

# **Algebra I**

Ezequiel Remus

# Resumen

La idea de este apunte es ordenar y reorganizar tanto definiciones como ejercicios resueltos de la materia **Algebra I** correspondiente a una de las materias obligatorias para las carreras de Matematicas y Computación de la **UBA**.

## Índice

<b>1. Conjuntos</b>	<b>4</b>
1.1. Teoremas, Definiciones básicas sobre Conjuntos . . . . .	4
1.1.1. ¿Que es un conjunto? . . . . .	4
1.1.2. Operaciones entre conjuntos . . . . .	4
1.2. Tablas de Verdad de la lógica proposicional . . . . .	6
1.2.1. Tablas de verdad y conectores logicos . . . . .	6
1.3. Producto Cartesiano . . . . .	6
<b>2. Relaciones</b>	<b>7</b>
2.1. Relaciones en un conjunto . . . . .	7
<b>3. Funciones</b>	<b>8</b>
3.1. ¿Que es una función? . . . . .	8
3.2. Funciones inyectivas, sobreyectivas y biyectivas . . . . .	8
<b>4. Números Naturales</b>	<b>9</b>
4.1. ¿Qué son los números naturales ( $\mathbb{N}$ )? . . . . .	9
4.2. La suma de Gauss y la serie Geométrica . . . . .	9
4.2.1. La suma de Gauss . . . . .	9
4.2.2. La serie Geométrica . . . . .	9
4.3. Sumatoria . . . . .	9
4.4. Productoria . . . . .	10
4.5. El conjunto inductivo $\mathbb{N}$ y el principio de inducción . . . . .	10
4.6. Inducción Completa . . . . .	10
4.7. Sucesión de Fibonacci . . . . .	11
4.8. Sucesión de Lucas . . . . .	11
4.9. Inducción Completa . . . . .	11
<b>5. Combinatoria</b>	<b>12</b>
5.1. Cardinal . . . . .	12
5.2. Cantidad de relaciones y funciones . . . . .	12
<b>6. Enteros</b>	<b>13</b>
6.1. Divisibilidad . . . . .	13
6.2. Congruencia . . . . .	14
6.3. Algoritmo de División . . . . .	14
6.4. Maximo Comun Divisor . . . . .	15
6.5. Números Coprimos . . . . .	16
6.6. Primos y Factorización . . . . .	16
6.7. Ecuaciones Lineales Diofanticas . . . . .	17
6.8. Ecuaciones Lineales de Congruencia . . . . .	18
6.9. Teorema Chino del Resto . . . . .	19
6.10. Pequeño Teorema de Fermat . . . . .	19
<b>7. Números Complejos</b>	<b>20</b>
7.1. Motivación y Definiciones Iniciales . . . . .	20
7.2. Forma Binomial. Inverso. Modulo. Conjugado . . . . .	20
7.3. Modulo . . . . .	20
7.4. Inverso . . . . .	20
7.5. Forma Trigonometrica . . . . .	21
7.6. Resultados obtenidos a través del Teorema de De Moivre . . . . .	21
7.7. Raices n-ésimas de un numero $\mathbb{C}$ . . . . .	21

7.8. El Grupo $G_n$ de raíces n-ésimas de la Unidad . . . . .	21
---	----

# 1. Conjuntos

## Nota:

A partir de acá, deberíamos sobreentender que notaremos con letras mayúsculas (A,B,C,...) como conjuntos. El conjunto U esta definido como el *conjunto universal*, el cual contiene a todos los demás conjuntos.

## 1.1. Teoremas, Definiciones básicas sobre Conjuntos

### 1.1.1. ¿Que es un conjunto?

#### Definición 1.1.1 (informal de conjuntos) :

Un conjunto es una colección ordenada o desordenada de elementos. Se le otorgara a cada elemento la propiedad de **pertenecer o no** a un dado conjunto.

#### Definición 1.1.2 (subconjunto e inclusión) :

Dados dos conjuntos A y B, tenemos que B es subconjunto de A si es que todo elemento de B pertenece al conjunto A. A su vez, se dice que B esta contenido en A lo cual se nota:  $B \subseteq A$

#### Observación 1.1.1 (Igualdad entre conjuntos) :

Dos conjuntos A y B son iguales si tienen exactamente los mismo elementos. Esto es que A este contenido en B y que B este contenido en A. En notación matematica, esto es:

$$A=B \iff B \subseteq A \wedge A \subseteq B$$

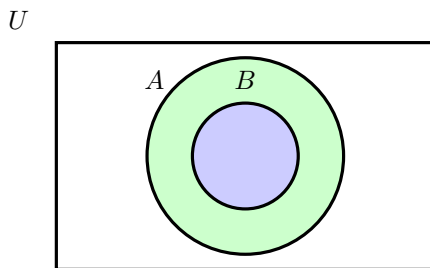


Figura 1: Diagrama de  $B \subseteq A$

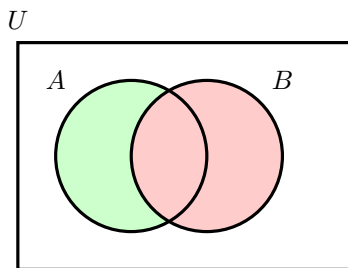


Figura 2: Diagrama de  $A \not\subseteq B$

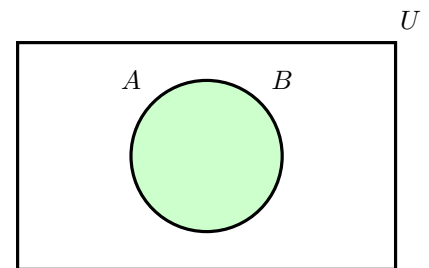


Figura 3: Diagrama de  $A = B$

#### Definición 1.1.3 (Conjunto de Partes) :

Dado un conjunto A. El Conjunto de Partes de A, es un conjunto  $\mathcal{P}(A)$  el cual esta formado por todos los subconjuntos de A posibles. Es decir, los elementos del conjunto  $\mathcal{P}(A)$  son subconjuntos del conjunto A.

### 1.1.2. Operaciones entre conjuntos

#### Definición 1.1.4 (Complemento) :

Sea A un subconjunto de un conjunto universal U. El complemento de A en U se nota  $A^c$  o  $A'$ . Es decir:

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

#### Definición 1.1.5 (Unión) :

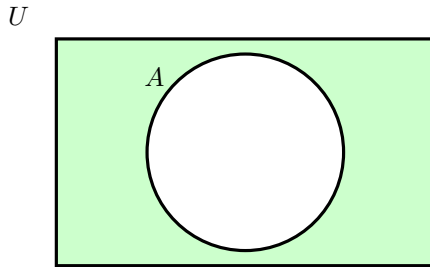
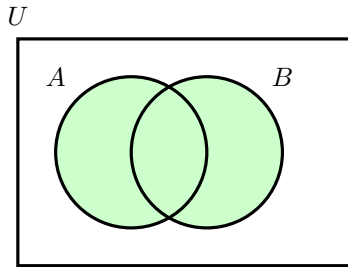
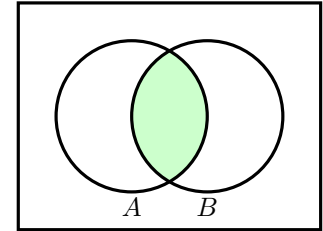
Sean A y B subconjuntos de un conjunto referencial U. La unión de A y B es el conjunto  $A \cup B$  de los elementos de U que pertenecen a A o a B. Es decir:

$$A \cup B = \{x \in U : (x \in A) \vee (x \in B)\}$$

**Definición 1.1.6 (Intersección) :**

Sean  $A$  y  $B$  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:

$$A \cap B = \{x \in U : (x \in A) \wedge (x \in B)\}$$

Figura 4: Diagrama de  $A^c$ Figura 5: Diagrama de  $A \cup B$ Figura 6: Diagrama de  $A \cap B$ 

**Observación 1.1.2** Notemos que a diferencia de la unión y la intersección no dependen del conjunto universal.

**Proposición 1.1.1 (Leyes de De Morgan y Distributivas) :**

Dados los conjuntos  $A, B, C$ :

**Leyes de De Morgan**

i)  $(A \cap B)^c = A^c \cup B^c$

ii)  $(A \cup B)^c = A^c \cap B^c$

**Leyes de Distributivas**

i)  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

ii)  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

**Definición 1.1.7 (Diferencia) :**

$$A - B := A \cap B^c$$

Por lo que :

$$x \in (A - B) \leftrightarrow (x \in A) \wedge (x \in B^c) \leftrightarrow (x \in A) \wedge (x \notin B)$$

**Definición 1.1.8 (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:

$$A \triangle B = \{x \in U : (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$$

Vale

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

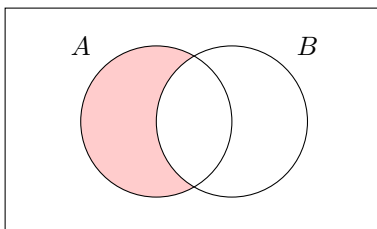


Figura 7: Diferencia Común

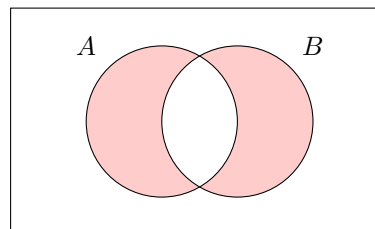


Figura 8: Diferencia Simétrica

## 1.2. Tablas de Verdad de la lógica proposicional

Las tablas de verdad son otra forma de visualizar la falsedad o veracidad de una proposición. Por como están definidas las operaciones entre conjuntos, las tablas de verdad son de fácil aplicación.

