# Proyecto de programa de Matemática Discreta II

1. **Nombre de la asignatura:** Matemática discreta II
2. **Créditos:** 9 créditos
3. **Objetivo de la asignatura:** El estudiante deberá:

   1) Comprender y manejar ciertas estructuras algebraicas como ser Grupos, Anillos y Cuerpos. Especial énfasis se pondrá en los grupos finitos y en los cuerpos finitos, por su interés en Informática. Deberá comprender aplicaciones modernas de dichos contenidos como ser Teoría de Códigos de detección y corrección de errores, Máquinas de Estado Finito, y Criptografía.

   2) Fortalecer la capacidad de realizar razonamientos por analogía en problemas similares planteados en éste y en el curso de Matemática Discreta 1.

4. **Metodología de enseñanza:** Curso teórico práctico de 2 horas semanales de clases teoricas, 3 horas semanales de clases prácticas, y 4 horas semanales de dedicación domiciliaria.
5. **Temario:**

   a) Anillo de los enteros, Divisibilidad y Aritmética Modular. Aplicaciones a la Criptografia (1): sistemas clásicos y sistema de clave pública RSA (introductorio).

   b) Grupos. Subgrupos. Grupos Ciclicos. Teorema de Lagrange. Homomorfismos y subgrupos normales. Grupo cociente. Teoremas de homomorfismos. Productos directos. Teorema de Cauchy. Grupos Abelianos Finitos. Grupos de Matrices. Aplicaciones a los Códigos de detección y corrección de errores (1) (Codigos Lineales). Grupo Simétrico. Aplicaciones a la Criptografia (2): sistemas de clave privada, descripción elemental de DES.

   c) Estructura de los anillos. Propiedades. Subanillos. Homomorfismos, isomorfismos, ideales.

   d) Anillos de Boole, Algebras de Boole. Aplicaciones a las redes lógicas (introductorio). Mapas de Karnaugh.

   e) Campos finitos. Anillos de polinomios. Polinomios irreducibles. Representación de cuerpos finitos sobre $\mathbb{Z}_p$ mediante polinomios irreducibles. Aplicaciones a los códigos de detección y corrección de errores (2): códigos basados en polinomios sobre cuerpos finitos. Aplicación a la Criptografía (3): sistemas basados en logaritmos discretos.

f) Máquinas de estado finito. Máquinas de Turing.

6. **Bibliografía:**

**Básica:** Grimaldi, R. P. Matemática discreta y combinatoria, primera edición, Ed. Addisson Wesley ISBN 0-201-64406-1.

**Complementaria:** Herstein I.N. Algebra Abstracta. Grupo Editorial Iberoamérica. ISBN 0-02-353820-1
Birkhoff G. & MacLane S. Algebra Moderna. Vicens-Vives. ISBN 84-316-1226-6
Birkhoff G. & Bartee T.C. Modern Applied Algebra Ed. McGraw-Hill ISBN 07-0053381-2
Liu C.L Elementos de Matemáticas Discretas Ed. Mc Graw Hill. ISBN 970-10-0743-3

7. **Conocimientos previos:** Es imprescindible un dominio de los temas correspondientes al programa de Matemática Discreta 1. Es tambien necesario un buen dominio de los temas correspondientes al álgebra lineal, y al cálculo diferencial e integral en una variable.

# CRONOGRAMA TENTATIVO DE REFERENCIA DE MATEMATICA DISCRETA II(1998)

- Semanas 1, 2 y 3.

  Anillo de los enteros. Divisibilidad y aritmética modular. Aplicaciones.

- Semanas 4, 5, 6 y 7.

  Grupos. Subgrupos. Homomorfismos. Subgrupos normales. Cocientes. Grupos abelianos. Grupo Simétrico. Aplicaciones.

  Algebra de Boole. Aplicaciones a las redes lógicas. (introductorio). Mapas de Karnaught.

- Semanas 8, 9 y 10

  Anillos. Subanillos. Ideales. Homomorfismos. Anillos de Boole. Algebras de Boole.

- Semanas 11 a 14 Campos finitos. Anillos de polinomios. Polinomios irreducibles. Representación de cuerpos finitos sobre $\mathbb{Z}_p$ mediante polinomios irreducibles. Aplicaciones.

- Semanas 15 a 16 Máquinas de estado finito. Máquinas de Turing.

Modalidad de los cursos y procedimientos de evaluación.

Los estudiantes serán evaluados mediante dos parciales, los cuales se realizaran, el primero luego de la 7ma. semana de clases, y el segundo, una vez finalizado el curso. De los resultados obtenidos en los parciales surgirán tres posibilidades: a)exoneración del examen final, b)suficiencia en el curso, que habilita a rendir examen hasta que el curso sea dictado nuevamente, c)insuficiencia en el curso, por lo cual reprueba, debiendo reinscribirse en el mismo. Sumando los resultados de los parciales se podrá obtener un total de 100 puntos: un máximo de 40 puntos en el primer parcial y un máximo de 60 puntos en el segundo. Los parciales no tienen un puntaje mínimo exigible. La exoneración del examen final se logra acumulando como mínimo 60 puntos. La suficiencia se logra acumulando como mínimo 25 puntos. Quien no llegue a 25 puntos deberá recursar. La inasistencia a un parcial no inhabilita al estudiante a aprobar o exonerar el curso.

Aprobado por REs.del Consejo de Fac. de Ing. con fecha 3.12.97, Exp.85.457