

# IIC3253

Teoría de Grupos

# Grupos

Un grupo es un par  $(G, *)$ , donde  $G$  es un conjunto y  $*$  :  $G \times G \rightarrow G$  es una operación que satisface:

**Neutro.** Existe  $e \in G$  tal que para todo  $a \in G$

$$e * a = a * e = a$$

**Inversos.** Para todo  $a \in G$  existe  $a^{-1} \in G$  tal que

$$a * a^{-1} = a^{-1} * a = e$$


**Asociatividad.** Para todos  $a, b, c \in G$  se tiene


$$(a * b) * c = a * (b * c)$$

# Grupos: Ejemplos

$$(\mathbb{Z}, +) ?$$



¿Neutro? El 0 


¿Inversos? Dado  $a \in \mathbb{Z}$ ,  $-a$  también está en  $\mathbb{Z}$  


¿Asociatividad? Viene de la suma 

# Grupos: Ejemplos

$$(\mathbb{Q}, \cdot) ?$$



¿Neutro? El 1 


¿Inversos? Dado  $q \in \mathbb{Q}$ ,  $1/q$  también está en  $\mathbb{Q}$  


¿Asociatividad? Viene de la multiplicación 

# Grupos: Ejemplos

$$(\mathbb{Q} \setminus \{0\}, \cdot) ?$$




¿Neutro? El 1 

¿Inversos? Dado  $q \in \mathbb{Q} \setminus \{0\}$ ,  $1/q$  también está en  $\mathbb{Q} \setminus \{0\}$  

¿Asociatividad? Viene de la multiplicación 

# Grupos: Ejemplos

$$(\mathbb{N}, +) ? \quad \times$$


¿Neutro? El 0 

¿Inversos? Dado  $a \in \mathbb{N}$ ,  $-a$  no está en  $\mathbb{N}$  

# Grupos: Ejemplos

$$(\mathbb{Z}, \cdot) ?$$





¿Neutro? El 1 

¿Inversos? Dado  $a \in \mathbb{Z}$  con  $a \neq 1$ ,  $1/a$  no está en  $\mathbb{Z}$  


# Grupos: Ejemplos

$(\{0, 1, 2, 3\}, + \bmod 4)$  ?

¿Neutro? El 0 

¿Inversos? Dado  $a \in \{0, 1, 2, 3\}$ ,  $(4 - a) \bmod 4$  está en  $\{0, 1, 2, 3\}$   
y tenemos que  $(a + (4 - a) \bmod 4) \bmod 4 = 0$  

¿Asociatividad?


$((a + b) \bmod 4 + c) \bmod 4 = (a + (b + c) \bmod 4) \bmod 4$  



# Grupos: Ejemplos

$(\{1, 3, 7, 9\}, \cdot \bmod 10) ?$

¿Multiplicación  $\bmod 10 : \{1, 3, 7, 9\} \rightarrow \{1, 3, 7, 9\}$ ?

¿Neutro? El 1 

¿Inversos? Son todos los primos relativos con el 10 

¿Asociatividad?

$$((a \cdot b) \bmod 10 \cdot c) \bmod 10 = (a \cdot (b \cdot c) \bmod 10) \bmod 10$$

# Grupos: Ejemplos

Dado  $n \in \mathbb{N}$ , todas las permutaciones

$$\pi : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$$

¿Cuál es la operación?

Las permutaciones son funciones,  
podemos usar composición ( $\circ$ )

Siendo  $A_n$  el conjunto de todas las permutaciones de  $\{1, \dots, n\}$ , demuestre que  $S_n = (A_n, \circ)$  es un grupo

# Algunas preguntas

¿Es la operación  $*$  siempre conmutativa?

¿Puede haber una segunda identidad?


¿Puede un elemento tener dos inversos?


¿Puede un elemento tener un inverso por la izquierda y otro inverso por la derecha?