### 1.2.1. Tablas de verdad y conectores lógicos

Sean  $p$  y  $q$  proposiciones, tenemos que:

Not				or	xor	and	implica	si y solo si
$p$	$\neg p$	$p$	$q$	$p \vee q$	$p \underline{\vee} q$	$p \wedge q$	$p \Rightarrow q$	$p \Leftrightarrow q$
V	F	V	V	V	F	V	V	V
V	F	V	F	V	V	F	F	F
F	V	F	V	V	V	F	V	F
F	V	F	F	F	F	F	V	V

Los conectores lógicos coinciden con las definiciones de las tablas de operaciones de conjuntos. Teniendo en cuenta que dados dos conjuntos A y B contenidos en un conjunto referencial U nuestras proposiciones serian algo como:

$$\left[ p : (x \in A) \quad y \quad q : (x \in B) \right] \quad (1)$$

Estas proposiciones así definidas tienen 4 posibilidades de veracidad para cualquier  $x \in U$

Vemos, que las operaciones se reducen a las siguientes analogías respecto de las tablas de verdad para conectores lógicos :

1. Complemento: Se corresponde con el **NOT**
2. Unión: La unión entre dos conjuntos se corresponde con el **OR**
3. Intersección : Se corresponde con un **AND**
4. Diferencia Simétrica: Se corresponde con un **XOR**
5. Inclusión : Se corresponde con la **implicación**
6. Igualdad: Se corresponde con un **si y solo si**.
7. Diferencia:  $A - B$  se obtiene de la definición  $A - B = A \cap B^c$

## 1.3. Producto Cartesiano

**Definición 1.3.1** (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:

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

## 2. Relaciones

**Definición 2.0.1** (Relación) Sean  $A, B$  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  $B$ .

Dados  $x \in A, y \in B$  y una relación  $\mathcal{R}$  de  $A$  en  $B$ , se dice que  $x$  está relacionado con  $y$  por la relación  $\mathcal{R}$ , lo cual lo notamos  $x\mathcal{R}y$  y esto se da si  $(x, y) \in \mathcal{R}$ . Caso contrario la notación es  $x\not\mathcal{R}y$ .

### 2.1. Relaciones en un conjunto

Las relaciones en un conjunto son relaciones de un conjunto en si mismo.

**Definición 2.1.1** (Relación en un conjunto)

Sea un conjunto  $A$ , se dice que  $\mathcal{R}$  es una relación en  $A$  si:  $\mathcal{R} \subseteq A \times A$

**Definición 2.1.2** (Reflexividad, simetría, antisimetría y transitividad) Sean un conjunto  $A$  y  $\mathcal{R}$  una relación en  $A$ , entonces:

- **Reflexividad:**  $\mathcal{R}$  se dice **reflexiva** si  $(x, x) \in \mathcal{R}, \forall x \in A$  (Es decir:  $x\mathcal{R}x, \forall x \in A$ ). En grafos es un bucle en el mismo elemento.
- **Simetría:**  $\mathcal{R}$  se dice **simétrica** si:  $\forall (x, y) \in A, x\mathcal{R}y \Rightarrow y\mathcal{R}x$ . Lo que es la doble flecha entre nodos en un grafo.
- **Antisimetría:**  $\mathcal{R}$  se dice **antisimétrica** si:  $\forall (x, y) \in A, x\mathcal{R}y$  e  $y\mathcal{R}x \Rightarrow x = y$
- **Transitividad:**  $\mathcal{R}$  se dice **transitiva** si:  $\forall x, y, z \in A, x\mathcal{R}y$  e  $y\mathcal{R}z \Rightarrow x\mathcal{R}z$

**Definición 2.1.3** (Relación de equivalencia y de orden) Sea  $A$  un conjunto y  $\mathcal{R}$  una relación en  $A$ .

- **Relación de equivalencia:** Cuando la relación cumple con ser reflexiva, simétrica y transitiva.
- **Relación de orden:** Cuando la relación cumple con ser reflexiva, antisimétrica y transitiva.

**Definición 2.1.4** (Clase de equivalencia (definición informal))

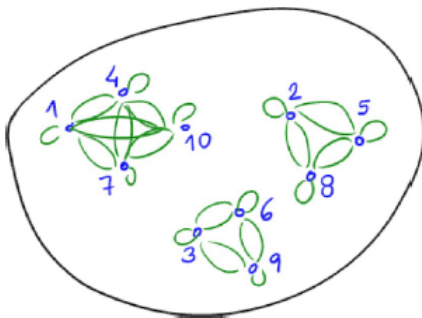
La clase de equivalencia de  $x \in A$  es el subconjunto de  $A$  formado por todos los elementos  $y$  de  $A$  relacionados con  $x$ ,  $y$  se nota  $\overline{x}$

### Ejemplo de Clase de equivalencia:

Dado un conjunto  $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ , se puede definir la relación de equivalencia " $\sim$ " talque  $x$  está relacionado con  $y$  ( $x \sim y$ ) si y solo si al dividir  $x$  e  $y$  por 3 resultan tener ambos elementos el mismo resto.

Entonces, podemos ver que:

Si dividimos a  $x = 1$  por 3 y  $y = 4$  por 3 se obtiene que ambos tienen resto 1, por lo tanto  $1 \sim 4$ . También que  $3 \sim 6$  y que  $6 \sim 9$  y por propiedad transitiva, como es una relación de equivalencia  $3 \sim 9$ , lo cual es cierto ya que todos son múltiplos de 3. Esto nos permite "separar" los números que están relacionados unos con los otros de los que no según la misma relación de equivalencia como sigue:



En la figura se ve claramente que:

$$\overline{1} = \overline{4} = \overline{7} = \overline{10} = \{1, 4, 7, 10\}$$

$$\overline{2} = \overline{5} = \overline{8} = \{2, 5, 8\}$$

$$\overline{3} = \overline{6} = \overline{9} = \{3, 6, 9\}$$

Esto nos da que un conjunto de clases de equivalencia:

$$\{\overline{1}, \overline{2}, \overline{3}\}$$

Siendo estos conjuntos **Disjuntos dos a dos** o **Disjuntos por pares**. Por lo que, lo que se hizo fue dividir el conjunto  $A$  en tres subconjuntos disjuntos entre sí cuya unión de dichos conjuntos nos da  $A$ .

**Definición 2.1.5** (Definición formal de Clase de Equivalencia) Sean  $A$  un conjunto y  $\sim$  una Relación de equivalencia en  $A$ . Para cada  $x \in A$ , la clase de equivalencia de  $x$  es el conjunto:

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

**Proposición 2.1.1** (Propiedad Fundamental de las clases de equivalencia) Sean  $A$  un conjunto y  $\sim$  una Relación de equivalencia en  $A$ . Sean  $x, y \in A$ , entonces o bien  $\bar{x} \cap \bar{y}$ , o bien  $\bar{x} = \bar{y}$

**Proposición 2.1.2** (Relaciones de equivalencia y particiones) Sea  $A$  un conjunto. Hay una manera natural de asociarle a una relación de equivalencia en  $A$  una partición de  $A$ . Recíprocamente, a toda partición se le puede asociar una relación de equivalencia y estas asociaciones son inversas una de la otra.

### 3. Funciones

#### 3.1. ¿Que es una función?

**Definición 3.1.1** (Función) Sean  $A$  y  $B$  conjuntos, y sea  $\mathcal{R}$  una relación de  $A$  en  $B$ . Se dice que  $\mathcal{R}$  es una función cuando todo elemento  $x \in A$  esta relacionado con algún  $y \in B$ , y este elemento  $y$  es único. Es decir:

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

**Observación 3.1.1** Los elementos del conjunto  $A$  (el dominio) deben estar todos relacionados con un elemento del conjunto  $B$  (denominado codominio). Además, si un mismo elemento del conjunto  $A$  apunta a dos elementos diferentes del conjunto  $B$ , entonces esta relación no es función.

Por otro lado, el primer problema puede solucionarse **restringiendo el dominio**.

