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

EXAMEN - 7 DE FEBRERO DE 2019. DURACIÓN: 210 MINUTOS

N° de examen	Cédula	Apellido y nombre

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 resultado visto en el curso, deben especificarlo enunciando el resultado que usan. Presentar una respuesta final a la pregunta sin justificación carece de validez.

Ejercicio 1.

a. Sean $(G, *, e)$ un grupo y sea $g \in G$. Definir orden de g en G (que se anota $\mathrm{o}(g)$ o bien $|g|$), sea finito o infinito.

b. Dados un grupo finito $(G, *)$, y elementos $x, y \in G$, tales que $xy = yx$, con $\mathrm{o}(x) = a$, $\mathrm{o}(y) = b$, m=mcm(a, b) y d=mcd(a, b), entonces, probar que $\mathrm{o}(xy)|m$, y que $\frac{m}{d}|\mathrm{o}(xy)$.

c. Considerar el grupo U(19) (también se usa la notación $\mathrm{U}(19) = \mathbb{Z}_{19}^*$) y calcular el orden de 4, 18 y 4×18, usando la parte anterior.

Ejercicio 2.

a. Definir cuándo dos enteros, $x, y \in \mathbb{Z}$ son congruentes módulo $n \in \mathbb{N}^*$.
Enunciar el Teorema de Euler y el Teorema de Fermat.

b. Sean p, a, b naturales tales que p es primo, $b \equiv 0$ mód$(p-1)$ y p no divide a a. Encontrar (en función de p) el menor natural x que satisface las siguientes condiciones:

$$a^b x^3 + 8x \equiv 5x^2 + 4 \text{ mód}(p);$$
$$x \not\equiv 1 \text{ mód}(p);$$
$$x > p.$$

(Sug.: Factorizar el polinomio: $g(x) = x^3 - 5x^2 + 8x - 4$).

c. Sea x el natural hallado en la parte anterior. Calcular $(x-p)^{10325}$ mód(35).

Ejercicio 3.

a. i) Definir raíz primitiva.

ii) Probar que 2 y 22 son raíces primitivas en U(53) (también se usa la notación $U(53) = \mathbb{Z}_{53}^*$).

b. Andrea y Basilio acuerdan comunicarse estableciendo una clave privada mediante el método de Diffie-Hellman. Deciden usar el módulo primo $p = 53$ y como base $g = 22$. Andrea elige el entero $m = 5$, enviándole a Basilio g^m mód(53), mientras que Basilio envía a Andrea $20 \equiv g^n$ mód(53).

i) ¿Cuál es la clave privada que acuerdan Andrea y Basilio?

ii) ¿Es la clave acordada una raíz primitiva en U(53)? Jusitfique su respuesta.

c. Andrea le envía a Basilio el siguiente mensaje:

LA GATA GATINA

Y Basilio le responde con un mensaje encriptado utilizando la clave hallada en b. i), y usando el método de cifrado César, con el alfabeto

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

EGRDMYWRDSMCCS

¿Cuál fue la respuesta de Basilio?