UNIVERSIDAD DEL VALLE DE GUATEMALA
CAMPUS CENTRAL
FACULTAD DE CIENCIAS Y HUMANIDADES

UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

Iniciativa Académica de Teoría de los Números

1 Identificación

Curso:	MM3023 – Seminario 1 de Matemática	**Créditos:**	4
Ciclo:	Segundo	**Requisitos:**	Cálculo 1
Año:	2021		Álgebra Lineal 1
			Álgebra Abstracta 1
Profesor:	Alan Reyes–Figueroa	**Horario:**	Martes y jueves – 17:20-18:55
Email:	agreyes	**Sala:**	Por definir

Sitio Web del Curso:

- https://pfafner.github.io/tn2021

Office Hours:

- Viernes de 17:00 a 18:00 hrs, o por solicitud del estudiante. También pueden enviar sus dudas a través del correo electrónico institucional.

2 Descripción

Este es un curso introductorio a la teoría de números. El curso hace una revisión de los temas clásicos en teoría básica de números, aunque introducizos desde una perspectiva más desde un enfoque algebraico, y haciendo uso de propiedades de estructuras como grupos y anillos. Se hace una revisión de los tópicos y conceptos tradicionales en teoría de números, introduciendo algunos métodos y aplicaciones recientes. El curso pretende que el estudiante adquiera un conocimiento básico sobre el tema, de modo que pueda continuar profundizando esta área a través de sus estudios de postgrado o estudio personal. El curso se apoya en una colección de herramientas algebraicas y analíticas y herramientas de computación, y trata de dar un enfoque aplicado al curso. Se requiere que el estudiante tenga un conocimiento de diversas áreas de matemática, como álgebra lineal, álgebra abstracta, y que domine al menos un lenguaje de programación.

El curso inicia con una introducción a las propiedades de los números enteros, y los fundamentos de la aritmética. Se sigue con el estudio de aritmética modular (congruencias), así como la solución de ecuaciones lineales y sistemas de ecuaciones lineales enteras, y se introducen los teoremas principales del curso: teorema de Fermat, teorma de Euler, teorema Chino del residuo. Este tema continua con el estudio de residuos cuadráticos, así como la teoría de raíces primitivas y la Ley de reciprocidad cuadrática. Al final de este bloque se integran algunas aplicaciones de la teoría de números en computación, principalmente métodos para determinación de primos y factoración de enteros, así como métodos de criptografía y cifrado de información, y métodos computacionales para multiplicación de números y poliomios. Seguidamente, se estudian temas en fracciones continuas y teoría de la aproximación; así como algunas ecuaciones diofantinas básicas, como el teorema de las sumas de cuadrados y se hace una revisión de métodos algebraicos como los enteros gaussianos y enteros de Eisenstein. Al final del curso se hace una introducción a la teoría analítica de números, donde se estudian las principales funciones aritméticas, la distribución de números primos y teoremas de estimación. Se hace una introducción al teorema de los números primos y otros métodos analíticos.

El curso cuenta con una parte práctica, en la que el estudiante implementará en código computacional algunos de los algoritmos estudiados. Parte fundamental del curso es utilizar las herramientas aprendidas en varios proyectos aplicados donde se utilizan herramientas del curso en el ámbito computacional.

3 Competencias a Desarrollar

Competencias genéricas

1. Piensa de forma crítica y analítica.
2. Resuelve problemas de forma estructurada y efectiva.
3. Desarrolla habilidades de investigación y habilidades de comunicación a través de seminarios y presentaciones ante sus colegas.

Competencias específicas

1.1 Entiende y domina los fundamentos matemáticos que formalizan la aritmética y las propiedades de los números enteros y racionales.

1.2 Conoce y profundiza los principales teoremas y métodos de solución de congruencias y ecuaciones diofantinas básicas.

1.3 Comprende los conceptos algebraicos y analíticos relacionados con técnicas empleadas en teoría de números.

2.1 Aplica métodos y técnicas comunes para la solución de problemas asociados con divisibilidad, congruencias, y en general con propiedades de números enteros.

2.2 Aplica de forma efectiva computacionales para resolver problemas aplicados relacionados con la teoría de números.

2.3 Utiliza un enfoque global para resolver problemas. Utiliza herramientas auxiliares en su solución, como álgebra lineal, cálculo, distribuciones e inferencia estadística.

3.1 Desarrolla todas las etapas de una investigación o proyecto aplicado donde se utilizan elementos del análisis de datos: anteproyecto, formulación de hipótesis, diseño experimental, metodología, resultados y conclusiones.

3.2 Escribe un reporte técnico sobre la solución de un problema de interés en teoría de números, teórico o aplicado. Concreta un análisis riguroso y conclusiones importantes.

3.3 Comunica de manera efectiva, en forma escrita, oral y visual, los resultados de su investigación.

4 Metodología Enseñanza Aprendizaje

El curso se desarrollará durante diecinueve semanas, con cuatro períodos semanales de cuarenta y cinco minutos para desenvolvimiento de la teoría, la resolución de ejemplos y problemas, comunicación didáctica y discusión. Se promoverá el trabajo colaborativo de los estudiantes por medio de listas de ejercicios. El curso cuenta con una sesión de laboratorio semanal para la implementación de algoritmos y la práctica de las técnicas de análisis de datos.

El resto del curso promoverá la revisión bibliográfica y el auto aprendizaje a través de la solución de los ejercicios del texto, y problemas adicionales, y el desarrollo de una monografía. Se espera que el alumno desarrolle su trabajo en grupo o individualmente, y que participe activamente y en forma colaborativa durante todo el curso.

