

Teoría de Números 2024

Corto 03

18.noviembre.2024

1. **(2.5 puntos).**

Mario y Jorge, en sus respectivos seminarios, nos hablaron sobre algunos mecanismos criptográficos y de cifrado de la información.

- ¿Cuál es la diferencia principal de la criptografía de curvas elípticas y cómo se compara RSA de curvas elípticas, en contraste con el RSA tradicional?
- En sus palabras, ¿cuál es la importancia de la teoría de números en la criptografía moderna?

2. **(2.5 puntos).**

En la charla *Una pequeñísima introducción a los números p -ádicos*, Ximena nos explicó detalles de estos cuerpos numéricos.

- Mencione dos motivaciones o aspectos por los cuales puede ser importante estudiar los números p -ádicos.
- ¿Qué analogías y diferencias puede ver entre los números p -ádicos y el sistema base 10 usual?

3. **(2.5 puntos).**

La conferencia de Luis, sobre la criba de Atkin-Berstein, introdujo un aspecto computacional importante en la teoría de números.

- ¿Qué ventajas o desventajas ve en usar la criba de Atkin-Berstein para determinar si $n > 1$ es primo, comparado contra otros tests de primalidad?
- ¿Se podría usar la criba de Atkin-Berstein para encontrar pares de primos gemelos? Opine.

4. **(2.5 puntos).**

Gaby nos habló sobre el método de Karatsuba, conocido también como el método de multiplicación rápida.

- Muestre que la complejidad del algoritmo de Karatsuba es $O(n^{\log_2 3})$.
 - Desde el punto de vista histórico, ¿por qué es importante este método?
 - ¿Por qué es importante desde una perspectiva computacional?
-