**Definición 3.1.2** (Igualdad de Funciones) Sean  $f, g : A \rightarrow B$  funciones. Se tiene:

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

**Definición 3.1.3** (Imagen) Sea  $f : A \rightarrow B$  función. La **imagen** de  $f$ , que se nota  $Im(f)$ , es el subconjunto de elementos de  $B$  que estan relacionados con algún elemento de  $A$ . Es decir:

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

#### 3.2. Funciones inyectivas, sobreyectivas y biyectivas

**Definición 3.2.1** (Funciones Inyectivas, sobreyectivas y biyectivas) Sea  $f : A \rightarrow B$  una función. Se dice que:

- $f$  es **inyectiva** si para todo elemento  $y \in B$  existe a lo sumo un elemneto  $x \in A$  para el cual  $f(x) = y$ . Dicho de otra forma,  $f$  es inyectiva si para todo  $x, x' \in A$  tales que  $f(x) = f(x')$  se tiene que  $x = x'$ .
- $f$  es **sobreyectiva** si para todo elemento  $y \in B$  existe al menos un elemento  $x \in A$  para el cual  $f(x) = y$ . Dicho de otra manera,  $f$  es sobreyectiva si  $Im(f) = B$ .
- $f$  es **biyectiva** si es a la vez inyectiva y sobreyectiva, es decir para todo elemento  $y \in B$  existe exactamente un elemento  $x \in A$  para el cual  $f(x) = y$ .

**Definición 3.2.2** (Composición de funciones) Sean  $A, B, C$  conjuntos, y  $f : A \rightarrow B, g : B \rightarrow C$  funciones. Entonces la composición de  $f$  con  $g$ , que se nota  $g \circ f$ , definida por

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

**Definición 3.2.3** (Función inversa) Sea  $f : A \rightarrow B$  biyectiva, entonces  $f^{-1} : B \rightarrow A$  se llama **función inversa** y es una función que satisface que  $\forall y \in B f^{-1}(y) = x \Leftrightarrow f(x) = y$

**Proposición 3.2.1** (Biyectividad y Función inversa) Sea  $f : A \rightarrow B$  una función:

- Si  $f$  es biyectiva, entonces  $f^{-1} \circ f = id_A$  y  $f \circ f^{-1} = id_B$
- Si existe una función  $g : B \rightarrow A$  tal que  $g \circ f = id_A$  y  $f \circ g = id_B$  Entonces  $f$  es biyectiva y  $f^{-1} = g$



## 4. Números Naturales

### 4.1. ¿Qué son los números naturales ( $\mathbb{N}$ )?

Los naturales son, informalmente el conjunto:

$$\mathbb{N} = \{1, 2, 3, \dots, 1001, 1002, \dots\}$$

En este conjunto se puede sumar y multiplicar (No existen los números negativos):

$$\text{si } m, n \in \mathbb{N} \Rightarrow m + n \in \mathbb{N} \wedge m \cdot n \in \mathbb{N}$$

Propiedades que se satisfacen en este conjunto de números son:

- Conmutatividad:  $m + n = n + m$  y  $m \cdot n = n \cdot m \forall m, n \in \mathbb{N}$
- Asociatividad:
- Distributividad del producto sobre la suma:

### 4.2. La suma de Gauss y la serie Geométrica

#### 4.2.1. La suma de Gauss

Supongamos que queremos sumar una cierta cantidad  $n$  de números, de manera que:

$$r = 1 + 2 + 3 + 4 + \dots + n$$

Este procedimiento se puede generalizar como sigue:

$$\forall n \in \mathbb{N} : 1 + 2 + 3 + \dots + (n - 1) + n = \frac{n(n + 1)}{2}$$

Notar que este siempre será un número natural y que  $n(n + 1)$  siempre es un número **par**.

#### 4.2.2. La serie Geométrica

Sea un número  $q$  cualquiera, queremos sumar las  $n + 1$  primeras potencias de  $q$ :

$$1 + q + q^2 + \dots + q^{n-1} + q^n$$

Esto resulta en:

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

## 4.3. Sumatoria

**Definición 4.3.1** (Sumatoria) 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  $a_i$** , la cual representa la suma de los primeros  $n$  términos de la sucesión  $(a_i)_{i \in \mathbb{N}}$ :

$$\sum_{i=1}^n a_i = a_1 + \dots + a_n$$

La cual por recurrencia se define de la siguiente forma:

$$\sum_{i=1}^1 a_i = a_1 \quad \text{y} \quad \sum_{i=1}^{n+1} a_i = a_i + a_{n+1}, \forall n \in \mathbb{N}$$

**Propiedad 4.3.1** (Propiedades de sumatorias)

- $\left( \sum_{i=1}^n a_i \right) + \left( \sum_{i=1}^n b_i \right) = \sum_{i=1}^n (a_i + b_i)$
- $c \cdot \sum_{i=1}^n a_i = \sum_{i=1}^n c \cdot a_i$

## 4.4. Productoria

**Definición 4.4.1** 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  $(a_i)_{i \in \mathbb{N}}$ :

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

Siendo por recursión:

$$\prod_{i=1}^1 a_i = a_1 \text{ y } \prod_{i=1}^{n+1} a_i = \left( \prod_{i=1}^n a_i \right) \cdot a_{n+1}, \forall n \in \mathbb{N}$$

**Propiedad 4.4.1** (Propiedad de la productoria)

$$\left( \prod_{i=1}^n a_i \right) \cdot \left( \prod_{i=1}^n b_i \right) = \prod_{i=1}^n (a_i \cdot b_i)$$

## 4.5. El conjunto inductivo $\mathbb{N}$ y el principio de inducción

**Definición 4.5.1** (Conjunto Inductivo) Sea  $H \subseteq \mathbb{R}$  un conjunto. Se dice que  $H$  es un conjunto inductivo si se cumplen las dos condiciones siguientes:

- $1 \in H$
- $\forall x, x \in H \Rightarrow x + 1 \in H$

**Teorema 4.5.1** (Principio de Inducción)

Sea  $p(n)$ ,  $n \in \mathbb{N}$ , una afirmación sobre los números naturales. Si  $p$  satisface

- Caso Base:  $p(1)$  es verdadera
- Paso Inductivo:  $\forall h \in \mathbb{N}, p(h) \text{ Verdadera} \Rightarrow p(h+1) \text{ Verdadera}$

Entonces,  $p(n)$  es Verdadero,  $\forall n \in \mathbb{N}$  ( $h := \text{Hipotesis} \Rightarrow p(h) := \text{Hipotesis Inductiva (HI)}$ )

**Teorema 4.5.2** (Principio de Inducción Corrido) Sea  $n_0 \in \mathbb{Z}$  y sea  $p(n)$ ,  $n \leq n_0$ , una afirmación sobre  $\mathbb{Z}_{n_0}$ . Si  $p$  satisface :

- Caso Base:  $p(n_0)$  es Verdadera
- Paso Inductivo:  $\forall h \leq n_0, p(h) \text{ Es Verdadera} \Rightarrow p(h+1) \text{ es Verdadera}$  y entonces  $p(n)$  es Verdadera  $\forall n \in \mathbb{N}$

## 4.6. Inducción Completa

**Teorema 4.6.1** (Princiío de inducción - II)

Sea  $p(n)$ ,  $n \in \mathbb{N}$ , una afirmación sobre los números naturales. Si  $p$  satisface

- Caso Base:  $p(1)$  y  $p(2)$  son Verdaderas
- Paso Inductivo:  $\forall h \in \mathbb{N}, p(h) \text{ y } p(h+1) \text{ Verdaderas} \Rightarrow p(h+2) \text{ Verdadera}$

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

**Teorema 4.6.2** (Princiío de inducción - II corrido)

Sea  $n_0 \in \mathbb{Z}$  y sea  $p(n)$   $n \leq n_0$ , una afirmación sobre los  $\mathbb{Z}_{\leq n_0}$ . Si  $p$  satisface:

- i Base:  $p(n_0)$  y  $p(n_0+1)$  son Verdaderas
- Paso Inductivo:  $\forall h \leq n_0, p(h) \text{ y } p(h+1) \text{ Verdaderas} \Rightarrow p(h+2) \text{ Verdadera}$

entonces,  $p(n)$  es verdadera,  $\forall n \in \mathbb{Z}_{\leq n_0}$

## 4.7. Sucesión de Fibonacci

Fibonacci presento el siguiente problema: Imaginemos que colocamos una pareja de conejos bebés en un área cerrada ¿Cuántos conejos habra despues de  $n$  meses si:

1. Los conejos nunca mueren.
2. Cada pareja de conejos produce una nueva pareja de conejos cada mes
3. Comienzan a tener parejitas luego de dos meses de nacida

Dadas estas condiciones se obtiene la sucesión de Fibonacci  $(F_n)_{n \in \mathbb{N}_0}$ :

$$F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n, \forall n \in \mathbb{N}_0$$

**Proposición 4.7.1** (Termino General de la Sucesión de Fibonacci)

$$F_n = \frac{1}{\sqrt{5}}(\phi^n - \bar{\phi}^n)$$

Donde:

$$\phi = \frac{1 + \sqrt{5}}{2} \simeq 1,61803 \quad \wedge \quad \bar{\phi} = \frac{1 - \sqrt{5}}{2} < 0$$

