

Universidad de la República - Facultad de Ingeniería - IMERL: Matemática  
Discreta 2, semipresencial

PRIMER PARCIAL - 3 DE DICIEMBRE DE 2015. DURACIÓN: 3 HORAS

N° de parcial	Cédula	Apellido y nombre

**Ejercicio 1.**

- Probar que 2 es raíz primitiva módulo 53.
- Hallar todos los  $x \in \mathbb{Z}$  tales que  $x^{19} \equiv 32 \pmod{53}$ .
- Archibaldo y Baldomero quieren pactar una clave común empleando el protocolo Diffie-Hellman. Para ésto fijan el primo 53 y la raíz primitiva  $g = 2$ . Archibaldo selecciona el número  $m = 28$  y le remite el número 49 a Baldomero. Baldomero selecciona el número  $n = 5$ . ¿Cuál es la clave  $k$  común que acordaron Archibaldo y Baldomero?

**Ejercicio 2.**

- Sea  $(G, *)$  un grupo finito y  $H$  un subgrupo de  $G$ . Definimos la siguiente relación en  $G$ :

$$g \sim g' \Leftrightarrow g * (g')^{-1} \in H.$$

Probar que la relación definida es una relación de equivalencia.

- Sean  $G, K$  grupos finitos y  $f : G \rightarrow K$  un homomorfismo de grupos. Probar que  $\text{Ker}(f)$  es un subgrupo de  $G$ .
- Probar el teorema de órdenes para grupos:

*Sean  $G$  y  $K$  dos grupos finitos y  $f : G \rightarrow K$  un homomorfismo de grupos. Entonces*

$$|G| = |\text{Ker}(f)| |\text{Im}(f)|.$$

**Ejercicio 3.**

- Sea  $f : G \rightarrow K$  un homomorfismo de grupos y  $g \in G$  un elemento de orden  $o(g)$  finito. Probar que  $o(f(g)) \mid o(g)$ .
- Para los pares de grupos  $G$  y  $K$ , determinar si existen homomorfismos no triviales  $f : G \rightarrow K$ . Si existen encontrarlos todos, de lo contrario justificar por qué no existen.
  - $G = \mathbb{Z}_6$  el grupo de enteros módulo 6 y  $K = S_3$  el grupo de permutaciones de 3 elementos.
  - $G = S_6$  el grupo de permutaciones de 6 elementos y  $K = \mathbb{Z}_7$  el grupo de enteros módulo 7.
- Sean  $G = D_{12}$  el grupo dihedral y  $K = S_3 \times U(8)$  el producto cartesiano de los grupos  $S_3$  (permutaciones de 3 elementos) y  $U(8)$ . ¿Son isomorfos estos grupos? De serlo, dar un isomorfismo entre ellos, de lo contrario justificar por qué no lo son.