

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

SEGUNDO PARCIAL - 30 DE NOVIEMBRE DE 2017. DURACIÓN: 4 HORAS

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 (nombre del teorema, lema, etc.) Presentar una respuesta final a la pregunta sin justificación carece de validez.

Ejercicio 1.

- a. Probar que 2 es raíz primitiva módulo 19.
- b. Sea p es primo y g una raíz primitiva módulo p . Si m es el orden de g en $U(p^2)$, probar que $p - 1 \mid m$.
- c. Hallar una raíz primitiva módulo $19^2 = 361$.
- d. Probar que si x es un entero impar y p es un primo impar, entonces que $x^m \equiv 1 \pmod{2p^2} \Leftrightarrow x^m \equiv 1 \pmod{p^2}$.
- e. Hallar una raíz primitiva módulo 722.

Ejercicio 2. Sea $G = U(241)$ y $H = \{h \in G, \text{ tal que } o(h) \mid 24\}$.

- a. Probar que si $x \notin H$ y $x^2 \in H$ entonces $o(x) \in \{16, 48\}$.
- b. Probar que $\#H = 24$ (*sugerencia: 241 es primo*).
- c. Probar que $H = \langle \bar{2} \rangle$ y listar los elementos de H .
- d. Probar, utilizando lo anterior, que $o(\overline{11}) = 48$.
- e. Sabiendo que $10^5 \equiv 2^{20} \pmod{241}$, hallar $o(\overline{10})$.
- f. Hallar (justificando) una raíz primitiva módulo 241 (puede quedar expresada como producto de potencias).
- g. Para utilizar el método Diffie Hellman de intercambio de 5 clave, Ana y Bruno eligen g una raíz primitiva módulo 241. Si Ana elige el exponente $a = 50$ y Bob elige el exponente $b = 56$, probar que la clave fijada es $k = 15$ o $k = 225$.

Ejercicio 3. Sea G un grupo y $H < G$. Consideramos en G la relación de equivalencia $g \sim k \Leftrightarrow gk^{-1} \in H$ (NO es necesario verificar que es relación de equivalencia).

- a. Probar que si C es una clase de equivalencia, entonces $\#C = |H|$.
- b. Probar que si $F : G \rightarrow A$ es un homomorfismo de grupos y $H = \ker(F)$ entonces para $g, k \in G$ se tiene que $g \sim k \Leftrightarrow F(g) = F(k)$.
- c. Enunciar y demostrar el Teorema de órdenes para homomorfismos de grupos.
- d. Probar que si $F : G \rightarrow A$ es un homomorfismo sobreyectivo entre grupos finitos, entonces $a^{|G|} = e_A$ para todo $a \in A$.