

Teoría de Números 2023

Tópicos Sugeridos para Seminario

23.octubre.2023

A continuación se listan algunos tópicos que pueden servir como temas para el seminario de fin de curso.

1. Cribas (e.g. *Quadratic Sieve*, Sundaram, Atkin, Pritchard, ...)
2. Los problemas de Landau (historia y situación actual).
3. Algoritmo de Tonelli-Shanks para hallar raíces módulo p .
4. Teoría e índices y logaritmo discreto (Método de Pollard, Método *Kangaroo* de Pollard).
5. Factoración de enteros (método $\rho - 1$ de Pollard, método $p + 1$ de Williams, ...)
6. Test de primalidad: (e.g. Miller-Rabin, Solovay-Strassen, Lucas-Lehmer, Frobenius, ...)
7. Otros test de primalidad: (e.g. AKS, Baillie-PSW, Pocklington, ...).
8. Aplicaciones en criptografía: RSA, ElGamal.
9. Multiplicación rápida: Algoritmo de Karatsuba.
10. Factoración cuántica: Algoritmo de Shor.
11. Números p -ádicos.
12. Aritmética de curvas elípticas.
13. Puntos racionales sobre curvas elípticas.
14. La función P de Weiestrass.
15. Solución de el último teorema de Fermat.
16. Avances en la solución de la conjetura de Goldbach (situación actual).
17. La función zeta de Riemann (situación actual).
18. Formas modulares.
19. El grupo Monstruo y la conjetura Monstrous Moonshine.
20. Software y lenguajes para calcular en Teoría de Números.
21. Aspectos históricos o personajes importantes en teoría de números.

Son apenas sugerencias. Si ustedes tienen alguna otra temática de interés para el curso, la pueden proponer como .

Fechas importantes:

Elección de tema	jueves 02 de noviembre
Entrega de presentación (borrador)	domingo 12 de noviembre
Presentaciones	del 16 al 23 de noviembre

Entregables:

- Presentación en formato .pdf. Código utilizado (en el caso que implementen algoritmos).