# 20341: FONAMENTS DE MATEMÀTICA DISCRETA

(Titulació d'Enginyeria en Informàtica – Segon semestre)

## Programa:

### Capítol 1: Aritmètica. (5 setmanes)

Anells, ideals. L'anell dels enters.
Divisió entera.
Mínim comú múltiple i màxim comú divisor. Algorisme d'Euclides. Ident. de Bézout.
Nombres primers.
Congruències. Equacions diofàntiques lineals.
Aritmètica modular. Els anells $Z_m$.
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: criptosistema RSA.

### Capítol 2: L'anell de polinomis. (4 setmanes)

Divisió de polinomis.
Mínim comú múltiple i màxim comú divisor. Algorisme d'Euclides. Ident. de Bézout.
Polinomis irreductibles. Algorisme de Berlekamp.
Zeros d'un polinomi.
Congruències mòdul un polinomi.
Els anells $K[x]/(m(x))$.

### Capítol 3: Cossos finits. (4 setmanes)

Construcció explícita de cossos finits.
Característica i cos primer. Cardinal d'un cos finit.
Ordre d'un element. Elements primitius en un cos finit.
Descomposició $x^n - x$ en factors.
Representació vectorial i potencial dels elements d'un cos finit.
Polinomis mínims, polinomis primitius.
Calculabilitat en cossos finits i registres de desplaçament amb retroalimentació lineal.
Aplicació a la codificació: codis BCH.