materia.

Sean $a, b \in \mathbb{Z}$ no ambos nulos. Entonces

$$\begin{aligned}
 &\frac{a}{(a : b)} \perp \frac{b}{(a : b)} \\
 &\begin{cases} a = (a : b)a' \\ b = (a : b)b' \end{cases} \text{ con } a' \perp b'
 \end{aligned}$$

Propiedades de coprimos

1. Sean $a, c, d \in \mathbb{Z}$ con $c, d \neq 0$, entonces

$$c|a \text{ y } d|a \text{ y } c \perp d \implies cd|a$$

2. Sean $a, b, d \in \mathbb{Z}$ con $d \neq 0$. Entonces

$$d|ab \text{ y } d \perp a \implies d|b$$

Teórica 13 - Los números primos

Número primo y número compuesto

Sea $p \in \mathbb{Z}$ es **primo** si $p \neq 0, \pm 1$ y a tiene únicamente los dos divisores positivos 1 y p .

$$p = \{p \in \mathbb{N} : p \text{ es primo}\} = \{2, 3, 5, 7, 11, 13, 17, \dots\}$$

$a \in \mathbb{Z}$ es **compuesto** si $a \neq 0, \pm 1$ y existe d con $d \mid a$ y $1 < d < |a|$.

🧐 **Observación:**

- Sea $a \in \mathbb{Z}$, $a \neq 0, \pm 1$. Entonces existe $p \in \mathbb{P}$ (p primo positivo) tal que $p \mid a$.
- Existen infinitos primos (positivos).

Criba de Eratóstenes

El concepto de Criba de Eratóstenes consta de establecer una lista de n números naturales ≥ 2 con una cota superior $m \in \mathbb{N}$, en donde marcamos un número, empezando con el primero de la lista y posteriormente tachamos todos los números múltiplos de ese número. Una vez que terminamos de tachar todos los números múltiplos de ese número marcado, pasamos al siguiente e iteramos el procedimiento. Al final logramos que todos los números marcados son primos.

Observación: Si n es compuesto ($n \in \mathbb{N}$) $\implies \exists p \in P/p \mid n$ con $p \leq \sqrt{n}$.

Conjeturas abiertas

- **Conjetura de los primos gemelos:** Dados dos números primos $a, b \in \mathbb{N}$, se dice que son primos gemelos si $\text{dist}(a, b) = 2$.
- **Conjetura de Goldbach:** $\forall n \geq 4$ par es suma de 2 primos (positivos). Verificado para n par hasta $4 \cdot 10^{18}$.
- No se conoce fórmulas que producen primos.

Cosas que se saben:

- **Teorema de primos:**

$$\pi(n) = \#\{p \in P/p \leq n\}$$

$$\pi(n) \sim \frac{n}{\ln n}$$

- **Teorema de primos en progresión aritmética**
Sean $n, d \in \mathbb{N}$ con $n \perp d$, $\{n + kd, k \in \mathbb{N}_0\}$ contiene ∞ primos, $\{m, n + d, n + 2d, \dots\}$.
- Si $2^p - 1$ es primo, se llama primo de **Mersenne**.

$2^{82589903} - 1$ es el primo más grande conocido a la fecha y tiene 24862048 dígitos.

- Si $n^{2^n} + 1$ es primo, se llama primo de **Fermat**.

Algoritmos de primos

- Primes is in P - Manindra Agrawal, Neeraj Kayal, Nitin Saxena.
- Sea $n \in \mathbb{N}$ compuesto. ¿Le puedo encontrar los factores? NO, es difícil (para números grandes).

El Teorema Fundamental de la Aritmética

Sea p primo, y sean $a, b \in \mathbb{Z}$. Entonces $p \mid ab \implies p \mid a \text{ o } p \mid b$.

Generalización: Sea $p \in \mathbb{Z}$,

- Sean $a_1, \dots, a_n \in \mathbb{Z} : p \mid a_1 \dots a_n \implies p \mid a_i$ para algún $i, 1 \leq i \leq n$.
- Sean $a \in \mathbb{Z}$ y $n \in \mathbb{N}, p \mid a^n \implies p \mid a$.

Teorema fundamental de la aritmética (TFA)

Sea $a \in \mathbb{Z}$ con $a \neq 0, \pm 1$. Entonces existen primos positivos distintos p_1, \dots, p_r (para algún $r \in \mathbb{N}$) y $m_1, \dots, m_r \in \mathbb{N}$ tales que $a = \pm p_1^{m_1} \dots p_r^{m_r}$ y esta escritura es única (salvo cambiar el orden de los primos).

Ejemplos: $328 = 2^3 \cdot 7 \cdot 11$ y $770 = 2 \cdot 5 \cdot 7 \cdot 11$.

 **Observación:**

- Sean p, q primos positivos \neq . Entonces $p \nmid q$ y $q \nmid p$. Son coprimos!

Producto y potencias de números

Sean $a, b \in \mathbb{Z}, a, b \neq 0, \pm 1$. Sea:

$$a = \pm p_1^{m_1} \dots p_r^{m_r} \text{ con } m_1, \dots, m_r \in \mathbb{N}_0$$

$$b = \pm p_1^{n_1} \dots p_r^{n_r} \text{ con } n_1, \dots, n_r \in \mathbb{N}_0$$

$$(328 = 2^3 \cdot 7 \cdot 11 \text{ y } 770 = 2 \cdot 5 \cdot 7 \cdot 11)$$

Entonces:

- $ab = \pm p_1^{m_1+n_1} \dots p_r^{m_r+n_r}$.
- Para $n \in \mathbb{N}, a^n = (\pm 1)^n p_1^{nm_1} \dots p_r^{nm_r}$

Teórica 14 - Divisores de un número y MCD, MCM y factorización



Si conocemos la factorización en primos de un número conocemos a sus divisores (y cuántos son)

Divisores y cantidad

Sea $a \in \mathbb{Z}$, $a \neq 0, \pm 1$. Si la factorización en primos de a es

$$a = \pm p_1^{m_1} \dots p_r^{m_r} \quad \text{con } m_1, \dots, m_r \in \mathbb{N}$$

Entonces

1. $Div(a) = \{\pm p_1^{n_1} \dots p_r^{n_r} \mid \text{donde } 0 \leq n_1 \leq m_1, \dots, 0 \leq n_r \leq m_r\}$
2. $Div_+(a) = (m_1 + 1) \dots (m_r + 1)$ y además:
 $\#Div(a) = 2 \cdot (m_1 + 1) \dots (m_r + 1)$

🧐 **Observación:** Sean $a, d \in \mathbb{Z}$ con $d \neq 0$, entonces:

$$d|a \iff d^n|a^n \quad \forall n \in \mathbb{N}$$

Factorización y MCD

Sean $a, b \in \mathbb{Z}$ no nulos, con

$$a = p_1^{m_1} \dots p_r^{m_r} \quad \text{con } m_1, \dots, m_r \in \mathbb{N}_0$$

$$b = p_1^{n_1} \dots p_r^{n_r} \quad \text{con } n_1, \dots, n_r \in \mathbb{N}_0$$

Entonces

$$(a : b) = p_1^{\min\{m_1, n_1\}} \dots p_r^{\min\{m_r, n_r\}}$$

🧐 **Observación:** Sean $a, b, c \in \mathbb{Z}$ no nulos, entonces:

- $a \perp b \iff$ no tienen primos en común
- $a \perp b$ y $a \perp c \iff a \perp bc$
- $a \perp b \iff a^m \perp b^n \quad \forall m, n \in \mathbb{N}$
- $(a^n : b^n) = (a : b)^n$ (Importante: tiene que ser el mismo exp.)

Mínimo común múltiplo (positivo)

💡 El mínimo común múltiplo se nota $[a : b]$ y está definido para $a, b \neq 0$

Sean $a, b, c \in \mathbb{Z}$ no nulos. Si

$$a = p_1^{m_1} \dots p_r^{m_r} \quad \text{con } m_1, \dots, m_r \in \mathbb{N}_0$$

$$a = p_1^{n_1} \dots p_r^{n_r} \quad \text{con } n_1, \dots, n_r \in \mathbb{N}_0$$

Entonces

$$[a : b] = p_1^{\max\{m_1, n_1\}} \dots p_r^{\max\{m_r, n_r\}}$$

Ejemplos:

$$1. [12 : 18] = 36 \iff [2^2 \cdot 3 : 2 \cdot 3^2] = 2^2 \cdot 3^2$$

Propiedades del mínimo común múltiplo

1. Cualquier múltiplo común es múltiplo del MCM


Si $a|m$ y $b|m$, entonces $[a : b]|m$.

$$2. (a : b)[a : b] = |a \cdot b|.$$

Teórica 15 - Ecuaciones diofánticas

Sea $aX + bY = c$ con $a, b, c \in \mathbb{Z}$ y a y b no nulos

$$S = \{(x, y) \in \mathbb{Z}^2 : aX + bY = c\}$$

 **Observación:** Si $a = 0$ (o $b = 0$) $\implies bY = C$ su solución entera es $\iff b \mid c$ $S = \{\frac{c}{b}\}$. Es por ello que podemos considerar el caso $a \neq 0$ y $b \neq 0$.

