UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE CIENCIAS MATEMÁTICAS

SÍLABO

1. INFORMACIÓN GENERAL

1.1 Curso	:	Teoría de números
1.2 Código	:	MA281
1.3 Programa Académico	:	Computación Científica
1.4 Créditos	:	2
1.5 Prerrequisitos	:	MA100. Matemática Básica. (1^{er} Sem)
1.6 Tipo de curso	:	Obligatorio
1.7 Área de Estudios	:	Estudios Generales
1.8 Número de Semanas	:	16
1.9 Horas por semana	:	1 HT; 2 HP;
1.10 Ciclo	:	I
1.11 Modalidad de aprendizaje	:	Presencial
1.12 Periodo Académico	:	2026-I
1.13 Inicio del semestre	:	
1.14 Fin del semestre	:	

2. PROFESORES

Atención previa coordinación con el profesor

3. INTRODUCCIÓN AL CURSO

La Teoría de Números es una rama fundamental de las matemáticas puras que estudia las propiedades de los números enteros, siendo la base de múltiples aplicaciones en matemática computacional, criptografía y teoría de la información. Este curso proporciona al estudiante las herramientas teóricas y algorítmicas para analizar problemas de divisibilidad, primalidad, congruencias y ecuaciones diofánticas, desarrollando un pensamiento lógico-abstracto riguroso. El enfoque computacional permite implementar y validar los conceptos teóricos, sentando las bases para áreas como la criptografía de clave pública y los algoritmos de factorización.

4. OBJETIVOS

- Comprender y aplicar los principios fundamentales de la divisibilidad, el algoritmo de Euclides y el teorema fundamental de la aritmética.
- Analizar y resolver problemas de congruencias lineales y sistemas de congruencias utilizando el Teorema Chino del Resto.
- Estudiar las funciones aritméticas básicas y sus aplicaciones en la distribución de números primos.
- Introducir los conceptos de residuos cuadráticos y la ley de reciprocidad cuadrática, comprendiendo su importancia teórica.
- Implementar algoritmos numéricos básicos (Euclides, primalidad, exponenciación modular) para validar los conceptos teóricos.

5. RESULTADOS DEL ESTUDIANTE

ABET-1) Habilidad para identificar, formular y resolver problemas técnicos o científicos ampliamente definidos mediante la aplicación de conocimientos de matemáticas y ciencias y/o temas técnicos en áreas relevantes para la disciplina. (Usage)

6. TEMAS

Unidad 1: Divisibilidad y Congruencias (16 horas)	
Resultados esperados: ABET-1	
Temas	**Aprendizaje esperado (*Learning Outcomes*)**
▪ Axiomas de los números enteros: Principio de Buena Ordenación e Inducción Matemática. ▪ Divisibilidad: Algoritmo de la División, Máximo Común Divisor (Algoritmo de Euclides extendido) y lema de Bézout. ▪ Números primos y compuestos. Teorema Fundamental de la Aritmética. Infinidad de primos. ▪ Congruencias: definición, propiedades algebraicas y clases residuales módulo n. ▪ Aplicaciones computacionales: implementación del algoritmo de Euclides y pruebas de primalidad básicas.	▪ Comprender los axiomas fundamentales de los números enteros y la técnica de demostración por inducción [Familiarizarse]. ▪ Utilizar el algoritmo de Euclides extendido para calcular el máximo común divisor y la identidad de Bézout [Usar]. ▪ Demostrar propiedades básicas de números primos y congruencias, aplicándolas en problemas elementales [Evaluar].
Lecturas : [**Rosen2011**], [**Apostol1976**]	

