Introducción a la Matemática Discreta

Manuel Murillo Tsijli

Editorial Tecnológica de Costa Rica

4a edición

Introducción a la Matemática Discreta

Introducción a la Matemática Discreta

Manuel Murillo Tsijli

Editorial Tecnológica de Costa Rica

Primera edición.
Editorial Tecnológica de Costa Rica, 2004.

Segunda edición.
Editorial Tecnológica de Costa Rica, 2007.

Tercera edición.
Editorial Tecnológica de Costa Rica, 2009.

Cuarta edición.
Editorial Tecnológica de Costa Rica, 2010.

511.3
M977-i4

Murillo Tsijli, Manuel
Introducción a la matemática discreta / Manuel Murillo Tsijli. -- 4a. ed. -- Cartago, Costa Rica : Editorial Tecnológica de Costa Rica, 2010.
454 páginas.
ISBN 978-9977-66-224-4.
1. Matemática discreta 2. Lógica 3. Conjuntos 4. Relaciones binarias 5. Funciones

© **Editorial Tecnológica de Costa Rica**
Correo electrónico: *editorial@itcr.ac.cr*
Instituto Tecnológico de Costa Rica
Apdo. 159-7050, Cartago
Tel: (506) 2550-2297 / 2550-2336 / 2550-2392
Fax: (506) 2552-5354
Hecho el depósito de ley.

A Héctor y Felipe,
por quienes, en ocasiones sin saberlo,
he cruzado ríos, atravesado valles,
escalado montañas y domado volcanes.

Agradezco profundamente a los colegas y amigos
Evelyn Agüero, Manuel Alfaro,
José Luis Espinoza, Alicia León,
Félix Núñez y Geovanny Sanabria
por sus oportunos comentarios y valiosas sugerencias.
Su interés y apoyo contribuyeron a la
publicación de esta nueva edición.

Contenido

Presentación **13**

Prólogo **17**

Simbología **21**

Capítulo 1. Fundamentos de lógica **25**

1.1 Introducción 27

1.2 Conectivas lógicas 44

1.3 Leyes de la lógica 57

1.4 Inferencias lógicas 62

1.5 Formas normales 77

1.6 Cuantificadores 81

1.7 Inferencias cuantificadas 96

1.8 Métodos de demostración 99

Capítulo 2. Teoría de conjuntos **109**

2.1 Definiciones y operaciones 111

2.2 Conjuntos numéricos 127

2.3 Diagramas de Venn 133

2.4 Leyes de conjuntos 137

2.5 Cardinalidad 141
2.6 Familias de conjuntos 151
2.7 Resultados y demostraciones 155

Capítulo 3. Relaciones binarias 167
3.1 Definiciones y operaciones 169
3.2 Matrices y grafos asociados 175
3.3 Propiedades de las relaciones 187
3.4 Relaciones de equivalencia 198
3.5 Relaciones de orden 206

Capítulo 4. Funciones 213
4.1 Conceptos y definiciones 215
4.2 Funciones lineal y cuadrática 231
4.3 Operaciones con funciones 237
4.4 Funciones inversas 244
4.5 Equipotencia 253
4.6 Principios de conteo 260

Capítulo 5. Inducción y recursividad 267
5.1 Notación Σ y Π 269
5.2 Inducción matemática 276
5.3 Recursividad 293

Capítulo 6. Estructuras algebraicas 307
6.1 Estructuras algebraicas 309
6.2 Grupos 320
6.3 Otros grupos 332
6.4 Subgrupos 336
6.5 Homomorfismos de grupos 343

Capítulo 7. Bases y congruencias numéricas 353

7.1 Sistemas de numeración 355

7.2 Representación en bases enteras 363

7.3 Aritmética en distintas bases 368

7.4 Representación en bases fraccionarias 372

7.5 Congruencias numéricas 376

7.6 Resultados importantes 384

Apéndice A. Solución de algunos ejercicios 389

Bibliografía 439

Índice temático 443

Sobre el autor 453

Presentación

Esta obra está dirigida principalmente a estudiantes de Matemática y de Computación. Sin embargo, también es de interés para todas aquellas personas que encuentran en las matemáticas el lenguaje universal con el que se pueden explicar los fenómenos que se presentan en nuestro entorno y, por supuesto, a todos los que ven en ella una puerta que los llevará hacia la búsqueda del conocimiento orientado al desarrollo científico y tecnológico.