## 4.8. Sucesión de Lucas

Una sucesión de Lucas es una sucesión  $(a_n)_{n \in \mathbb{N}_0}$  definida recursivamente por:

$$a_0 = a, a_1 = b, a_{n+2} = ca_{n+1} + da_n, \forall n \in \mathbb{N}_0$$

Con  $a, b, c, d, \in \mathbb{C}$

Si consideramos la ecuación  $X^2 - cX - d = 0$  asociada a la sucesión  $(a_n)_{n \in \mathbb{N}_0}$ . Suponiendo que esta tiene dos raíces, tales que:

$$r^2 = cr + d \text{ y } \bar{r}^2 = c\bar{r} + d$$

Se dan las siguientes afirmaciones:

1. Las sucesiones  $(r^n)_{n \in \mathbb{N}_0}$ ,  $(\bar{r}^n)_{n \in \mathbb{N}_0}$  y cualquier combinación de la forma:

$$(\lambda_n)_{n \in \mathbb{N}_0} = (\alpha r^n + \beta \bar{r}^n)_{n \in \mathbb{N}_0}$$

Satisfacen la misma recurrencia que la sucesión de Lucas  $(a_n)_{n \in \mathbb{N}_0}$  siendo la recurrencia la siguiente:

$$\lambda_{n+2} = c\lambda_{n+1} + d\lambda_n, \forall n \in \mathbb{N}$$

2.  $\exists! (\lambda_n)_{n \in \mathbb{N}_0} = (\alpha r^n + \beta \bar{r}^n)_{n \in \mathbb{N}_0}$  que satisface las **condiciones iniciales**  $\lambda_0 = a, \lambda_1 = b$

Resultado del cual sale de resolver:

$$\begin{cases} \alpha + \beta = a & \Rightarrow \alpha = \frac{b - a\bar{r}}{r - \bar{r}} \\ \alpha r + \beta \bar{r} = b & \Rightarrow \beta = \frac{ar - b}{r - \bar{r}} \end{cases}$$

Concluyendo que  $(a_n)_{n \in \mathbb{N}_0} = (\lambda_n)_{n \in \mathbb{N}_0} = (\alpha r^n + \beta \bar{r}^n)_{n \in \mathbb{N}_0}$

3. Dada la ecuación asociada  $X^2 - cX - d = 0$  con solo una raíz ( $X^2 - cX - d = (X - r)^2$ ). En este caso, las sucesiones  $(r^n)_{n \in \mathbb{N}_0}$  y  $(nr^{n-1})_{n \in \mathbb{N}_0}$  satisfacen la misma recurrencia y tambien cualquier combinación lineal con **las condiciones iniciales**  $\lambda_0 = a, \lambda_1 = b$ , se tiene que el termino general para  $a_n$  cuando  $r \neq 0$ , es:

$$a_n = ar^n + (b - ar)nr^{n-1}, \forall n \in \mathbb{N}_0$$

## 4.9. Inducción Completa

**Teorema 4.9.1** (Principio de Inducción Completa) Sea  $p(n), n \in \mathbb{N}$  una afirmación en los numeros naturales. Si  $p$  satisface:

- Caso Base:  $p(1)$  es Verdadera
- Paso Inductivo:  $\forall h \in \mathbb{N}, p(1) \cdots p(h)$  es Verdadera  $\Rightarrow p(h+1)$  es verdadera

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

## 5. Combinatoria

### 5.1. Cardinal

#### Definición 5.1.1 (Cardinal)

Dado el conjunto  $A$ , el cardinal de  $A$  ( $\#A$ ) a la cantidad de elementos distintos que tiene  $A$ .

#### Observación 5.1.1 (Cardinal de un Subconjunto)

Sea  $A$  un conjunto finito y  $B \subseteq A$ , entonces  $\#B \leq \#A$

#### Propiedad 5.1.1 (Cardinales de Union, Interseccion, Complemento y otros)

1.  $A \wedge B$  conjuntos disjuntos (sin ningun elemento en comun), entonces:  $\#(A \cup B) = \#A + \#B$
2. Si  $A \wedge B$  no son disjuntos (tienen al menos un elemento en comun), entonces:  $\#(A \cup B) = \#A + \#B - \#(A \cap B)$
3. Si  $U$  es un conjunto finito, entonces:  $\#(A^c) = \#U - \#A$
4.  $\#(A - B) = \#A - \#(A \cap B)$
5.  $\#(A \triangle B) = \#A + \#B - 2\#(A \cap B)$
6.  $\#(A \times B) = \#A \cdot \#B$
7.  $\#(\mathcal{P}(A)) = 2^{\#A}$
8.  $\#(A^n) = (\#A)^n$

### 5.2. Cantidad de relaciones y funciones

#### Propiedad 5.2.1 (Cantidad de Relaciones)

Sean  $A_m$  y  $B_n$  conjuntos finitos, con  $m$  y  $n$  elementos respectivamente. Entonces, la cantidad de relaciones que hay de  $A_m$  en  $B_n$  es igual a  $2^{mn}$

#### Propiedad 5.2.2 (Cantidad de Funciones)

Sean  $A_m$  y  $B_n$  conjuntos finitos, con  $m$  y  $n$  elementos respectivamente. Entonces, la cantidad de funciones que hay de  $A_m$  en  $B_n$  ( $\#(f : A \rightarrow B)$ ) es igual a  $n^m$ .

#### Propiedad 5.2.3 (Cardinal de Conjuntos y Funciones)

Sean  $A$  y  $B$  Conjuntos finitos:

- $f : A \rightarrow B$  inyectiva  $\Rightarrow \#A \leq \#B$
- $f : A \rightarrow B$  sobreyectiva  $\Rightarrow \#A \geq \#B$
- $f : A \rightarrow B$  biyectiva  $\Rightarrow \#A = \#B$

#### Definición 5.2.1 (Cantidad de Funciones Inyectivas)

Sean  $A_m$  y  $B_n$  conjuntos finitos, con  $m$  y  $n$  elementos respectivamente, donde  $m \leq n$ . Entonces, la cantidad de funciones inyectivas de  $f : A_m \rightarrow B_n$  que hay son:

$$n \cdot (n - 1) \cdots (n - m + 1) = \frac{n!}{(n - m)!}$$

#### Definición 5.2.2 (Cantidad de Biyecciones (Permutaciones))

Sea  $n \in \mathbb{N}$ . La cantidad de funciones biyectivas que hay entre dos conjuntos de  $n$  elementos o cantidad de permutaciones esta dado por el factorial de los  $n$  elementos de los conjuntos:

$$\#(f : A_n \rightarrow B_n) = n! = n \cdot (n - 1) \cdots 2 \cdot 1 = \prod_{i=1}^n i$$

Definicion por recurrencia del factorial:

$$0! = 1 \quad \wedge \quad n! = n \cdot (n - 1)!, \quad \forall n \in \mathbb{N}$$

**Teorema 5.2.1** (Numero Combinatorio)

Sean  $n \in \mathbb{N}$  y sea  $A_n$  un conjunto de  $n$  elementos. Para  $0 \leq k \leq n$ , la cantidad de subconjuntos con  $k$  elementos del conjunto  $A_n$

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

(Formas de elegir  $k$  elementos de un conjunto de  $n$ )

**Observación 5.2.1** (Recordar)

- $\binom{n}{0} = \binom{n}{n} = 1$
- $\binom{n}{1} = \binom{n}{n-1} = n$
- $\binom{n}{k} = \binom{n}{n-k}$
- $2^n = \sum_{k=0}^n \binom{n}{k}$

**Teorema 5.2.2** (Binomio de Newton)

$$(x - y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}, \quad \forall n \in \mathbb{N}_0$$

## 6. Enteros

### 6.1. Divisibilidad

**Definición 6.1.1** Divisibilidad Sean  $a, d \in \mathbb{Z}$  con  $d \neq 0$ . Se dice que  $d$  divide a  $a$  y se nota  $d|a$  si se cumple:

$$d|a \Leftrightarrow \exists k \in \mathbb{Z} : a = k \cdot d$$

**Propiedad 6.1.1** De la divisibilidad

- (i)  $d \neq 0 \Rightarrow d|0$ , pues  $k = 0$  cumple  $0 = k \cdot d$
- (ii)  $d|a \Leftrightarrow -d|a$ . Se concluye  $d|a \Leftrightarrow |d| \mid |a|$
- (iii)  $a \neq 0, d|a \Rightarrow |d| \leq |a|$
- (iv) Los únicos inversibles en  $\mathbb{Z}$  son el 1 y el  $-1$ .
- (v)  $d|a$  y  $a|d \Leftrightarrow a = \pm d$
- (vi)  $d|a$  y  $d|b \Rightarrow d|a + b$  (no vale la vuelta)
- (vii)  $d|a$  y  $d|b \Rightarrow d|a - b$  (no vale la vuelta)
- (viii)  $d|a, c \in \mathbb{Z} \Rightarrow d|c \cdot b$
- (ix)  $d|a \Rightarrow d^n | a^n, \forall n \in \mathbb{N}$
- (x)  $d|a \cdot b \not\Rightarrow d|a$  y  $d|b$  (esto solo se cumplirá cuando  $d$  es primo)

**Definición 6.1.2** Primos y Compuestos Se dice que  $a \in \mathbb{Z}$  es un número primo si  $a \neq 0, \pm 1$  y tiene únicamente 4 divisores ( $\pm 1, \pm a$ ).

