

ÍNDICE SISTEMÁTICO

	<u>PÁGINA</u>
Sumario	5
Prólogo	7
Unidad didáctica 1. Conjuntos	11
Objetivos de la Unidad	13
1. Introducción	14
2. Definiciones	14
2.1. Conjunto	14
2.2. Conjuntos bien definidos: comprensión y extensión	16
2.3. Elementos: pertenencia	17
2.4. Referencial, conjunto vacío \emptyset , unitario y pares	18
2.5. Igualdad de conjuntos	19
3. Subconjuntos	19
3.1. Definición	19
3.2. Conjuntos anidados	20
3.3. Partes de un conjunto y conjunto de las partes	22
3.4. Partición de un conjunto	23
3.5. Propiedades de la inclusión \subset	24
4. Diagramas de Venn	25

5. Operaciones con conjuntos	29
5.1. Implicaciones y equivalencias. Cuantificadores	31
5.1.1. Implicaciones y equivalencias	31
5.1.2. Cuantificadores	32
6. Leyes de operaciones con conjuntos. Álgebra de conjuntos	32
7. Principio de inclusión-exclusión	36
8. Conjunto producto	37
9. Axiomática de Zermelo-Fraenkel para teoría de conjuntos	38
10. Fundamentación de la matemática a partir del conjunto vacío: definición de números naturales por Von Neumann	39
Conceptos básicos a retener	41
Ejercicios voluntarios	41
Referencias bibliográficas	42
Unidad didáctica 2. Relaciones, aplicaciones y funciones (RAF) ...	43
Objetivos de la Unidad	45
1. Introducción	46
2. Relaciones	47
2.1. Definición	47
2.2. Tipos de relaciones	47
2.2.1. Relaciones unarias o monarias	47
2.2.2. Binarias	47
2.2.3. N-arias	47
2.3. Dominio, recorrido y campo de una relación	49
2.4. Operaciones entre relaciones: restricción; conversa o inversa; producto relativo	50
2.4.1. Representación de relaciones	51
2.5. Propiedades de las relaciones	52
2.6. Composición de relaciones	55
2.7. Relación de equivalencia	56
2.8. Relaciones de orden: mayorantes, minorantes. Límites. Cardinales y ordinales	57
3. Aplicaciones	59
3.1. Definición	59
3.2. Restricción de una aplicación	60
3.3. Grafo de una aplicación	60
3.4. Tipos de aplicaciones	60
3.5. Composición de aplicaciones	63

4. Funciones	64
4.1. Generalidades	64
4.2. Descripción de conjuntos	65
4.3. Ejemplo del uso de funciones: el calendario universal	65
4.4. Funciones de dispersión: funciones «Hash»	68
5. Morfismos	69
Conceptos básicos a retener	73
Ejercicios voluntarios	73
Referencias bibliográficas	75
Unidad didáctica 3. Combinatoria	77
Objetivos de la Unidad	79
1. Introducción	80
2. Principios básicos de conteo	81
2.1. Principio de Dirichlet (1805-1859) o «principio del palomar» o, aun, «principio de las sillas»	81
2.2. Principios de cardinalidad	84
3. Variaciones	85
3.1. Formación y número de variaciones simples	85
3.2. Determinación de la variación que ocupa un lugar determinado	89
3.3. Recíproco	90
3.4. Con repetición	91
3.5. El problema de Ramsey	92
4. Permutaciones	94
4.1. Formación ordenada de las permutaciones	94
4.2. Determinación de la permutación que ocupa un lugar determinado ..	96
4.3. Con repetición	97
4.4. Desórdenes	100
5. Combinaciones	100
5.1. Formación de las combinaciones	100
5.2. Determinación de la combinación que ocupa un lugar determinado ..	103
5.3. Combinaciones con repetición	105
5.4. Números combinatorios	108
6. «Principio de la criba» o de «inclusión-exclusión»	109
6.1. Definiciones y ejemplos	109
6.2. Combinaciones con repetición limitada	110
7. Cuadro-resumen	112

Conceptos básicos a retener	114
Ejercicios voluntarios	114
Referencias bibliográficas	115
Unidad didáctica 4. Inducción	117
Objetivos de la Unidad	119
1. Introducción	120
2. La axiomática de Peano y la inducción matemática	125
2.1. Axiomática de Peano	125
2.2. Inducción matemática	127
3. Inducción matemática o completa	129
3.1. Definición formal	129
3.2. Ejemplos de inducción matemática	132
3.3. Generalización de la inducción	133
3.4. Inducciones estructurales	135
3.5. Inducciones mutuas	136
4. Sumas y construcciones relacionadas	138
4.1. Definiciones	138
4.2. Identidades que implican sumas	140
4.3. Sumas dobles y matrices	143
5. Recursividad	144
5.1. Demostraciones por recursividad	144
5.2. Definiciones recursivas	146
5.3. Sucesiones descendentes	148
5.4. El principio de demostración por recursividad	149
6. Relaciones de recurrencia	150
6.1. Introducción	150
6.2. Tipos de relaciones de recurrencia	151
6.3. Relaciones de recurrencia homogéneas	152
6.4. Ecuaciones de recurrencia no homogéneas	155
Conceptos básicos a retener	160
Ejercicios voluntarios	160
Referencias bibliográficas	161
Unidad didáctica 5. Aritmética modular	163
Objetivos de la Unidad	165

