

SEGUNDO PARCIAL – JUEVES 29 DE JUNIO DE 2023

Nro de Lista	Cédula	Apellido y nombre

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

**Ejercicio 1.** Sea  $(G, \cdot)$  un grupo finito con neutro  $e$  y  $g \in G$  con orden  $o(g)$ .

- a) (2 puntos) Defina el orden de  $g$ , el orden de  $G$  y enuncie el Teorema de Lagrange.

**Solución:** Ver notas Definición 3.7.6., orden de  $G$  es la cantidad de elementos de  $G$ , ver notas Teorema 3.8.1.

- b) (5 puntos) Probar que  $g^m = e$  si y solo si  $o(g) | m$ .

**Solución:** Ver notas Proposición 3.7.8. parte 4.

- c) Sean  $x, y \in G$ .

- i) (3 puntos) Dar un ejemplo en el que  $xy = yx$  y  $o(xy) \neq o(x) \cdot o(y)$ .

**Solución:** Tomar  $G = \mathbb{Z}_2$  y  $x = y = 1$ .

- ii) (3 puntos) Dar un ejemplo en el que  $\text{mcd}(o(x), o(y)) = 1$  y  $o(xy) \neq o(x) \cdot o(y)$ .

**Solución:** Tomar  $G = S_3$ , con  $x$  un elemento de orden 3 e  $y$  un elemento de orden 2, pero no hay elementos de orden 6 en  $G$ .

- iii) (7 puntos) Probar que si  $xy = yx$  y  $\text{mcd}(o(x), o(y)) = 1$  entonces  $o(xy) = o(x) \cdot o(y)$ .

**Solución:** Ver notas Lema 4.1.7.

**Ejercicio 2.**

- a) (10 puntos) Enuncie y prueba el Teorema de órdenes para homomorfismos de grupos  $f : G \rightarrow K$ .

**Solución:** Ver notas Teorema 3.9.8.

- b) (6 puntos) Encuentre todos los homomorfismos  $f : U(7) \rightarrow \mathbb{Z}_9$ . Debe escribir cada homomorfismo explícitamente en la forma  $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ f(1) & f(2) & f(3) & f(4) & f(5) & f(6) \end{pmatrix}$ .

**Solución:**  $U(7) = 1, 2, 3, 4, 5, 6$  y un generador es 3, ya que  $3^2 = 9 \not\equiv 1 \pmod{7}$  y  $3^3 = 27 \equiv 6 \not\equiv 1 \pmod{7}$ . Todo homomorfismo  $f$  de  $U(7)$  en  $\mathbb{Z}_9$  es de la forma  $f(3^n) = n \cdot k$  para algún  $k \in \mathbb{Z}_9$  tal que  $o(k) | o(3) = 6$ . Se cumple que  $o(k) = o(1) / \text{mcd}(o(1), k) = 9 / \text{mcd}(9, k)$ , por lo que  $o(k) | 6$  si  $k = 0, 3, 6$ . Notar que  $3^0 \equiv 1 \pmod{7}$ ,  $3^1 \equiv 3 \pmod{7}$ ,  $3^2 \equiv 2 \pmod{7}$ ,  $3^3 \equiv 6 \pmod{7}$ ,  $3^4 \equiv 4 \pmod{7}$ ,  $3^5 \equiv 5 \pmod{7}$ . Entonces hay tres morfismos y explícitamente son

$$\begin{aligned} & \bullet \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 0 \cdot 0 & 2 \cdot 0 & 1 \cdot 0 & 4 \cdot 0 & 5 \cdot 0 & 3 \cdot 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \\ & \bullet \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 0 \cdot 3 & 2 \cdot 3 & 1 \cdot 3 & 4 \cdot 3 & 5 \cdot 3 & 3 \cdot 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 6 & 3 & 3 & 6 & 0 \end{pmatrix} \\ & \bullet \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 0 \cdot 6 & 2 \cdot 6 & 1 \cdot 6 & 4 \cdot 6 & 5 \cdot 6 & 3 \cdot 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 3 & 6 & 6 & 3 & 0 \end{pmatrix} \end{aligned}$$

- c) (4 puntos) Decidir si existe o no un isomorfismo  $f : U(7) \rightarrow U(9)$ . En caso afirmativo mostrar uno explícitamente (de la forma mostrada en el ítem anterior).