Sea  $n \in \mathbb{N}$

¿Qué operación nos da un grupo para  $\{0, 1, \dots, n - 1\}$ ?

$$a + b \mod n$$

¿Neutro? El 0 

¿Inversos? Dado  $a \in \{0, \dots, n - 1\}$ ,  $(n - a) \mod n$  está en  $\{0, \dots, n\}$  y  $(a + (n - a) \mod n) \mod n = n \mod n = 0$  

$(\mathbb{Z}_n, + \mod n)$  es el grupo aditivo de los enteros en módulo  $n$ .


¿Y si tratamos con la multiplicación?

¡Hay elementos que no tienen inverso!

El número 0 y todo  $a \in \{1, \dots, n-1\}$  tal que  $MCD(a, n) > 1$

¿Y si los sacamos?

¿Multiplicación mod 10 :  $\{1, 3, 7, 9\} \rightarrow \{1, 3, 7, 9\}$ ?

¿Neutro? El 1 

¿Inversos? Gracias Euclides!

$\mathbb{Z}_n^*$

Grupo multiplicativo de los enteros módulo  $n$   
\*de los primos relativos con  $n$  en módulo  $n$

$$\mathbb{Z}_{10}^*$$

$$\{1, 3, 7, 9\}$$

$$\mathbb{Z}_{11}^*$$

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$\mathbb{Z}_p^* \text{ para } p \text{ primo sus elementos son } \{1, \dots, n-1\}$$

# $\mathbb{Z}_n^*$ y sus subgrupos

Un subgrupo de  $(G, *)$  es un conjunto  $H \subseteq G$  tal que  $(H, *)$  también es un grupo.

¿Qué subgrupos tiene  $\mathbb{Z}_{10}^* = (\{1, 3, 7, 9\}, \cdot \bmod 10)$ ?

$$(\{1\}, \cdot \bmod 10) \quad \checkmark$$

$$(\{1, 3, 7, 9\}, \cdot \bmod 10) \quad \checkmark$$

$$(\{1, 9\}, \cdot \bmod 10) \quad \checkmark$$

¿Qué subgrupos tiene  $\mathbb{Z}_{12}^*$ ?

$$\{1, 5, 7, 11\}$$

$$(\{1\}, \cdot \bmod 12) \checkmark$$

$$(\{1, 5, 7, 11\}, \cdot \bmod 12) \checkmark$$

$$(\{1, 5\}, \cdot \bmod 12) \checkmark$$

$$(\{1, 7\}, \cdot \bmod 12) \checkmark$$

$$(\{1, 11\}, \cdot \bmod 12) \checkmark$$



¿Y si  $n$  es primo?

$$\mathbb{Z}_5^* = (\{1, 2, 3, 4\}, \cdot \bmod 5)$$

$$(\{1\}, \cdot \bmod 5) \quad \checkmark$$

$$(\{1, 2, 3, 4\}, \cdot \bmod 5) \quad \checkmark$$

$$(\{1, 4\}, \cdot \bmod 5) \quad \checkmark$$

$$\mathbb{Z}_7^* = (\{1, 2, 3, 4, 5, 6\}, \cdot \bmod 7)$$

$$(\{1\}, \cdot \bmod 7) \checkmark$$

$$(\{1, 2, 3, 4, 5, 6\}, \cdot \bmod 7) \checkmark$$

$$(\{1, 2, 4\}, \cdot \bmod 7) \checkmark$$

$$(\{1, 6\}, \cdot \bmod 7) \checkmark$$

$$\mathbb{Z}_{11}^* = (\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}, \cdot \bmod 11)$$

$$(\{1\}, \cdot \bmod 11) \checkmark$$

$$(\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}, \cdot \bmod 11) \checkmark$$

