Electivo de Básico:
Números, Grupos y Códigos.

Profesora: Anita Rojas

Requisitos: Mínimo: Álgebra y Geometría I. Máximo: Estructuras algebraicas.

Horario: Martes y Miércoles 10.15 a 11.45. Sala de Física-Matemáticas.

Contenidos

En este curso se cubrirá material introductorio respecto de *Criptografía* (envío de mensajes secretos) y Corrección de errores (agregar redundancia a un mensaje de tal forma que se permita detección y/o corrección de errores).

Los tópicos que se revisarán incluyen: teoría elemental de números, lo que se aplicará a códigos de llave pública, e introducción a la teoría de grupos, los que se aplicarán a la detección de errores. En el curso se pondrá especial enfasis en la escritura de demostraciones y lenguaje matemático. Se revisarán temas como: Inducción matemática, números primos, Teorema de Factorización única, clases de congruencias, entre otros.

Metodología

El curso se basará en el libro *Numbers, Groups and Codes,* de J. F. Humphreys and M. Y. Prest. Se espera estimular el uso de programas computacionales como GAP, SAGE y MAGMA.

Evaluación

1. Tareas regulares: Se asignarán cada 1 o 2 semanas. Entrega por escrito, en grupos de a 3, exposición de algunos problemas.
2. 2 pruebas: Semana del 12 de Noviembre y Semana del 10 de Diciembre.

Ponderación

$$P * 0{,}6 + T * 0{,}4,$$

donde P es el promedio de las pruebas y T el de tareas.

Bibliografía

- J. F. Humphreys and M. Y. Prest. Numbers, Groups and Codes (libro guía).