

EXAMEN – LUNES 17 DE JULIO DE 2023

Nro de Lista	Cédula	Apellido y nombre

Escribir nombre y cédula en todas las hojas que se entreguen. Deben justificar todas sus respuestas.

Ejercicio 1. (24 puntos)

- a) (4 puntos) Enuncie la igualdad (o identidad) de Bézout.
- b) (12 puntos) Enuncie y pruebe el Lema de Euclides para enteros coprimos.
- c) (8 puntos) Pruebe que $\sqrt[3]{4}$ es irracional.

Ejercicio 2. (30 puntos)

- a) (14 puntos) Sean a, b, c enteros no nulos con $\text{mcd}(a, b) = 1$. Pruebe que la ecuación diofántica $ax + by = c$ tiene infinitas soluciones y determínelas en función de un parámetro $t \in \mathbb{Z}$.
- b) (8 puntos) Considere el conjunto $S = \{(3 + 13t, 4 + 18t) : t \in \mathbb{Z}\}$. Encuentre a, b y c enteros no nulos con $\text{mcd}(a, b) = 1$ tales que se verifique: $(x, y) \in S \Leftrightarrow ax + by = c$ (en otras palabras, S debe ser el conjunto solución de la diofántica $ax + by = c$).
- c) (8 puntos) Encuentre todos los $(x, y) \in S$ que verifiquen el siguiente sistema:
$$\begin{cases} x \equiv 1 \pmod{18}, \\ y \equiv 2 \pmod{13}. \end{cases}$$

Ejercicio 3. (30 puntos) Sea $n \geq 2$ un entero.

- a) (4 puntos) Probar que si $d|n$ y $d < n$ entonces existe un primo $p|n$ tal que d divide a $\frac{n}{p}$.
- b) Sea (G, \cdot) un grupo con neutro e y $g \in G$ que verifica $g^n = e$.
 - i) (8 puntos) Probar que $o(g)$ divide a n .
 - ii) (8 puntos) Probar que si $g^{\frac{n}{p}} \neq e$ para todo primo $p|n$ entonces $o(g) = n$.
- c) (10 pts) Sea $g \in \mathbb{Z}$ con $1 < g < 46$. Probar que si $47 \nmid g^{23} - 1$ entonces g es raíz primitiva mód. 47.

Ejercicio 4. (16 puntos)

- a) (8 puntos) Describa el criptosistema RSA y explique porque se considera seguro cuando los primos p y q están bien elegidos.
- b) (8 puntos) Describa un posible ataque al RSA cuando los primos p y q están muy próximos (en el caso de describir un método/algoritmo estime el costo del mismo).

ESCRIBA AQUI SU DESARROLLO...