Universidad de Chile Facultad de Ciencias

Nombre del curso: Teoría de Numeros

Semestre: Primavera

Área de Formación: Especializada

Modalidad: Presencial y Semestral

Carácter: Obligatorio

Carrera: Pedagogía en Matemáticas y Física, Lic. en Ciencias Exactas. **Profesor:** Jorge Soto Andrade

No de créditos (SCT): 6

No de horas directas (sincrónicas y asincrónicas) semanales: 3 (catedra) + 1,5 (ayudantía)

Clases: 2 **Ayudantías:** 2 (paralelas)

Requisitos: Algebra y Geometria 1 y 2. Algebra Lineal

Descripción de la actividad curricular: Objetivos Generales:

1. Lograr que los estudiantes reflexionen sobre la construcción conjuntista de los sistemas numéricos de la matemática, desde $\mathbb{N}$ hasta $\mathbb{H}$.
2. Lograr que los estudiantes discernan, planteen y aborden por diversos métodos, preguntas y problemas que involucren los números naturales y los números enteros (problemas aritméticos).
3. Lograr que los estudiantes descubran la aplicabilidad de las propiedades aritméticas de los enteros y sus conexiones con otras áreas del saber.

Objetivos Específicos :

1. Conocer la construcción conjuntista de los sistemas numéricos de la matemática.
2. Descubrir las diversas facetas y aplicaciones de la congruencia módulo un entero.
2. Transitar de la definición recursiva a la caracterización explícita de secuencias numéricas.
3. Practicar geometría enumerativa sobre los cuerpos finitos y la q-analogía.

Evaluación y Requisitos de aprobación :

La evaluación del curso estará basada en:

- Una nota TG por Trabajos grupales en grupos aleatorios de 3 o 4, a informar al final de la segunda sesión de cada semana, generalmente. A esta nota contribuyen también suplementariamente (llapa) los EV (Ejercicios Voluntarios) propuestos durante el curso.
- Una nota P por dos pruebas tradicionales realizadas durante el semestre.
- Una nota A de ayudantía, definida por los ayudantes.

La nota final es el promedio ponderado

$$0,5*TG+0,3*P+0,2*A$$

de las 3 notas TG, P y A.

Si la nota final N es menor o igual a 3,9, el alumno(a) deberá rendir examen.

Temáticas o contenidos del curso (listado *lineal* tentativo):

1. **Introducción:** Las preguntas de la teoría de números (aritmética). Su relevancia científica y tecnológica (codificación).
2. **Construcción conjuntista de los naturales. Construcción de $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{Q}_p$, $\mathbf{C}$, $\mathbf{H}$.**
3. **Historia de la Teoría de Números.** Racontos históricos. Preguntas clásicas, particularmente sobre números primos y descomposiciones aditivas en potencias (e. g.: probabilidad que un número sea primo, densidad de los primos, descomposiciones en sumas de cuadrados, de cubos, etc.).
4. **Sucesiones enteras definidas recursivamente.** Sucesión de Fibonacci (número de formas de subir una escalera), Jacobsthal y otras análogas. Generalizaciones (escalera al cielo, divina proporción...). Interpretación probabilista (paseos al azar en polígonos regulares y poliedros regulares). Obtención de fórmulas explícitas por variados métodos (e.g. por análisis y síntesis espectral: diagonalización de matrices, o via interpretación sistémica, reduciendo dos pasos de memoria a uno). Imposibilidad de generación polinomial de las sucesiones enteras clásicas. Interpolación polinomial de Lagrange (via álgebra lineal elemental).
5. **Congruencias módulo un entero:** Motivaciones (aplicación a ecuaciones diofánticas y otras), representaciones y metaforizaciones diversas. Congruencias geométricas y aritméticas (punto de vista unificador de F. Klein). Sistemas dinámicos en los enteros modulo m . Fenomenología de órbitas (puntos fijos, sumideros, atractores, ciclos...). Explicaciones aritméticas de los tipos de órbitas. El caso m primo. Cuadrados y otras potencias en un cuerpo finito.
6. **Sistemas de congruencias y el teorema chino de los restos.** Ejemplos motivadores. Resolución artesanal de sistemas de congruencias según distintos módulos (caso favorable de módulos relativamente primos). Analogía con la interpolación de Lagrange. Obtención inmediata de una fórmula explícita para las soluciones (caso favorable) análoga al Polinomio de Lagrange. Extensión al caso general.
7. **Ecuaciones diofánticas.** Ejemplos históricos. Reducción modular. Principio de Hasse. Hensel y los números p -ádicos. Aplicaciones.
8. **Álgebra lineal sobre un cuerpo finito $\mathbf{F}_p$.** Preguntas motivadoras: E. g.: ¿probabilidad que una matriz $n \times n$ sea inversible sobre $\mathbf{F}_p$? Cuerpos finitos como análogos bebé de $\mathbf{R}$. Geometría enumerativa: conteo de número de k -subespacios vectoriales en n dimensiones. Coeficientes binomiales de Gauss y q – análogos.
9. **Tópicos optativos:**

- Números p-ádicos (motivados por ecuaciones diofánticas o por el árbol binario infinito y su frontera y modelos cosmológicos...)
- Números hiper-reales.
- Funciones de Euler y de Möbius.
- Reciprocidad cuadrática.
- Aplicaciones a la criptografía.

Bibliografía de apoyo comentada (disponibles en uchile o en la web):

Halmos, P. (2010). Naïve Set Theory. Martino Pub.

Notable introducción a la teoría ingenua de conjuntos. Incluye la construcción conjuntista de los naturales.

Beiler, A. H. (1966). Recreations in the Theory of Numbers. New York, NY: Dover.

Silverman, J. H. (2012). A friendly introduction to number theory. New Jersey: Pearson.

Dos textos introductorios sumamente amenos, el segundo más sistemático que el primero.

Ribenboim, Pablo (2000). My Numbers, My Friends. Popular lectures on number theory. New York, NY: Springer.

Texto introductorio relativamente amigable de un experto brasileño en teoría de números, pero más avanzado que los anteriores.

Vinogradov (1955). An introduction to the theory of numbers, New York, NY: Pergamon
Un clásico de la teoría de números, escrito por uno de los maestros del tema.

Guelfond, A. O. (1984). Resolución de ecuaciones en números enteros. Lecciones Populares de Matematicas. Moscú: Editorial MIR.

Un buen compendio "popular" de los métodos de solución de ecuaciones, de un discípulo notable de Vinogradov, traducido directamente del ruso al castellano.