Matemática Discreta

Ingeniería Técnica en Informática de Gestión

2007-2008

Prof. Juan Antonio López Ramos (CITE III, 1.42.0)

La asignatura Matemática Discreta abarca iniciaciones a diversas materias cuyos métodos discretos tienen aplicación en numerosos apartados de las Matemáticas y en la Computación. Como ejemplos pueden citarse la Teoría de Números, con aplicación en métodos de conteo, complejidad algorítmica o Criptografía; la teoría de Anillos de Polinomios, con aplicaciones también en Criptografía o en Teoría de la Información y la Codificación; la Teoría de Grafos y su relación con los métodos de optimización o las estructuras de datos, el álgebra booleana y sus aplicaciones en la Teoría de Lenguajes y, por supuesto, la Lógica.

El objetivo de esta asignatura es que el alumno domine los conceptos y técnicas en los diversos campos en los que se les introduce y conozca sus aplicaciones en los diversos campos de la Informática. Esto último trata de conseguirse con la realización de guiones prácticos para cada tema en los que se utiliza el programa *Matemática* y que se llevan a cabo en las clases de prácticas.

La asignatura consta de 60 horas de clase, de las cuales 30 corresponden a horas de teoría y las otras 30 son horas dedicadas a la realización de los guiones prácticos anteriormente citados y la resolución de relaciones de problemas que complementen las clases teóricas.

Temario

Tema 1. Conjuntos, aplicaciones y relaciones.

Contenidos: Este primer tema aparece como una base teórica sobre la que se construye el resto de la asignatura. El concepto de *conjunto* es algo que a lo largo de la historia ha aparecido en todas las ramas de las Matemáticas. Se exponen las distintas formas en las que un conjunto puede ser definido, la relación de pertenencia de un elemento a un conjunto y el concepto de subconjunto. Se presentan conjuntos notables como son el conjunto vacío y el conjunto de las partes de un conjunto y las operaciones básicas entre conjuntos: unión, intersección, complemento, diferencia, unión disjunta y producto cartesiano. El concepto de producto cartesiano da lugar a los dos siguientes puntos del tema: una *aplicación* de un conjunto A en otro B no es más que un subconjunto del producto cartesiano de A por B y una *relación binaria* en un conjunto A es, a su vez, un subconjunto del producto cartesiano de A por sí mismo. Se estudian los conceptos de dominio y recorrido de una aplicación y los distintos tipos de aplicaciones atendiendo a éstos, es decir *aplicaciones inyectivas, sobreyectivas y biyectivas*. Finalmente, se presentan las distintas propiedades que puede satisfacer una relación binaria y así, aparecen los dos tipos de relaciones binarias que serán esenciales para el tema siguiente, como son los de *relación binaria de equivalencia y relación binaria de orden.* Asimismo se introduce el concepto de conjunto cociente dado por una relación binaria de equivalencia.

Objetivos Mínimos: Conocer los conceptos de conjunto, aplicación y relación binaria, saber establecer perfectamente la pertenencia de un elemento a un conjunto y la relación de que un conjunto sea subconjunto de otro e identificar los distintos tipos de aplicaciones y relaciones binarias estudiados en el tema.

Duración: 2 hora de teoría y 2 hora de prácticas.

Tema 2. Números naturales y enteros.

Contenidos: Se introducen el conjunto de los números naturales y el concepto de definición recurrente. Obtenemos el "orden de los naturales" como un ejemplo de relación binaria de orden en dicho conjunto. De forma natural es introducido entonces el conjunto de los números enteros y se define una relación de orden en el mismo. Debido a las buenas propiedades de este orden, esto nos permite la obtención de un algoritmo para la división de números enteros. A continuación se expone el *Principio de Inducción* de los números naturales y sus consecuencias para la demostración de propiedades de conjuntos numerables, como los sistemas de numeración. Un resultado básico en teoría de números y que utiliza el principio de

inducción para ser probado es el *algoritmo de Euclides* para el cálculo del máximo común divisor de dos números enteros. Como consecuencia del mismo obtendremos el *Teorema de Bezout* que caracteriza cuando dos números enteros son coprimos o el *Teorema Fundamental de la Aritmética* que establece que el conjunto de números primos es infinito. Finalmente, otra consecuencia importante del Algoritmo de Euclides es la resolución de las denominadas ecuaciones lineales diofánticas (con dos incógnitas). Para finalizar el tema se introduce el concepto de congruencia de números enteros como un ejemplo de relación binaria de equivalencia y aparece, de forma natural, un ejemplo de conjunto cociente dado por la relación de equivalencia de los números enteros. Se estudian las estructuras inducidas en el mismo por la suma y la multiplicación de números enteros y finalmente se introducen las ecuaciones y sistemas de ecuaciones lineales en congruencias, dando como método para resolver estos últimos, el *Algoritmo del Resto Chino*. Finalmente se explican dos teoremas clásicos de la Teoría de Números como son el *Pequeño Teorema de Fermat y el Teorema de Euler*. En clase de prácticas se verá un ejemplo de la relación entre la Teoría de Números y la criptografía, como es el sistema RSA.

