Fonaments de Matemàtica Discreta

Enginyeria Informàtica.

1. **Aritmètica**
   - Anells, ideals. L'anell dels enters.
   - Divisió entera.
   - Mínim comú múltiple i màxim comú divisor. Algorisme d'Euclides. Identitat de Bézout.
   - Nombres primers.
   - Congruències. Equacions diofàntiques lineals.
   - Aritmètica modular. Els anells $\mathbf{Z}_m$.
   - 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.

2. **L'anell de polinomis $K[x]$**
   - Divisió de polinomis.
   - Mínim comu múltiple i màxim comu divisor. Algorisme d'Euclides. Identitat de Bézout.
   - Polinomis irreductibles. Algorisme de Berlekamp.
   - Zeros d'un polinomi.
   - 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.
   - Descomposició $x^{p^n} - x$ en factors.
   - Representació vectorial i representació potencial dels elements d'un cos finit.
   - Polinomis mínims, polinomis primitius.
   - Calculabilitat en cossos finits i registres de desplaçament amb retroalimentació lineal (LFSR).
   - Aplicació a la codificació: codis BCH.

BIBLIOGRAFIA BÀSICA

- N.L. Biggs, "Discrete Mathematics"
  Oxford University Press, 1985
  (En castellà: "Matemática Discreta", Vicens Vives, 1994)

- M. Castellet i I. Llerena, "Algebra Lineal i Geometria"
  Manuals de la Universitat Autonoma de Barcelona, 1990

- L. Childs, "A concrete introduction to higher algebra"
  Undergraduate Texts in Mathematics, Springer-Verlag, 1979

- J. Rifà i L. Huguet,
  "Comunicación Digital, Teoría Matemática de la Información, Codificación Algebraica, Criptología"
  Masson Barcelona, 1991