Ejemplos:


- $5x + 9y = 1$, donde $S \neq \emptyset$ pues por ejemplo $x_0 = 2, y_0 = -1$.
- $4x + 6y = 7$, donde $S \neq \emptyset$ pues el termino de la izquierda es par.
- $18x - 12y = 2$, donde $S \neq \emptyset$ pues $(18 : 12) = 6$.
 $\exists s, t \in \mathbb{Z} : 6 = 18s + 12t$ y si c es combinación entera de 18 y 12, entonces $6 \mid c$.
- $4x + 6y = 2$, donde $S \neq \emptyset$, por ejemplo $x_0 = -1$ e $y_0 = 1$.
- $18x - 12y = 60$, donde $S \neq \emptyset$, pues $6 \mid 60$.
 $18x - 12y = 60 \iff \underbrace{3x - 2y}_{(3:2)=1} = 10,$

Cuando se divide por el máximo común divisor a ambos términos de la igualdad, se coprimiza, así es más viable encontrar una solución a ojo. Si no encuentro una solución a ojo, utilizo el Algoritmo de Euclides para lograr escribir el 1 ($(3 : 2)$ en este caso) como combinación lineal entera y después multiplico todo por c .

$$\implies 3 \cdot 1 - 2 \cdot 1 = 1 \implies \underbrace{3 \cdot 10}_{x_0} - \underbrace{2 \cdot 10}_{y_0} = 10.$$

Proposición: Sea $aX + bY = c$ con $a, b, c \in \mathbb{Z}$ y a y b no nulos y sea $S = \{(x, y) \in \mathbb{Z}^2 : aX + bY = c\}$. Entonces $S \neq \emptyset \iff (a : b) \mid c$.

Algoritmo de ecuaciones diofánticas

 ¿Cómo son todas las soluciones cuando $(a : b) = c$?

Para resolver la ecuación diofántica $a, b, c \in \mathbb{Z}$ con $a \neq 0, b \neq 0$.

1. **Coprimizo la ecuación:** $aX + bY = c \iff a'X + b'Y = c'$, con $a' = \frac{a}{(a:b)}, b' = \frac{b}{(a:b)}$ y $c' = \frac{c}{(a:b)} \in \mathbb{Z}$.
2. Sea $(x_0, y_0) \in \mathbb{Z}^2$ una solución particular. Se busca a ojo o aplicando el algoritmo de Euclides:
 $1 = s \cdot a' + t \cdot b' \implies c' = \underbrace{sc'}_{x_0} \cdot a' + \underbrace{tc'}_{y_0} \cdot b' \implies a' \cdot x_0 + b' \cdot y_0 = c'.$
3. El conjunto S de todas las soluciones es:

$$S = \{(x, y) \in \mathbb{Z}^2 : x = x_0 + kb', y = y_0 - ka', k \in \mathbb{Z}\}$$

Ecuaciones de congruencia

Sea $aX \equiv c \pmod{b}$ con $a, b \neq 0$ tiene solución $\iff (a : b) \mid c$.

En ese caso coprimizando:

$$aX \equiv c \pmod{b} \iff a'X \equiv c' \pmod{b'} \iff x \equiv x_0 \pmod{b'}$$

Donde $a' = \frac{a}{(a:b)}$, $b' = \frac{b}{(a:b)}$ y $c' = \frac{c}{(a:b)} \in \mathbb{Z}$, y donde x_0 es una solución particular.

🗣️ **Observación:** $aX \equiv c \pmod{b} \iff aX + bY = c$

Algoritmo de ecuaciones de congruencia

Sea $aX \equiv c \pmod{m}$ con $a, c \in \mathbb{Z}, m \in \mathbb{N}, a \neq 0$


1. Reducir $a, c \pmod{m}$, donde podemos suponer que $a \leq a, c < m$.
2. Necesito saber si tiene solución entera, chequeo $(a : m) \mid c$:
Si $(a : m) \nmid c \implies$, no existe solución y el algoritmo termina acá.
Si $(a : m) \mid c \implies$, existe solución y **coprimizo**:
 $aX \equiv c \pmod{m} \iff a'X \equiv c' \pmod{m'}$, donde $a' = \frac{a}{(a:b)}$, $m' = \frac{m}{(a:b)}$ y $c' = \frac{c}{(a:b)} \in \mathbb{Z}$.
3. Ahora que $a' \perp m'$, puedo limpiar los factores comunes entre a' y c' (los puedo simplificar): \iff
 $a'X \equiv c' \pmod{m'} \iff \iff a''X \equiv c'' \pmod{m'}$.
Con $a'' = \frac{a'}{(a':b')}$ y $c'' = \frac{c'}{(a':b')} \in \mathbb{Z}$.
4. Encuentro una solución particular con $0 \leq x_0 < m'$ y tenemos:

$$aX \equiv c \pmod{m} \iff x \equiv x_0 \pmod{m'}$$

Teórica 16 - Sistemas de ecuaciones de congruencia y Teorema chino del resto

$$ax \equiv c \pmod{m} \xLeftrightarrow{(a:m)|c} a'x \equiv c' \pmod{m'} \iff x \equiv x_0 \pmod{m'} \quad \text{con } 0 \leq x_0 \leq m'$$

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \vdots \\ x \equiv c_k \pmod{m_k} \end{cases}$$

 $x \equiv c \pmod{m} \implies x \equiv c \pmod{d} \text{ si } d|m$


Lo primero que hay que hacer es decidir si un sistema es compatible o incompatible, simplificar el sistema, quebrarlo de forma tal que los módulos sean coprimos dos a dos.

Cuando tenemos un sistema que tiene siempre el mismo número del lado derecho de la congruencia y **cuyos módulos son coprimos dos a dos**, podemos simplificar de la siguiente forma:

$$\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 3 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases} \iff x \equiv 3 \pmod{4 \cdot 3 \cdot 5}$$

Nota para el lector: Estos ejemplos de desarrollo de sistemas de ecuaciones de congruencia fue copiado de los apuntes de María Marino.

Teorema chino del resto

 Motivado por la resolución del problema de contar soldados, donde la cantidad de soldados era menor a 44000, Por Sun -Tzu.

Sean $m_1, \dots, m_n \in \mathbb{N}$ coprimos dos a dos ($\forall i \neq j$, se tiene $m_i \perp m_j$), es decir, no importa que pares de números m_i e m_j que agarre, siempre van a ser coprimos.

Entonces, dados $c_1, \dots, c_n \in \mathbb{Z}$ cualesquiera, el sistema de ecuaciones de congruencia:

$$\begin{cases} X \equiv c_1 \pmod{m_1} \\ X \equiv c_2 \pmod{m_2} \\ \dots \\ X \equiv c_n \pmod{m_n} \end{cases}$$

Es equivalente al sistema $X \equiv x_0 \pmod{m_1 m_2 \dots m_n}$ para algún x_0 con $0 \leq x_0 < m_1 m_2 \dots m_n$

Teórica 17 - El pequeño teorema de Fermat

Pequeño Teorema de Fermat (PMF)

Sea p primo, y sea $a \in \mathbb{Z}$. Entonces:

1. $a^p \equiv a \pmod{p}$
2. $p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}$

Comentarios:

- El PTF no vale en general si p no es primo:

$$3^4 \not\equiv 3 \pmod{4} \text{ ya que } 81 \equiv 1 \pmod{4} \quad (\text{Ejemplo})$$

- $a^p \equiv a \pmod{p} \iff (p \nmid a \implies a^{p-1} \equiv 1 \pmod{p})$, es decir, la primera propiedad vale si y solo si la segunda también lo hace.

Corolario: Sea p primo, entonces $\forall a \in \mathbb{Z}$ tal que $p \nmid a$ se tiene:

$$a^n \equiv a^{R_{p-1}(n)} \pmod{p}, \forall n \in \mathbb{N}$$

Ejemplos:

- Calcular $r_{11}(27^{2154})$:

$$\begin{aligned} 27^{2154} &\equiv 27^{2154} \pmod{11} \\ &\equiv 5^{2154} \pmod{11} \\ &\equiv 5^4 \pmod{11} \quad \text{pues } r_{\underbrace{10}_{p-1}}(2154) = 4 \\ &\equiv 5^2 \cdot 5^2 \pmod{11} \\ &\equiv 3 \cdot 3 \pmod{11} \\ 27^{2154} &\equiv 9 \pmod{11} \end{aligned}$$

- Calcular $r_{11}(24^{13^{1521}})$:

$$\begin{aligned} 24^{13^{1521}} &\equiv 2^{13^{1521}} \pmod{11} \\ 13^{1521} &\equiv ? \pmod{10} \quad \text{calculo el resto del exponente por PMF} \\ &\equiv 3^{1521} \pmod{10} \\ &\equiv 3^{2 \cdot 760 + 1} \equiv (3^2)^{760} \cdot 3 \pmod{10} \\ &\equiv 9^{760} \cdot 3 \pmod{10} \\ &\equiv -1^{760} \cdot 3 \pmod{10} \\ 13^{1521} &\equiv 3 \pmod{10} \\ 24^{13^{1521}} &\equiv 2^3 \equiv 8 \pmod{11} \quad \text{reemplazo el exponente por su congruencia} \end{aligned}$$

Tests de primalidad

Test de Miller - Rabin

Dado m impar con $m - 1 = 2^s d$ (d impar) y $1 < a < m$. Calculamos:

$$a^d \equiv ? \pmod{m} \quad y \quad a^{2^r d} \equiv ? \pmod{m} \quad \text{para } 0 \leq r < s$$

Si $a^d \not\equiv 1 \pmod{m}$ y $a^{2^r d} \not\equiv -1 \pmod{m}$ para $0 \leq r < s$, entonces m es compuesto (con seguridad).

