

Nro de prueba	Cédula	Apellido y nombre

Ejercicios de múltiple opción

Ejercicio 1	Ejercicio 2

Ejercicio 1 (10 puntos) Sea $0 \leq m < 297$ tal que $m \equiv 108^{132} \pmod{297}$. Indicar cuál de las opciones es correcta:

- A. $m = 135$.
B. $m = 27$.
C. $m = 108$.
D. $m = 81$.

Ejercicio 2 (10 puntos) Sean $n = 341$ y $e = 13$. Para los datos anteriores sea la función de descifrado $D : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ definida por el protocolo RSA. Indicar cuál de las opciones es correcta:

- A. $D(y) = y^{12} \pmod{n}$
B. $D(y) = y^{277} \pmod{n}$
C. $D(y) = y^{105} \pmod{n}$
D. $D(y) = y^{157} \pmod{n}$

Ejercicios de desarrollo

Ejercicio 3 (40 puntos)

- Dado $n \in \mathbb{N}$, definir congruencia módulo n .
- Sea $n = 10x + y$, probar que $n \equiv 0 \pmod{7}$ si y solo si $x - 2y \equiv 0 \pmod{7}$.
- Enunciar el Teorema Chino del Resto y demostrarlo solo para el caso de dos ecuaciones.
- Hallar el menor par $x > 199$ que cumpla $2x + 3 \equiv 4 \pmod{5}$ y $3x + 4 \equiv 3 \pmod{7}$.

Ejercicio 4 (40 puntos)

- Definir morfismo de grupos.
- Enunciar y demostrar el Teorema de órdenes.
- Dado un número primo **impar** p se define $f : U(p) \rightarrow U(p)$ la función dada por $f(\bar{x}) = \bar{x}^2$.
 - Probar que f es un morfismo de grupos.
 - Calcular el núcleo de f para $p = 3, 5$ y 7 .
 - Calcular el núcleo de f en general y deducir cuantos elementos tiene la imagen de f .