# Teoría de Números 2025

Lista 06

27.octubre.2025

Responder a las siguientes preguntas. En cada caso ilustre su explicación con un ejemplo o contraejemplo concreto.
Proporcione referencias en cada respuesta.

1. Explique qué es un pseudoprimo, y qué es un pseudoprimo en base $a$?

2. ¿Qué hay mas: primos o pseudoprimos? Proporcione evidencia de su respuesta.

3. Explique cómo funciona el test de primalidad y haga una implementación computacional con ejemplos.

4. Explique cómo funciona el método de intercambio de llaves de Diffie-Hellman.
   ¿Cuál es la práctica recomendada por el estándar RFC 7919 para Diffie-Hellman? ¿Por qué?

5. ¿Cuál es la diferencia principal de la criptografía de curvas elípticas y cómo se compara el RSA de curvas elípticas, en contraste con el RSA tradicional?

6. En sus palabras, ¿cuál es la importancia de la teoría de números en la criptografía moderna?

7. ¿Cuál es la relación entre el algoritmo de Euclides y la fracción continua de un racional? Dé ejemplos.