

Fonaments de la Matemàtica Discreta

| [Objectius](#) | [Programa](#) | [Bibliografia](#) | [Avaluació](#) |

Enginyeria Tècnica Informàtica de Gestió i de Sistemes, 2n semestre, 2003-2004.

Codi
21294

Escola Universitària d'Informàtica

Professorat:

- Dolors Herbera (grup 10)
Horari d'atenció: dimecres d'11 a 13 i a hores convingudes;
despatx S/258
E-mail: <mailto:dolors@mat.uab.es>
Tel. 937 287 729.
- Cristina Fernández (grup 20)
Horari d'atenció: dilluns de 10 a 11, dijous de 9 a 10 i a hores convingudes; despatx S/260
E-mail: cristina@ccd.uab.es
Tel. 937 287 757.
- Mercè Villanueva (grup 50)
Horari d'atenció: dimecres de 17 a 19 i a hores convingudes;
despatx S/260
E-mail: <mailto:merce.villanueva@autonoma.edu>
Tel. 937 287 757.

Objectius:

En la part de combinatòria:

- repassar les fórmules enumeratives elementals i algunes de llurs aplicacions més conegudes, tot atenent els dos factors clau: repetició i ordre;
- presentar i practicar el càlcul combinatori mitjançant funcions generadores;

- introduir la formulació i la resolució de les equacions lineals recurrents.

En la part corresponent a l'aritmètica:

- deduir els resultats principals en l'aritmètica dels enters;
- utilitzar-los, en la pràctica, en la simplificació de càlculs i operacions diverses;
- presentar dues aplicacions cabdals en el món de les comunicacions: els codis correctors d'errors i els mètodes criptogràfics.

Programa de l'assignatura:

1. COMBINATÒRIA I (dues setmanes)
 - Regla de la suma i regla del producte
 - Permutacions
 - Combinacions i nombres binomials
 - Teorema binomial i teorema multinomial
 - Principi d'inclusió/exclusió
2. COMBINATÒRIA II (tres setmanes)
 - Funcions generadores ordinàries
 - Funcions generadores exponencials
 - Particions dels naturals
 - Equacions lineals recurrents
 - Plantejament
 - Resolució iterativa
 - Mètode de les arrels
3. ARITMÈTICA (cinc setmanes)
 - Grup, anell i cos. Concepte i exemples
 - Axioma d'ordenació. Divisió entera
 - Màxim comú divisor
 - Algorisme de les divisions successives. Identitat de Bézout
 - Equacions diofàntiques lineals
 - Nombres primers. Teorema de factorització

- Congruències. Teorema del residu
- L'anell $\mathbb{Z}_m$. Aritmètica modular
- Teorema d'Euler i teorema de Fermat

4. CODIS CORRECTORS D'ERRORS I CRIPTOGRAFIA (tres setmanes)

- Codis correctors d'errors
 - Conceptes bàsics
 - Codis lineals binaris
 - Construcció de codis lineals
 - Detecció i correcció d'errors
- Criptografia
 - Conceptes bàsics
 - Esquemes clàssics
 - Mètodes moderns
 - L'algorisme RSA

Bibliografia:

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. J.M. BRUNAT, E. VENTURA (2001). *Informació i codis.* .
Politext 114, Edicions UPC, ISBN 84-8301-528-5.
4. F. COMELLAS *et al.* (1996). *Matemàtica discreta.*
Politext 26, Edicions UPC, ISBN 84-8301-062-3.
5. R.P. GRIMALDI (1989). *Matemáticas discreta y combinatoria.*

Addison-Wesley Iberoamericana, ISBN 0-201-64406-1.

Complementària

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.

Avaluació de l'assignatura:

La qualificació definitiva serà el resultat de la suma de la nota de l'examen final més la d'una prova parcial. Aquesta prova es durà a terme abans de la Setmana Santa, inclourà -únicament- els dos temes de combinatòria i permetrà obtenir fins a 1,5 punts. La puntuació addicional obtinguda no es mantindrà per a la qualificació definitiva en la segona convocatòria (setembre). Finalment, la prova parcial no exclourà matèria. Dit d'una altra manera, en l'examen final hi pot aparèixer també algun exercici dels dos temes de combinatòria.

© *Unitat de Combinatòria i Comunicació Digital, 2000-2004*
Darrera modificació: 2004-01-30