$$(\{1, 5, 3, 4, 9\}, \cdot \bmod 11) \checkmark$$

$$(\{1, 10\}, \cdot \bmod 11) \checkmark$$

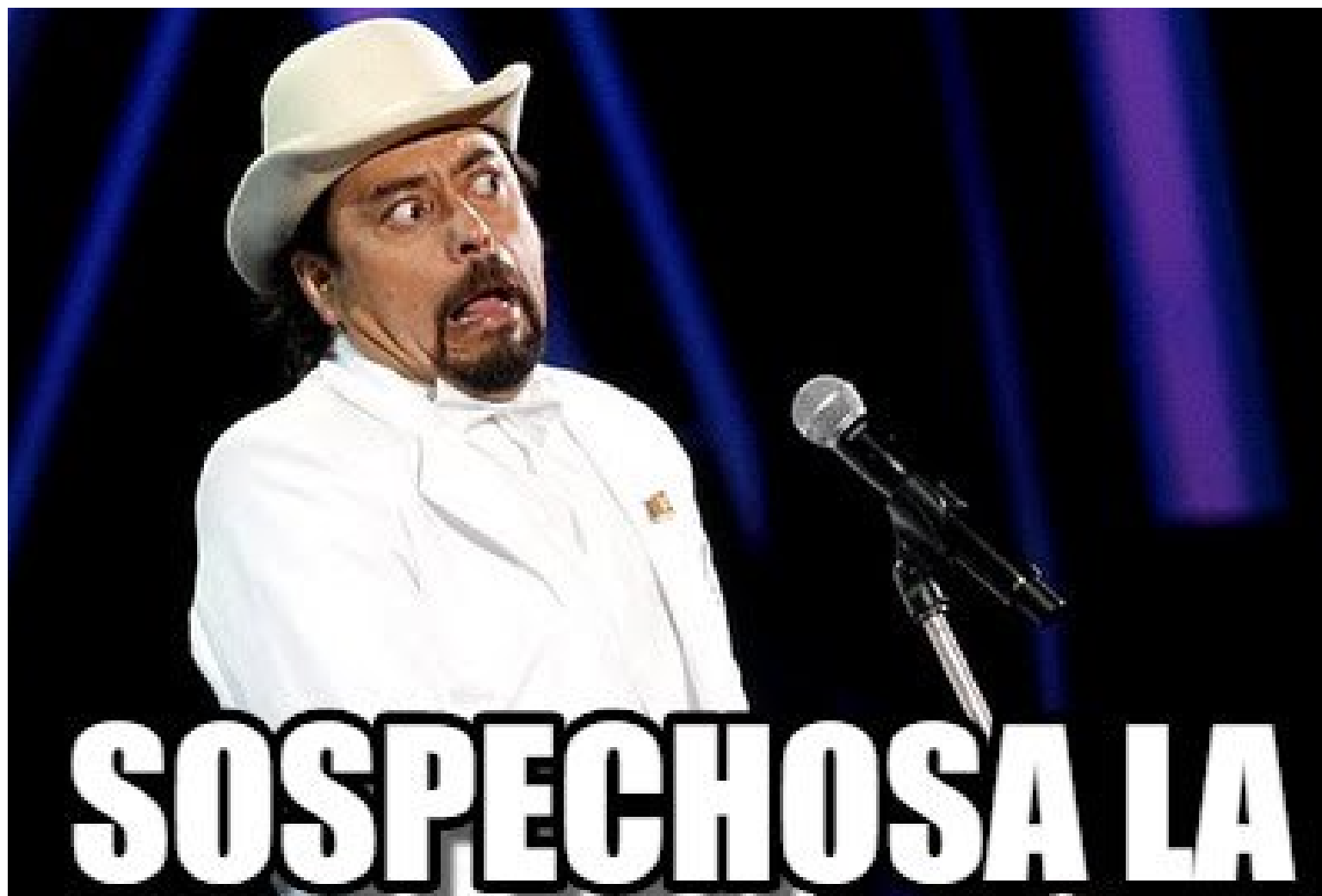
Cantidad de elementos de  $G$ : *orden* de  $G$

$\mathbb{Z}_{11}^*$	$\{1, 5, 3, 4, 9\}$	Grupo de orden 10
	$\{1, 10\}$	Subgrupos de orden 1, 2, 5 y 10

$\mathbb{Z}_7^*$	$\{1, 2, 4\}$	Grupo de orden 6
	$\{1, 6\}$	Subgrupos de orden 1, 2, 3 y 6

$\mathbb{Z}_5^*$	$\{1, 4\}$	Grupo de orden 4
		Subgrupos de orden 1, 2 y 4

$\mathbb{Z}_{17}^*$	...	Grupo de orden 16
		Subgrupos de orden 1, 2, 4, 8 y 16



**COSA**

¿Podremos demostrar que el tamaño de un subgrupo siempre divide al tamaño del grupo?