Contiene los temas que habitualmente se imparten en un curso de matemática discreta de nivel universitario, como base para una formación académica sólida. Uno de sus objetivos principales es presentar los contenidos de forma rigurosa y atractiva; para ello, se han escogido diversos ejemplos donde se observan los métodos de demostración usuales en la matemática.

Se ha tratado de que los temas sean asimilados en forma paulatina. Con ese propósito se han incluido, al final de cada sección, ejercicios ilustrativos de los temas expuestos, y de la mayoría de ellos se puede encontrar la solución, parcial o completa, en el Apéndice A. Además, los conceptos o definiciones más importantes se presentan en recuadros sombreados para recalcar su importancia.

En esta nueva edición se han incluido algunos teoremas importantes con sus respectivas demostraciones; para mayor claridad, el final de ellas se indica con el símbolo $\square$.

Asimismo, se presenta una cantidad considerable de ejemplos que ayudarán al lector a comprender los conceptos que aquí se desarrollan. Dichos ejemplos son una guía para resolver los ejercicios propuestos; en la medida de lo posible debe observarse, en cada ejemplo desarrollado, el método expuesto; se ha intentado que éstos sean lo más explicativos posible. El final de cada uno se indica con el símbolo ■.

El procedimiento expuesto para resolver cada ejemplo o ejercicio no siempre es único. Debe intentarse y quizá encuentre uno que sea igualmente efectivo y eficiente.

Puede suceder que algunos de los contenidos de esta obra ya sean dominados por el lector; sin embargo, se quiere fortalecer aquellos que, por su importancia, se convierten en herramientas esenciales para la comprensión de los temas en cursos posteriores y para su formación académica integral y su desarrollo profesional.

En el capítulo 1 se presenta una introducción a la lógica. Se inicia con las proposiciones lógicas, se enuncian las leyes esenciales de la lógica, las reglas de inferencia, cuantificadores y sus diversas aplicaciones. Se presenta un resumen de los principales métodos de demostración que se utilizan a lo largo del texto y se presenta un interesante aporte sobre la enseñanza de la demostración de implicaciones, del profesor M.Sc. Geovanny Sanabria.

En el capítulo 2 se introduce la teoría de conjuntos. Se inicia con las operaciones básicas de conjuntos, simplificación de expresiones y su representación mediante diagramas de Venn, además de incluir una nueva sección dedicada al tema de las familias de conjuntos. En la última sección de este capítulo se profundiza sobre la demostración de proposiciones que involucran conjuntos.

En el capítulo 3 se presenta el tema de las relaciones binarias, sus operaciones básicas y algunas propiedades que permiten clasificarlas. Se profundiza en las relaciones de equivalencia y en las de orden, particiones inducidas, grafos, matriz asociada a una relación y algunas aplicaciones.

En el capítulo 4 se introduce el tema de las funciones desde un punto de vista teórico y práctico, como extensión de una relación binaria. Se profundiza en los conceptos de inyectividad y sobreyectividad, en las operaciones con funciones y las funciones inversas.

En el capítulo 5 se presenta el método de demostración conocido como el *principio de inducción matemática*. Se aplica este método para probar, principalmente, proposiciones cuantificadas que involucran igualdades, desigualdades y divisibilidad. Por último, se aborda el tema de la recursividad, sobre todo en el campo de las relaciones recurrentes y la búsqueda de su fórmula explícita, mediante el análisis hacia atrás y la ecuación característica; en esta sección se incluyen algunos ejemplos interesantes relacionados con el análisis numérico aplicado a la solución de ecuaciones.

En el capítulo 6 se hace una introducción al tema de las estructuras algebraicas, con especial interés en grupos y subgrupos.

