Fonaments de Matemàtica Discreta

[Objectius] [Programa] [Bibliografia] [Avaluació] [Observacions] [Material docent]

Fòrum

Enginyeria Informàtica, 2n semestre, curs 2000-2001. *Codi 24969*

Escola Tècnica Superior d'Enginyeria

Professorat:

Francesc Bars (Grup I, problemes)
- Consultes presencials: dimecres i divendres 15:00-16:00 a C1/130
- Consultes virtuals: francesc@mat.uab.es

Miquel Llebrés (Grup I, teoria; Grup II problemes)
- Consultes presencials: dimarts 15:00-17:00 a C1/220
- Consultes virtuals: llabres@mat.uab.es

Enric Nart (Grup III, teoria i problemes)
- Consultes presencials: dimarts 10:00-11:00 i divendres 12:00-13:00 a C1/326
- Consultes virtuals: nart@mat.uab.es

Mercè Villanueva (Grup II, teoria; Grup IV teoria i problemes)
- Consultes presencials: dimecres 9:00-10:00 i divendres 12:00-13:00 a C5/145
- Consultes virtuals: merce@ccd.uab.es

Objectius:

L'assignatura està dividida en tres capítols. En el primer s'estudien, fonamentalment, els resultats principals en l'aritmètica dels enters. En el segon s'estudia l'anell de polinomis fent un paral.lelisme amb el capítol anterior. Finalment, en l'últim capítol s'estudia la construcció i manipulació de cossos finits. A banda de la formalització dels resultats es busca la seva aplicació pràctica en la simplificació dels càlculs en les diverses estructures estudiades. També, es destaca la incidència que aquests temes presenten en els codis correctors d'errors i en els mètodes criptogràfics.

Programa de l'assignatura:

1. Aritmètica

- Anells. L'anell dels enters.
- Divisió entera.
- Màxim comú divisor. Algorisme d'Euclides.
- Identitat de Bézout. Equacions diofántiques lineals.
- Nombres primers.
- Congruències.
- Aritmètica modular. L'anell Z_m
- Teorema xinès de les restes.
- Funció multiplicativa d'Euler. Teorema de Fermat i teorema d'Euler.
- L'algorisme d'elevar i multiplicar.
- Aplicació a la criptografia: criptografia RSA.

2. L'anell de polinomis
   - Divisió de polinomis.
   - Màxim comú divisor. Algorisme d'Euclides. Ident. de Bézout.
   - Polinomis irreductibles.
   - Zeros de polinomis.
   - Congruències mòdul un polinomi.
   - Els anells $K[x]/(m(x))$.

3. Cossos finits
   - Construcció explícita de cossos finits.
   - Característica i cos primer. Cardinal d'un cos finit.
   - Ordre d'un element. Elements primitius en un cos finit.
   - Representació vectorial i potencial dels elements d'un cos finit.
   - Polinomis mínims, polinomis primitius.
   - Descomposició x^n-x en factors

Bibliografia:

- 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.
- N.L. BIGGS (1985). *Discrete Mathematics.* Oxford University Press, ISBN 0-19-853426-4. (Edició en castellà: *Matemática Discreta.* Vicens Vives, 1994.)
- L. CHILDS (1992). *A Concrete Introduction to Higher Algebra.* UTM, Springer-Verlag, ISBN 0-387-90333-X.
- J. RIFÀ, L. HUGUET (1991). *Comunicación digital.* Masson, ISBN 84-311-0576-3.

Avaluació de l'assignatura:

Hi haurà un examen final que inclourà tota la matèria del programa i puntuará sobre 10. A més hi haurà una prova escrita sobre el capítol 1. Aquesta prova no eliminarà matèria i la nota s'afegirà a la de l'examen final. Aquesta nota no es guardarà per la convocatòria de setembre ni per cap d'altra posterior.

Observacions:

Trobareu el llistat dels problemes de classe i models d'exàmens de cursos passats en la secció de Material Docent.
