

EXAMEN – JUEVES 10 DE FEBRERO DE 2022

Nro de Examen	Cédula	Apellido y nombre

Escribir nombre y cédula en todas las hojas que se entreguen. Deben justificar todas sus respuestas.

**Ejercicio 1.** Sea  $(G, *)$  un grupo de orden primo con elemento neutro  $a$ .

- Demostrar que todo elemento  $x \in G$  con  $x \neq a$  es un generador de  $G$ .
- Demostrar que  $G$  es isomorfo a  $\mathbb{Z}_p$  donde  $p = |G|$ .
- Determine cuales de las siguientes tablas de multiplicar corresponden a la tabla de Cayley de algún grupo y justifique porqué.

Cuadro 1: Posibles tablas de Cayley

*	a	b	c	d	e	f	g
a	a	b	c	d	e	f	g
b	b	a	d	c	g	e	f
c	c	g	e	f	a	d	b
d	d	c	b	a	f	g	e
e	e	f	a	g	c	b	d
f	f	e	g	b	d	a	c
g	g	d	f	e	b	c	a

*	a	b	c	d	e
a	a	b	c	d	e
b	b	c	e	a	d
c	c	e	d	b	a
d	d	a	b	e	c
e	e	d	a	c	b

**Ejercicio 2.** Sean  $(G, *, e_G)$  y  $(K, \cdot, e_K)$  dos grupos.

- Definir homomorfismo de grupo de  $G$  en  $K$ .
- Si  $F : G \rightarrow K$  es un homomorfismo, probar que
  - $F(e_G) = e_K$ .
  - $F(g^{-1}) = F(g)^{-1}$ ,  $\forall g \in G$ .
  - Si  $g \in G$  y  $o(g) < \infty$ , entonces  $o(F(g)) \mid o(g)$ .
- ¿Cuántos homomorfismos  $F : U(25) \rightarrow K$  existen en cada uno de los siguientes casos?
  - $K = \mathbb{Z}_{21}$
  - $K = \mathbb{Z}_{15}$

Sigue en la parte de atrás...

**Ejercicio 3.** En este ejercicio, para  $a \in \mathbb{Z}$  denotamos por  $\bar{a}$  a su clase en  $\mathbb{Z}_{21}$ .

- a. Probar que no existe homomorfismo  $\phi : \mathbb{Z}_{21} \rightarrow \mathbb{Z}_{21}$  tal que  $\phi(\bar{6}) = \bar{8}$ .
- b. Sea  $\phi : \mathbb{Z}_{21} \rightarrow \mathbb{Z}_{21}$  un homomorfismo tal que  $\phi(\bar{6}) = \bar{9}$ .
  - i) Hallar  $\phi(\bar{18})$  y  $\phi(\bar{3})$ .
  - ii) Hallar  $\phi$  si se sabe además que  $\phi(\bar{14}) = \bar{7}$ .

**Ejercicio 4.**

- a. Considere el criptosistema RSA con módulo  $n = pq$  y funciones de cifrado  $E(x) = x^e \pmod{n}$  y descifrado  $D(x) = x^d \pmod{n}$ . Indique qué hipótesis deben satisfacer  $d$  y  $e$  y demuestre que

$$D(E(x)) \equiv x \pmod{n}$$

para todo  $x \in \mathbb{Z}_n$ .

- b. Dados primos  $p = 19$ ,  $q = 29$  y  $e = 5$ , calcular explícitamente la función de descifrado  $D$ .
- c. Descifrar el mensaje cifrado  $x = 2$ .