Si $a^d \equiv 1 \pmod{m}$ ó para algún r , $a^{2^r d} \equiv -1 \pmod{m}$, entonces m es "probablemente primo".

Probamos que para cada m compuesto \exists un "testigo" a con $1 < a < m$ tal que:

$$a^d \not\equiv 1 \pmod{m} \quad y \quad a^{2^r d} \not\equiv -1 \pmod{m} \quad \text{para } 0 \leq r < s$$

En realidad, más aún, $\frac{3}{4}$ de los $a < m$ son testigos...

Con k repeticiones del test, si da que m es "probablemente primo", entonces la probabilidad de haber fallado, es decir, la probabilidad de que en realidad sea compuesto, es menor que $(\frac{1}{4})^k$

Teórica 18 - Sistema Criptográfico RSA y Teorema Euler-Fermat

Pequeña generalización del Teorema de Fermat

Sean p, q primos distintos y sea $a \in \mathbb{Z}$ con $a \perp pq$.

Entonces

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$$

$$\text{y si } m \equiv r \pmod{(p-1)(q-1)} \implies a^m \equiv a^r \pmod{pq}$$

Teorema de Euler-Fermat

Sea $p \in \mathbb{N}$ primo y $a \in \mathbb{Z}$ tal que $p \nmid a$. Entonces:

$$a^{p \cdot (p-1)} \equiv 1 \pmod{p^2}$$

Sistema RSA

1. Bob elige 2 primos muy grandes p y q , y a partir de estos se construye $n = pq$.
2. Tome e con $1 \leq e < (p-1)(q-1)$ tal que $e \perp (p-1)(q-1)$.
3. Resuelve $eX \equiv 1 \pmod{(p-1)(q-1)}$.
Sea d con $1 \leq d < (p-1)(q-1)$ una solución particular.

Clave privada: (n, e)

Clave publica: (n, d)



Como funciona el algoritmo?

1. Alice tiene un mensaje aa con $1 \leq a < n$ para mandarle a Bob:

$$a \implies a^d \equiv \underbrace{c(a)}_{a < n} \pmod{n}$$

2. Bob recibe $c(a)$ y lo eleva a la e :

$$\begin{aligned} c(a)^e &\equiv a^{de} \pmod{pq} \\ &\equiv a^1 \pmod{pq} \leftarrow \text{Bob recupera } a \\ de &\equiv 1 \pmod{(p-1)(q-1)} \end{aligned}$$

3. Bob tiene mensaje con $1 \leq a < n = pq$ tal que a se convierte en $a^e \equiv c(a) \pmod{pq}$ con $0 \leq c(a) < pq$, donde:

$$\begin{aligned} a^e &\equiv c(a) \pmod{pq} \\ &\equiv a \pmod{pq} \\ ed &\equiv 1 \pmod{(p-1)(q-1)} \end{aligned}$$

Teórica 19 - Números complejos

Cuerpos

Sea K un conjunto, y sean $+, \cdot : K \times K \rightarrow K$ dos operaciones en K (usualmente la suma y el producto). Se dice que $(K, +, \cdot)$ es un **cuerpo** si:

- $+$ y \cdot son operaciones asociativas y conmutativas. Es decir $\forall x, y, z \in K$ se tiene la asociatividad y la conmutatividad.
- Existe un elemento neutro para la suma, que se nota 0_K , es decir $\forall x \in K$ se tiene $x + 0_K = x$, y un elemento neutro para el producto, que se nota 1_K , es decir $\forall x \in K$ se tiene $x \cdot 1_K = x$.
- Cualquiera sea $x \in K$, x tiene un inverso aditivo, u opuesto, que se nota $-x$, es decir que su suma es igual a 0_K , y cualquiera sea $x \in K, x \neq 0$, x tiene un inverso multiplicativo que se nota x^{-1} , es decir $x \cdot x^{-1} = 1_K$.
- La operación \cdot es distributiva sobre $+$, $\forall x, y, z \in K$.

Observación: En particular, cuando K es un cuerpo, notando $K^\times \times K^\times \rightarrow K^\times$, y tanto $(K, +)$ como (K^\times, \cdot) son grupos abelianos.

Números complejos: generalidades

Frente a la necesidad de encontrar raíces negativas se introduce una cantidad imaginaria i , que no pertenece a \mathbb{R} , que satisface $i^2 = -1$. Se "agrega" esa cantidad al cuerpo de los números reales, construyendo el "menor" conjunto que contiene a \mathbb{R} y a i , y donde se puede sumar y multiplicar (respetando la distributividad): a este conjunto lo llamamos el conjunto de los números complejos \mathbb{C} . Donde $\{z = a + b \cdot i; a, b \in \mathbb{R}\} \subset \mathbb{C}$.

Suma (y resta) y multiplicación de números complejos.

$$\begin{aligned} \bullet (a + b \cdot i) + c + d \cdot i &= (a + c) + (b + d) \cdot i \\ \bullet (a + b \cdot i) \cdot (c + d \cdot i) &= (ac - bd) + (ad + bc) \cdot i \end{aligned}$$

El cuerpo \mathbb{C} es un cuerpo que "contiene" al cuerpo de los números reales $\mathbb{R} : \forall a \in \mathbb{R}, a = a + 0 \cdot i \in \mathbb{C}$.

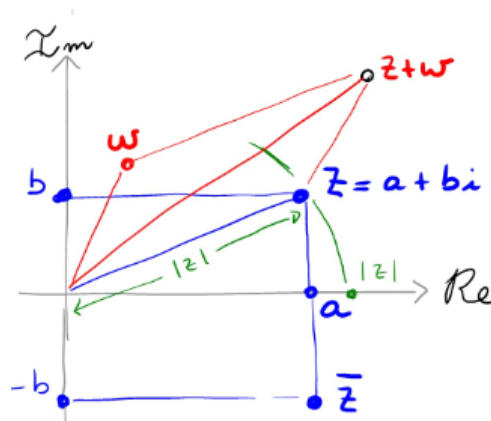
Inverso multiplicativo de $z = a + bi$, con $a \cdot b \neq 0$:

$$z^{-1} = \frac{a - bi}{a^2 + b^2}$$

Forma binomial, parte real, parte imaginaria, conjugado, modulo

- Dado $z \in \mathbb{C}$, la forma $z = a + b \cdot i$ con $a, b \in \mathbb{R}$ se llama la forma binomial de z , su parte real es $\Re(z) := a \in \mathbb{R}$ y su parte imaginaria es $\Im(z) := b \in \mathbb{R}$.
- Dado $z \in \mathbb{C}$, la forma $z = a + b \cdot i$ con $a, b \in \mathbb{R}$, el conjugado de z es $\bar{z} := a - b \cdot i \in \mathbb{C}$. y el modulo de z es $|z| = \sqrt{a^2 + b^2} \in \mathbb{R}_{\geq 0}$.

Se representa z y esas cantidades en el plano complejo, así como la operación suma, que se hace con la regla del paralelogramo. Se nota que por el Teorema de Pitágoras, $|z| = \text{dist}(z, 0)$, es decir $|z| \geq 0$ mide la distancia del número complejo z al origen 0 .



Además se tiene las siguientes relaciones entre \bar{z} y $|z|$:

$$z \cdot \bar{z} = |z|^2, \quad \forall z \in \mathbb{C} \quad \text{y} \quad z^{-1} = \frac{\bar{z}}{|z|^2}, \quad \forall z \in \mathbb{C}^\times.$$

Propiedades del conjugado y del módulo

Para todo $z \in \mathbb{C}$, se tiene:

- $\overline{\bar{z}} = z$,
- $z = \bar{z} \Leftrightarrow z \in \mathbb{R}$,
- $z + \bar{z} = 2\Re(z)$
- $z - \bar{z} = 2\Im(z)i$
- $|\Re(z)| \leq |z| \quad \text{e} \quad |\Im(z)| \leq |z|$

Además, para todo $z, \omega \in \mathbb{C}$, se tiene:

- $\overline{z + \omega} = \bar{z} + \bar{\omega}$
- $\overline{z \cdot \omega} = \bar{z} \cdot \bar{\omega}$
- Si $z \neq 0$, $\overline{z^{-1}} = \bar{z}^{-1}$.
- Si $z \neq 0$, $\overline{z^k} = \bar{z}^k, \forall k \in \mathbb{Z}$.
- $|z + \omega| \leq |z| + |\omega|$
- $|z \cdot \omega| = |z| \cdot |\omega|$
- Si $z \neq 0$, $|z^{-1}| = |z|^{-1}$
- Si $z \neq 0$, $|z^k| = |z|^k, \forall k \in \mathbb{Z}$.