5 Contenido

1. Propiedades de los números enteros: Divisivilidad. MDC y MMC. Teorema de Bézout. Algoritmo de Euclides. Teorema Fundamental de la Aritmética. Representación de números enteros. Criterios de divisibilidad.

2. Aritmética modular: Congruencias. Bases. El anillo $\mathbb{Z}/n\mathbb{Z}$ de enteros módulo n. La función de Euler y el Teorema de Fermat. Orden y raíces primitivas. Solución de ecuaciones lineales: Teorema Chino del Resto. Congruencias de grado 2: residuos cuadráticos, símbolo de Legendre. La Ley de Reciprocidad Cuadrática. Congruencias de grado superior.

3. Aproximación: Fracciones continuas, reducidas y buenas aproximaciones. Fracciones continuas periódicas. Espectro de Markov y Legendre. Aproximaciones diofantinas. Teorema de Kinthchine.

4. Ecuaciones diofantinas: Teorema de Pitágoras y sumas de cuadrados. Problema de Waring. Teorema de Minkowski. Descenso infinito. Ecuación de Markov. Último teorema de Fermat. Enteros de Gauss y de Eisenstein. Ecuación de Pell. Algunos resultados algebraicos.

5. Aspectos computacionales: Tests de primalidad. Método ρ de Pollard. Test de AKS. Secuencias recurrentes. Criptografía y métodos de cifrado básico. Método Diffie-Helmann. Método RSA. El algoritmo de Karatsuba. Multiplicación usando FFT.

6. Teoría analítica de números: Funciones aritméticas. Función de Möbius y la fórmula de inversión. Estimativas sobre primos: Teorema de Chebyshev, Postulado de Bertrand. Otras funciones aritméticas. La distribución de números primos. El Teorema de los números primos.

7. Introducción a las curvas elípticas.

6 Bibliografía

Textos:

- D. Burton (1982). *Elementary Number Theory*. 7th Edition. McGraw-Hill.
- I. Niven y H. Zuckerman (1991). *An Introduction to the Theory of Numbers*. 5th Edition. Wiley.
- Tom Apostol (2010). *Introduction to Analytic Number Theory*. Springer.
- Kenneth Rosen (2011). *Elementary Number Theory and Its Applications*.

Referencias adicionales

- G. Jones y J. M. Jones (1998). *Elementary Number Theory*. Springer.
- W. Stein (2009). *Elements of Number Theory: Primes, Congruences, and Secrets*. Springer.
- J. Stillwell (2003). *Elements of Number Theory*. Springer.
- F. Brochero, C. Moreira, N. Saldanha, E. Tengan (2012). *Teoria dos Números*. IMPA.

Referencias avanzadas

- G. H. Hardy y E. M. Wright (1968). *An Introduction to the Theory of Numbers*. Oxford Press.
- K. Chandrasekharan (1969). *Introduction to Analytical Number Theory*. Springer.
- K. Ireland y M. Rosen (1980). *A Classical Introduction to Modern Number Theory*. Springer.

7 Actividades de evaluación

Actividad	Cantidad aproximada	Porcentaje
Listas de ejercicios	10 a 15	85%
Seminarios	1 ó 2	15%

8 Cronograma

Semana	Tópico	Fecha	Actividades
1	Introducción y motivación al curso. Inducción matemática y Principio de Dirichlet.	05-09 julio	
2	Divisibilidad. MDC y MMC. Teorema de Bézout. Algoritmo de Euclides.	12-16 julio	
3	Primos y su distribución. El Teorema Fundamental de la Aritmética.	19-23 julio	
4	Representación de números en bases numéricas. Criterios de divisibilidad.	26-30 julio	
5	Congruencias. Bases. El anillo $\mathbb{Z}/n\mathbb{Z}$ de enteros módulo n. La función de Euler y el Teorema de Fermat.	02-06 agosto	
6	Orden y raíces primitivas. Solución de ecuaciones lineales: Teorema Chino del Resto.	09-13 agosto	
7	Congruencias de grado 2: residuos cuadráticos, símbolo de Legendre. Ley de Reciprocidad Cuadrática.	16-20 agosto	
8	Congruencias de orden superior. Lema de Hensel.	23-27 agosto	
9	Fracciones continuas, reducidas y buenas aproximaciones. Fracciones continuas periódicas.	30 agosto-03 sept	
10	Espectro de Markov y Legendre. Aproximaciones diofantinas. Teorema de Kinthchine.	06-10 septiembre	
	Semana de asueto	13-17 septiembre	
11	Series de Farey. Aproximaciones racionales. Geometría de los números.	20-24 septiembre	
12	Ecuaciones diofantinas: Teorema de Pitágoras y sumas de cuadrados. Problema de Waring.	27 sept - 01 octubre	
13	Descenso infinito. Ecuación de Markov. Último teorema de Fermat. Enteros de Gauss y de Eisenstein.	04-08 octubre	
14	Ecuación de Pell. Algunos resultados algebraicos.	11-15 octubre	
15	Tests de primalidad. Método ρ de Pollard. Test de AKS. Secuencias recurrentes.	18-22 octubre	
16	Criptografía y métodos de cifrado básico. Método de, Diffie-Helmann. Método RSA.	25-29 octubre	
17	Funciones aritméticas. Función de Möbius y la fórmula de inversión.	01-05 noviembre	
18	Estimativas sobre primos: Teorema de Chebyshev, Postulado de Bertrand.	08-12 noviembre	
19	La distribución de números primos. El Teorema de los números primos.	15-19 noviembre	Seminarios
20	Introducción a las curvas elípticas.	22-26 noviembre	Seminarios