Fonaments de Matemàtica Discreta

Programa Enginyeria

1. Combinatoria
   (a) Combinatoria elemental: Permutacions, variacions i combinacions amb i sense repeticions. [Bigg89], [Ande90]
   (b) Problemes d'aparellaments i assignacions. [Ande90]
   (c) Recurrència i tècniques recursives. Programació dinàmica. [Bigg89]
   (d) Funcions generadores. Particions d'un enter positiu. [Bigg89], [Ande90]
2. Aritmètica
   (a) Divisió entera. Ideals. [CaLl90]
   (b) Màxim comú divisor i nombres primers. Teorema de Bezout. [CaLl90]
   (c) L'algorisme de les divisions successives. [Rifa92]
   (d) Aritmètica modular. L'anell $Z/(m)$. [CaLl90]
   (e) Congruències i equacions diofàntiques lineals. [CaLl90]
   (f) Teorema de Dirichlet. [Rifa92]
   (g) Teorema dels residus xinesos. [GåTa88]
   (h) Sobre el cost computacional de les operacions aritmètiques. [GåTa88]
   (i) Aplicacions a la Criptografia. Criptosistema RSA. [RiHu91]
3. L'anell de polinomis $K[x]$.
   (a) Divisió entera i ideals de l'anell de polinomis $K[x]$ a coeficients a un cos. [CaLl90]
   (b) Màxim comú divisor i polinomis irreductibles. [CaLl90]
   (c) L'algorisme de les divisions successives en el cas de l'anell de polinomis $K[x]$. El teorema de Diriclet. [Rifa92]

(d) Els anells $K[x]/(m(x))$. Cossos finits no trivials. [CaLl90]

4. Cossos finits

   (a) Introducció. Característica i cos primer. Funció multiplicativa d'Euler. [Bigg89]

   (b) Polinomis primitius i elements primitius en un cos finit. [Bigg89]

   (c) Representació vectorial dels elements d'un cos finit i representació potencial. Logaritmes de Zech. [RiHu91]

   (d) Construcció explícita de cossos finits. [RiHu91]

   (e) Calculabilitat en cossos finits i registres de desplaçament amb retroalimentació lineal (*LFSR*). [RiHu91]

   (f) Aplicacion a la correcció d'errors en les transmissions digitals. [Bigg89]

Temporització i Ordre d'execució:

Capítol	Setmanes
2	4 (o 5)
3	3
4	4 (o 5)
1	(Fins a final de curs)

Bibliography

[Ande90] I.Anderson, "*A First Course in Combinatorial Mathematics*", Clarendon Press, Oxford 1990.

[Bigg89] N.L.Biggs, "*Discrete Mathematics*", Clarendon Press. Oxford, 1989.

[CaLl90] M.Castellet, I.Llerena, "*Àlgebra Lineal i Geometria*", Pub. UAB, 1990.

[GåTa88] L.Gårding, T.Tambour, "*Algebra for Computer Science*", Springer-Verlag, 1988.

[RiHu91] J.Rifà, L.Huguet, "*Comunicación Digital, Teoría Matemática de la Información, Codificación Algebraica, Criptología*", Masson Barcelona, 1991.

[Rifa92] J.Rifà, "*L'algorisme de les divisions successives i les seves aplicacions*". Document intern. 1992.