Forma trigonométrica (o polar) de un número complejo

Se tiene que:

$$z = r(\cos \theta + i \operatorname{sen} \theta)$$

Donde:

$$r = |z| \quad \text{y} \quad \theta \text{ es tal que } \cos \theta = \frac{\Re(z)}{|z|} \text{ y } \operatorname{sen} \theta = \frac{\Im(z)}{|z|}.$$

Se opta por adoptar para la expresión $r(\cos \theta + i \operatorname{sen} \theta)$ la notación exponencial $r \cdot e^{\theta i}$, que se denomina la Fórmula de Euler, ya que él fue el primero en demostrar su validez:

$$r \cdot e^{\theta i} = r(\cos \theta + i \operatorname{sen} \theta), \quad \forall \theta \in \mathbb{R}$$

Por lo tanto $z = r e^{\theta i}$ donde $r = |z| \in \mathbb{R}_{>0}$ y $\theta \in \mathbb{R}$ es tal que $\cos \theta = \frac{\Re(z)}{|z|}$ y $\operatorname{sen} \theta = \frac{\Im(z)}{|z|}$.

Donde el ángulo no está determinado en forma única, ya que sabemos que:

$$\cos \theta = \cos(\theta + 2k\pi) \text{ y } \operatorname{sen} \theta = \operatorname{sen}(\theta + 2k\pi), \forall k \in \mathbb{Z}$$

Así:

$$e^{\theta i} = e^{(\theta + 2k\pi)i}, \quad \forall k \in \mathbb{Z},$$

$$s e^{\varphi i} = r e^{\theta i} \iff \begin{cases} s = r \\ \varphi = \theta + 2k\pi \text{ para algún } k \in \mathbb{Z} \end{cases}$$

Si elegimos θ con $0 \leq \theta < 2\pi$, entonces este ángulo está determinado en forma única y se denomina el argumento de z que se denota $\arg z$.

🗨️ **Observación:**

- $\bar{z} = r(\cos(-\theta) + i \operatorname{sen}(-\theta)) = r e^{-\theta i}$
- $z^{-1} = r^{-1}(\cos(-\theta) + i \operatorname{sen}(-\theta)) = r^{-1} e^{-\theta i}$

Formula de de Moivre

Sean $z = r(\cos \theta + i \operatorname{sen} \theta) = r e^{\theta i}$ y $w = s(\cos \varphi + i \operatorname{sen} \varphi) = s e^{\varphi i}$ con $r, s \in \mathbb{R}_0$ y $\theta, \varphi \in \mathbb{R}$. Entonces:

$$z \cdot w = r s (\cos(\theta + \varphi) + i \operatorname{sen}(\theta + \varphi)) = r s e^{(\theta + \varphi)i}$$

Es decir:

$$r e^{\theta i} \cdot s e^{\varphi i} = r s e^{(\theta + \varphi)i}.$$

En particular,

$$0 \leq \arg(z) + \arg(w) - 2k\pi < 2\pi.$$

con $k = 0$ o 1 elegido de modo tal que:

$$0 \leq \arg(z) + \arg(w) - 2k\pi < 2\pi.$$

Expresión trigonométrica de una potencia

Sean $z = r(\cos \theta + i \operatorname{sen} \theta) = r e^{\theta i}$ y $w = s(\cos \varphi + i \operatorname{sen} \varphi) = s e^{\varphi i}$ con $r, s \in \mathbb{R}_0$ y $\theta, \varphi \in \mathbb{R}$. Entonces:

- $\frac{z}{w} = \frac{r}{s}(\cos(\theta - \varphi) + i \operatorname{sen}(\theta - \varphi)) = \frac{r}{s} e^{(\theta - \varphi)i}$
- $z^n = r^n(\cos(n\theta) + i \operatorname{sen}(n\theta)) = r^n e^{n\theta i}$, para todo $n \in \mathbb{Z}$.

Raíces cuadradas de números complejos

Sea $z \in \mathbb{C}$. Entonces existe $\omega \in \mathbb{C}$ tal que $\omega^2 = (-\omega)^2 = z$. Si $z \neq 0$, entonces z tiene exactamente dos raíces cuadradas distintas, que son ω y $-\omega$.

Ejemplo: Calcular las raíces cuadradas complejas de $z = 3 - 4i$.

Planteemos $\omega^2 = z$ donde $\omega = x + yi \in \mathbb{C}$ con $x, y \in \mathbb{R}$ a determinar. Esto implica $|\omega^2| = |z|$, es decir $|\omega|^2 = |z|$ también. Por lo tanto, de $\omega^2 = 3 - 4i$ y $|\omega^2| = |3 - 4i| = \sqrt{25} = 5$, obtenemos las ecuaciones:

$$\begin{cases} x^2 - y^2 + 2xyi = 3 - 4i \\ x^2 + y^2 = 5 \end{cases} \iff \begin{cases} x^2 - y^2 = 3 \\ 2xy = -4 \\ x^2 + y^2 = 5 \end{cases}$$

De la primera ecuación $2x^2 = 5 + 3 = 8$, y de la tercera $2y^2 = 5 - 3 = 2$. Luego:

$$x = \pm \sqrt{\frac{8}{2}} = \pm \sqrt{4} = \pm 2 \text{ e } y = \pm \sqrt{\frac{2}{2}} = \pm \sqrt{1} = \pm 1$$

O sea que en principio tenemos 4 posibilidades, eligiendo x e y positivos y/o negativos. Pero la segunda condición nos dice que $xy = -2$, el producto es negativo, por lo tanto si se toma $x = 2$ se debe tomar $y = -1$ y si se toma $x = -2$ se debe tomar $y = 1$: los candidatos a raíces cuadradas son:

$$\omega = 2 - i \quad \text{y} \quad \omega' = -\omega = -2 + i$$

Efectivamente, es inmediato verificar que $\omega^2 = (-\omega)^2 = (4 - 1) + 2(-2)i = 3 - 4i$.

🧐 **Observación:** $\forall x, y \in \mathbb{Z}$ se tiene que:

$$\begin{cases} x^2 - y^2 = \Re(z) \\ 2xy = \Im(z) \\ x^2 + y^2 = |z| \end{cases}$$

Teórica 20 - Raíces enésimas, grupo G_n y raíces primitivas de la unidad (1 y 2)

Raíces n -ésimas de números complejos

Sea $n \in \mathbb{N}$ y sea $z = se^{\varphi i} \in \mathbb{C}^\times$, con $s \in \mathbb{R}_{>0}$ y $0 \leq \varphi < 2\pi$. Entonces z tiene n raíces n -ésimas $w_0, \dots, w_{n-1} \in \mathbb{C}$, donde

$$\omega_k = s^{1/n} e^{\theta_k i} \quad \text{donde} \quad \theta_k = \frac{\varphi + 2k\pi}{n} \quad \text{para } 0 \leq k \leq n-1.$$

El grupo G_n de raíces n -ésimas de la unidad

Sea $n \in \mathbb{N}$. El conjunto de raíces n -ésimas de la unidad, es decir:

$$G_n := \{\omega \in \mathbb{C} : \omega^n = 1\} = \left\{ \omega_k = e^{\frac{2k\pi}{n} i}, 0 \leq k \leq n-1 \right\} \subseteq \mathbb{C}$$

El conjunto G_n tiene n elementos distintos en \mathbb{C} que forman un n -ágono regular en la circunferencia unidad del plano complejo, empezando desde el 1.

G_n es un grupo abeliano

Sea $n \in \mathbb{N}$:

1. $\forall \omega, z \in G_n$ se tiene que $\omega \cdot z \in G_n$.
2. $1 \in G_n$.
3. $\forall \omega \in G_n$, existe $\omega^{-1} \in G_n$.

Estas tres propiedades muestran que G_n es un grupo abeliano dentro del grupo multiplicativo $(\mathbb{C}^\times, \cdot)$: es un subconjunto de \mathbb{C} cerrado para la operación producto, el producto es claramente asociativo y conmutativo (pues es el producto de \mathbb{C} que lo es), el elemento neutro 1 de \mathbb{C} pertenece a ese subconjunto, y además cada elemento en G_n tiene inverso en G_n .

Además se tiene que, sea $n \in \mathbb{N}$ y sea $\omega \in G^n$. Entonces:

1. $|\omega| = 1$.
2. Sea $m \in \mathbb{Z}$ tal que $n|m$. Entonces $\omega^m = 1$.
3. Sean $m, m' \in \mathbb{Z}$ tales que $m \equiv m' \pmod{n}$, entonces $\omega^m = \omega^{m'}$. En particular $\omega^m = \omega^{r_n(m)}$.
4. $\omega^{-1} = \bar{\omega} = \omega^{n-1}$

Ejemplo de propiedad de sumatorias de números complejos

$$1 + \omega + \omega^2 + \omega^3 + \omega^4 = \sum_{i=0}^4 \omega^i = \begin{cases} 5 & \text{si } \omega = 1 \\ \frac{\omega^5 - 1}{\omega - 1} = \frac{1-1}{\omega-1} = 0 & \text{si } \omega \neq 1 \end{cases}$$

Intersección de grupos G_n

Sean $n, m \in \mathbb{N}$:

1. $n \mid m \implies G_n \subset G_m$.
2. $G_n \cap G_m = G_{(n:m)}$.
3. $G_n \subset G_m \iff n \mid m$.

