Universidad de la República **Matemática Discreta 2**
Facultad de Ingeniería
Instituto de Matemática y Estadística

EXAMEN- 23 DICIEMBRE 2023.

Cédula de identidad	APELLIDO, Nombre	Número de lista

1	2	3	4	5	6

Versión 2.

Ejercicios de respuesta verdadero (V) o falso (F):
(Cada ejercicio vale: 5 puntos, respuesta incorrecta resta 3 puntos.)

Ejercicio 1.
Sea G un grupo tal que $|G| = 45$. Existe $g \in G$, $g \neq e$, tal que: $g = g^{-1}$.

Ejercicio 2.
Sean a, m, k y n enteros positivos. Si $m \equiv k \pmod{\varphi(n)}$ entonces $a^m \equiv a^k \pmod{n}$.

Ejercicio 3.
El conjunto de números enteros que al dividirlos simultaneamente por 2 y 3 me dan resto 1 es exactamente el conjunto $\{x \in \mathbb{Z} : x = 1 + 6k, k \in \mathbb{Z}\}$.

Ejercicio 4.
El criptosistema de clave pública RSA es muy útil porque una vez que conocemos el valor $\varphi(n)$ no existe un algoritmo que encuentre la función de descifrado (que es equivalente a encontrar el inverso de e módulo $\varphi(n)$).

Ejercicios de respuesta múltiple opción:
(Cada ejercicio vale: 15 puntos, respuesta incorrecta resta 3 puntos.)

Ejercicio 5. El resto de dividir 7^{77} entre 200 es:

(A) 0.

(B) 1.

(C) 7.

(D) Ninguna de las anteriores.

Ejercicio 6.

Sean a y b enteros positivos. Considere las siguientes proposiciones:

(i) Si m es un número primo divisor de a que no divide a b y n un número primo divisor de b que no divide a a, entonces $\mathrm{mcd}(\frac{a}{m}, b) = \mathrm{mcd}(a, \frac{b}{n})$.

(ii) Si m es un divisor de a que no divide a b y n un divisor de b que no divide a a, entonces $\mathrm{mcd}(\frac{a}{m}, b) = \mathrm{mcd}(a, \frac{b}{n})$.

Entonces elija la opción correcta:

(A) sólo (i) es verdadera

(B) sólo (ii) es verdadera

(C) las dos son verdaderas

(D) las dos son falsas

Preguntas de respuesta por desarrollo escrito:

- **Pregunta 1:** (25 puntos)

  Sean $n, a \in \mathbb{Z}$ tales que $\mathrm{mcd}(a, n) = 1$, entonces demostrar que $a^{\varphi(n)} \equiv 1 \pmod{n}$.

  (No se puede demostrar como corolario del teorema de Lagrange).

- **Pregunta 2:** (25 puntos)

  a) Defina homomorfismo de grupos y orden de un elemento.

  b) Pruebe que si G y H son grupos finitos, $g \in G$ y $\varphi : G \to H$ es un homomorfismo de grupos entonces el orden de $\varphi(g)$ divide al orden de g.