EXAMEN DE MATEMÁTICA DISCRETA 2

Nombre	C.I.	No. de prueba .....

Duración: 4:00 horas. Sin material y sin calculadora.
Es necesario mostrar la resolución de los ejercicios, presentar únicamente la respuesta final carece de valor.

Ejercicio 1.

A. Sea G un grupo finito y $g, h \in G$.

(i) Probar que si $o(g) = n$ y $n = km$ con $k, m \in \mathbb{N}$, entonces $o(g^m) = k$

(ii) Probar que si $gh = hg$ y $\text{mcd}(o(g), o(h)) = 1$ entonces $o(gh) = o(g)o(h)$.

(iii) ¿Es cierto lo anterior si $gh \neq hg$? Probar o encontrar un contraejemplo.

B. Sea $b \in \mathbb{N}$ tal que $b^{280} \equiv 400 \,(\text{mód } 401)$ y $b^{16} \equiv 39 \,(\text{mód } 401)$.

(i) Probar que el orden de $\overline{b}$ en $U(401)$ es 80.

(ii) Con el dato adicional de que el orden de $\overline{2}$ en $U(401)$ es 200, hallar un par de enteros $x, y \in \mathbb{Z}$ tales que $2^x b^y$ es raíz primitiva módulo 401. *(No es necesario probar que $o(\overline{2}) = 200$).*

Ejercicio 2.

A. Hallar todos los pares de naturales (a, b) que verifican que $ab = 21\,\text{mcd}(a, b)$ y $a \equiv \text{mcd}(a, b)$ (mód b).

B. Investigar si los siguientes sistemas tienen solución entera, y en caso de tenerla, hallar todas las soluciones:

(i) $\begin{cases} x \equiv 34 \pmod{49} \\ x \equiv 11 \pmod{21} \\ x \equiv 7 \pmod{9} \end{cases}$ **(ii)** $\begin{cases} x \equiv 20 \pmod{49} \\ x \equiv 13 \pmod{21} \\ x \equiv 7 \pmod{9} \end{cases}$

Ejercicio 3. Sean p y q dos primos distintos y $n = pq$. Sea $e \in \mathbb{N}$ tal que $\text{mcd}(e, \varphi(n)) = 1$ y $E : \mathbb{Z}_n \to \mathbb{Z}_n$ la función de encriptado utilizada en el sistema RSA con clave (n, e); es decir $E(x) = x^e$ (mód n).

A. Probar que si $ed \equiv 1$ (mód $\varphi(n)$), entonces la función $D : \mathbb{Z}_n \to \mathbb{Z}_n$ dada por $D(y) = y^d$ (mód n) desencripta.

B. Sean $p = 41$ y $q = 47$ y $n = pq$.

(i) Si $e = 459$, probar que $\text{mcd}(\varphi(n), e) = 1$ y hallar la función de desencriptado D.

(ii) Hallar los restos de dividir 494^{459} entre 41 y entre 47.

(iii) Hallar $E(494)$ (perteneciente a $\{0, 1, 2, \cdots, n-1\}$).
(Sugerencia: utilizar la parte (ii). Puede resultarle útil que $47 \times 7 - 41 \times 8 = 1$).