En el capítulo 7 se hace una breve introducción al tema de los sistemas de numeración con distintos tipos de bases, además de las congruencias numéricas y su utilidad, siempre como herramientas fundamentales en la programación de computadoras. Además, se muestran algunos teoremas importantes en la teoría de números, en el contexto de las congruencias, como son los teoremas de Wilson, Fermat, Euler y otros.

En el apéndice A se aporta la solución, parcial o completa, de la mayoría de los ejercicios de cada una de las secciones.

Como aportes importantes de esta nueva edición están la inclusión de las secciones 1.7, 2.2, 2.3, 2.6, 3.2, 3.4, 3.5, 4.2, 4.3, 4.5, 4.6, 5.1, 6.3, 6.4, y de una cantidad considerable de ejemplos, ejercicios y soluciones que sin duda hará más clara la exposición de los temas aquí tratados.

Manuel Murillo

Prólogo

Matemática discreta, también conocida como matemática finita, es el estudio de las estructuras matemáticas que son fundamentalmente discretas, en el sentido de que no requieren la noción de continuidad.

Algunos de los conceptos de la matemática discreta no son nuevos, pero como disciplina matemática independiente, es relativamente nueva y ha tenido un crecimiento vertiginoso en las últimas décadas, principalmente debido a su conexión con las ciencias de la computación y su rápido desarrollo.

Los que introdujeron las nociones básicas de la matemática discreta fueron los hindúes. En el siglo VI, ellos ya conocían las fórmulas para, primero, el número de permutaciones de un conjunto con n elementos y, segundo, para el número de subconjuntos, de cardinalidad k, de un conjunto de n elementos. La matemática combinatoria tuvo sus orígenes en los trabajos de Pascal y de De Moivre durante el siglo XVII, y siguió su desarrollo con Jacob Bernoulli y Leonard Euler, principalmente con las ideas de éste último sobre la teoría de grafos. Por otro lado, los métodos probabilísticos iniciados por Paul Erdös se han convertido en una potente herramienta para la combinatoria y la teoría de probabilidad. En realidad, la matemática discreta es una disciplina que unifica diversas áreas de las matemáticas (combinatoria, probabilidad, aritmética y grafos, entre otras) y sus conceptos aparecen, con frecuencia, en muchas ramas de las matemáticas y de otras disciplinas.

La matemática discreta es el ámbito de las matemáticas que se relaciona más de cerca con las computadoras, pues en éstas la información se almacena y se manipula en forma discreta (palabras formadas por ceros y unos), se necesita contar objetos (unidades de memoria, unidades de tiempo), estudiar relaciones entre conjuntos finitos (búsquedas en bases de datos) y analizar procesos que incluyan un número finito de pasos (algoritmos). Entonces los conceptos y notaciones de la matemática discreta son útiles para estudiar y expresar objetos o problemas en algoritmos y lenguaje de programación.

Es posible encontrar aplicaciones en la teoría de la información, tratamiento digital de datos, física estadística, biología molecular, geometría discreta y computacional, criptografía, modelos discretos aplicados a la industria y ciencias de la computación. Debido a sus importantes aplicaciones, el estudio de las estructuras discretas es una de las áreas que está generando más desarrollo e interés en las matemáticas en las últimas décadas.

Para mí es un honor poder elaborar el prólogo de esta obra sobre matemática discreta, escrita por mi colega Manuel Murillo, profesor del Instituto Tecnológico de Costa Rica, y publicada por la Editorial Tecnológica de Costa Rica. En la obra, el desarrollo de los temas se presenta de forma clara, precisa, elegante y con el rigor matemático necesario.

En cada uno de los capítulos se hace una breve introducción y, además, los distintos conceptos y resultados importantes se ilustran con numerosos ejemplos resueltos que figuran intercalados entre el desarrollo teórico de cada sección en cada capítulo, finalizando la sección con una serie de ejercicios propuestos que de seguro ayudará a afianzar los conocimientos adquiridos con el estudio de la sección en cuestión.