Luego, se dice compuesto cuando no es primo

## 6.2. Congruencia

**Definición 6.2.1** Congruencia Sea  $d \in \mathbb{Z}$ ,  $d \neq 0$ . Dados  $a, b \in \mathbb{Z}$ , se dice que  $a$  es congruente a  $b$  modulo  $d$  si se tiene que  $d \mid a - b$

$$a \equiv b \pmod{d} \Leftrightarrow d \mid a - b$$

**Proposición 6.2.1** La congruencia es una relación de equivalencia Sea  $d \in \mathbb{Z}$ ,  $d \neq 0$ . Sea  $\mathcal{R}$  la relación en  $\mathbb{Z}$  dada por:

$$a \mathcal{R} b \Leftrightarrow a \equiv b \pmod{d}, \quad \forall a, b \in \mathbb{Z}$$

Entonces  $\mathcal{R}$  es relación de equivalencia.

**Propiedad 6.2.1** De la congruencia Sea  $d \in \mathbb{Z}$ ,  $d \neq 0$ . Entonces:

$$1. \quad \forall a_1, a_2, b_1, b_2 \in \mathbb{Z}$$

$$a_1 \equiv b_1 \pmod{d} \text{ y } a_2 \equiv b_2 \pmod{d} \Rightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod{d}$$

$$2. \quad \forall a, b, c \in \mathbb{Z}$$

$$a \equiv b \pmod{d} \Rightarrow ca \equiv cb \pmod{d}$$

$$3. \quad \forall a_1, a_2, b_1, b_2 \in \mathbb{Z}$$

$$a_1 \equiv b_1 \pmod{d} \text{ y } a_2 \equiv b_2 \pmod{d} \Rightarrow a_1 a_2 \equiv b_1 b_2 \pmod{d}$$

$$4. \quad \forall a, b \in \mathbb{Z} \text{ y } n \in \text{natural}$$

$$a \equiv b \pmod{d} \Rightarrow a^n \equiv b^n \pmod{d}$$

## 6.3. Algoritmo de División

**Teorema 6.3.1** Algoritmo de División Dados,  $a, d \in \mathbb{Z}$  con  $d \neq 0$ ,  $k, r \in \mathbb{Z}$  que satisfacen:

$$a = k \cdot d + r \text{ con } 0 \leq r < d$$

A  $k$  se le da el nombre de conciente y a  $r$  el nombre de resto.

**Observación 6.3.1** Si  $0 \leq a < |d|$ , entonces  $a = 0 \cdot d + a$  implica que  $k = 0$  y el resto  $r = r_d(a) = a$ , pues  $a$  cumple la condición que tiene que cumplir el resto (se aplica la unicidad del cociente y el resto).

**Observación 6.3.2** Divisibilidad y Resto Sean  $a, d \in \text{entero}$ ,  $d \neq 0$ . Entonces:

$$r_d(a) = 0 \Leftrightarrow d \mid a \Leftrightarrow a \equiv 0 \pmod{d}$$

**Propiedad 6.3.1** Congruencia y Resto Sea  $d \in \text{entero}$ ,  $d \neq 0$ . Entonces:

$$(\alpha) \quad a \equiv r_d(a) \pmod{d}, \quad \forall a \in \mathbb{Z}$$

$$(\beta) \quad a \equiv r \pmod{d} \text{ con } 0 \leq r < d, \text{ entonces } r = r_d(a)$$

$$(\gamma) \quad r_1 \equiv r_2 \pmod{d} \text{ con } 0 \leq r_1, r_2 < d, \text{ entonces } r_1 = r_2$$

$$(\delta) \quad a \equiv b \pmod{d} \Leftrightarrow r_d(a) = r_d(b)$$

**Corolario 6.3.1** Tablas de Restos Sean  $a, b, d \in \mathbb{Z}$ ,  $d \neq 0$ . Entonces:

- $r_d(a + b) = r_d(r_d(a) + r_d(b))$
- $r_d(a \cdot b) = r_d(r_d(a) \cdot r_d(b))$
- $r_d(a^n) = r_d(r_d(a)^n)$

## 6.4. Maximo Comun Divisor

**Definición 6.4.1** *Maximo Común Divisor Sean  $a, b \in \mathbb{Z}$ , no ambos nulos. El **maximo comun divisor (mcd)** entre  $a$  y  $b$ , se nota  $(a : b)$ , es el mayor de los divisores comunes de  $a$  y  $b$ . Es decir:*

$$(a : b) | a, (a : b) | b \text{ y si } d | a \text{ y } d | b \Rightarrow d \leq (a : b)$$

**Proposición 6.4.1** *Sean  $a, b \in \mathbb{Z}$  no ambos nulos, y sea  $k \in \mathbb{Z}$ , entonces:*

$$\text{DivCom}(\{a, b\}) = \text{DivCom}(\{b, a - k \cdot b\})$$

$$\text{DivCom}_+(\{a, b\}) = \text{DivCom}(\{b, a - k \cdot b\})$$

*En particular,  $\forall k \in \mathbb{Z}$ ,  $(a : b) = (b, a - k \cdot b)$*

*Aplicando esto a  $r_b(a) = a - k \cdot b$ , se obtiene que  $(a : b) = (b, r_b(a))$*

**Teorema 6.4.1** *Algoritmo de Euclides Sean  $a, b \in \mathbb{Z}$  no ambos nulos. Existe  $l \in \mathbb{N}$  tal que en una sucesión finita de  $l + 1$  divisiones:*

$$\begin{aligned} a &= k_1 \cdot b + r_1 & \text{con } 0 \leq r_1 < |b| \\ b &= k_2 \cdot r_1 + r_2 & \text{con } 0 \leq r_2 < r_1 \\ r_1 &= k_3 \cdot r_2 + r_3 & \text{con } 0 \leq r_3 < r_2 \\ &\vdots \\ r_{l-2} &= k_l \cdot r_{l-1} + r_l & \text{con } 0 \leq r_l < r_{l-1} \\ r_{l-1} &= k_{l+1} \cdot r_l + r_{l+1} & \text{con } 0 \leq r_{l+1} < r_l \end{aligned}$$

*Se llega por primera vez al resto nulo  $r_{l+1}$ . Entonces  $(a : b) = r_l$ , el ultimo resto no nulo.*

**Observación 6.4.1** *Si  $a, b \in \mathbb{Z}$  son tales que  $a = 0$  y  $b \neq 0$ , ya sabemos que  $(a : b) = |b|$ . Por lo tanto, el Algoritmo de Euclides permite calcular el mcd de cualquier par de  $\mathbb{Z}$  no ambos nulos.*

**Teorema 6.4.2** *MCD y Combinación Entera Sean  $a, b \in \mathbb{Z}$ , no ambos nulos. Entonces existen  $s, t \in \mathbb{Z}$  tales que:*

$$(a : b) = s \cdot a + t \cdot b$$

**Observación 6.4.2** *Combinaciones enteras de  $a$  y  $b$  Si  $a, b \in \mathbb{Z}$  no ambos nulos, y  $c \in \mathbb{Z}$ .*

$$c = s' \cdot a + t' \cdot b \text{ para } s', t' \in \mathbb{Z} \Leftrightarrow (a : b) = c$$

**Proposición 6.4.2** *MCD y Divisores Comunes Si  $a, b \in \mathbb{Z}$  no ambos nulos, y sea  $d \in \mathbb{Z}$ , con  $d \neq 0$ . Entonces*

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

**Proposición 6.4.3** *MCD de múltiplo comun de dos números Si  $a, b \in \mathbb{Z}$  no ambos nulos, y sea  $k \in \mathbb{Z} \setminus \{0\}$ . Entonces:*

$$(k \cdot a : k \cdot b) = |k|(a : b)$$

**Teorema 6.4.3** *Equivalencias del mcd Si  $a, b \in \mathbb{Z}$  no ambos nulos, y sea  $d \in \mathbb{N}$ . Son equivalentes:*

1.  $d | a, d | b$  y si  $c | a$  y  $c | b$ , entonces  $c \leq d$
2.  $d | a, d | b$  y existen  $s, t \in \mathbb{Z}$  tales que  $d = sa + tb$
3.  $d | a, d | b$  y si  $c | b$ , entonces  $c | d$

*Un numero  $d \in \mathbb{N}$  que cumple cualquiera de esas 3 propiedades es el máximo comun divisor  $(a : b)$ .*

## 6.5. Números Coprimos

**Definición 6.5.1** *Números Coprimos* Se dice que  $a, b \in \mathbb{Z}$  no ambos nulos son coprimos, si y solo si  $(a : b) = 1$ . Es decir, si y solo si los únicos divisores comunes de  $a$  y  $b$  son  $\pm 1$ .

