

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

**Ejercicio 1.**

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

**Solución:** La primera ecuación es equivalente a  $5x \equiv 7 \pmod{7}$ , que tiene solución única módulo 7 pues  $\text{mcd}(5, 7) = 1$ . Es claro que  $x \equiv 0 \pmod{7}$  es solución.

La segunda ecuación es equivalente a  $4x \equiv 4 \pmod{9}$ , que tiene solución única módulo 9 pues  $\text{mcd}(4, 9) = 1$ . Es claro que  $x \equiv 1 \pmod{9}$  es solución.

Como  $\text{mcd}(7, 9) = 1$ , el sistema tiene solución única módulo  $7 \cdot 9$ . Se obtiene por el procedimiento estándar y es fácil verificar que  $x \equiv 28 \pmod{63}$  satisface ambas ecuaciones.

El menor entero positivo es entonces  $x = 28$ .

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

**Solución:** Como  $\text{mcd}(a, b) = 7$ , escribimos  $a = 7a_0$  y  $b = 7b_0$ . Sustituyendo en la primera ecuación resulta  $a_0^2 + b_0^2 = \frac{637}{49} = 13$ .

Calculando  $13 - i^2$  para  $i = 0, \dots, 3$  se determina que el único par de cuadrados que suman 13 es  $4 + 9$ . Considerando orden y signos encontramos ocho soluciones para  $(a_0, b_0)$ , a saber:  $\{(\pm 2, \pm 3), (\pm 3, \pm 2)\}$ .

Multiplicando por 7 obtenemos las parejas pedidas:

$$(14, 21), (14, -21), (-14, 21), (-14, -21), (21, 14), (21, -14), (-21, 14), (-21, -14)$$

**Ejercicio 2.**

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

**Solución:** Como 31 es primo,  $U(31)$  tiene 30 elementos y  $\varphi(30) = 8$  raíces primitivas.

Como  $2^5 \equiv 1 \pmod{31}$  sabemos que 2 no es raíz primitiva. Verificamos que  $3^{30/2} \equiv 30 \not\equiv 1 \pmod{31}$ ,  $3^{30/3} \equiv 25 \not\equiv 1 \pmod{31}$ ,  $3^{30/5} \equiv 16 \not\equiv 1 \pmod{31}$ , luego  $g = 3$  es una raíz primitiva.

Sabemos que todas las raíces primitivas serán de la forma  $g^i$  donde  $\text{mcd}(i, 30) = 1$ , es decir  $g, g^7, g^{11}, g^{13}, g^{17}, g^{19}, g^{23}, g^{29}$ .

Calculamos estas potencias módulo 31 obteniendo 3, 17, 13, 24, 22, 12, 11, 21.

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

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

**Solución:**  $r_1 = 3, r_2 = 11, r_3 = 12, r_4 = 13, r_5 = 17, r_6 = 21, r_7 = 22, r_8 = 24$ , y la secuencia es

$$16, 18, 4, 12, 8, 15, 19, 27, 20, 8, 26, 0.$$

- 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

**Solución:** PREMIOS\_TIZA

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

*VLMWSC LHF IY TJQP MLF \_ MT*

**Solución:** El texto cifrado corresponde a la secuencia

22, 11, 12, 23, 19, 2, 11, 7, 5, 8, 25, 20, 9, 7, 16, 12, 11, 5, 27, 12, 20.

Repetimos la expresión clave como la secuencia hallada en la parte b

16, 18, 4, 12, 8, 15, 19, 27, 20, 8, 26, 0, 16, 18, 4, 12, 8, 15, 19, 27, 20.

y restamos módulo 28 para obtener

6, 21, 8, 11, 11, 15, 20, 8, 13, 0, 27, 20, 21, 17, 12, 0, 3, 18, 8, 13, 0.

Traduciendo se obtiene el mensaje en claro

GUILLOTINA\_TU\_MADRINA

### Ejercicio 3.

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

**Solución:** Ver Teorema 3.8.1 en la página 55 de las notas del curso.

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

**Solución:** Sea  $G$  un grupo de orden  $p$  primo, y sea  $g \in G$  un elemento con  $g \neq e$  (que siempre existe pues  $p \geq 2$ ). El grupo  $\langle g \rangle$  generado por  $g$  es un subgrupo de  $G$  no trivial (porque  $g \neq e$ ).

Por el Teorema de Lagrange, el orden de  $\langle g \rangle$  divide a  $p$ ; como no es 1 debe ser  $p$ . Entonces  $\langle g \rangle = G$  y  $g$  es un generador de  $G$ .

En las notas esto aparece como parte 3 del Corolario 3.8.2.

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

**Solución:** Como  $G_1$  tiene orden primo y  $G_1 \cap G_2$  es un subgrupo de  $G_1$ , con el mismo razonamiento que en la parte anterior se deduce que el orden de  $G_1 \cap G_2$  es 1 o  $p$ . Si el orden de  $G_1 \cap G_2$  fuera  $p$  debería ser igual a  $G_1$ , pero también debería ser igual a  $G_2$ , lo que contradice  $G_1 \neq G_2$ .

Entonces  $G_1 \cap G_2$  es trivial.