El apéndice A contiene las demostraciones y soluciones, parciales o completas, de la mayoría de los ejercicios propuestos en cada una de las secciones, lo cual, sin duda, será de gran ayuda para los lectores en el proceso de enseñanza-aprendizaje.

Esta nueva edición conserva las fortalezas de la anterior e incorpora nuevas características y mejorías, proporcionando un equilibrio entre teoría y práctica. Incluye nuevas secciones, más ejercicios propuestos y sus soluciones, decenas de ejemplos adicionales y datos actualizados; por ejemplo, la mención del hallazgo de los primos de Mersenne número 45 y 46, en el 2008 y el número 47, en el 2009.

Las secciones incluidas son pertinentes y necesarias: inferencias que involucran proposiciones cuantificadas (sección 1.7); conjuntos numéricos (sección 2.2); diagramas de Venn (sección 2.3) como una representación figural de relaciones entre conjuntos; familias de conjuntos (sección 2.6); matriz y grafo asociado a una relación (sección 3.2); las relaciones de equivalencia (sección 3.4) para asociar elementos afines de un conjunto; las relaciones de orden (sección 3.5) para ordenar los elementos de un conjunto; conjuntos equipotentes, numerables y contables (sección 4.5); principios de conteo (sección 4.6) para introducir los conceptos fundamentales del arte de contar, como lo son las permutaciones y las combinaciones de objetos; los símbolos para sumas y productos (sección 5.1); subgrupos (sección 6.4) y la ampliación de los métodos de demostración, en la sección 1.8, con la inclusión de una propuesta del uso de demostraciones desde la lógica matemática, por ser un método que se adapta a la demostración desde la lógica intuitiva.

En el capítulo 5 (sección 5.3) se agregaron algunos ejemplos sobre el uso de la recursividad para determinar los puntos fijos de una función, lo cual representa una buena aplicación de la matemática discreta al análisis numérico.

Los ejercicios de lógica contextualizados con los habitantes de una galaxia ficticia denominada *Vacilonia* atrapan el interés de los lectores. Las referencias a los problemas abiertos, como la conjetura de Goldbach (todo número par mayor que dos es la suma de dos números primos), a conjeturas recién verificadas como la de Poincaré, a aplicaciones prácticas como la criptografía, arte o ciencia de cifrar y descifrar infor-

mación utilizando técnicas matemáticas, las falacias y las paradojas son algunas de las estrategias metodológicas utilizadas por el autor.

Los contenidos principales de un curso introductorio a la matemática discreta son: fundamentos de lógica, teoría de conjuntos, relaciones binarias, funciones, principio de inducción, recursividad y estructuras algebraicas, entre otros temas que se abordan tangencialmente, como las congruencias numéricas y los métodos de demostración, que son expuestos con claridad, rigor, elegancia y de forma agradable.

Estoy seguro de que este libro, especialmente esta reciente edición, será de interés y utilidad para estudiantes de computación, matemática e ingenierías, así como para la comunidad académica en general.

Edison De Faria Campos

Presidente, periodo 2006 – 2008
Asociación de Matemática Educativa

Centro de Investigaciones Matemáticas y Meta-Matemáticas
Escuela de Matemática
Universidad de Costa Rica

Simbología

$P,\ Q,\ R, \ldots$	denotan proposiciones
$\neg P$	negación de P
$P \wedge Q$	conjunción de P y Q
$P \vee Q$	disyunción de P y Q
$P \rightarrow Q$	P implica Q
$P \leftrightarrow Q$	P si y solo si Q
$P \Rightarrow Q$	si $P \rightarrow Q$ es tautología
$P \Leftrightarrow Q$	si $P \leftrightarrow Q$ es tautología
$P \equiv Q$	P equivalente a Q
V_0	denota una tautología
F_0	denota una contradicción
$\therefore$	por lo tanto
$(\Rightarrow\Leftarrow)$	contradicción
$\exists$	cuantificador existencial (existe)
$\nexists$	no existe
$\forall$	cuantificador universal (para todo)
$A,\ B,\ C, \ldots$	denotan conjuntos
$a,\ b,\ c, \ldots$	denotan elementos
$a \in A$	a pertenece a A
$A \subseteq B$	A es subconjunto de B
$A \subset B$	A es subconjunto propio de B