1. Estructuras algebraicas básicas	166
1.1. Semigrupos y monoides	166
1.2. Grupo	166
1.2.1. Isomorfismo entre grupos	167
1.2.2. Grupos finitos	169
1.3. Anillo	170
2. Aritmética entera	171
2.1. Definición	171
2.2. Axioma de buena ordenación	172
2.3. Divisibilidad	173
2.3.1. Teorema de la división entera	173
2.4. Sistemas de numeración	174
2.5. Representación de números enteros en el computador	176
2.6. Algoritmo de Euclides	177
2.6.1. Definición	177
2.6.2. El algoritmo	177
2.6.3. Teoremas de Lamé y Bézout y lema de Euclides	178
2.6.3.1. Teorema de Lamé (1795-1870)	178
2.6.3.2. Teorema de Bézout	178
2.6.3.3. Lema de Euclides	179
2.7. Criterios de divisibilidad: pruebas del 9 y del 11	179
2.7.1. Criterios de divisibilidad	179
2.7.2. Pruebas del 9 y del 11	186
3. Congruencias enteras	191
3.1. La calculadora de reloj	191
3.2. Definición	193
3.3. Aplicaciones de las congruencias	195
4. Ecuaciones diofánticas	200
Conceptos básicos a retener	204
Ejercicios voluntarios	204
Referencias bibliográficas	205
Unidad didáctica 6. Teoría de números	207
Objetivos de la Unidad	209
1. Reseña histórica	210

2. Cardinalidad y ordinalidad	212
3. Bases y sistemas de numeración	215
3.1. Bases de numeración: criterios formales y materiales de adecuación ..	215
3.1.1. Principio del valor relativo	216
3.1.2. Principio de Haenkel	216
3.1.3. Teorema fundamental	216
3.1.4. Cálculos en cualquier base	218
3.1.4.1. Criterios formales de adecuación	221
3.1.4.2. Criterios materiales de adecuación	222
3.1.5. Sistema binario	223
3.1.6. Ventajas e inconvenientes del sistema binario	225
3.1.6.1. Inconvenientes	225
3.1.6.2. Ventajas	226
4. Tipos de números	226
4.1. Números con «apellido»	227
4.2. Números figurados: números poligonales	228
5. Números primos y primos Mersenne	232
5.1. Introducción	232
5.2. Teorema fundamental de la aritmética	234
5.2.1. Teorema fundamental.....	234
5.2.2. Existen infinitos números primos	235
5.3. Primos Mersenne	237
Conceptos básicos a retener	241
Ejercicios voluntarios	241
Referencias bibliográficas	242
Unidad didáctica 7. Ampliación de teoría de números	243
1. Introducción	245
2. Más sobre los números primos	245
2.1. La criba de Eratóstenes	246
3. Ampliación de aritmética modular	250
3.1. El conjunto cociente \mathbb{Z}_m	250
3.2. Sistemas de congruencias lineales	255
3.3. Aritmética en \mathbb{Z}_m	258
3.4. La función de Euler	262
3.5. El teorema «pequeño» de Fermat	263
3.6. Más propiedades de la función $\phi(n)$	267

3.7. El teorema de Wilson	269
3.7.1. Demostración	269
4. Algunos problemas abiertos	270
5. Cifrado	271
5.1. Tipos de criptografía	272
5.2. Cifrado de Julio César	273
5.2.1. Cifrado de Julio César: formulación matemática	273
5.2.2. Cifrado de Julio César generalizado	275
5.2.3. Cifrado de Julio César mejorado	275
5.3. Cifrado con clave de un único uso	276
5.3.1. Procedimiento	276
5.4. Cifrado usando el teorema pequeño de Fermat	277
5.4.1. Ventajas e inconvenientes del cifrado usando el teorema pequeño de Fermat	279
5.5. Cifrado RSA	279
5.5.1. Metodología	281
5.5.2. ¿Por qué funciona esta codificación?	282
5.5.3. Seguridad del cifrado RSA de clave pública	283
5.5.4. RSA en el mundo real	285
5.5.5. Una historieta sobre RSA	285
5.6. Otros sistemas	287
6. Apéndice: lista de los primeros 1000 primos	288
Actividades de autocomprobación	292
Referencias bibliográficas	294
Unidad didáctica 8. Grafos	295
Objetivos de la Unidad	297
1. Definición de «grafo»	298
2. Clasificación de grafos: orientados y no orientados	300
3. Representación de grafos orientados	303
3.1. Diagramática	303
3.2. Matemática o computacional	304
3.3. Matriz asociada a un grafo	305
4. Reflexividad, simetría y transitividad en grafos	312
4.1. Grafo y cierre reflexivo	312
4.2. Grafos simétricos y antisimétricos	312
4.3. Grafo y cierre transitivo	313