Si tenemos un grupo  $(G, *)$ , llamaremos  $G$  al grupo y supondremos que  $*$  se deduce del contexto.

Sea  $G$  un grupo y  $H$  un subgrupo de  $G$

Dado  $g_0 \in G \setminus H$

¿Cuántos elementos tiene  $g_0H = \{g_0 * h \mid h \in H\}$ ?

Dado  $g_0 \in G \setminus H$

¿Cuántos elementos tiene  $g_0H = \{g_0 * h | h \in H\}$ ?

A lo más tiene  $|H|$  elementos distintos

Si  $g_0 * h_1 = g_0 * h_2$  entonces  $h_1 = h_2$ .

Tenemos que  $|g_0H| = |H|$

¿Puede  $g_0H \cap H$  ser no vacío?

$$g_0h_1 = h_2 \Rightarrow g_0 = h_2h_1^{-1}$$

Pero como  $H$  es subgrupo,  $h_2h_1^{-1} \in H \Rightarrow \Leftarrow$

Si  $G = H \cup g_0H$  entonces  $|G| = 2|H|$ .  
De lo contrario sea  $g_1 \in G \setminus (H \cup g_0H)$

¿Cuántos elementos tiene  $g_1H = \{g_1 * h | h \in H\}$ ?

¿Puede  $g_1H \cap H$  ser no vacío?

¿Puede  $g_0H \cap g_1H$  ser no vacío?

$$g_0h_1 = g_1h_2 \Rightarrow g_0h_1h_2^{-1} = g_1$$

Pero como  $H$  es subgrupo,  $h_1h_2^{-1} \in H$ . Luego  $g_1 \in g_0H \Rightarrow \Leftarrow$



Si  $G = H \cup g_0H \cup g_1H$  entonces  $|G| = 3|H|$ . De lo contrario sea  $g_2 \in G \setminus (H \cup g_0H \cup g_1H)$

## Teorema de Lagrange

Si  $G$  es un grupo finito y  $H$  es un subgrupo de  $G$ , entonces  $|H|$  divide a  $|G|$

# Subgrupos generados

Sea  $G$  un grupo y  $a \in G$ . Usando notación multiplicativa, definiremos

$$a^n = \underbrace{a * \cdots * a}_{n \text{ veces}}$$

Si tomamos la secuencia  $\{1, a, a^2, a^3, \dots\}$  eventualmente un elemento se tiene que repetir. Sea  $a^j = a^{j+k}$  la primera repetición

Tenemos entonces que  $a^j = a^j * a^k$  y por lo tanto  $a^k$  es el neutro

# Subgrupos generados

Tenemos entonces que  $a^j = a^j * a^k$  y por lo tanto  $a^k$  es el neutro

Implica que  $j = 0$ . Si no, no sería la primera repetición

Definamos  $\langle a \rangle = \{a^i \mid 0 \leq i < k\}$

¿Qué podemos decir de  $\langle a \rangle$ ?

¡Es un subgrupo de tamaño  $k$ !

