

Fonaments de la matemàtica discreta

Professor

<i>Nom</i>	<i>Dpt.</i>	<i>Despatx</i>	<i>Direcció e-mail</i>	<i>Telèfon</i>
Jaume Moncasi	Matemàtiques	S/259	jaume.moncasi@uab.cat	93.728.7729

IMPORTANT: Degut a la implantació del nou Grau en Enginyeria Informàtica, que comporta l'extinció dels estudis d'Enginyeria Tècnica en Informàtica de Sistemes i d'Enginyeria Tècnica en Informàtica de Gestió, el curs acadèmic 2010/11 les assignatures de primer curs d'aquestes dues titulacions s'impartiran seguint un model docent amb tutories presencials. La metodologia i els procediments d'avaluació d'aquesta assignatura s'especifiquen en aquesta guia docent. El curs vinent, 2011/12, ja no es faran tutories i només hi haurà les dues convocatòries d'examen. Una vegada extingit definitivament un curs del pla d'estudis, l'alumnat que no n'hagi superat les assignatures troncal i obligatòries, ha de continuar els estudis en el nou grau, amb el reconeixement de crèdits que s'hagi establert en la corresponent taula d'adaptació.

Continguts

1. Combinatòria I

1. Regla de la suma i del producte
2. Permutacions
3. Combinacions i nombres binomials
4. Teorema binomial i teorema multinomial
5. Principi d'inclusió/exclusió

2. Combinatòria II

1. Funcions generadores ordinàries
2. Equacions lineals recurrents
 - Plantejament
 - Resolució iterativa
 - Mètode de les arrels

3. Aritmètica

1. Introducció. Nombres enters
2. Propietat d'ordre dels nombres enters. Divisió entera
3. Divisibilitat de nombres enters. Màxim comú divisor
4. Identitat de Bézout. Algorisme de les divisions successives
5. Equacions diofàntiques lineals
6. Nombres primers. Teorema de factorització
7. Congruències. Teorema del residu
8. L'anell Z_m . Aritmètica modular
9. Teorema d'Euler i teorema de Fermat. Algorisme de multiplicar i elevar

4. Criptografia

1. Criptografia
 - Conceptes bàsics
 - Esquemes clàssics
 - L'algorisme RSA.

Metodologia docent

Hi haurà 3 llistats de problemes de la part de combinatòria i 3 llistats de problemes de la part d'aritmètica, a part del llistat de problemes del curs anterior. Es realitzaran sessions de 2 hores per resoldre dubtes sobre cada llistat de problemes, incidint en les parts on hi hagin més dubtes.

Avaluació

Criteris d'avaluació:

Atès que l'assignatura es pot dividir en dos blocs independents, es procedirà a l'avaluació de cada bloc per separat. Per tant, es realitzaran dues proves parcials d'avaluació (5 punts cada prova), una de combinatòria i una altra d'aritmètica. Per aprovar cal que la suma dels dos parcials sigui superior o igual a 5.

A la segona convocatòria es podrà realitzar la recuperació de la part de combinatòria, d'aritmètica o totes dues.

Calendari

Sessions dilluns de 15:00 a 17:00.

21-03-11: Combinatòria I
28-03-11: Funcions generadores
04-04-11: Equacions recurrents
11-04-11: **Prova de Combinatòria**
02-05-11: Introducció a l'aritmètica. Equacions diofàntiques
16-05-11: Congruències. Aritmètica modular
23-05-11: Teoremes Euler i Fermat. Criptosistema RSA
30-05-11: **Prova d'aritmètica**

08-06-11: Segona convocatòria (16:00)

Bibliografia bàsica

- 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.
- R.P. GRIMALDI (1989). *Matemàtiques discreta y combinatoria*. Addison-Wesley Iberoamericana, ISBN 0-201-64406-1.
- N.L. BIGGS (1994). *Matemàtica Discreta*. Vicens Vives, ISBN 84-316-3311-5.
- F. GARCÍA, G. HERNÁNDEZ, A. NEVOT (2003). *Problemas resueltos de Matemática Discreta*. ITES-Paraninfo, ISBN 84-9732-210-X.