Universidad de los Andes
Facultad de Ciencias

DEPARTAMENTO DE MATEMÁTICAS

OFRECIMIENTOS DE CURSOS

2021-10

Nivel del Curso 4: posgrado ___ 3: final de carrera ___ 2: mitad de carrera ___ 1: inicio de carrera _X__	**Nombre completo del curso en español**: Teoría de números
	Nombre completo del curso en inglés: Number theory
	Nombre abreviado en español (Máx. 30 caracteres contando espacios) Teoría de números
	Profesor: César Galindo

Descripción del curso en español:

Este curso es una introducción a algunas de los principales resultados, preguntas e ideas de la teoría de números clásica. Comenzaremos adquiriendo conocimiento de las herramientas y conceptos básicos en Teoría de Números tales como enteros, primos, divisibilidad, GCD, congruencias, teorema de Wilson y Fermat, pseudoprimos y funciones multiplicativas (como la función phi de Euler). Después, pasaremos a temas más avanzados, como criptografía y Seguridad informática, residuos cuadráticos, fracciones continuas. Estudiaremos aspectos computacionales y algorítmicos de cada tema según corresponda.

Descripción del curso en inglés:

This course is an introduction to some of the main results, questions and ideas of classical number theory. We will begin by acquiring knowledge of basic tools and concepts in Number Theory such as integers, primes, divisibility, GCD, congruences, Wilson and Fermat theorem, pseudoprimos and multiplicative functions (such as the Euler phi function). Then, we will move on to more advanced topics, such as cryptography and computer security, quadratic residuals and continuous fractions. We will study computational and algorithmic aspects of each topic as appropriate.

Prerrequisitos:

Universidad de los Andes
Facultad de Ciencias

Estructural.

1. **Objetivos:** Entender como construir ideas matemáticas profundas usando bases simples.
2. Escribir y entender argumentos matemáticos.

Ampliar la visión de la riqueza de las matemáticas

Contenido:

Factorización en primos
La sucesión de números primos
Congruencias módulo n
El teorema chino del resto
Calculando inversos y potencias grandes
Pruebas de primalidad
La estructura de (Z/pZ)^*
Introducción a la criptografía
El sistema de intercambio de llaves Diffie-Hellmande
El criptosistema RSA
Atacando a RSA
Introducción a la reciprocidad cuadrática
El criterio de Euler
Demostración de la reciprocidad cuadrática usando sumas de Gauss
Buscando raíces cuadradas

Introducción a la fracciones continuadas
Fracciones continuadas infinitas
Irracionales cuadraticos
Sumas de dos Cuadrados

Forma de Evaluación:

Tareas: 50%
Proyecto:
Anteproyecto: 5%
Escrito final: 30%
Exposición (video): 25%

Bibliografía:

Libro de Guía:
Elementary Number Theory: Primes, Congruences, and Secrets. Undergraduate Texts in Mathematics, Springer-Verlag. 2008.

El libro puede descargarse en forma gratuita de la página web del autor. Haga click aquí para ir a la pagina de descarga.

Otros libros:

Elementary Number Theory, 6th edition by Kenneth Rosen, Pearson. Se pidieron dos copias del libro a la biblioteca.

Niven, Ivan, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. Wiley, 1991.

Ireland, Kenneth F., and Michael I. Rosen. *A Classical Introduction to Modern Number Theory*. Springer, 1990.

Davenport, Harold, and James H. Davenport. *The Higher Arithmetic: An Introduction to the Theory of Numbers*. Cambridge University Press, 2008.