Implica que  $|\langle a \rangle| = k$  divide a  $|G|$

# $\mathbb{Z}_p^*$ con $p$ un número primo

Sea  $a \in \mathbb{Z}_p^*$  y supongamos  $|\langle a \rangle| = k$

$\mathbb{Z}_p^*$  tiene exactamente  $p - 1$  elementos

Luego  $k$  divide a  $p - 1$

Existe  $\alpha$  tal que  $\alpha \cdot k = p - 1$

$$a^{p-1} = a^{\alpha \cdot k} = (a^k)^\alpha = 1^\alpha = 1$$

$\mathbb{Z}_n^*$  **con**  $n \in \mathbb{N}$

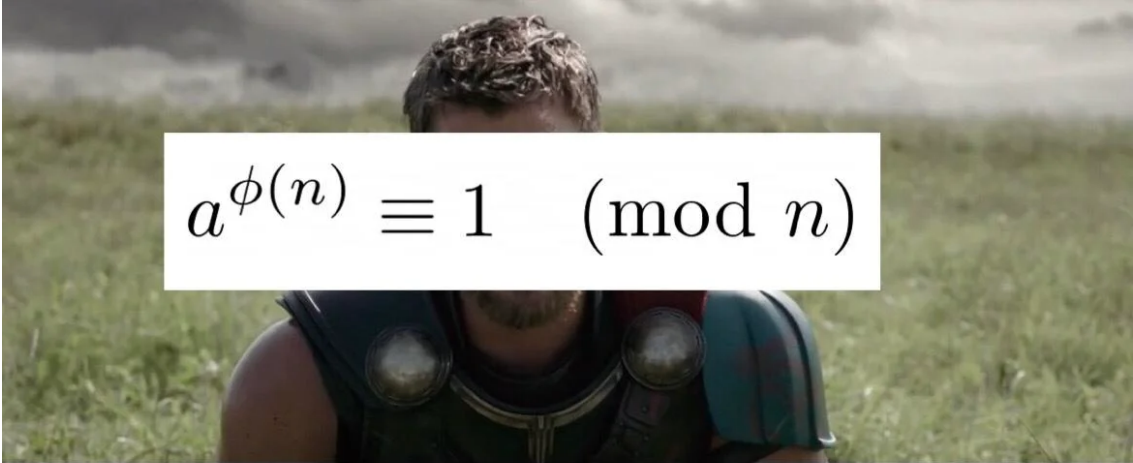
Sea  $a \in \mathbb{Z}_n^*$  y supongamos  $|\langle a \rangle| = k$

$\mathbb{Z}_n^*$  tiene exactamente  $\phi(n)$  elementos

Luego  $k$  divide a  $\phi(n)$

Existe  $\alpha$  tal que  $\alpha \cdot k = \phi(n)$

$$a^{\phi(n)} = a^{\alpha \cdot k} = (a^k)^\alpha = 1^\alpha = 1$$

A medium shot of Thor from the chest up, standing in a grassy field under a cloudy sky. He is wearing his Asgardian armor, including a blue and red chest plate with circular emblems and a blue helmet with a red plume. He has a serious expression.
$$a^{\phi(n)} \equiv 1 \pmod{n}$$

**I'm not as strong as you.**

A medium shot of Odin from the chest up, standing in a grassy field under a cloudy sky. He is wearing a light brown, textured tunic. He has a long white beard and a serious expression.
$$a^{p-1} \equiv 1 \pmod{p}$$

**No. You're stronger.**

@12\_Semitones

# RSA?

P, Q dos primos

$$N = P \cdot Q \quad \phi(N) = (P - 1) \cdot (Q - 1)$$

$e, d$  dos números tales que  $e \cdot d = \alpha \phi(N) + 1$

$$Enc(m) = m^e \mod N \quad Dec(c) = c^d \mod N$$

$$Dec(Enc(m)) = m^{e \cdot d} \mod N$$

$$= m^{\alpha \cdot \phi(N) + 1} \mod N = (m^{\phi(N)})^\alpha \cdot m \mod N$$





# Wait

¿Qué pasa si  $m$  no es primo relativo con  $N$ ?

$$m^{\alpha \cdot \phi(N) + 1} \equiv m \pmod{N}$$

es cierto para todo  $m \in \{1, \dots, N - 1\}$

Demuéstrelo.

Dado un grupo  $G$ , si existe  $a \in G$  tal que  $\langle a \rangle = G$ , decimos que  $G$  es un grupo *cíclico*

# No demostraremos que...

$\mathbb{Z}_p^*$  es siempre cíclico

¿Quién genera a  $\mathbb{Z}_7^*$ ?