

NOMBRE: **TEORÍA DE NÚMEROS.**

HRS./SEM.: 4

CLAVE: M11

Objetivo: Profundizar en el estudio de los números enteros en forma algebraica y enseñar la importancia de este estudio en diversas áreas aplicadas como la teoría de códigos.

1. *Los enteros.* Repaso de buen orden, divisibilidad y números primos; representación de enteros en distintas bases, operaciones de números en computadora; máximo común divisor, algoritmo de Euclides, teorema de factorización única y ecuaciones diofantinas lineales; números de Fermat.
2. *Congruencias.* Repaso de congruencias; congruencias lineales; teorema chino del residuo y sistemas de congruencias lineales; teorema pequeño de Fermat; teorema de Wilson; pseudo-primos; teorema de Euler.
3. *Criptografía.* Códigos de caracteres, códigos de bloques, códigos de exponenciales, criptografía de clave pública; códigos de Knapsack.
4. *Temas opcionales (al menos uno de los siguientes).*
 - Aplicaciones de congruencias, Criterios de divisibilidad; calendario perpetuo; torneos “todos contra todos”; almacenamiento de archivos en computadora y funciones “de hashing”.
 - Raíces primitivas. El orden de un entero y raíces primitivas; existencia de raíces primitivas para primos; el índice aritmético; número pseudo-aleatorias.
 - Reciprocidad cuadrática. Residuos cuadráticos; símbolo de Legendre, teorema de reciprocidad cuadrática, símbolo de Jacobi.
 - Teorema de inversión de Möbius, funciones multiplicativas

Requisitos:

- Álgebra Superior I

Bibliografía.

- [1]. Jones B., *Teoría de Números*, Trillas.
[2]. Niven I. Y Zuckerman H., *Introducción a la Teoría de los Números*, Editorial Limusa-Wiley.
[3]. Rosen K.H., *Elementary Number Theory and Its Applications*, Addison-Wesley, 1985.
[4]. Vinogradov I., *Fundamentos de la Teoría de los Números*, Editorial Mir, 1987.

Técnicas de enseñanza sugeridas

Exposición oral	(X)
Exposición audiovisual	()
Ejercicios dentro de clase	(X)
Seminarios	()
Lecturas obligatorias	()
Trabajos de investigación	()
Prácticas en taller o laboratorio	()
Prácticas de campo	()
Otras: Empleo de programas de cómputo	(X)

Elementos de evaluación sugeridos

Exámenes parciales	(X)
Exámenes finales	(X)
Trabajos y tareas fuera del aula	(X)
Participación en clase	(X)
Asistencia a prácticas	()
Otras:	()