G_n es un grupo cíclico

Sea $n \in \mathbb{N}$. Existe $\omega \in G_n$ tal que:

$$G_n = \{1, \omega, \omega^2, \dots, \omega^{n-1}\} = \{\omega^k, 0 \leq k \leq n-1\}$$

Raíces n -ésimas primitivas de la unidad

Sea $n \in \mathbb{N}$. Se dice que $\omega \in \mathbb{C}$ es una **raíz n -ésima primitiva** de la unidad si:

$$G_n = \{1, \omega, \dots, \omega^{n-1}\} = \{\omega^k, 0 \leq k \leq n-1\}.$$

Caracterización de las raíces n -ésimas primitivas de la unidad

Sea $n \in \mathbb{N}$, y sea $\omega \in \mathbb{C}$. Entonces ω es una raíz n -ésima primitiva de la unidad si y solo si:

$$\forall m \in \mathbb{Z}, \quad \omega^m = 1 \iff n \mid m$$

Raíces primitivas y potencias

Sean $n, k \in \mathbb{N}$ y sea $\omega \in \mathbb{C}$ un raíz n -ésima primitiva de la unidad. Entonces ω^k es una raíz n -ésima primitiva de la unidad si y solamente si $(n : k) = 1$, es decir que $n \perp k$.

Raíces primitivas en G_n

Sea $n \in \mathbb{N}$, y sea $w_k = e^{\frac{2k\pi}{n}i}$, $0 \leq k \leq n-1$. Entonces w_k es raíz n -ésima primitiva de la unidad si y solamente si $(n : k) = 1$, es decir $n \perp k$.

Las raíces primitiva en G_p

Sea p un primo. Entonces cualquiera sea k , $1 \leq k \leq p-1$, se tiene que $w_k = e^{\frac{2k\pi}{p}i}$ es raíz p -ésima primitiva de la unidad. Es decir $\forall \omega \in G_p$, $\omega \neq 1$, se tiene que ω es una raíz p -ésima primitiva de la unidad.

Suma y producto de los elementos de G_n

Sea $n \in \mathbb{N}$. Entonces:

$$\sum_{\omega \in G_n} \omega = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases}$$
$$\prod_{\omega \in G_n} \omega = \begin{cases} 1 & \text{si } n \text{ es impar} \\ -1 & \text{si } n \text{ es par} \end{cases}$$

Orden

Sea $w \in G_n$, se tiene que:

$$\text{ord}(w) = \min\{k \in \mathbb{N} : w^k = 1\}$$

Propiedad:

$$w \in G_n \text{ raíz primitiva} \iff \text{ord } w = n$$

🧐 **Observación:** $(\text{ord } w) | n$

Nota para el lector: Las notas sobre el orden fueron copiadas de los apuntes de Maria Marino.

Teórica 21 - El anillo de polinomios

El anillo de polinomios $K[X]$

Sea K un cuerpo, por ejemplo $K = \mathbb{Q}, \mathbb{R}$ o \mathbb{C} , donde p es un número primo (positivo). Se dice que f es un **polinomio con coeficientes** en K si f es de la forma:

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = \sum_{i=0}^n a_i X^i$$

para algún $n \in \mathbb{N}_0$, donde X es una indeterminada sobre K y $a_i \in K$ para $0 \leq i \leq n$. Los elementos $a_i \in K$ se llaman los **coeficientes** de f .

- El conjunto de todos los polinomios f con coeficientes en K se nota $K[X]$.
- Dos polinomios son iguales si y solo si coinciden todos sus coeficientes, es decir si:

$$f = \sum_{i=0}^n a_i X^i \wedge g = \sum_{i=0}^n b_i X^i \implies f = g \iff a_i = b_i, 0 \leq i \leq n$$



X : Indeterminada.

a_n o a_i : Coeficientes de f .

Observación: Si f no es el polinomio nulo, es decir $f \neq 0$, entonces se puede escribir para algún $n \in \mathbb{N}_0$ en la forma

$$f = \sum_{i=0}^n a_i X^i \text{ con } a_n \neq 0.$$

Grado de f :

Sea $f \in K[X]$ no nulo. Entonces:

- n es el **grado** de f y se nota $gr(f)$.
- a_n es el **coeficiente principal** de f y lo notaremos $cp(f)$.
- a_0 se denomina el **coeficiente constante** o **termino independiente** de f .
- Cuando $a_n = 1$, decimos que f es **mónico**.

Operaciones en $K[X]$

Las operaciones $+$ y \cdot del cuerpo K se trasladan al conjunto $K[X]$ en forma natural, se suma coeficiente a coeficiente y se multiplica aplicando la distributividad:

- Si $f = \sum_{i=0}^n a_i X^i, g = \sum_{j=0}^m b_j X^j \in K[X]$, entonces:

$$f + g = \sum_{i=0}^n (a_i + b_i) X^i \in K[X]$$

- Si $f = \sum_{i=0}^n a_i X^i, g = \sum_{i=0}^m b_i X^i \in K[X]$, entonces:

$$f \cdot g = \sum_{k=0}^{n+m} c_k X^k \in K[X] \text{ donde } c_k = \sum_{i+j=k} a_i b_j$$



Es una simple suma y multiplicación de polinomios, no es tan complejo como se ve.

Grado de la suma y del producto


Sea K un cuerpo y sean $f, g \in K[X]$ no nulos. Entonces:

- Si $f + g \neq 0$, entonces $gr(f + g) \leq \max\{gr(f), gr(g)\}$.
- $cp(f \cdot g) = cp(f) + cp(g)$. En particular, $f \cdot g \neq 0$ y $gr(f \cdot g) = gr(f) + gr(g)$.

El anillo $K[X]$

Sea K un cuerpo. Entonces, $(K[X], +, \cdot)$ es un anillo conmutativo (al igual que \mathbb{Z}). Más aun, al igual que en \mathbb{Z} , si se multiplican dos elementos no nulos, el resultado es no nulo, o dicho de otra manera:

$$\forall f, g \in K[X], f \cdot g = 0 \implies f = 0 \text{ o } g = 0.$$

 **Observación:** Esto se llama ser un dominio íntegro.

Inversibles de $K[X]$

Sea K un cuerpo. Entonces $f \in K[X]$ es inversible si y solo si $f \in K^\times$. O sea los elementos inversibles de $K[X]$ son los polinomios de grado 0.

$$f \in K[X] \text{ es inversible} \iff f \in K^\times (\exists g \in K[X] \text{ tq } f \cdot g = 1)$$

Teórica 22 - Divisibilidad, Algoritmo de división, MCD y TFA

Nota para el lector: Los apartados de algoritmo de Euclides, TFA y congruencia en $K[X]$, fueron copiados de las notas de Maria Marino.



Por lo que vimos en la sección anterior, $K[X]$ es un anillo conmutativo (más bien un dominio íntegro) que, al igual que \mathbb{Z} , no es un cuerpo, ya que no todo elemento no nulo es inversible: sabemos que los únicos polinomios inversibles son los polinomios constantes (no nulos). Tiene sentido entonces estudiar la divisibilidad así como hicimos en \mathbb{Z} . En esta sección haremos todo un paralelismo con la teoría desarrollada en \mathbb{Z} .

Divisibilidad

Sean $f, g \in K[X]$ con $g \neq 0$. Se dice que g divide a f , y se nota $g \mid f$, si existe un polinomio $q \in K[X]$ tal que $f = q.g$. O sea:

$$g \mid f \iff \exists q \in K[X] : f = q.g$$

En caso contrario, se dice que g no divide a f , y se nota $g \nmid f$.

Propiedades de la divisibilidad

- Todo polinomio $g \neq 0$ satisface que $g \mid 0$ pues $0 = 0.g$ (aquí $q = 0$).
- $g \mid f \iff c.g \mid f, \forall c \in K^\times$ (pues $f = q.g \iff f = (c^{-1}q).(c.g)$).
De la misma manera $g \mid f \iff g \mid d.f, \forall d \in K^\times$.
Se concluye que si $f, g \in K[X]$ son no nulos.

$$g \mid f \iff cg \mid df, \forall c, d \in K^\times \iff \frac{g}{cp(g)} \mid \frac{f}{cp(f)}$$



Observación: Todo polinomio tiene infinitos divisores. Pero no todo divisor g de f tiene un divisor mónico asociado, que es $g/cp(g)$.

- Sean $f, g \in K[X]$ no nulos tales que $g \mid f$ y $gr(g) = gr(f)$. Entonces $g = c.f$ para algún $c \in K^\times$.
- $g \mid f$ y $f \mid g \iff g = c.g$ para algún $c \in K^\times$ (pues tienen el mismo grado).
- Para todo $f \in K[X]$, $f \notin K$, se tiene $c \mid f$ y $c.f \mid f, \forall c \in K^\times$.




Así, todo f en esas condiciones tiene esas dos categorías distintas de divisores asegurados (los de grado 0 y los de su mismo grado que son de la forma cf , con $c \in K^\times$).

Hay polinomios que tienen únicamente esos divisores, y otros que tienen más. Esto motiva la separación de los polinomios en $K[X]$ no constantes en dos categorías, la de polinomios **irreducibles** y la de los polinomios **reducibles**.

Polinomios irreducibles y reducibles

Sea $f \in K[X]$:

- Se dice que f es **irreducible** en $K[X]$ cuando $f \notin K$ y los únicos divisores de f son de la forma $g = c$ o $g = c \cdot f$ para algún $c \in K^\times$. O sea f tiene únicamente dos divisores monicos (distintos), que son 1 y $f/\text{cp}(f)$.
- Se dice que f es **reducible** en $K[X]$ cuando $f \notin K$ y f tiene algún divisor $g \in K[X]$ con $g \neq c$ y $g \neq c \cdot f, \forall c \in K^\times$, es decir f tiene algún divisor $g \in K[X]$ con $0 < \text{gr}(g) < \text{gr}(f)$.

