

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

SEGUNDO PARCIAL (CUARTA PRUEBA)  
29 DE NOVIEMBRE DE 2018  
DURACIÓN: 3 HORAS

Nombre y Apellido	Cédula de identidad

Para cada pregunta o ejercicio, deben presentar claramente el razonamiento y cálculos realizados para obtener su respuesta final. Si una implicancia es válida debido a algún teorema, proposición o propiedad, deben especificarlo. Presentar una respuesta final a la pregunta sin justificación carece de validez.

**Ejercicio 1.** (A puntos)

- a. Probar que, si para todo  $d \neq \varphi(n)$  tal que  $d|\varphi(n)$ , se tiene que  $g^d \not\equiv 1 \pmod{n}$  entonces  $g$  es una raíz primitiva módulo  $n$ .
- b. Probar que  $g = 2$  es raíz primitiva en  $U(67)$ .
- c. Describir el método de Diffie-Hellmann.
- d.
  - Calcular  $34^{29} \pmod{67}$  por exponenciación rápida.
  - Calcular la clave en común que generan Ana y Bernardo, si toman  $p = 67$  (como primo),  $g = 2$  (como raíz primitiva), y  $m = 29$ ,  $n = 65$  (como parámetros de exponenciación).

**Ejercicio 2.** (B puntos)

En  $U(41)$ ,

- a. Probar que  $o(3) = 8$  y hallar los elementos de  $H = \langle 3 \rangle$ .  
  
(Recordar para lo que sigue que si  $y \notin H$  entonces  $o(y) \nmid 8$ .)
- b. Elegir un  $y \notin H$ . Verificar que  $y^8 \neq 1 \pmod{41}$  y hallar  $o(y)$ .
- c. Hallar  $g = 3^r y^s$  una raíz primitiva módulo 41.

**Ejercicio 3.** (C puntos) Sean  $f : G_1 \rightarrow G_2$  y  $g : G_2 \rightarrow G_3$  morfismos de grupos.

- a.
  - Probar que  $g \circ f$  es morfismo de grupos.
  - ¿Qué relación tienen  $\text{Im}(g \circ f)$  e  $\text{Im}(g)$ ? Justificar.Supongamos que  $|G_1| = m$ ,  $|G_2| = n$  y  $|G_3| = r$ , con  $m, n, r \in \mathbb{Z}$ .
- b.
  - Probar que  $|\text{Im}(f)|$  divide a  $\text{mcd}(m, n)$ .
  - Probar que  $|\text{Im}(g \circ f)|$  divide a  $\text{mcd}(m, n, r)$ .
- c. Resolver (encontrar todas las soluciones) en  $U(29)$  de la ecuación  $x^2 - 1 = 0$ . ¿Qué orden tienen las soluciones halladas?
- d. Sean  $G_1 = D_7$ , el grupo dihedral de orden 14,  $G_2 = S_5$  el grupo de permutaciones de 5 elementos,  $G_3 = \mathbb{Z}_{15}$ , y  $G_4 = U(29)$ .
  - Hallar todos los morfismos de dominio  $G_1$  y codominio  $G_3$  que factorizan por  $G_2$ .
  - Hallar todos los morfismos de dominio  $G_1$  y codominio  $G_4$  que factorizan por  $G_2$ .