**Observación 6.5.1** *Coprimos y Combinación Entera* Sean  $a, b \in \mathbb{Z}$  no ambos nulos. Entonces

$$(a : b) = 1 \Leftrightarrow \exists s, t \in \mathbb{Z} : 1 = sa + tb$$

**Propiedad 6.5.1** *Escenciales de divisibilidad con coprimidad* Sean  $a, b, c, d \in \mathbb{Z}$  con  $c \neq 0$  y  $d \neq 0$ . Entonces

$$1. \ c \mid a, d \mid a \text{ y } (c : d) = 1 \Rightarrow cd \mid a$$

$$2. \ d \mid ab \text{ y } (d : a) = 1 \Rightarrow d \mid b$$

**Proposición 6.5.1** *Coprimizando* Sean  $a, b \in \mathbb{Z}$  no ambos nulos. Entonces:

$$\left( \frac{a}{(a : b)} : \frac{b}{(a : b)} \right) = 1$$

Por lo tanto

$$a = (a : b)a' \quad b = (a : b)b'$$

Donde los números  $a' = \frac{a}{(a:b)}$  y  $b' = \frac{b}{(a:b)}$  son coprimos.

## 6.6. Primos y Factorización

**Proposición 6.6.1** *Todo número entero distinto de 0 y 1 es divisible por algún primo* Sea  $a \in \mathbb{Z}$ ,  $a \neq 0, \pm 1$ . Entonces, existe un número primo positivo  $p$ , tal que  $p \mid a$

**Corolario 6.6.1** *Cantidad de Primos* Existen infinitos primos positivos distintos.

**Teorema 6.6.1** *Propiedad Funcamental de los números primos* Sea  $p$  un primo y sean  $a, b \in \mathbb{Z}$ . Entonces:

$$p \mid a \cdot b \Rightarrow p \mid a \text{ o } p \mid b$$

**Proposición 6.6.2** *Sea  $p$  un número primo y sean  $a_1, \dots, a_n \in \mathbb{Z}$ , con  $n \geq 2$ . Entonces:*

$$p \mid a_1 \cdots a_n \Rightarrow p \mid a_i \text{ para algún } i, \quad 1 \leq i \leq n$$

En particular, dado  $a \in \mathbb{Z}$ , si  $p \mid a^n$  entonces  $p \mid a$

**Teorema 6.6.2** *Teorema fundamental de la Aritmetica* Sea  $a \in \mathbb{Z}$ ,  $a \neq 0, \pm 1$ . Entonces  $a$  se escribe en forma única como producto de primos positivos (factorización única), es decir:

$$a = \pm p_1^{m_1} \cdot \pm p_2^{m_2} \cdots \pm p_r^{m_r}$$

Esta escritura es única salvo permutación de primos.

**Observación 6.6.1** *Primos de productos y potencias* Sean  $a, b \in \mathbb{Z}$  no nulos de la forma

$$a = \pm p_1^{m_1} \cdot \pm p_2^{m_2} \cdots \pm p_r^{m_r}, \text{ con } m_i \in \mathbb{N}_0 \quad b = \pm p_1^{n_1} \cdot \pm p_2^{n_2} \cdots \pm p_r^{n_r}, \text{ con } n_i \in \mathbb{N}_0$$

Entonces:

$$\blacksquare \quad a \cdot b = (\pm p_1^{m_1} \cdots \pm p_r^{m_r}) \cdot (\pm p_1^{n_1} \cdots \pm p_r^{n_r}) = \pm p_1^{m_1+n_1} \cdots \pm p_r^{m_r+n_r}$$

Es decir,  $a \cdot b$  tiene exactamente los primos de  $a$  y  $b$  en su factorización y los exponentes se suman.

$$\blacksquare \quad a^n = (\pm p_1^{m_1} \cdots \pm p_r^{m_r})^n = (\pm 1)^n \cdot \pm p_1^{m_1 n} \cdots \pm p_r^{m_r n}$$

Es decir,  $a^n$  tiene exactamente los mismos primos que  $a$  en su factorización y los exponentes van multiplicados por  $n$ .

**Proposición 6.6.3** *Divisores de un número y cantidad* Sea  $a \in \mathbb{Z}$ ,  $a \neq 0 \pm 1$ , y sea  $a = \pm p_1^{m_1} \cdots p_r^{m_r}$  la factorización en primos de  $a$ . Entonces

$$1. \ d \mid a \Leftrightarrow d = \pm p_1^{n_1} \cdots p_r^{n_r} \text{ con } 0 \leq n_i \leq m_i$$



2.  $\#Div_+(a) = (m_1 + 1) \cdots (m_r + 1)$  y  $\#Div(a) = 2(m_1 + 1) \cdots (m_r + 1)$

**Proposición 6.6.4** *Divisores y Potencias Sean  $a, d \in \mathbb{Z}$  con  $d$  no nulo, y sea  $n \in \mathbb{N}$ . Entonces:*

$$d \mid a \Leftrightarrow d^n \mid a^n$$

**Proposición 6.6.5** *MCD y factorización Sean  $a, b \in \mathbb{Z}$  no nulos de la forma:*

$$a = \pm p_1^{m_1} \cdot \pm p_2^{m_2} \cdots \pm p_r^{m_r}, \text{ con } m_i \in \mathbb{N}_0 \quad b = \pm p_1^{n_1} \cdot \pm p_2^{n_2} \cdots \pm p_r^{n_r}, \text{ con } n_i \in \mathbb{N}_0$$

Entonces

$$(a : b) = p_1^{\min\{m_1, n_1\}} \cdot p_2^{\min\{m_2, n_2\}} \cdots p_r^{\min\{m_r, n_r\}}$$

**Corolario 6.6.2** *MCD de potencias Sean  $a, b \in \mathbb{Z}$  no nulos.*

1. Sean  $a, b \neq 0, \pm 1$ , con su factorización en primos  $a = \pm p_1^{m_1} \cdots \pm p_r^{m_r}$ , con  $m_i \in \mathbb{N}_0$   $b = \pm q_1^{n_1} \cdots \pm q_s^{n_s}$ , con  $n_i \in \mathbb{N}_0$  entonces:

$$(a : b) = 1 \Leftrightarrow p_i \neq q_i, \forall i, j$$

2.  $(a : b) = 1, (a : c) = 1 \Leftrightarrow (a : bc) = 1$

3.  $(a : b) = 1 \Leftrightarrow (a^m : b^n) = 1, \forall m, n \in \mathbb{N}$

4.  $(a^n : b^n) = (a : b)^n, n \in \mathbb{N}$

**Definición 6.6.1** *mínimo común múltiplo Sean  $a, b \in \mathbb{Z}$  no nulos. El mínimo común múltiplo entre  $a$  y  $b$ , que se nota  $[a : b]$ , es el menor número natural que es un múltiplo común de  $a$  y de  $b$*

**Proposición 6.6.6** *mcm y factorización Sean  $a, b \in \mathbb{Z}$  no nulos de la forma*

$$a = \pm p_1^{m_1} \cdot \pm p_2^{m_2} \cdots \pm p_r^{m_r}, \text{ con } m_i \in \mathbb{N}_0 \quad b = \pm p_1^{n_1} \cdot \pm p_2^{n_2} \cdots \pm p_r^{n_r}, \text{ con } n_i \in \mathbb{N}_0$$

Entonces

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

**Corolario 6.6.3** *Mcm y múltiplos comunes Sean  $a, b \in \mathbb{Z}$ , no ambos nulos y sea  $m \in \mathbb{Z}$ , con  $m \neq 0$ . Entonces*

$$a \mid m \text{ y } b \mid m \Leftrightarrow [a : b] \mid m$$

**Proposición 6.6.7** *Producto mcd y mcm Sean  $a, b \in \mathbb{Z}$ , no nulos entonces  $|a \cdot b| = (a : b)[a : b]$*

En particular, si  $a$  y  $b$  son coprimos entonces  $[a : b] = |a \cdot b|$

## 6.7. Ecuaciones Lineales Diofánticas

**Proposición 6.7.1** *Ecuación diofántica y mcd Sean  $a, b, c \in \mathbb{Z}$  con  $a, b \neq 0$ . La ec. diofántica:*

$$aX + bY = c$$

admite soluciones enteras si y solo si  $(a : b) \mid c$ . Es decir:

$$\exists (x_0, y_0) \in \mathbb{Z}^2 : ax_0 + by_0 = c \Leftrightarrow (a : b) \mid c$$

**Corolario 6.7.1** *Ecuación diofántica con  $a$  y  $b$  Coprimos Sean  $a, b, c \in \mathbb{Z}$  con  $a, b \neq 0$ .  $(a : b) = 1$ . Entonces la ecuación diofántica*

$$aX + bY = c$$

tiene soluciones enteras  $\forall c \in \mathbb{Z}$

**Definición 6.7.1** *Ecuaciones Diofánticas Equivalentes Sean  $aX + bY = c$  y  $a'X + b'Y = c'$  dos ecuaciones diofánticas.*

