

Teoría de Números 2024

Tópicos Sugeridos para Seminario

30.septiembre.2024

A continuación se listan algunos tópicos que han surgido dentro del curso o temas que no vamos a cubrir que pueden servir como temas para su seminario.

1. Criba de Atkin y otras cribas.
2. Los problemas de Landau.
3. Teoría e índices y logaritmo discreto.
4. Algoritmo de Tonelli-Shanks.
5. Método de Pollard para logaritmo discreto.
6. Método *Kangaroo* de Pollard.
7. Ecuación de Markov.
8. Números p-ádicos
9. Test de primalidad: (e.g. Miller-Rabin, Solovay-Strassen, Lucas-Lehmer)
10. Otros test de primalidad: (e.g. AKS, Baillie-PSW).
11. Aplicaciones en criptografía: Diffie-Hellman, RSA y ElGamal.
12. Multiplicación rápida: Algoritmo de Karatsuba.
13. Factoración cuántica: Algoritmo de Shor.
14. Aritmética de curvas elípticas.
15. Puntos racionales sobre curvas elípticas.
16. La función P de Weiestrass.
17. Solución del último teorema de Fermat.
18. Avances en la solución de la conjetura de Goldbach.
19. La función zeta de Riemann.
20. Formas modulares.
21. El grupo Monstruo y la conjetura Monstrous Moonshine.
22. Software y lenguajes para calcular Teoría de Números.
23. Temas en teoría analítica de números.
24. Temas en teoría algebraica de números.
25. Aspectos históricos o personajes importantes en teoría de números.

Los temas anteriores son apenas sugerencias. Como es habitual, los temas no se limitan sólo a estos, y si ustedes tienen alguna otra temática de interés para el curso, la pueden proponer como tema del seminario.

Fechas importantes:

Elección de tema	viernes 18 de octubre
Entrega de presentación (borrador)	viernes 08 de noviembre
Presentaciones	del 11 al 22 de noviembre