Polinomios y Factorización 2007

Programa

I.– Factorización en $\mathbb{Q}[x]$: algoritmos "densos".
  (a) Introducción y repaso. Algoritmo de von Schubert, 1793 (Kronecker, 1882).
  (b) Herramientas para la estructura de los algoritmos modernos:
    - Lema de Hensel (relación con los números p-ádicos y el teorema local-global de Hasse-Minkowski para formas cuadráticas).
    - Medida de Mahler y Altura de factores de polinomios - Factorización sobre cuerpos finitos (Algoritmo de Berlekamp, 1970)
  (c) El algoritmo de Zassenhaus, 1969, y los problemas de recombinación de factores
  (d) El algoritmo polinomial de Lenstra, Lenstra y Lovasz, 1982
    - Látices y búsqueda de vectores cortos en látices
    - Aplicación a la recombinación de factores
    - Otras aplicaciones
  (e) Mejoras: los resultados de Van Hoeij, 1998, 2005.

II.– Factorización en $K[x]$ y en $K[x_1, ..., x_n]$ con K cuerpo de números: algoritmos "densos".

III.– Factorización de polinomios ralos en $K[x]$ con K cuerpo de números:
  (a) Herramientas:
    - Valores absolutos en cuerpos de números y altura de números algebraicos, propiedades.
    - teorema de Dobrowolski, 1979 (Problema de Lehmer, 1933).
  (b) Algoritmo de Lenstra, 1999, para polinomios ralos (principio de la brecha).

IV.– Factorización de polinomios ralos en $K[x_1, ..., x_n]$.