 **Observación:** Todo polinomio de grado 1 en $K[X]$ es irreducible.

La divisibilidad de polinomios cumple exactamente las mismas propiedades que la divisibilidad de números enteros.

Algoritmo de división

Dados $f, g \in K[X]$ no nulos, existen únicos $q, r \in K[X]$ que satisfacen

$$f = q \cdot g + r \quad \text{con} \quad r = 0 \quad \text{o} \quad \text{gr}(r) < \text{gr}(g)$$

Se dice que q es el **cociente** y r es el **resto** de la división de f por g , que se denota $r_g(f)$.

Máximo Común Divisor

Sean $f, g \in K[X]$ no ambos nulos. El máximo común divisor entre f y g , que se nota $(f : g)$, es el polinomio monico de mayor grado que divide simultáneamente a f y a g .

Propiedades

- $(f : 0) = \frac{f}{\text{cp } f} \quad \forall f \in K[X] \neq 0$
- Sean $f, g \in K[X]$ con $g \neq 0$. Si $f = qg + r$ para $q, r \in K[X]$. Entonces

$$(f : g) = (g : r)$$

- Sea $c \in K^\times$, $(c : g) = 1$ con $g \neq 0$.
- Si $g|f \implies (f : g) = \frac{g}{\text{cp } g}$ con $g \neq 0$.

Algoritmo de Euclides



El Algoritmo de Euclides permite calcular el máximo común divisor entre dos polinomios (y es de hecho la única forma de calcular el máximo común divisor de polinomios arbitrarios).

Propiedades esenciales del Algoritmo de Euclides

- $(f : g) | f \wedge (f : g) | g$
- $\exists s, t \in K[X] : (f : g) = sf + tg$
- Si $h | f \wedge h | g \implies h | (f : g)$

Polinomios coprimos

Sean $f, g \in K[X]$ no ambos nulos.

Se dice que f y g son coprimos cuando $(f : g) = 1$.

Propiedad esencial:

$$(f : g) = 1 \iff \exists s, t \in K[X] : 1 = sf + tg$$

Propiedades:

Sean $f, g, h \in K[X]$

1. Para $g, h \neq 0$:

$$\text{Si } (g : h) = 1 \implies g|f \wedge g|f \implies gh|f$$

2. Para $g \neq 0$:

$$\text{Si } (g : h) = 1 \implies g|hf \implies g|f$$

3. Coprimizando:

$$\frac{f}{(f : g)} \text{ y } \frac{g}{(f : g)} \text{ son coprimos}$$

Polinomios irreducibles y Teorema Fundamental de la Aritmética para polinomios

Sea $f \in K[X]$ irreducible.

Entonces, si $g \in K[X]$ cualquiera

$$(f : g) = \begin{cases} 1 & \text{cuando } f \nmid g \\ \frac{f}{\text{cp } f} & \text{cuando } f|g \end{cases}$$

Propiedad fundamental de los polinomios irreducibles

Sea $f \in K[X]$ irreducible y $g, h \in K[X]$ cualesquiera. Entonces

$$f|gh \iff f|g \vee f|h$$

Teorema Fundamental de la Aritmética para Polinomios

Sea $f \in K[X]$ no constante.

Entonces existen

- **polinomios irreducibles mónicos distintos** g_1, \dots, g_r
- $m_1, \dots, m_r \in \mathbb{N}$
- $c \in K^X$

tales que

$$f = c \cdot g_1^{m_1} \cdot \dots \cdot g_r^{m_r}$$

Y esta escritura es **única**.

Observación:

En $\mathbb{C}[X]$ la factorización en irreducibles siempre es con polinomios de $\text{gr} = 1$. Pero no podemos calcularlos.

En $\mathbb{R}[X]$ la factorización en irreducibles siempre es con polinomios de $\text{gr} = 1$ ó $\text{gr} = 2$. Pero no podemos calcularlos.

En $\mathbb{Q}[X]$ la factorización en irreducibles es con polinomios de cualquier grado. Pero **sí los podemos calcular**.

Observaciones de la práctica:

1. Sea $P \in K[X] \implies$ el resto de dividir a P por $X - a$ es $P(a)$.
2. El cociente de dividir $X^n - 1$ por $X - 1$ es $X^{n-1} + X^{n-2} + \dots + X^2 + X + 1$.
3. Si tengo un resto r de dividir a f por g que no es mónico puedo reemplazarlo por el polinomio mónico $\frac{r}{\text{cp } r}$ para encontrar el MCD.

Congruencia en $K[X]$

Sean $f, g, h \in K[X]$ con h no nulo

$$f \equiv g \pmod{h} \iff h \mid f - g$$

Propiedades

1. La congruencia en $K[X]$ define una relación de equivalencia.
2. Relación con la suma

$$\left. \begin{array}{l} f_1 \equiv g_1 \pmod{h} \\ f_2 \equiv g_2 \pmod{h} \end{array} \right\} \implies f_1 + f_2 \equiv g_1 + g_2 \pmod{h}$$

3. Relación con el producto

$$\left. \begin{array}{l} f_1 \equiv g_1 \pmod{h} \\ f_2 \equiv g_2 \pmod{h} \end{array} \right\} \implies f_1 \cdot f_2 \equiv g_1 \cdot g_2 \pmod{h}$$

4. $f \equiv g \pmod{h} \implies f^n \equiv g^n \pmod{h} \quad \forall n \in \mathbb{N}$
5. r es el resto de la división de f por $h \iff f \equiv r \pmod{h} \wedge (r = 0 \vee \text{gr } r < \text{gr } h)$

Teórica 23 - Evaluación y raíces múltiples

Sea $f \in K[X]$ un polinomio, entonces f en forma natural una función

$$f : K \rightarrow K \quad f(x) = a_n x^n + \dots + a_1 x + a_0 \quad \forall x \in K$$

Esta función se llama función **evaluación**.

Propiedades

Sea $f, g \in K[X]$. Entonces

- $(f + g)(x) = f(x) + g(x) \quad \forall x \in K$
- $(f \cdot g)(x) = f(x) \cdot g(x) \quad \forall x \in K$
- Si $g \neq 0$ y $f = q \cdot g + r$ entonces

$$f(x) = q(x) \cdot g(x) + r(x)$$

🧐 **Observación:** Sea f polinomio constante, o sea $f = 0$ ó $gr(f) = 0$. $f = c \in K$. Entonces:

$$f(x) = c \quad \forall x \in K$$

Raíces

Sean $f \in K[X]$ un polinomio y $x \in K$. Si $f(x) = 0$, se dice que x es una **raíz** de f (en K).

Equivalencias de raíz

$$\begin{aligned} x \in K \text{ es raíz de } f &\iff f(x) = 0 \\ &\iff X - x \mid f \\ &\iff f = q \cdot (X - x) \text{ para algún } q \in K[X]. \end{aligned}$$

Es decir, si $f \neq 0$, $X - x$ es un factor irreducible (monico) en la descomposición en irreducibles de $f \in K[X]$.

Teorema del resto

Dados $f \in K[X]$ y $x \in K$, se tiene que:

$$r_{X-x}(f) = f(x)$$

🧐 **Observaciones:**

- $g \mid f$ y $g(x) = 0$, entonces $f(x) = 0$
- 0 es raíz de $f \iff a_0 = 0$
- Sea $f = c$ polinomio constante con $c \in K^X$ entonces f no tiene raíces.
- $f = a \cdot x + b$ con $a \neq 0$. Entonces la raíz de f es $-\frac{b}{a}$
- Sean $f, g \in K[X]$ no ambos nulos y $x \in K$. Entonces

$$f(x) = g(x) = 0 \iff (f : g)(x) = 0$$


Multiplicidad de las raíces

Sea $f \neq 0$ con $f \in K[X]$, y sea $x \in K$, se tiene que:

- Sea $m \in \mathbb{N}_0$. Existe $q \in K[X]$ tal que:

$$f = (X - x)^m q \quad \text{con} \quad q(x) \neq 0$$

Donde la **multiplicidad** de x con respecto a f se denota: $\text{mult}(x; f) = m$.

 **Observación:** $\text{mult}(x; f) \leq \text{gr } f$

- Se dice que x es **raíz simple** de f si y solo si:

$$f = (X - x)q \quad \text{con} \quad q(x) \neq 0$$

- Se dice que x es **raíz múltiple** de f si y solo si:

$$f = (X - x)^2 \cdot q$$

para algún $q \in K[X]$

- Se dice que $x \in K$ es una **raíz doble** de f cuando $\text{mult}(x; f) = 2$ y que es una **raíz triple** de f cuando $\text{mult}(x; f) = 3$.

