

Nº de examen	Cédula	Apellido y nombre

Para cada pregunta o ejercicio, deben presentar claramente el razonamiento y cálculos realizados para obtener su respuesta final. Si una implicancia es válida debido a algún teorema, proposición o propiedad, deben especificarlo (nombre del teorema, lema, etc.) Presentar una respuesta final a la pregunta sin justificación carece de validez.

### Ejercicio 1.

- a. Sean  $0 \neq a, b \in \mathbb{Z}$ , probar que

$$\text{mcd}(a, b) = \min\{s > 0 : s = ax + by \text{ con } x, y \in \mathbb{Z}\}.$$

- b. Sean  $a, b \in \mathbb{Z}$ , probar que la ecuación diofántica  $ax + by = c$  tiene solución si y solo si  $\text{mcd}(a, b) | c$ .

- c. Hallar todas las soluciones módulo 62 de la ecuación

$$26 \equiv 262 \pmod{62}.$$

### Ejercicio 2.

- a. Resolver los siguientes sistemas de congruencias:

$$\text{i) } \begin{cases} x \equiv 0 \pmod{11} \\ x \equiv 8 \pmod{17} \end{cases} \quad \text{ii) } \begin{cases} x \equiv 33 \pmod{44} \\ x \equiv 25 \pmod{34} \end{cases}$$

- b. Sean  $p$  y  $q$  dos primos distintos. Describir el criptosistema RSA usando  $p$  y  $q$  (especificar cuáles datos son públicos y cuáles privados y definir las funciones  $E$  y  $D$  de cifrado y descifrado respectivamente).

- c. Probar que en el criptosistema RSA, la función de descifrado  $D$  es la función inversa de la función de cifrado  $E$ .

- d. Mostrar con un ejemplo por qué, en el sistema RSA, es necesario que los primos  $p$  y  $q$  sean distintos.

- e. Con los primos 11 y 17 utilizar el criptosistema RSA con  $e = 171$  para cifrar el número  $x = 121$ .

### Ejercicio 3.

- a. Definir grupo.

- b. Sea  $(G, \times)$  un grupo, probar que el neutro es único.

- c. Sea  $(G, \times)$  un grupo y  $g \in G$ , probar que el inverso de  $g$  es único.

- d. Sean  $G$  y  $K$  dos grupos y  $f : G \rightarrow K$  un homomorfismo. Probar que si  $g \in G$  es un elemento de orden finito entonces

$$o(f(g)) \mid o(g).$$

- e. Hallar todos los homomorfismos  $f : U(13) \rightarrow \mathbb{Z}_9$  (sugerencia: hallar una raíz primitiva módulo 13).