**Solución:** El grupo  $U(9)$  también es cíclico de orden 6 con generador 2, por lo que si tomamos el morfismo  $f(3^k) = 2^k$  tiene que ser un isomorfismo, explícitamente:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2^0 & 2^2 & 2^1 & 2^4 & 2^5 & 2^3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 7 & 5 & 8 \end{pmatrix}.$$

### Ejercicio 3.

- a) (3 puntos) Describa el método Diffie-Hellman de intercambio de clave.

**Solución:** Ver notas 5.2.1.

- b) Imagine que usted utiliza el método Diffie-Hellman con el agente X, acordando como primo  $p = 101$  y como raíz primitiva  $g$ , la más pequeña posible.

- i) (5 puntos) Encuentre  $g$ .

**Solución:** Empecemos probando con  $g = 2$ . Como  $\varphi(101) = 100 = 2^2 5^2$  para ver si es raíz primitiva módulo 101 alcanza con probar que  $2^{100/2} = 2^{50} \not\equiv 1 \pmod{101}$  y  $2^{100/5} = 2^{20} \not\equiv 1 \pmod{101}$ . Utilizamos el método de exponenciación rápida para calcular dichas potencias.

Primero vemos que  $2^{2^0} = 2$ ,  $2^{2^1} = 2^2 = 4$ ,  $2^{2^2} = 4^2 = 16$ ,  $2^{2^3} = 16^2 = 256 \equiv 54 \pmod{101}$ ,  $2^{2^4} = 54^2 = 2916 \equiv 88 \pmod{101}$ . Entonces como  $20 = 16 + 4$  tenemos que  $2^{2^0} = 2^{16+4} = 2^{16} 2^4 \equiv 88 \cdot 16 \pmod{101} \equiv 95 \pmod{101} \not\equiv 1 \pmod{101}$ .

Por otro lado  $2^{50} = (2^{20})^{2^8} 2^2 \equiv (-6)^2 \cdot 54 \cdot 4 \pmod{101} \equiv 36 \cdot 54 \cdot 4 \pmod{101} \equiv 100 \pmod{101} \not\equiv 1 \pmod{101}$ .

- ii) (2 puntos) Suponga que usted elige como número secreto  $n = 20$ , ¿Qué número le enviará usted por el canal al agente X?

**Solución:** Hay que enviar  $2^{20} \pmod{101} = 95$  por lo visto antes.

- iii) (2 puntos) Si el agente X le envía por el canal el número 3, ¿Cuál sería el valor de la clave acordada? (debe expresar el resultado explícitamente).

**Solución:** La clave es  $3^{20} \pmod{101}$  y usando exponenciación rápida como antes vemos que  $3^{2^0} = 3$ ,  $3^{2^1} = 3^2 = 9$ ,  $3^{2^2} = 9^2 = 81 \equiv -20 \pmod{101}$ ,  $3^{2^3} = (-20)^2 = 400 \equiv -4 \pmod{101}$ ,  $3^{2^4} \equiv (-4)^2 \pmod{101} \equiv 16 \pmod{101}$  entonces  $3^{2^0} = 3^{16+4} = 3^{16} 3^4 \equiv 16 \cdot (-20) \pmod{101} \equiv 84 \pmod{101}$ .

- c) (8 puntos) Ahora que ya tienen una clave acordada  $0 < k < 101$ , el agente X le pide que exprese la clave  $k$  en la forma  $k = 10a + b$  con  $0 \leq b < 10$  y le avisa que de ahora en más usted recibirá todos los mensajes cifrados con un criptosistema afín, usando como función de cifrado la función  $E(x) = ax + b \pmod{27}$  y utilizando la tabla de abajo para codificar cada caracter. Si usted recibe el mensaje cifrado PD, ¿Cuál es el mensaje original? (se cifran los mensajes letra por letra).

A	B	C	D	E	F	G	H	I	J	K	...	O	P	Q	R	...	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	...	15	16	17	18	...	23	24	25	26

**Solución:** Como  $k = 84$  entonces  $a = 8$ ,  $b = 4$ . La función de descifrado es  $D(y) = a^{-1}(y - b) \pmod{27}$ . Usando el AEE vemos que  $8^{-1} \equiv 17 \pmod{27}$ . Entonces para descifrar P que corresponde a 16 esto es  $17 \cdot (16 - 4) = 204 \equiv 15 \pmod{27}$  que corresponde a O. La D corresponde a 3 que cuando la desciframos es  $17(3 - 4) = -17 \equiv 10 \pmod{27}$  que corresponde a la letra K. Por lo tanto el mensaje descifrado es OK.