Objetivos mínimos: El alumno ha de ser capaz de usar el Principio de Inducción para probar propiedades sobre conjuntos de números naturales o la obtención de fórmulas; resolver ecuaciones lineales diofánticas y plantear problemas cuya solución venga dada por una de estas ecuaciones; conocer la estructura de conjuntos cocientes de números enteros dados por relaciones de congruencia, así como resolver ecuaciones y sistemas de ecuaciones lineales en congruencias y como antes, plantear problemas relacionados con estas ecuaciones y sistemas.

Duración: 8 horas de teoría y 8 horas de prácticas.

Tema 3. Grupos.

Contenidos: El concepto de grupo ya nos ha aparecido de forma natural en el tema anterior en el caso de tratar con conjuntos de números enteros o conjuntos cocientes de números enteros dados por relaciones de congruencia. Se introduce entonces formalmente el concepto de *grupo* y se exponen también los de subgrupo, subgrupo generado por un conjunto y subgrupo cíclico. Aparece de forma natural el concepto de orden de un elemento en un grupo. Se enumeran entonces diversos ejemplos conocidos ya por el alumno como los anteriormente citados o grupos de matrices, grupos dados por un conjunto finito y una tabla de operaciones para el mismo y se estudia un ejemplo muy importante en Computación como es el *grupo de las permutaciones de un conjunto finito o grupo simétrico* y sus subgrupos destacados como son el *grupo alternado* y el *grupo diédrico*. Se estudian distintas representaciones de las permutaciones y métodos y fórmulas para operar de forma rápida con ellas así como para determinar si pertenecen o no a estos subgrupos destacados.

Objetivos mínimos: Se ha de ser capaz si un conjunto dado con una operación definida sobre el mismo constituye o no un grupo; operar correctamente con permutaciones, calcular el orden, signatura e inverso de una permutación o calcular subgrupos de permutaciones como el alternado, el diédrico o simplemente el subgrupo generado por un conjunto de permutaciones.

Duración: 6 horas de teoría y 6 de prácticas.

Tema 4. Anillos de Polinomios.

Contenidos: El concepto que sigue de forma natural al de grupo es el de anillo. Se define formalmente *anillo* exponen ejemplos ya conocidos por el alumno como los números enteros, los conjuntos cocientes de números enteros por relaciones de congruencias, anillos de matrices o anillos de polinomios. Un concepto básico en Matemáticas es el de reducibilidad de un polinomio, con una gran aplicación, por ejemplo, en Teoría de la Información y la Codificación. Se dan criterios de irreducibilidad de polinomios sobre el conjunto de los números enteros como el *teorema del resto*, *el criterio de Eisenstein* y *el criterio del módulo finito*.

Objetivos mínimos: El alumno ha de poder determinar si un conjunto dado con dos operaciones en el mismo tiene estructura de anillo así como determinar la irreducibilidad de un polinomio usando los criterios de irreducibilidad.

Duración: 2 horas de teoría y 2 horas de prácticas.

Tema 5. Introducción a la Teoría de Grafos.

Contenidos: En este tema se trata de introducir al alumno en una de las áreas de la Matemática Discreta con aplicaciones más diversas en Computación. En primer lugar se enseña a definir un *grafo no dirigido* manera formal a partir de tres posibles definiciones, es decir, a partir de su representación gráfica, de sus conjuntos de vértices y aristas y a partir de su matriz de adyacencias. Se tratan el concepto de *subgrafo*, los distintos tipos de caminos en un grafo y la distancia entre dos vértices y el grado de un vértice. Como resultado en este apartado cabe destacar el teorema que relaciona el número de caminos entre dos vértices y las potencias de la matriz de adyacencias de dicho grafo. A continuación se estudian diversos tipos de grafos: *grafos conexos*, *grafos de Euler*, así como el teorema que los caracteriza, *grafos de Hamilton*, *grafos bipartidos* y caracterizaciones de los mismos, *grafos bipartidos con emparejamiento* y algoritmos que determinan su existencia, *árboles* y el concepto de *grafo plano* y el *Teorema de Kuratowski* que los caracteriza. Para finalizar el tema se introduce el concepto de *grafo dirigido* y se hace notar la existencia de una teoría paralela a la anterior para este nuevo tipo de grafos.

