

Fonaments de matemàtica discreta

Curs 2000/2001

<http://ccd.uab.es>

Enginyeria Tècnica Informàtica
Escola Universitària d'Informàtica de Sabadell

UAB

2 Programa

2.1 Combinatòria enumerativa

Regla del producte i regla de la suma

Permutacions

Combinacions i nombres binomials

El teorema binomial

Principi d'inclusió-exclusió

Funcions generadores ordinàries

Funcions generadores exponencials

Equacions recurrents lineals:

Plantejament

Resolució iterativa

Mètode de les arrels

2.2 Aritmètica

Grup, anell i cos

Axioma d'ordenació. Divisió entera

Màxim comú divisor. Nombres primers

Algorisme de les divisions successives. Identitat de Bézout

Teorema de factorització

Equacions diofàntiques lineals

Congruències. Teorema del residu (xinès)

L'anell Z_m . Aritmètica modular

Funció $\Phi(n)$. Teorema d'Euler i teorema de Fermat

Aplicació a la criptografia: l'algorisme *RSA*

2.3 Polinomis i cossos finits

L'anell de polinomis $Z_p[x]$

Divisió i màxim comú divisor

Factorització i polinomis irreductibles

L'anell $Z_p[x]/(m(x))$: aritmètica i propietats

Característica, ordre i element primitiu

Teorema de Lagrange i conseqüències

Construcció de $GF(q)$

Polinomis mínims i polinomi primitiu

Aplicació a la codificació: els codis *BCH*