Unidad 2: Ecuaciones Diofánticas y Teorema Chino del Resto (16 horas)	
Resultados esperados: ABET-1	
Temas	**Aprendizaje esperado (*Learning Outcomes*)**
▪ Ecuaciones diofánticas lineales: condiciones de solubilidad y método de solución general. ▪ Teorema Chino del Resto para sistemas de congruencias lineales con módulos coprimos. ▪ Aritmética modular: anillo $\mathbb{Z}_n$, unidades y divisores de cero. ▪ Teoremas de Fermat y Euler. Función ϕ de Euler y sus propiedades. ▪ Aplicaciones en criptografía básica: cifrado César y fundamentos de RSA.	▪ Identificar las condiciones de existencia de soluciones para ecuaciones diofánticas lineales [Familiarizarse]. ▪ Aplicar el Teorema Chino del Resto para resolver sistemas de congruencias y problemas de calendario [Usar]. ▪ Utilizar los teoremas de Fermat y Euler para simplificar cálculos de potencias modulares y analizar estructuras algebraicas básicas [Evaluar].
Lecturas : [**Rosen2011**], [**Burton2011**]	

Unidad 3: Funciones Aritméticas y Teoría de Números Multiplicativa (16 horas)	
Resultados esperados: ABET-1	
Temas	**Aprendizaje esperado (*Learning Outcomes*)**
▪ Funciones aritméticas: Definición y ejemplos (tau, sigma, phi, mu). ▪ Convolución de Dirichlet y la fórmula de inversión de Möbius. ▪ Números perfectos, amigos y abundantes. Conjeturas abiertas. ▪ Ordenes y raíces primitivas módulo un primo. ▪ Logaritmos discretos: definición y aplicaciones en protocolos de intercambio de clave (Diffie-Hellman).	▪ Reconocer las propiedades de las funciones aritméticas más importantes [Familiarizarse]. ▪ Aplicar la inversión de Möbius para resolver problemas de conteo en teoría de números [Usar]. ▪ Calcular órdenes y raíces primitivas, relacionándolas con la estructura cíclica de $\mathbb{Z}_p^*$ [Evaluar].
Lecturas : [**Apostol1976**], [**Nathanson2000**]	

Unidad 4: Residuos Cuadráticos y Aplicaciones Computacionales (16 horas)	
Resultados esperados: ABET-1	
Temas	**Aprendizaje esperado (*Learning Outcomes*)**
▪ Residuos cuadráticos y no cuadráticos. Símbolo de Legendre y sus propiedades. ▪ Ley de Reciprocidad Cuadrática. Demostración y aplicaciones en el cálculo del símbolo de Legendre. ▪ Símbolo de Jacobi y su uso en tests de primalidad probabilísticos. ▪ Introducción a los tests de primalidad: Test de Miller-Rabin. ▪ Factorización de enteros: método $p-1$ de Pollard y nociones del algoritmo RSA.	▪ Determinar si un número es residuo cuadrático módulo un primo utilizando el símbolo de Legendre [Familiarizarse]. ▪ Aplicar la Ley de Reciprocidad Cuadrática para calcular símbolos de Legendre y Jacobi de manera eficiente [Usar]. ▪ Implementar algoritmos básicos de prueba de primalidad y factorización, analizando su complejidad y limitaciones [Evaluar].
Lecturas : [**Rosen2011**], [**Hoffstein2008**]	

7. PLAN DE TRABAJO

7.1 Metodología

Se fomenta la participación individual y en equipo para exponer sus ideas, motivándolos con puntos adicionales en las diferentes etapas de la evaluación del curso.

7.2 Sesiones Teóricas

Las sesiones de teoría se llevan a cabo en clases magistrales donde se realizarán actividades que propicien un aprendizaje activo, con dinámicas que permitan a los estudiantes interiorizar los conceptos.

7.3 Sesiones Prácticas

Las sesiones prácticas se llevan en clase donde se desarrollan una serie de ejercicios y/o conceptos prácticos mediante planteamiento de problemas, la resolución de problemas, ejercicios puntuales y/o en contextos aplicativos.

8. SISTEMA DE EVALUACIÓN

********* EVALUATION MISSING ********

9. BIBLIOGRAFÍA BÁSICA