

Objectius: S'estudiaran els aspectes matemàtics més rellevants de la combinatòria enumerativa, la recurrència, l'aritmètica i la teoria de grafs. Els problemes combinatoris i la recurrència apareixen en l'anàlisi d'algorismes i en la determinació de la complexitat computacional. L'aritmètica modular és el fonament de diverses tècniques criptogràfiques. La teoria de grafs facilita la modelització d'estructures de dades i l'estudi dels problemes de xarxes i d'optimització.

Avaluació: Es basarà en un examen escrit de resolució d'exercicis sobre els temes de l'assignatura i en l'avaluació continuada a les sessions de problemes i de pràctiques.

Temari

Aritmètica entera i modular

Algorisme de divisió entera. Representació de nombres en base arbitrària. Nombres primers. Màxim comú divisor i mínim comú múltiple. Algorisme d'Euclides. Identitat de Bézout. Congruències. Suma i producte mòdul un enter. Divisors de zero i elements invertibles. Càlcul d'inversos. Sistemes d'equacions en congruències. Funció d'Euler. Fonament del mètode RSA d'encryptació. Generació de nombres pseudoaleatoris.

Combinatòria i recurrència

Principi de les caixes. Principi d'inclusió i exclusió. Desarranjaments. Variacions i variacions amb repetició. Permutacions. Coeficients binomials i multinomials. Permutacions amb repetició. Combinacions amb repetició. Particions d'un nombre enter. Particions d'un conjunt. Nombres de Stirling. Composició de permutacions. Descomposició de permutacions en cicles disjunts. Paritat d'una permutació. Conjugació. Definicions recursives. El principi d'inducció. Successions en forma recurrent. Resolució de recurrències lineals homogènies. Exemples no homogenis.

Teoria de grafs

Definicions bàsiques. Taules d'adjacències. Isomorfisme de grafs. Grafs bipartits. Representació matricial. Recorreguts i cicles. Grafs eulerians i hamiltonians. Planaritat i fórmula d'Euler. Arbres. Algorísmica en grafs.

Bibliografia orientativa

Biggs, N. L., *Matemática discreta*, Vicens Vives, Barcelona, 1994.

Comellas, F. i altres, *Matemàtica discreta*, Edicions UPC, Barcelona, 1994.

Trias, J., *Matemàtica discreta. Problemes resolts*, Edicions UPC, Barcelona, 2001.