Objetivos mínimos: Se ha de ser capaz de determinar un grafo a partir de cualquiera de las definiciones así como de distinguir los distintos tipos de grafos, además de aplicar estos conceptos para la resolución de problemas de computación o de índole real.

Duración: 6 horas de teoría y 6 horas de prácticas.

Tema 6. Retículos y Álgebras de Boole.

Contenidos: El concepto de orden estudiado en el primer tema da lugar a la existencia de elementos notables en un conjunto ordenado, como son el de máximo, mínimo, elemento maximal y minimal, cotas inferiores y superiores y supremo e ínfimo. Aparece entonces el concepto de *retículo ordenado*. Su representación gráfica constituye un grafo dirigido. Se define *retículo algebraico* y se establece la equivalencia entre ambas definiciones de retículo. Se estudian diversos tipos de retículos: *retículos distributivos*, así como métodos de identificación rápida de los mismos, *retículos acotados y retículos complementados*. Aparece entonces el concepto de *álgebra de Boole* y se establece el Teorema de Representación de álgebras de Boole finitas.

Objetivos mínimos: Calcular los elementos notables en un conjunto parcialmente ordenado y establecer y se trata o no de un retículo y, en su caso decidir si es distributivo y complementado; usar el teorema de representación de álgebras de Boole finitas para determinar si un retículo finito es o no una de dichas álgebras de Boole.

Duración: 4 horas de teoría y 4 horas de prácticas.

Tema 7. Introducción a la Lógica Proposicional.

Contenidos: En este daremos un ejemplo de álgebra de Boole infinita como es el álgebra de las proposiciones lógicas. Se introducen las proposiciones lógicas y las conectivas y se formalizarán, usando este lenguaje, expresiones del lenguaje natural. Finalmente se usarán las propiedades de álgebra de Boole para probar la validez de razonamientos lógicos.

Objetivos mínimos: Formalización de expresiones de lenguaje natural y demostración de razonamientos lógicos usando las operaciones y propiedades del álgebra de Boole.

Duración: 2 horas de teoría y 1 horas de prácticas.

Evaluación

La evaluación de la asignatura se llevará a cabo siguiendo los siguientes porcentajes:

- un 20% correspondiente a un examen de prácticas sobre los guiones de prácticas realizados a lo largo del curso y que se llevará a cabo durante la última hora de prácticas del curso.

- el 80% restante se evaluará sobre un examen escrito tradicional en fecha a determinar por la Escuela Politécnica Superior de la Universidad de Almería y en el que habrá dos partes de igual valor, una correspondiente a preguntas de teoría y otra a la resolución de problemas.

Bibliografía

- M.ANZOLA, J. CARUNCHO. *Problemas de Álgebra. Tomo I.*
- C. BERGE. *Graphes*. Ed. Gauthier-Villars.
- J.R. DURBIN. *Modern Algebra*. Ed. John Wiley.
- J.B. FRALEIGH. *Álgebra abstracta*. Ed. Addison-Wesley Iberoamericana. Tercera Edición.
- J.R. GARCÍA ROZAS, y L. OYONARTE ALCALÁ. *Problemas Resueltos de Álgebra Básica y Matemática Discreta*. Servicio de publicaciones de la UALM. 1999.
- A. GILL. *Applied algebra for the computer siences*. Ed. Prentice-Hall.
- F. HARARY. *Graph theory*. Ed. Addison-Wesley.
- A.I. KOSTRIKIN. *Introducción al álgebra*. Ed. McGraw-Hill. Segunda edición.
- R. LIDL, G. PILZ. *Applied abstract*. Ed. Springer-Verlag.
- S. LIPSCHUTZ. *Matemática Discreta*. Ed. McGraw-Hill. Serie Schaum.
- S. LIPSCHUTZ. *Teoría de conjuntos y temas afines*. Ed. McGraw-Hill. Serie Schaum.
- M. MIGNOTTE. *Mathematics for computer algebra*. Ed. Springer-Verlag.
- L.E. SIGLER. *Algebra*. Ed. Reverté.