



E.T.S. de Ingeniería Informática

Ingeniería Informática

Programa de la asignatura

Introducción a la Matemática Discreta

Curso 2000-2001

Tema 1: Aritmética entera

El conjunto \mathbf{Z} de los números enteros. Definiciones recursivas. Inducción matemática: conjuntos inductivos, el método de inducción. Divisores. Máximo común divisor: algoritmo de Euclides. La identidad de Bezout. Mínimo común múltiplo. Ecuaciones diofánticas lineales. Números primos y factorización. Distribución de Primos. Primos de Fermat y Mersenne. Test de primalidad y factorización.

Tema 2: Aritmética modular

Aritmética modular. Congruencias lineales. Sistemas de congruencias lineales: Teorema Chino del Resto. Sistemas de congruencias no lineales: una generalización del Teorema Chino del Resto. La aritmética en \mathbf{Z}_p : el Pequeño Teorema de Fermat y el Teorema de Wilson. Pseudoprimos: tests de base a y números de Carmichael. Test de Lucas-Lehmer. Unidades. La función de Euler. Aplicaciones: criptografía **RSA** .

Tema 3: Técnicas de contar

El principio de adición. El principio de inclusión y exclusión. Contar en tablas. Funciones, palabras y variaciones: variaciones sin repetición y permutaciones. Números binómicos: combinaciones con repetición y Teorema del binomio.

Tema 4: Recursión

Recursiones lineales homogéneas. Recursiones lineales no homogéneas con coeficientes constantes.

Bibliografía:

- **I. Andersen.** *Introducción a la combinatoria*. Ed. Vicens Vives, 1993.
- **N.L.Biggs.** *Matemática Discreta*. Ed. Vicens Vives, 1994.
- **F.J. Cobos.** *Introducción a la Matemática Discreta*. Apuntes disponibles en la dirección: http://www.ma1.us.es/docencia/apuntes/ap_IMD.pdf
- **R.P. Grimaldi.** *Matemáticas discreta y combinatoria*. Ed. Addison-Wesley Iberoamericana, 1989.
- **G.A. Jones y J.M. Jones.** *Elementary Number Theory*. Springer-Verlag, 1998.