Teoría de Números

grupo CF02

19 de enero al 15 de abril del 2026

PROFESOR: **Mario Pineda Ruelas**. Oficina en el edificio AT- 338. Correo electrónico mpr.zqrc@gmail.com

HORARIO Y SALÓN DE CLASE: Lunes (B203), miércoles (B102) y jueves (C117) de 10 a 12 hrs.

ASESORIAS: Consultas con previa cita o desde el correo electrónico. También te sugiero que al inicio de cada clase puedes plantear tus dudas y así compartimos la respuesta con tus compañeros del curso.

OBJETIVO DEL CURSO: Estudio de las soluciones de polinomios lineales y cuadráticos con coeficientes en un campo finito de cardinalidad p, donde p es un número primo impar. Para ésto, debemos estudiar la teoría de divisibilidad en $\mathbb{Z}$, teoría de residuos y la ley de reciprocidad cuadrática.

Temario del curso

(1) **El anillo de los enteros**

- Grupos y anillos.
- Inducción y Principio del Buen orden en $\mathbb{Z}$. Algoritmo de la división en el anillo $\mathbb{Z}$.
- Máximo común divisor y mínimo común múltiplo.
- Puntos enteros sobre rectas en $\mathbb{R}^2$.
- Números primos y Teorema Fundamental de la Aritmética.
- Reflexiones sobre la factorización no única.

(2) **Congruencias.**

- El anillo $\mathbb{Z}/m\mathbb{Z}$.
- Suma y producto en el anillo $\mathbb{Z}/m\mathbb{Z}$.
- Sistemas completos de residuos (SCR), sistemas reducidos de residuos (SRR) y la función φ de Euler.
- El grupo de unidades de $\mathbb{Z}/m\mathbb{Z}$.
- Campos finitos con p elementos.
- Teorema de Euler.
- El Pequeño Teorema de Fermat y el orden de un elemento en un grupo.

(3) **Congruencias especiales.**

- Solución de la congruencia lineal en un campo finito.
- Solución de sistemas de congruencias lineales.
- Teorema Chino del Residuo.
- Propiedades de la función φ de Euler.
- **Criptografía.**

(4) **Cuadrados en un campo finito.**

- Solución de la congruencia $ax^2 + bx + c \equiv 0$ en $\mathbb{Z}/p\mathbb{Z}[x]$.
- Símbolo de Legendre y sus propiedades aritméticas.
- Lema de Gauss y Lema de Jacobi.
- Ley de Reciprocidad Cuadrática de Gauss.

Bibliografía

1. Pineda-Ruelas, M. *Enteros, aritmética modular y grupos finitos.* Universidad Autónoma Metropolitana, Colección CBI 2015.
2. Cualquier libro de teoría de números elemental que encuentres en la biblioteca...hay muchos.

Calificación final: Tres evaluaciones parciales con solo una reposición o examen global. Para acreditar el curso deberás aprobar las tres evaluaciones y tu calificación será el promedio de las tres. Si repruebas algún examen parcial podrás reponerlo en la fecha del global y no tendrás derecho a global. Tu calificación final será el promedio de los tres exámenes parciales aprobados, en el segundo caso, tu calificación será lo que obtengas en el examen global. La escala es $[6,\ 7.5) = \mathbf{S}$; $[7.5,\ 8, 5) = \mathbf{B}$; $8.5 \to \infty = \mathbf{MB}$.

Te recuerdo que el curso es una materia optativa del plan de estudios de la Licenciatura en Matemáticas, así que llegas por tu propio gusto, no estarás en contra de tu voluntad y por tanto, espero que disfrutes los temas.