

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

SEGUNDO PARCIAL - 27 DE JUNIO DE 2019. DURACIÓN: 3:30 HORAS

N° de parcial	Apellido y Nombre	Cédula

Ejercicio 1.

- a. Sean G un grupo y dos elementos $x, y \in G$ de orden finito. Probar que si $xy = yx$ y $\text{mcd}(o(x), o(y)) = 1$, entonces $o(xy) = o(x)o(y)$.
- b. Sean G un grupo y $g \in G$. Probar que $|\langle g \rangle| = o(g)$.

Ejercicio 2.

- a. Probar que 98 es raíz primitiva módulo 101.
- b. Hallar un elemento de $U(101)$ de orden 25.
- c. Alicia y Beatriz quieren acordar una clave común utilizando el protocolo Diffie-Hellman. Para ello acuerdan públicamente el uso de $p = 101$ y $g = 98$ como raíz primitiva. Alicia elige en secreto un número n y le envía $g^n \equiv 11 \pmod{101}$ a Beatriz. Beatriz elige en secreto $m = 31$ y le envía $g^m \equiv 83 \pmod{101}$ a Alicia.
¿Cuál es la clave común k acordada?

Ejercicio 3. Para los siguientes grupos G, K , determinar si existen homomorfismos $f : G \rightarrow K$ no triviales. En caso afirmativo dar un ejemplo, justificando que es un homomorfismo.

- a. Para un primo impar p , $G = \mathbb{Z}_p$ el grupo de enteros módulo p y $K = S_{p-1}$ el grupo de permutaciones de $p - 1$ elementos.
- b. $G = \mathbb{Z}_{100}$ el grupo de enteros módulo 100, y $K = U(101)$ el grupo de invertibles módulo 101.
- c. $G = U(12)$ el grupo de invertibles módulo 12 y \mathbb{Z}_4 el grupo de enteros módulo 4.

Ejercicio 4.

- a. Describir el criptosistema RSA.
- b. Probar que la función de descifrado del criptosistema RSA descifra correctamente.