5. Equivalencia asociada a un grafo	314
5.1. Equivalencia	314
6. Tipos de grafos	315
6.1. Simple, parcial y subgrafo	315
6.2. Grafo completo	316
7. Cortes, cociclo y cocircuito de un grafo	317
7.1. Definiciones	317
7.2. Grafo sin circuitos: test de verificación de la existencia y localización de circuitos	318
7.3. Conexidad: simple y fuerte	320
7.4. Grafo reducido, orientación en grafos. Conexidad casi y semi-fuerte ...	322
8. Operaciones con grafos	323
9. Morfismos en grafos	324
9.1. Isomorfismo	324
9.2. Homomorfismo	327
9.3. Grafos homeomorfos	328
10. Árboles	331
10.1. Definición	331
Conceptos básicos a retener	333
Ejercicios voluntarios	333
Referencias bibliográficas	333
Unidad didáctica 9. Ampliación de teoría de grafos	335
1. Introducción	336
2. Árboles recubridores	336
2.1. Procedimiento para hacer crecer un árbol	338
2.2. Algoritmo de Prim	341
2.3. Kruskal	344
3. Coloraciones	347
3.1. Algoritmo voraz para colorear un grafo	349
3.2. Algunos resultados	351
4. Grafos planos	352
4.1. Grafos planares y grafos duales	352
4.2. El teorema de los cuatro colores	355

5. Caminos mínimos	356
5.1. Dijkstra	356
6. Eulerianos y hamiltonianos	361
6.1. Algoritmo de Fleury	362
6.2. Grafos hamiltonianos	365
6.3. Problema del viajante	366
Actividades de auto comprobación	368
Referencias bibliográficas	370
Unidad didáctica 10. Álgebra de Boole	371
Objetivos de la Unidad	373
1. La algebrización de la lógica	374
1.1. La lógica aristotélica	375
1.2. La lógica de Hamilton y De Morgan	379
1.3. La lógica matemática	380
2. La concepción de la matemática por Boole	382
3. Álgebra de Boole	386
3.1. Introducción	386
3.2. Operaciones booleanas fundamentales y sus propiedades	387
3.2.1. Operaciones y conectivas lógicas: bases lógicas	387
3.2.2. Propiedades	391
3.2.3. Principio de dualidad	392
3.2.4. Ley de absorción	392
3.2.5. Relación de inclusión	392
3.2.6. Interpretaciones del álgebra de Boole	393
3.2.6.1. Interpretación conjuntista	393
3.2.6.2. Proposicional	393
3.2.6.3. Estructural	394
3.2.6.4. Numérica	394
3.2.6.5. Otras interpretaciones: teoría de la conmutación	395
3.2.6.6. Variables booleanas	396
3.3. Tablas de verdad. Proposiciones lógicas y funciones de variables booleanas	396
3.3.1. Tablas veritativas	396
3.3.2. Operaciones de Sheffer y Pierce	398
3.3.3. Funciones booleanas	400

3.4. Formas canónicas	402
3.5. Funciones de estructura	403
3.6. Estudio de una función booleana	404
4. Reducción de las funciones booleanas con métodos gráficos	406
4.1. Expresiones booleanas	406
4.2. Simplificación de funciones booleanas	408
4.2.1. Diagrama de Veitch	409
4.2.2. Diagrama o mapa de Karnaugh	411
4.2.3. Método de Quine-McCluskey	413
4.2.4. Otros métodos de reducción	414
4.2.5. Consensus	414
5. Aplicaciones del álgebra de Boole	415
5.1. Tablas lógicas de análisis: tablas de decisión y variables	415
5.1.1. Tablas de decisión	415
5.1.2. Tablas de variables	417
5.2. Álgebra de Boole y circuitos eléctricos	418
5.3. Demostración automática de teoremas: álgebra de Robbins versus álgebra de Boole	423
Conceptos básicos a retener	425
Ejercicios voluntarios	425
Referencias bibliográficas	426