Decimos que son equivalentes si tienen exactamente las mismas soluciones  $(x, y) \in \mathbb{Z}^2$ . En este caso adoptamos la notación:

$$aX + bY = c \Leftrightarrow a'X + b'Y = c'$$

**Observación 6.7.1** *Ec. Diofántica y ec. coprimizada Sean  $a, b, c \in \mathbb{Z}$  con  $a, b \neq 0$  tales que  $(a : b) \mid c$*

Definamos  $a' = \frac{a}{(a : b)}, b' = \frac{b}{(a : b)}, c' = \frac{c}{(a : b)}$ . Entonces

$$aX + bY = c \iff a'X + b'Y = c'$$

**Proposición 6.7.2** La ecuación diofántica nula (Homogenea) Sean  $a, b \in \mathbb{Z}$ , no nulos.  
El conjunto  $S_0$  de soluciones diofánticas  $aX + bY = 0$  es

$$S_0 = \{(x, y) \in \mathbb{Z}^2 : x = b'k, y = -a'k\} \text{ con } a' = \frac{a}{(a : b)}, \quad b' = \frac{b}{(a : b)}$$

**Teorema 6.7.1** La ecuación diofántica general Sean  $a, b, c \in \mathbb{Z}$  con  $a, b \neq 0$   
El conjunto  $S$  de soluciones enteras de la ecuación diofántica  $aX + bY = c$ , es:

- $S = \emptyset$  cuando  $(a : b) \nmid c$
- $S = \{(x, y) \in \mathbb{Z}^2 : x = x_0 + b'k, y = y_0 - a'k, k \in \mathbb{Z}\}$ , donde  $(x_0, y_0)$  es una solución particular cualquiera de la ecuación y  $a' = \frac{a}{(a : b)}, \quad b' = \frac{b}{(a : b)}$  cuando  $(a : b) \mid c$

## 6.8. Ecuaciones Lineales de Congruencia

**Definición 6.8.1** Ecuaciones de Congruencia equivalentes Sean  $aX \equiv c \pmod{m}$  y  $a'X \equiv c' \pmod{m'}$  dos ecuaciones de congruencia. Decimos que son equivalentes si tienen exactamente las mismas soluciones  $x \in \mathbb{Z}$ . en ese caso adoptamos la notación.

$$aX \equiv c \pmod{m} \iff a'X \equiv c' \pmod{m'}$$

Cabe notar que  $aX \equiv c \pmod{m}$  tiene al menos una solución  $x_0 \in \mathbb{Z} \Leftrightarrow$  la ec. diof  $aX - mY = c$  admite al menos una solución  $(x_0, y_0) \in \mathbb{Z}^2$  lo cual se da  $\Leftrightarrow (a : m) = (a : -m) = c$

**Proposición 6.8.1** Ec. de Congruencia, mcd y ecuación coprimizada Sea  $m \in \mathbb{N}$ . Dados  $a, c \in \mathbb{Z}$ , la ecuación de congruencia  $aX \equiv c \pmod{m}$  tiene soluciones enteras  $\Leftrightarrow (a : m) \mid c$

Si ese es el caso, sean  $a' = \frac{a}{(a : m)}, c' = \frac{c}{(a : m)}, m' = \frac{m}{(a : m)}$  Entonces

$$aX + bY = c \iff a'X + b'Y = c'$$

**Observación 6.8.1** Simplificando factores comunes en ecuaciones de congruencia-I Sean  $m' \in \mathbb{N}$  y  $a', c', d \in \mathbb{Z}$  no nulos. Entonces

$$\forall x \in \mathbb{Z}, (da')x \equiv dc' \pmod{dm'} \Leftrightarrow a'x \equiv c' \pmod{m'}$$

**Corolario 6.8.1** Ecuación de congruencia con  $a$  y  $m$  coprimos Sean  $m \in \mathbb{N}$  y  $a \in \mathbb{Z}$  tal que  $a$  y  $m$  son coprimos. Entonces, la ecuación de congruencia  $aX \equiv c \pmod{m}$  tiene soluciones enteras cualquiera sea  $c \in \mathbb{Z}$

**Teorema 6.8.1** La ecuación de Congruencia Sean  $m \in \mathbb{N}$  y sean  $a, c \in \mathbb{Z}$  con  $a \neq 0$   
El conjunto  $S$  de soluciones enteras de la ecuación de congruencia

$$aX \equiv c \pmod{m}$$

es

- $S = \emptyset$ , cuando  $(a : m) \nmid c$
- $S = \{x \in \mathbb{Z} : x \equiv x_0 \pmod{m'}\}$  donde  $x_0 \in \mathbb{Z}$  es una solución particular cualquiera de la ecuación  $aX \equiv c \pmod{m}$  o de la ecuación equivalente  $a'X \equiv c' \pmod{m'}$  donde  $a' = \frac{a}{(a : m)}, c' = \frac{c}{(a : m)}$  y  $m' = \frac{m}{(a : m)}$ , cuando  $(a : m) \mid c$ , ya que

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

Mas aún, existe una única solución  $x_0 \in \mathbb{Z}$  que satisface  $0 \leq x_0 < m'$

**Observación 6.8.2** Simplificando factores comunes en ec. de congruencia-II Sean  $m \in \mathbb{N}$  y  $a, c, d \in \mathbb{Z}$  con  $a, d$  no nulos. Si  $d$  y  $m$  son coprimos, entonces se tiene la siguiente equivalencia de ecuaciones de congruencia:

$$(da)X \equiv dc \pmod{m} \iff (a)X \equiv c \pmod{m}$$

## 6.9. Teorema Chino del Resto

### Proposición 6.9.1 Sistemas Equivalentes

1. Sean  $m_1, \dots, m_n \in \mathbb{N}$  coprimos dos a dos, es decir  $(m_i : m_j) = 1$  para todo  $i \neq j$ . Entonces,  $\forall c \in \mathbb{Z}$

$$\begin{cases} X \equiv c (m_1) \\ X \equiv c (m_2) \\ \vdots \\ X \equiv c (m_n) \end{cases} \iff X \equiv c (m_1 \cdot m_2 \cdot \dots \cdot m_n)$$

2. Sean  $m, m' \in \mathbb{N}$  tales que  $m' \mid m$ . Entonces,  $\forall c, c' \in \mathbb{Z}$

- Si  $c \not\equiv c' (m')$ ,  $\begin{cases} X \equiv c' (m') \\ X \equiv c (m) \end{cases}$  es incompatible.
- Si  $c \equiv c' (m')$ ,  $\begin{cases} X \equiv c' (m') \\ X \equiv c (m) \end{cases} \iff X \equiv c (m)$

**Teorema 6.9.1** Teorema Chino del Resto Sean  $m_1, \dots, m_n \in \mathbb{N}$  coprimos dos a dos, es decir  $(m_i : m_j) = 1$  para todo  $i \neq j$ . Entonces,  $\forall c_1, \dots, c_n \in \mathbb{Z}$ , el sistema de ecuaciones de congruencia

$$\begin{cases} X \equiv c_1 (m_1) \\ X \equiv c_2 (m_2) \\ \vdots \\ X \equiv c_n (m_n) \end{cases}$$

tiene soluciones enteras

Mas aún,

$$\begin{cases} X \equiv c (m_1) \\ X \equiv c (m_2) \\ \vdots \\ X \equiv c (m_n) \end{cases} \iff X \equiv x_0 (m_1 \cdot \dots \cdot m_n)$$

donde  $x_0 \in \mathbb{Z}$  es una solución particular cualquiera del sistema, y se tiene

$$S = \{x \in \mathbb{Z} : x \equiv x_0 (x_0 m_1 \cdot \dots \cdot m_n)\}$$

En particular, existe una única solución  $x_0 \in \mathbb{Z}$  que satisface  $0 \leq x_0 < m_1 \cdot \dots \cdot m_n$

## 6.10. Pequeño Teorema de Fermat

**Teorema 6.10.1** Pequeño Teorema de Fermat Sea  $p$  un primo positivo. entonces  $\forall a \in \mathbb{Z}$

1.  $a^p \equiv a (p)$
2.  $p \nmid a \Rightarrow a^{p-1} \equiv 1 (p)$

**Corolario 6.10.1** Congruencia y Potencias Sea  $p$  un primo positivo. Entonces,  $\forall a \in \mathbb{Z}$  talque  $p \nmid a$  y  $n \in \mathbb{N}$ , se tiene

$$n \equiv r (p-1) \Rightarrow a^n \equiv a^r (p)$$

En particular,  $p \nmid a \Rightarrow a^n \equiv a^{r_{p-1}(n)} (p)$

## 7. Números Complejos

### 7.1. Motivación y Definiciones Iniciales

Se nos presenta el siguiente problema:

**Problema:**  $\nexists r \in \mathbb{R} : r^2 = -1$ , pues  $r^2 > 0, \forall r \in \mathbb{R}$

Y a este problema, se propone la siguiente solución:

**Solución:** Se define el cuerpo  $\mathbb{C} := \begin{cases} (a, b \in \mathbb{R}) \subseteq \mathbb{C} \\ i = \sqrt{-1} \in \mathbb{C} \end{cases}$ . Donde,  $\{z = a + ib; a, b \in \mathbb{R}\} \subseteq \mathbb{C}$