Derivada en $K[X]$

Sea $f \in K[X]$ con $f = a_n \cdot X^n + \dots + a_1 \cdot X + a_0$ entonces se establece la derivada de f como f' y se define como:

$$f' = n \cdot a_n \cdot X^{n-1} + (n-1) \cdot a_{n-1} \cdot X^{n-2} + \dots + a_1$$

Propiedades

Sean $f, g \in K[X]$

1. $(f + g)' = f' + g'$
2. $(f \cdot g)' = f' \cdot g + f \cdot g'$
3. $(g \circ f)' = g'(f) \cdot f' \implies [(X - x)^m]' = m \cdot (X - x)^{m-1}$
4. $f'' = (f')' \in K[X]$
Y para $m \in \mathbb{N}$, $f^{(m)} = (f^{(m-1)})'$

Nota para el lector: Estas propiedades fueron copiadas de los apuntes de Maria Marino.

Raíz múltiple y derivadas

Sea $f \in K[X]$ y $x \in K$. Entonces

1. x es **raíz múltiple** de $f \iff f(x) = 0 \wedge f'(x) = 0$.
2. x es **raíz simple** de $f \iff f(x) = 0 \wedge f'(x) \neq 0$.

Multiplicidad en f y f'

Sea $K = \mathbb{Q}, \mathbb{R}$ ó \mathbb{C} , y $x \in K$. Se tiene:

$$1. \text{mult}(x; f) = m \iff f(x) = 0 \wedge \text{mult}(x; f') = m - 1$$

$$2. \text{mult}(x; f) = m \iff \begin{cases} f(x) = 0 \\ f'(x) = 0 \\ \vdots \\ f^{(m-1)}(x) = 0 \\ f^{(m)}(x) \neq 0. \end{cases}$$

Si $x \in \mathbb{C} - \mathbb{R}$ es raíz de $f \in \mathbb{R}[X] \iff \bar{x}$ es raíz de f

Cantidad de raíces en $K[X]$

Sea $f \in K[X]$ no nulo

- Sean $x_1, x_2 \in K$ raíces distintas de f tales que $\text{mult}(x_1; f) = m_1$ y $\text{mult}(x_2; f) = m_2$. Entonces $(X - x_1)^{m_1}(X - x_2)^{m_2} \mid f$.
- Sean $x_1, \dots, x_r \in K$ raíces distintas de f tales que

$$\text{mult}(x_1; f) = m_1, \dots, \text{mult}(x_r; f) = m_r$$

Entonces

$$(X - x_1)^{m_1} \dots (X - x_r)^{m_r} \mid f$$

Sea K un cuerpo y sea $f \in K[X]$ un polinomio no nulo de grado n . Entonces f tiene a lo sumo n raíces en K **contadas con multiplicidad**. Es decir, la cantidad de raíces está dada por la **suma de la multiplicidad de cada raíz de f** .

Raíces racionales

Lema de Gauss

Sea $f = a_n \cdot X^n + \dots + a_0 \in \mathbb{Z}[X]$ con $a_n \neq 0 \wedge a_0 \neq 0$. Si $\frac{c}{d} \in \mathbb{Q}$ con $c \in \mathbb{Z}$, $d \in \mathbb{N}$ y $c \perp d$. Entonces:

$$f\left(\frac{c}{d}\right) = 0 \implies c \mid a_0 \wedge d \mid a_n$$

Algoritmo para calcular las raíces en \mathbb{Q} de f en $\mathbb{Z}[X]$

Sea $a_0 \neq 0$, el coeficiente del término independiente y $a_n \neq 0$, el coeficiente principal, entonces:

Se establece los $\mathcal{D}iv(a_0) \in \mathbb{Z}$ como los posibles numeradores.

Se establece los $\mathcal{D}iv_+(a_n) \in \mathbb{Z}$ como los posibles denominadores.

Para cada $c \in \mathcal{D}iv(a_0) \in \mathbb{Z}$ y $d \in \mathcal{D}iv_+(a_n)$ con $c \perp d$, chequeo si $f\left(\frac{c}{d}\right) = 0$.

Si $f\left(\frac{c}{d}\right) = 0 \implies \frac{c}{d}$ es raíz de f . Sin embargo este método no nos dice la multiplicidad de cada raíz, es por ello que para averiguar la multiplicidad de cada raíz puedo:

- Derivar y evaluar en la derivada de f si es 0.

- Realizar división de polinomios y evaluar, en el cociente, la raíz (repetir este proceso hasta que el cociente evaluado sea $\neq 0$).

Proposición:

Sea $P \in \mathbb{Q}[X]$ y sean $a, b, c \in \mathbb{Q}$ tal que $c > 0$, $b \neq 0$ y $\sqrt{c} \notin \mathbb{Q}$.

Entonces $a + b \cdot \sqrt{c}$ es raíz de $P \iff a - b \cdot \sqrt{c}$ es raíz de P .

Nota para el lector: Esta proposición fue copiada de las notas de Maria Marino.

Teórica 22 - Divisibilidad, Algoritmo de división, MCD y TFA

Teórica 24 - Cantidad de raíces y raíces en Q

Cantidad de raíces en $K[X]$

Sea $f \in K[X]$ no nulo

- Sean $x_1, x_2 \in K$ raíces distintas de f tales que $\text{mult}(x_1; f) = m_1$ y $\text{mult}(x_2; f) = m_2$. Entonces $(X - x_1)^{m_1}(X - x_2)^{m_2} \mid f$.
- Sean $x_1, \dots, x_r \in K$ raíces distintas de f tales que

$$\text{mult}(x_1; f) = m_1, \dots, \text{mult}(x_r; f) = m_r$$

Entonces

$$(X - x_1)^{m_1} \dots (X - x_r)^{m_r} \mid f$$

Sea K un cuerpo y sea $f \in K[X]$ un polinomio no nulo de grado n . Entonces f tiene a lo sumo n raíces en K **contadas con multiplicidad**. Es decir, la cantidad de raíces está dada por la **suma de la multiplicidad de cada raíz de f** .

Raíces racionales

Lema de Gauss

Sea $f = a_n \cdot X^n + \dots + a_0 \in \mathbb{Z}[X]$ con $a_n \neq 0 \wedge a_0 \neq 0$. Si $\frac{c}{d} \in \mathbb{Q}$ con $c \in \mathbb{Z}$, $d \in \mathbb{N}$ y $c \perp d$.

Entonces:

$$f\left(\frac{c}{d}\right) = 0 \implies c \mid a_0 \wedge d \mid a_n$$

Algoritmo para calcular las raíces en Q de f en $\mathbb{Z}[X]$

Sea $a_0 \neq 0$, el coeficiente del término independiente y $a_n \neq 0$, el coeficiente principal, entonces:

Se establece los $\text{Div}(a_0) \in \mathbb{Z}$ como los posibles numeradores.

Se establece los $\text{Div}_+(a_n) \in \mathbb{Z}$ como los posibles denominadores.

Para cada $c \in \text{Div}(a_0) \in \mathbb{Z}$ y $d \in \text{Div}_+(a_n)$ con $c \perp d$, chequeo si $f\left(\frac{c}{d}\right) = 0$.

Si $f\left(\frac{c}{d}\right) = 0 \implies \frac{c}{d}$ es raíz de f . Sin embargo este método no nos dice la multiplicidad de cada raíz, es por ello que para averiguar la multiplicidad de cada raíz puedo:

- Derivar y evaluar en la derivada de f si es 0.
- Realizar división de polinomios y evaluar, en el cociente, la raíz (repetir este proceso hasta que el cociente evaluado sea $\neq 0$).

Proposición:

Sea $P \in \mathbb{Q}[X]$ y sean $a, b, c \in \mathbb{Q}$ tal que $c > 0$, $b \neq 0$ y $\sqrt{c} \notin \mathbb{Q}$.

Entonces $a + b \cdot \sqrt{c}$ es raíz de $P \iff a - b \cdot \sqrt{c}$ es raíz de P .

Nota para el lector: Esta proposición fue copiada de las notas de Maria Marino.

Teórica 25 - Factorización en $K[X]$ y $C[X]$



Como ya se mencionó, todo polinomio no constante en $K[X]$ se factoriza en forma única como producto de polinomios irreducibles monicos en $K[X]$, multiplicados por su cociente principal en K . Estudiaremos en lo que sigue mas en detalle como puede ser esa factorización según quien es el cuerpo K .

Recuerdo: Reducibles vs. Raíces

1. Todo polinomio $f = a \cdot x + b \in K[X]$, gr $f = 1$ es irreducible y su factorización es:

$$f = a \left(x + \frac{b}{a} \right) \in K[X]$$

2. Sea $f \in K[X]$ con gr $f \geq 2$

- Si f tiene una raíz en $K[X]$ entonces f es reducible, ya que:

$$f = a_n \cdot x^n + \dots + a_1 \cdot x + a_0$$

y sea $x \in K$ raíz de f entonces:

$$f = a_n \cdot (X - x) \cdot q$$

con gr $q = n - 1$.

 **Observación:** No vale la recíproca.

Polinomios cuadráticos en $K[X]$

Proposición:

Sea $f = a \cdot X^2 + b \cdot X + c$, con $a, b, c \in K$ y $a \neq 0$.

Se define el determinante de f como $\Delta = \Delta(f) = b^2 - 4ac \in K$.

Si existe $\omega \in K$ tal que $\omega^2 = \Delta$, entonces las raíces de un polinomio cuadrático, x_1 y x_2 se define como:

$$x_{1,2} = \frac{-b \pm \omega}{2a}$$

y f se factoriza en $K[X]$ como

$$f = a \cdot (X - x_1) \cdot (X - x_2)$$

Polinomios cuadráticos en $R[X]$, $Q[X]$ y $C[X]$

La reducibilidad de los polinomios cuadráticos en $K[X]$, y consecuentemente en $R[X]$, $Q[X]$ y $C[X]$, dependen de Δ .

