Introducción a la Matemática Discreta

1er curso de Ingeniería en Informática

Primer Cuatrimestre

Curso 2005/2006

Programa

Aritmética entera

El conjunto 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.

Aritmética modular

Aritmética modular. Congruencias lineales. Sistemas de congruencias lineales: Teorema Chino del Resto. La aritmética en Z_p: el Pequeño Teorema de Fermat y el Teorema de Wilson. Test de pseudoprimalidad: pseudoprimos y números de Carmichael. Test de Lucas-Lehmer. La función de Euler. Aplicaciones: criptografía RSA.

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.

Recursión

Recurrencias lineales homogéneas. Recurrencias lineales no homogéneas con coeficientes constantes. Funciones generadoras.

Bibliografía

- **I. Anderson**: ***Introducción a la combinatoria.*** Ed. Vicens Vives. 1993.
- **N.L. Biggs**: ***Matemática discreta.*** Ed. Vicens Vives. 1994.
- **F.J. Cobos Gavala**: ***Introducción a la Matemática Discreta.*** Apuntes disponibles aquí .
- **R.P. Grimaldi**: ***Matemáticas discreta y combinatoria.*** Addison-Wesley Iberoamericana. 1994.
- **G.A. Jones y J.M. Jones**: ***Elementary Number Theory.*** Springer-Verlag. 1998.

Metodología

Consultar la Página de material para el curso actual.

Evaluación

Consultar la Guía Docente

Prácticas

Se realizarán tres prácticas de laboratorio que serán obligatorias. Para aprobar la asignatura será necesario haber obtenido una evaluación positiva de las mismas.