$[a, b]$	intervalo cerrado
$]a, b[$	intervalo abierto
$\mathbb{N}$	$\{0, 1, 2, \dots\}$
$\mathbb{N}^*$	$\{1, 2, \dots\}$
$\mathbb{Z}$	$\{\dots, -2, -1, 0, 1, 2, \dots\}$
$\mathbb{Z}^*$	$\mathbb{Z} - \{0\}$
$\mathbb{Q}$	conjunto de los números racionales
$\mathbb{I}$	conjunto de los números irracionales
$\mathbb{R}$	conjunto de los números reales
$\mathbb{R}^*$	$\mathbb{R} - \{0\}$
$\mathbb{R}^+$	conjunto de los números reales positivos
$A - B$	diferencia de conjuntos
$A \cup B$	unión de conjuntos
$A \cap B$	intersección de conjuntos
$A \triangle B$	diferencia simétrica de conjuntos
$\lvert A \rvert$	cardinalidad de A
$\varnothing$ o $\{\ \}$	conjunto vacío
$\mathcal{U}$	conjunto universo
$A \approx B$	conjuntos equipotentes
$a \approx b$	aproximación de números
$A \preceq B$	A de menor potencia que B
$A \times B$	conjunto producto de A y B
(a, b), (a, b, c)	par ordenado y triplete ordenado
$P(A)$ o 2^A	conjunto potencia de A
$\overline{A}$ o $\complement_A^{\mathcal{U}}$	complemento de A
$\mathcal{R}$, $\mathcal{S}$, $\mathcal{T}, \dots$	denotan relaciones
$a\mathcal{R}b$	a se relaciona con b
$\dot{a}$ o $\overline{a}$ o $[a]$	clase de equivalencia de a
$A/\mathcal{R}$	conjunto cociente
$D_{\mathcal{R}}$	dominio de $\mathcal{R}$

$\mathcal{R}[A]$	rango de $\mathcal{R}$
$G_{\mathcal{R}}$	gráfico de $\mathcal{R}$
$\mathcal{S} \circ \mathcal{R}$	composición de $\mathcal{R}$ y $\mathcal{S}$
$f,\ g,\ h, \ldots$	denotan funciones
$f \circ g$	composición de f y g
$\lvert x \rvert$	valor absoluto de x
$\lceil x \rceil$	función techo
$\lfloor x \rfloor$	función piso o parte entera
$\chi_A(x)$	función característica de A
$f(E)$	imagen del conjunto E
$f^{-1}(F)$	imagen inversa del conjunto F
$f^{-1}(x)$	función inversa de f
$\mathcal{O}(s)$	órbita de s
$n!$	factorial de n
$(\mathcal{G}, *)$	grupo
$*,\ \perp,\ \otimes,\ \oplus, \ldots$	denotan operaciones binarias
$\mathcal{H} < \mathcal{G}$	$\mathcal{H}$ subgrupo de $\mathcal{G}$
S_n	grupo simétrico
$o(\mathcal{G})$	orden del grupo $\mathcal{G}$
$\varphi(n)$	función de Euler
$\equiv$	equivalencia o congruencia
$E_p(m)$	exponente de p en factorización prima de m
N_f	núcleo del homomorfismo f
$\mathbb{Z}_n$	partición de $\mathbb{Z}$ módulo n
$\mathbb{N}_n$	$\{1, 2, 3, \ldots, n\}$
$P(n, r)$	permutaciones
$C(n, r)$	combinaciones
B^A	funciones de A en B
$\mathcal{I}(A, B)$	funciones inyectivas de A en B
$\mathcal{B}(A, B)$	funciones biyectivas de A en B

∞	infinito
$\aleph_0$	aleph cero
$\sum$	suma
$\prod$	producto
$a\|b$	a divide a b
m.c.d.(a, b)	máximo común divisor de a y b
sii	si y solo si
hqd	hay que demostrar que

Capítulo 1

Fundamentos de lógica

"Tweedledee (a Alicia): *Sé lo que estás pensando, pero no es así de todas formas.*
Tweedledum: *Al contrario, si fue así, podría ser; y si fuera así, sería; pero como no es, no es. La lógica es así*".

