

# **FUNDAMENTOS DE LA MATEMÁTICA DISCRETA (21294)**

**Curso 01-02**

## **Objetivos:**

En la parte de combinatoria:

- repasar las formas enumerativas elementales y algunas de sus aplicaciones más conocidas siempre atendiendo los dos factores clave: repetición y orden;
- presentar y practicar el cálculo combinatorio mediante funciones generadoras;
- introducir la formulación y la resolución de las ecuaciones lineales recurrentes.

En la parte de aritmética:

- deducir los resultados principales en la aritmética de los enteros;
- utilizarlos, en la práctica, en la simplificación de cálculos y operaciones diversas;
- presentar dos aplicaciones capitales en el mundo de las comunicaciones: los códigos correctores de errores y los métodos criptográficos.

## **Programa de la asignatura:**

1. Combinatoria I
  - Regla de la suma y regla del producto
  - Permutaciones
  - Combinaciones y números binomiales
  - Teorema binomial y teorema multinomial
  - Principio de inclusión/exclusión.
2. Combinatoria II
  - Funciones generadoras ordinarias
  - Funciones generadoras exponenciales
  - Particiones de los naturales
  - Ecuaciones lineales recurrentes
    - \* Planteamiento
    - \* Resolución iterativa
    - \* Método de las raíces
3. Aritmética
  - Grupo, anillo y cuerpo. Concepto y ejemplos
  - Axioma de ordenación. División entera
  - Máximo común divisor.
  - Algoritmo de las divisiones sucesivas. Identidad de Bezout
  - Números primos. Teorema de factorización
  - Ecuaciones diofánticas lineales
  - Congruencias. Teorema del residuo
  - El anillo  $Z_m$ . Aritmética modular
  - Teorema de Euler y teorema de Fermat

#### 4. Códigos correctores de errores i criptografía

- Códigos correctores de errores
  - Conceptos básicos
  - Códigos lineales binarios
  - Construcción de códigos lineales
  - Detección y corrección de errores
- Criptografía
  - Conceptos básicos
  - Esquemas clásicos
  - Métodos modernos
  - El algoritmo RSA

#### Bibliografía:

Bàsica:

1. J.M. BASART, J. RIFÀ, M. VILLANUEVA (1997). *Fonaments de matemàtica discreta. Elements de combinatòria i d'aritmètica.* Col·lecció Materials de la UAB, n. 36, ISBN 84-490-0855-7.
2. N.L. BIGGS (1994). *Matemática Discreta.* Vicens Vives, ISBN 84-316-3311-5.
3. F. COMELLAS *et al.* (1996). *Matemàtica discreta.* Politext 26, Edicions UPC, ISBN 84-8301-062-3.
4. L. CHILDS (1992) *A Concrete Introduction to Higher Algebra.* UTM, Springer-Verlag, ISBN 0-387-90333-X.
5. R.P. GRIMALDI (1989). *Matemáticas discreta y combinatoria.* Addison-Wesley Iberoamericana, ISBN 0-201-64406-1.

Complementaria:

1. J. RIFÀ, L. HUGUET (1991). *Comunicación digital.* Masson, ISBN 84-311-0576-3.
2. F.S. ROBERTS (1984). *Applied Combinatorics.* Prentice-Hall Inc., ISBN 0-13-039313-4.
3. A. TUCKER (1984). *Applied Combinatorics.* John Wiley & Sons, ISBN 0-471-63579-0.

#### Evaluación de la asignatura

La calificación definitiva será el resultado de la suma de la nota del examen final más la de una prueba parcial. Esta prueba se llevará a término antes de la Semana Santa, incluirá -únicamente- los dos temas de combinatoria y permitirá obtener hasta 1,5 puntos. La puntuación adicional obtenida no se mantendrá para la calificación definitiva en la segunda convocatoria (septiembre). Finalmente, la prueba parcial no excluirá materia. Dicho de otro modo, en el examen final puede aparecer también algún ejercicio de los dos temas de combinatoria.