27991 **Matemàtica Discreta**

Tipus: Obligatòria *Crèdits:* 12

Curs 2001-2002

Presentació i Objectius de l'assignatura

Amb el nom de Matemàtica Discreta, se solen incloure un conjunt força ampli de temes de matemàtiques que han esdevingut importants d'uns anys ençà com a conseqüència de l'aparició de la Informàtica. Així, per exemple, podríem parlar de criptosistemes o teoria codis per a la transmissió de la informació, o de la teoria de grafs, o de combinatòria, entre d'altres. En molts d'ells hi intervenen temes clàssics d'àlgebra com ara la teoria de grups i la divisibilitat, que seran dos dels que estudiarem a fons en aquest curs. A banda de la seva actualitat, la Matemàtica Discreta ens proporciona un marc adequat per començar a estudiar àlgebra, veient de seguida les seves aplicacions des d'un punt de partida més concret. Una de les pretensions d'aquesta assignatura és, doncs, introduir l'alumne a les eines algebraiques bàsiques.
En la primera part del curs (capítols 1, 2 i 3) es dedica especial atenció a l'ús adequat del llenguatge matemàtic. Així, es fa una breu introducció a les aplicacions entre conjunts i les relacions d'equivalència, donant ja uns primers models discrets que s'apliquen a problemes concrets de combinatòria.
En la segona part del curs (capítols 4, 5 i 6), a partir d'exemples ben coneguts, com són els nombres enters i els polinomis, s'introdueix l'alumne al procés d'abstracció observant les propietats anàlogues dels dos anells. S'aprofiten aquests exemples per estudiar estructures algebraiques (anells, grups, cossos finits).
Aquesta assignatura hauria de contribuir a que l'alumne adquirís una adequada formació matemàtica, havent vist un bon nombre de teoremes i demostracions, que el permeti començar a entendre quan una demostració és necessària (sempre!) i a construir-la ell mateix. També ha d'adquirir hàbits crítics davant les afirmacions matemàtiques (pròpies o alienes) i, sobretot, ha de desenvolupar un esperit combatiu davant dels problemes. Per això, es dedicarà atenció especial als exemples, per la seva importància intrínseca i el seu valor formatiu a l'hora de contestar negativament una pregunta o a l'hora d'entendre millor un enunciat.

Programa

1. Conjunts i aplicacions

Llenguatge bàsic de conjunts.

Aplicacions entre conjunts. Aplicacions injectives, exhaustives i bijectives. Composició.

Permutacions. Descomposició en cicles disjunts. Signe.

Relacions d'equivalència i particions. Conjunt quocient.

2. Combinatòria

Aplicacions entre conjunts i compteig. Principi de les caixes. Principi de l'addició.

Funcions de paraules i seleccions. Seleccions ordenades sense repetició.

Subconjunts. Seleccions no ordenades sense repetició. Nombres binomials.

Seleccions ordenades amb repetició. Teorema del binomi.

Principi de la criba. La funció d'Euler.

Nombre de particions d'un conjunt en k parts.

Distribucions i nombres multinomials. Teorema multinomial.

Elements de probabilitat: Espai mostral, esdeveniment, probabilitat. Independència.

3. Nombres naturals i inducció. Conjunts infinits.

Ordenació dels nombres naturals. Definicions recursives. Principi d'inducció.

Progressions aritmètiques i geomètriques.

Conjunt finit/infinit.

Conjunt numerable/no numerable.

4. Enters i congruències

Divisió entera. Màxim comú divisor i mínim comú múltiple.

Algorisme d'Euclides. Equacions diofàntiques.

Nombres primers entre ells i nombres primers. Factorització en primers.

Congruències. Relació d'equivalència. Els anells $\mathbb{Z}/(m)$.

El criptosistema RSA.

Noció d'anell, d'ideal i de morfisme d'anells.

5. Polinomis

Definició de l'anell de polinomis sobre un cos.

Divisió entera de polinomis. Màxim comú divisor i mínim comú múltiple.

Polinomis irreductibles i polinomis primers entre ells. Descomposició en irreductibles.

Zeros d'un polinomi.

Números complexes. Arrels d'un número complex. Descomposició en irreductibles a $\mathbb{C}[x]$ i a $\mathbb{R}[x]$.

Polinomis sobre el cos de p elements.

Els anells $K[x]/(m(x))$.

6. Grups

Definició de grup. Exemples bàsics: grups de permutacions, $\mathbb{Z}/(m)$, grups de matrius, grup dels invertibles d'un anell, grups moviments.

Subgrups. Teorema de Lagrange.

Subgrup normal i grup quocient. Morfisme de grups. Teorema d'isomorfisme.

Classificació dels grups cíclics.

7. Cossos finits

Característica d'un cos finit. Cos primer i nombre d'elements d'un cos finit.

Teorema de l'element primitiu.

Caracterització dels cossos finits.

Bibliografia bàsica

- N. L. BIGGS, *Matemática Discreta*, Ed Vicens Vives, 1994.
- J. DORRONSORO, E. HERNÁNDEZ, *Números, grupos y anillos*, Addison-Wesley/Universidad Autónoma de Madrid, 1996.

Bibliografia complementària

- J. M. BASART, J. RIFÀ, M. VILLANUEVA, *Fonaments de Matemàtica Discreta*, Materials UAB, 36. 1997.
- P. M. COHN, *Algebra. Volume 1. Second edition*, John Wiley & sons 1989.
- F. CEDÓ, V. GISIN, *Àlgebra Bàsica*, Manuals de la Universitat Autònoma de Barcelona. Publicacions UAB, 1997.

Professors

grup 1. teoria: Jaume Moncasi (despatx C1/120), problemes: Ramon Antoine (despatx C1/212).
grup 2. teoria i problemes: Rosa Camps (despatx C1/120).

Avaluació

Convocatòria de juny:
Sobre 10 punts de la convocatòria de juny, la nota s'obté sumant les següents tres quantitats:

1. **El resultat de multiplicar per 0.1** la nota (sobre 10) de l'examen de la primera part del curs, que es farà durant el període intrasemestral (del 3 al 5 de desembre).
2. **El resultat de multiplicar per 0.15** la nota (sobre 10) obtinguda a partir del lliurament de problemes (a determinar) i de les entrevistes que es faran al llarg del curs amb els professors.
3. **El resultat de multiplicar per 0.75 la nota d'examen.** Aquesta nota d'examen es pot obtenir d'una de les dues formes següents:
   a) Per parcials: Es farà el primer parcial durant el període d'exàmens del primer quadrimestre. El segon parcial es farà durant el mes de juny. Si p és la nota del primer parcial sobre 10 i s la del segon sobre 10, la nota d'examen serà igual a $0.4p + 0.6s$. Per poder obtenir una nota d'examen per parcials caldrà que $p \geq 3$ i $s \geq 4$.
   b) Per final: També hi haurà un examen final, global de tota l'assignatura. En aquest cas, la nota de l'examen final (sobre 10) serà considerada la nota d'examen.

Convocatòria de setembre:
Hi haurà un examen global de tota l'assignatura. La nota d'aquest examen serà l'única que s'utilitzarà, al 100%, per qualificar la segona convocatòria.