Lewis Carroll

Introducción
Conectivas lógicas
Leyes de la lógica
Inferencias lógicas
Formas normales
Cuantificadores
Inferencias cuantificadas
Métodos de demostración

En este capítulo se hace una formalización de la lógica, aquella que se utiliza todos los días para razonar, debatir, deducir, comprender e inferir. Cuando se dice, por ejemplo: "solo las personas mayores de 18 *años pueden votar" y "Héctor tiene* 17 *años", se concluye lógicamente que "Héctor no puede votar"; o cuando se dice que la expresión "el hielo es caliente" es falsa, sin duda se emite un juicio de valor o conclusión a partir del conocimiento adquirido con anterioridad o a partir de las diferentes premisas.*

Se inicia con la terminología propia de toda teoría matemática, luego con la particular de la lógica formal y simbólica: conectivas, cuantificadores, proposiciones, entre otros términos, y se clasifican estas proposiciones con base en las tablas de verdad. Luego se ven las leyes de la lógica y las reglas de inferencia, con su respectiva aplicación. Al final se definen los cuantificadores y se trabaja con proposiciones cuantificadas.

Para profundizar el tema tratado en este capítulo, es recomendable consultar las referencias bibliográficas [2], [5], [7], [12], [15], [31] *y para el tema de las paradojas, el interesante artículo* [30].

1.1 Introducción

Para algunos, la *lógica* es la teoría del pensar, la ciencia de los límites del pensar justo y razonado; para otros, se puede definir brevemente como el estudio del razonamiento. En este caso, la lógica es la teoría de

la inferencia, véase [5]. Su estudio es importante porque ayuda a razonar de forma correcta y, con ello, a no incurrir en las llamadas falacias argumentativas. Las leyes de la deducción son innatas en los seres humanos, pero su uso no es obligado y pueden ser ignoradas, incluso, como es el caso de algunas normas morales, sin darse cuenta de ello. Conocer estas leyes con mayor profundidad permite su aplicación.

Algunos de los argumentos lógicos más originales corresponden al matemático y Reverendo Charles Lutwidge Dodgson (1832-1898), conocido por su seudónimo Lewis Carroll, quien además fue lógico, dibujante, fotógrafo y poeta. Catedrático de la Universidad de Cambridge, en Inglaterra, y autor prolífico, dentro de sus obras destacan *Lógica Simbólica*, *Alicia en el País de las Maravillas* y *Silvia y Bruno*. Él mismo explica en su bella obra *Lógica Simbólica* las razones del por qué es importante el estudio de este tema:

> *"La lógica simbólica dará a usted claridad de pensamiento, la habilidad para ver su camino a través de un acertijo, el hábito de arreglar sus ideas en una forma adecuada y clara, y, lo más valioso, el poder para detectar falacias y separar las piezas de los argumentos endebles e ilógicos que encontramos continuamente en libros, periódicos, discursos, y aún sermones, y que fácilmente engañan a aquellos que nunca se han tomado la molestia de dominar este fascinante arte".* (Véase [24]).

El concepto de lógica tiene sus orígenes en los estoicos, probablemente en Zenón de Elea (490-430 a.C.), discípulo de Parménides, aunque la primera lógica sistemática se debe a Aristóteles de Estagira (384-322 a.C.), quien, en uno de los escritos referentes a este tema, se ocupa de las teorías del concepto del *juicio*, de la *conclusión* y de la *prueba*, y es a partir de él que queda constituida como una disciplina propia.

La llamada *lógica inductiva* se caracteriza por el razonamiento de que, a partir de observaciones específicas, se conduce a conclusiones generales y por supuesto que con ella es posible obtener una idea correcta