Polinomios cuadráticos en $\mathbb{R}[X]$

Si $f = a \cdot X^2 + b \cdot X + c$ tiene raíz en $\mathbb{R} \iff \Delta \geq 0$. Por lo tanto:

$$\begin{cases} f \text{ reducible} & \iff \Delta \geq 0 \\ f \text{ irreducible} & \iff \Delta < 0 \end{cases}$$

Polinomios cuadráticos en $\mathbb{Q}[X]$

Si $f = a \cdot X^2 + b \cdot X + c$ tiene raíz en \mathbb{Q} entonces $\sqrt{\Delta} \in \mathbb{Q}$.

Si $\Delta \in \mathbb{Q}^2$ entonces f tiene 2 raíces en \mathbb{Q} y f es reducible.

Sea $f \in K[X]$ con $\text{gr } f = 2$ ó $\text{gr } f = 3$, entonces:

$$f \text{ es reducible en } K[X] \iff f \text{ tiene raíz en } K$$

Polinomios cuadráticos en $\mathbb{C}[X]$

Todo polinomio de grado 2 tiene 2 raíces en \mathbb{C} (contadas con multiplicidad) y por lo tanto es reducible.

Factorización en $\mathbb{C}[X]$

💡 Recuerdo:

- Sea f un polinomio de grado 2 en $\mathbb{C}[X]$ y sean sus raíces z_1, z_2 . f puede factorizarse como:

$$f = a \cdot (X - z_1) \cdot (X - z_2)$$

- Sea $f = X^n - z$ con $z \in \mathbb{C}$
 - $z = 0 \implies f$ tiene una raíz, 0, con multiplicidad n
 - $z \neq 0 \implies f$ tiene n raíces distintas $w_k \in \mathbb{C}$, $0 \leq k < n$, $\theta = \arg z$, donde

$$w_k = |z|^{1/k} \cdot e^{\frac{\theta + 2k\pi}{n}i}$$

Entonces

$$f = (X - w_0) \cdot \dots \cdot (X - w_{n-1}) \in \mathbb{C}$$

Donde f tiene n raíces simples distintas y su factorización es con polinomios de grado 1.

Teorema Fundamental del Álgebra

Sea $f \in \mathbb{C}[X]$ un polinomio no constante.

Entonces:

- f tiene al menos una raíz z en \mathbb{C} tal que $f(z) = 0$.
- Todo polinomio no constante en $\mathbb{C}[X]$ de grado n tiene exactamente n raíces contadas con multiplicidad en \mathbb{C} .
- Los únicos polinomios irreducibles en $\mathbb{C}[X]$ son los de grado 1.

Irreducibles y factorización en $\mathbb{C}[X]$

- Sea $f \in \mathbb{C}[X]$. Entonces f es irreducible en $\mathbb{C}[X]$ si y solo si $\text{gr}(f) = 1$, es decir $f = aX + b \in \mathbb{C}[X]$ con $a \neq 0$.
- Sea $f \in \mathbb{C}[X] - \mathbb{C}$. Entonces la factorización en irreducibles de f en $\mathbb{C}[X]$ es de la forma:

$$f = c(X - z_1)^{m_1} \cdots (X - z_r)^{m_r}$$

donde $z_1, \dots, z_r \in \mathbb{C}$ son distintos, $m_1, \dots, m_r \in \mathbb{N}$ y $c \in \mathbb{C}^\times$.

Teórica 26 - Factorización en $\mathbb{R}[X]$

💡 **Recuerdo:**

- Para $f \in \mathbb{R}[X]$ con $\text{gr}(f) = 1$, entonces f es irreducible en $\mathbb{R}[X]$ y f tiene raíz en \mathbb{R} .
- Para $f = aX^2 + bX + c \in \mathbb{R}[X]$, $a \neq 0$, f tiene raíz $\iff \Delta = b^2 - 4ac \geq 0$.
Entonces f es reducible en $\mathbb{R}[X]$ $\iff f$ tiene raíz en \mathbb{R} .
- El polinomio $f = (X^2 + 1)(X^2 + 2), \dots, (X^2 + n)$, con $n \in \mathbb{N}$, $n \geq 2$, tiene grado $2n$, es reducible pero no tiene raíz.

Sea $f \in \mathbb{R}[X]$ de grado n impar, entonces f tiene (al menos) una raíz $d \in \mathbb{R}$.

En particular, si el $\text{grado}(f) \geq 3$ es impar, entonces f es irreducible en $\mathbb{R}[X]$.

🧐 **Observación:** Sea $f \in \mathbb{R}[X]$, y $z \in \mathbb{C}$. Entonces:

$$f(\bar{z}) = \overline{f(z)}$$

Sea $f \in \mathbb{R}[X]$ y sea $z \in \mathbb{C} - \mathbb{R}$. Entonces:

1. $f(z) = 0 \iff f(\bar{z}) = 0$
2. $\text{mult}(z; f) = \text{mult}(\bar{z}; f)$
3. $(X - z) \cdot (X - \bar{z})$, sabiendo que z y \bar{z} son raíces de f , entonces:

$$\begin{aligned}(X - z)(X - \bar{z}) &= X^2 - (z + \bar{z})X + z \cdot \bar{z} \\ &= X^2 - 2\text{Re}(z) \cdot X + |z|^2\end{aligned}$$

es un polinomio irreducible en $\mathbb{R}[X]$.

4. $(X - z)(X - \bar{z}) \mid f$ en $\mathbb{R}[X]$.

5. Si $\text{mult}(z; f) = m \in \mathbb{N}$ entonces:

$$[(X - z)(X - \bar{z})]^m \mid f \text{ en } \mathbb{R}[X]$$

Polinomios irreducibles en $\mathbb{R}[X]$

💡 ¿Cuáles son los polinomios irreducibles en $\mathbb{R}[X]$?

- Todos los de grado 1.
- Los de grado 2 con $\Delta = b^2 - 4ac < 0$

No hay ningún polinomio de grado ≥ 3 irreducible en $\mathbb{R}[X]$.

Factorización de f en $\mathbb{R}[X]$



Sea $f \in \mathbb{R}[X]$ con $\text{gr}(f) \geq 1$

$$f = c \cdot (X - x_1)^{m_1} \dots (X - x_r)^{m_r} (X^2 + b_1X + c_1)^{n_1} \dots (X^2 + b_sX + c_s)^{n_s}$$


Donde:

- $c \in \mathbb{R}^X$
- $x_1, \dots, x_r \in \mathbb{R}, m_1, m_r \in \mathbb{N}$.
- $b_1, c_1, \dots, b_s, c_s \in \mathbb{R} \quad n_1, \dots, n_s \in \mathbb{N}$
- $\Delta_i = b_i^2 - 4c_i < 0$, para $1 \leq i \leq s$

Algoritmos para contar raíces reales de un polinomio en $\mathbb{R}[X]$

- Regla de los signos de Descartes (determina el número de raíces positivas y negativas de un polinomio).
 **Observación:** En la teórica no se da detalles de este algoritmo por lo que adjunto [hipervínculo de Wikipedia](#).
- Sucesión de Sturm
 **Observación:** En la teórica no se da detalles de este algoritmo por lo que adjunto [hipervínculo de Wikipedia](#).

Factorización en $\mathbb{Q}[X]$

 Recuerdo de lo que ya sabemos sobre Polinomios en $\mathbb{Q}[X]$

1. Si $f \in \mathbb{Q}[X]$ es de grado 1 $\implies f$ es irreducible en $\mathbb{Q}[X]$ y f tiene raíz en \mathbb{Q} .
2. Sea $f \in \mathbb{Q}[X]$ de grado 2 ó 3. Entonces:
 f es reducible en $\mathbb{Q}[X] \iff f$ tiene raíz en \mathbb{Q}
3. Existen polinomios en $\mathbb{Q}[X]$ reducibles y sin raíz de cualquier grado > 3 .
4. Por el criterio de Eisenstein, se puede probar que para todo $n \in \mathbb{N}$ se tiene que:
 - $X^n - 2$ es irreducible en $\mathbb{Q}[X]$
 - Para p primo, $X^{p-1} + X^{p-2} + \dots + X + 1$ es irreducible en $\mathbb{Q}[X]$.

 **Observación:**

Cuando se tienen raíces de la forma $a + b\sqrt{d}$ con $a, b, d \in \mathbb{Q}, d > 0, b \neq 0$ y $\sqrt{d} \notin \mathbb{Q}$, entonces:

- $g = (X - (a + b\sqrt{d}))(X - (a - b\sqrt{d})) \in \mathbb{Q}[X]$ y es irreducible en $\mathbb{Q}[X]$.
- Sea $f \in \mathbb{Q}[X]$, entonces:

$$f(a + b\sqrt{d}) = 0 \iff f(a - b\sqrt{d}) = 0$$

- $\text{mult}(a + b\sqrt{d}; f) = \text{mult}(a - b\sqrt{d}; f)$, y además:

$$\text{mult}(a + b\sqrt{d}; f) = m \implies g^m \mid f \text{ en } \mathbb{Q}[X]$$

Acá terminan todas las teóricas de la materia. 😊