Donde el cuerpo cumple con las operaciones:

- $z + w = (a + bi) + (c + di) = (a + c) + (b + d)i$
- $z \cdot w = (a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i$

**Importante!:**  $i = \sqrt{-1}, i^2 = -1, i^3 = -i, i^4 = 1.$   $\rightarrow$  **General:**  $\forall n \in \mathbb{N}, \begin{cases} i^{4n} = 1 \\ i^{4n+1} = i \\ i^{4n+2} = -1 \\ i^{4n+3} = -i \end{cases}$

### 7.2. Forma Binomial. Inverso. Modulo. Conjugado

**Definición 7.2.1** Forma Binomial  $a, b \in \mathbb{R} \Rightarrow$  se dice que un  $z \in \mathbb{C}$  esta escrito en *Forma Binomial*, cuando esta escrito de la forma:  $z = a + bi$ . Se dice que:  $a$  es la parte real de  $z$  ( $\Re(z) = a$ ) y que  $b$  es la parte imaginaria de  $z$  ( $\Im(z) = b$ )

**Definición 7.2.2** Conjugado El *conjugado* en forma binomial se define como:  $\bar{z} = a - bi$

**Propiedad 7.2.1** 1.  $\bar{\bar{z}} = z$

2.  $z \cdot \bar{z} = |z|^2$
3.  $z + \bar{z} = 2\Re(z)$
4.  $z - \bar{z} = 2\Im(z)$
5.  $\overline{z + w} = \bar{z} + \bar{w}$
6.  $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$
7.  $\overline{z^{-1}} = \bar{z}^{-1}$
8.  $\overline{z^k} = \bar{z}^k$

### 7.3. Modulo

El modulo de un complejo se define como:  $|z| = \sqrt{a^2 + b^2}$ , donde  $\Re(z) = a$  y  $\Im(z) = b$

**Propiedad 7.3.1** 1.  $|\Re(z)| \leq |z| \wedge |\Im(z)| \leq |z|$

2.  $|z + w| \leq |z| + |w|$
3.  $|z \cdot w| \leq |z| \cdot |w|$
4.  $|z^{-1}| = |z|^{-1}$
5.  $|z^k| = |z|^k$

### 7.4. Inverso

El inverso de un complejo se calcula como:  $z^{-1} = \frac{\bar{z}}{|z|^2}$

**Propiedad 7.4.1** 1.  $z^{-1}z = 1$

2.  $\overline{z^{-1}} = \bar{z}^{-1}$
3.  $|z^{-1}| = |z|^{-1}$

## 7.5. Forma Trigonometrica

La forma trigonométrica de un complejo o **forma polar** se define como:  $z = r(\cos(\theta) + i \sin(\theta))$ .  
Por otro lado, se tiene que:  $e^{i\theta} = \cos(\theta) + i \sin(\theta) \Rightarrow z = re^{i\theta}$

Donde, en ambos casos: 
$$\begin{cases} r = |z| \\ \cos(\theta) = \frac{\Re(z)}{|z|} \\ \sin(\theta) = \frac{\Im(z)}{|z|} \\ 0 \leq \theta < 2\pi \end{cases}$$

Grados	0°	30°	45°	60°	90°	180°	270°	360°
Radianes	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$	$\pi$	$\frac{3\pi}{2}$	$2\pi$
Seno	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1	0	-1	0
Coseno	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0	-1	0	1
Tangente	0	$\frac{\sqrt{3}}{3}$	1	$\sqrt{3}$	no definida	0	no definida	0

## 7.6. Resultados obtenidos a través del Teorema de De Moivre

<b>Conjugado:</b>	$\bar{z} = r(\cos(-\theta) + i \sin(-\theta)) = re^{-i\theta}$
<b>Inverso:</b>	$z^{-1} = r^{-1}(\cos(-\theta) + i \sin(-\theta)) = r^{-1}e^{-i\theta}$
<b>Producto:</b>	$z \cdot w = rs(\cos(\theta + \varphi) + i \sin(\theta + \varphi)) = rse^{(\theta + \varphi)i}$
<b>Cociente:</b>	$\frac{z}{w} = \frac{r}{s}(\cos(\theta - \varphi) + i \sin(\theta - \varphi)) = \frac{r}{s}e^{(\theta - \varphi)i}$
<b>Potencias:</b>	$z^n = r^n(\cos(n\theta) + i \sin(n\theta)) = r^n e^{n\theta i}$

## 7.7. Raíces n-ésimas de un número $\mathbb{C}$

**Teorema 7.7.1**  $n \in \mathbb{N}$ ,  $z = se^{i\varphi} \in \mathbb{C}^x$ ,  $s \in \mathbb{R}_{>0} \wedge 0 \leq \varphi < 2\pi \Rightarrow z$  tiene  $n$  raíces  $w_i \in \mathbb{C}$ . Donde: 
$$\begin{cases} w_k = s^{1/n} e^{\theta_k i} \\ \theta_k = \frac{\varphi + 2k\pi}{n} \\ 0 \leq k < n \end{cases}$$

## 7.8. El Grupo $G_n$ de raíces n-ésimas de la Unidad

**Definición 7.8.1**  $G_n = \{w \in \mathbb{C} : w^n = 1\} = \{w_k = e^{\frac{2\pi k i}{n}}; 0 \leq k \leq n-1\} \subseteq \mathbb{C}^x$

**Propiedad 7.8.1**  $((G_n, \cdot))$  Es grupo Abeliano Sea  $n \in \mathbb{N} \Rightarrow \begin{cases} (1) \quad \forall w, z \in G_n \Rightarrow w \cdot z \in G_n \\ (2) \quad 1 \in G_n \\ (3) \quad \forall w \in G_n \exists w^{-1} \in G_n \end{cases}$

**Propiedad 7.8.2**  $n \in \mathbb{N} \wedge w \in G_n$

1.  $|w| = 1$
2.  $m \in \mathbb{Z} : n|m \Rightarrow w^m = 1$
3.  $m, m' \in \mathbb{Z} / m \equiv m'(n) \Rightarrow w^m = w^{m'} \text{ (En particular, } w^m = w^{r_n(m)})$
4.  $w^{-1} = \bar{w} = w^{n-1}$

**Propiedad 7.8.3**  $(G_n \cap G_m = G_{(n:m)})$

1.  $n|m \Rightarrow G_n \subset G_m$
2.  $G_n \cap G_m = G_{(n:m)}$
3.  $G_n \subset G_m \Rightarrow n|m$

**Propiedad 7.8.4** ( $G_n$  es cíclico)

$n \in \mathbb{N} \Rightarrow \exists w \in G_n / G_n = \{1, w, w^2, \dots, w^{n-1}\}$ . Notar que no todo  $w \in G_n$  cumple dicha consigna.

**Definición 7.8.2** (Raíz  $n$ -ésima primitiva de la unidad)

Sea  $n \in \mathbb{N}$ .  $w \in \mathbb{C}$  es  $n$ -ésima primitiva de la unidad, sii  $G_n = \{1, w, w^2, \dots, w^{n-1}\} = \{w^k; 0 \leq k \leq n-1\}$

**Observación 7.8.1**  $w \in G_n^*$  ( $w$  es primitiva)  $\Rightarrow 0 \leq k \neq j \leq n-1; w^k \neq w^j$ , pues  $G_n$  tiene  $n$  elementos distintos y por esto dos potencias de  $w$  no pueden coincidir.

**Proposición 7.8.1**  $w$  es primitiva si  $\forall m \in \mathbb{Z}; w^m = 1 \Leftrightarrow n|m$

**Corolario 7.8.1** (Raíces Primitivas y Potencias)

$n, k \in \mathbb{N} \wedge w \in \mathbb{C}; w \in G_n^* \Rightarrow w^k$  es primitiva  $\Leftrightarrow (n : k) = 1$

**Corolario 7.8.2** (Raíces Primitivas en  $G_n$ )

$n \in \mathbb{N} \wedge w_k = e^{\frac{2k\pi}{n}i}; 0 \leq k \leq n-1 \Rightarrow w_k \in G_n^* \Leftrightarrow (n : k) = 1$

**Corolario 7.8.3** (Raíces Primitivas en  $G_p$ )

$p := \text{primo} \Rightarrow k : 1 \leq k \leq p-1$  (es decir, para cualquier  $k$  distinto de 0)  $\Rightarrow w_k = e^{\frac{2k\pi}{p}i}$  es primitiva de  $G_p$ . Es decir,  $\forall w \in G_p; w \neq 1$  se tiene que  $w$  es  $p$ -ésima primitiva de la unidad.

**Propiedad 7.8.5** (Suma y producto de los elementos de  $G_n$ )

$$n \in \mathbb{N}: \quad (i) \sum_{w \in G_n} w = 0 \quad (ii) \prod_{w \in G_n} w = \begin{cases} 1 & n \text{ impar} \\ -1 & n \text{ par} \end{cases}$$