

# Teoría de Números 2022

## Tópicos Sugeridos para Seminario

29.septiembre.2022

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. Teoría algebraica de números. Sí pero ¿cuál?
10. Test de primalidad: (e.g. Miller-Rabin, Solovay-Strassen,
11. Otros test de primalidad: (e.g. AKS).
12. Aplicaciones en criptografía: Diffie-Hellman, RSA y ElGamal.
13. Multiplicación rápida: Algoritmo de Karatsuba.
14. Factoración cuántica: Algoritmo de Shor.
15. Aritmética de curvas elípticas.
16. Puntos racionales sobre curvas elípticas.
17. La función  $P$  de Weiestrass.
18. Solución de el último teorema de Fermat.
19. Avances en la solución de la conjetura de Goldbach.
20. La función zeta de Riemann.
21. Formas modulares.
22. El grupo Monstruo y la conjetura Monstruos Moonshine.
23. Software y lenguajes para calcular TN.
24. 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	jueves 27 de octubre
Entrega de informe y presentación (borrador)	viernes 18 de noviembre
Presentaciones	del 21 al 25 de noviembre