Segundo parcial - 4 de julio de 2014. Duración: 3 horas y media

N° de parcial	Cédula	Apellido y nombre	Salón

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	␣
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

Ejercicio 1.

a. Sea $n \in \mathbb{Z}^+$, y g un entero coprimo con n. Probar que si a es el orden de $\overline{g}$ en $U\left(n^2\right)$ y b es el orden de $\overline{g}$ en $U(n)$, entonces $b \mid a$.

b. Sea $p = 19$.

i) Probar que 10 es raíz primitiva módulo p.

ii) ¿Es 10 raíz primitiva módulo p^2? Pueden utilizar los siguientes datos: $10^5 \equiv 3 \pmod{p^2}$ y $3p^2 = 1083$.

iii) Para cada $k \in \mathbb{Z}^+$ hallar una raíz primitiva módulo $2p^k$.

Ejercicio 2.

a. Si $f : G \to K$ es un homomorfismo de grupos probar que $o(f(g)) \mid o(g)$ para todo $g \in G$.

b. En cada parte, hallar todos los homomorfismos $f : G \to K$ justificando debidamente.

i) $G = S_4$ con la composición como operación y $K = \mathbb{Z}_{35}$ con la suma de clases como operación.

ii) $G = \mathbb{Z}_{15}$ y $K = \mathbb{Z}_6$, ambos grupos con la suma de clases como operación.

Ejercicio 3. Sea G un grupo y $g \in G$ de orden finito. Probar que:

a. Si $k \in \mathbb{Z}^+$, entonces $o(g^k) = \dfrac{o(g)}{\operatorname{mcd}(o(g), k)}$.

b. Si $H = \langle g \rangle$, entonces existen $\varphi(o(g))$ elementos en H que generan H.

Ejercicio 4.

a. Ana y Bruno quieren acordar una clave común usando el protocolo Diffie-Hellman. Para ello eligen el primo $p = 1009$ y la raíz primitiva $g = 11$. Ana elige el número $m = 260$ le envía a Bruno el número 1005. Bruno elige el entero $n = 8$. ¿Cuál es la clave k común que acordaron Ana y Bruno?.

b. Ahora Ana quiere comunicarse con Bruno través de un sistema Vigenere donde la palabra clave consiste de 3 letras de la siguiente manera: se toma la clave k común acordada en la parte anterior y se la escribe en base 28:

$$k = L_2 28^2 + L_1 28 + L_0.$$

Luego la clave común resulta de sustituir en $L_2L_1L_0$ por sus respectivas letras (por ejemplo si $k = 25 \cdot 28^2 + 0 \cdot 28 + 2$ entonces la clave común será `YAC`).

i) Calcular la clave k como $L_2L_1L_0$.

ii) Usando la clave anterior descifrar el siguiente mensaje: `WUFAGHFCWÑKZBXHEÑ␣DXMUG`.

Ejercicio 5. Enunciar y demostrar el Teorema de Lagrange para grupos.