Departamento de Matemática Aplicada I

Introducción a la Matemática Discreta

1er curso de Ingeniería Técnica en Informática

Primer cuatrimestre

Curso 2002/2003

En http://ma1.eii.us.es/PDoc hay contenidos de interés para los alumnos de esta asignatura

Programa

Aritmética entera

Números enteros. Inducción. Definiciones recursivas. Divisibilidad y el algoritmo de Euclides. Ecuaciones diofánticas. Números primos. Test de primos. Factorización. Contando números primos. Búsqueda de primos grandes.

Prácticas: Cálculo recursivo de la sucesión de Fibonacci. El crecimiento de las funciones exponenciales. Ejecución del algoritmo de Euclides. Cálculo de la identidad de Bézout. Resolución de algunas ecuaciones diofánticas mediante el algoritmo extendido de Euclides.

Congruencias

Congruencias. Operaciones aritméticas. Unidades. Algoritmo de cálculo de inversos. Teorema Chino del Resto. Función de Euler. Teoremas de Fermat y de Euler. Test de primos. Función de Euler y Factorización. Aritmética modular y criptografía. El criptosistema RSA. Potencias de exponente grande.

Prácticas: Operaciones aritméticas en Cálculo de inversos en Usos prácticos del Teorema Chino del Resto. Experimentos con la función de Euler. Intercambio de mensajes cifrados con distintos criptosistemas clásicos. Criptoanálisis. Generación de claves RSA. Intercambio de mensajes codificados con RSA.

Funciones, algoritmos y combinatoria

Introducción. Funciones inversas. Funciones inyectivas y sobreyectivas. Funciones y algoritmos. Complejidad y eficiencia. El problema de contar. Las reglas de la suma y el producto. El principio de distribución. Permutaciones. Contar subconjuntos: combinaciones. Números combinatorios y el Teorema del Binomio. Principio de inclusión y exclusión. Funciones inyectivas, palabras y variaciones. Contando con repetición.

Prácticas: Experiencias con funciones de un solo sentido: logaritmo discreto, potencias en Pruebas de distintos algoritmos para el número combinatorio. Ejecución de algoritmos recursivos e iterados.

Recursión

Funciones generatrices. Ejemplos. Descomposición de enteros. Recurrencias lineales. Procedimientos recursivos. Recurrencias lineales no homogéneas. Recurrencias y funciones generatrices. Estrategias recursivas.

Bibliografía

- **I. Anderson**: ***Introducción a la combinatoria.*** Ed. Vicens Vives. 1993.
- **N.L. Biggs**: ***Matemática discreta.*** Ed. Vicens Vives. 1994.
- **R.P. Grimaldi**: ***Matemáticas discreta y combinatoria.*** Ed. Addison-Wesley Iberoamericana. 1994.
- **D.E. Knuth**: ***El arte de programar ordenadores. Vol. I: Algoritmos fundamentales.*** Ed. Reverté. 1986.

Metodología

Apuntes

El Departamento no tiene publicados apuntes de esta asignatura. Deberán usarse las notas de clase y la bibliografía.

Boletines de problemas

Existe una colección de problemas propuestos.

NUEVO También se pueden consultar las soluciones de los últimos exámenes:

- 5 de febrero de 2002

Evaluación

Se realizará un examen en la fecha fijada por el centro. Este examen consistirá en varios ejercicios de carácter teórico práctico. Para aprobar la asignatura será necesario haber realizado las prácticas o haber superado un examen de prácticas.

Prácticas

Se realizarán 3 prácticas, que serán obligatorias.

Las prácticas se realizarán en los días y horas que se pueden consultar aquí.

Los alumnos que realicen la totalidad de las prácticas no necesitarán examinarse de las mismas. Para los que no estén en este caso se realizará un examen, que será necesario superar para poder aprobar la asignatura. Este examen consistirá en varios ejercicios

relacionados con las prácticas y se hará en un laboratorio. Aquellos alumnos que hayan realizado las prácticas en el curso anterior no necesitarán hacerlas en este curso.

Se utilizarán programas diseñados especialmente para estas prácticas. Los alumnos que lo deseen podrán obtener una copia del programa de instalación.

Profesores

- **Álvarez Solano, Víctor**
  Grupo 1 de gestión (teoría) y grupo 3 de gestión.
- **Cáceres Sansaloni, Mª Teresa**
  Grupo 2 de sistemas (teoría) y grupo 4 de sistemas.
- **Gómez Martín, José Ramón**
  Grupo 3 de sistemas (teoría).
- **Portillo Fernández, José Ramón**
  Grupo 1 de sistemas (prácticas), grupo 2 de sistemas (prácticas), grupo 3 de sistemas (prácticas), grupo 1 de gestión (prácticas) y grupo 2 de gestión (prácticas).
- **Valeiras Reina, Gerardo**
  Grupo 1 de sistemas (teoría) y grupo 2 de gestión (teoría).

Tutorías

Los horarios de tutoria y asistencia al alumnado se publicarán en el Departamento.