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

EXAMEN - 14 DE DICIEMBRE DE 2016 DURACIÓN: 3 HORAS Y MEDIA

N° de examen	Cédula	Nombre y apellido

Ejercicio 1.

a. Halle el menor entero positivo x tal que $\begin{cases} 5x - 3 \equiv 4 \pmod 7 \\ 4x + 2 \equiv 6 \pmod 9 \end{cases}$

b. Halle todas las parejas de enteros (a, b) tales que $a^2 + b^2 = 637$ y $\operatorname{mcd}(a, b) = \frac{x}{4}$ (x hallado en el ítem anterior).

Ejercicio 2.

a. Calcular todas las raíces primitivas de U(31). ¿Cuántas son?

b. Ordenar en forma creciente las raíces primitivas halladas en el ítem anterior: $r_1 < r_2 < r_3 < r_4 < \ldots$. Luego escribir la secuencia:

$(r_1{+}r_4), (r_6{-}r_1), (r_5{-}r_4), (r_3), (r_2{-}r_1), (r_8{-}r_3{+}r_1), (r_7{-}r_1), (r_8{+}r_1), (r_5{+}r_1), (r_2{-}r_1), (r_5{+}r_3{-}r_1), (r_8{-}r_6{-}r_1)$

c. Traducir la expresión anterior usando:

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

d. Utilizando el método de Vigenère decodificar el texto siguiente, usando la expresión clave hallada en el ítem anterior:

$$VLMWSCLHFIYTJQPMLF\text{␣}MT$$

Ejercicio 3.

a. Enunciar y demostrar el Teorema de Lagrange para grupos finitos.

b. Probar que todo grupo de orden p primo es cíclico.

c. Sea G un grupo y sean G_1 y G_2 dos subgrupos *distintos* de orden p primo.
¿Qué puede decir sobre $G_1 \cap G_2$?