Índice general

Prólogo v

Prólogo del Autor ix

1. TEORÍA DE LA DIVISIBILIDAD 1
- 1.1. Introducción . . . 1
- 1.2. La relación de divisibilidad . . . 2
- 1.3. Máximo común divisor . . . 3
- 1.4. Mínimo común múltiplo . . . 5
- 1.5. Algoritmo de la división . . . 5
- 1.6. Identidad de Bezout . . . 7
- 1.7. Teorema fundamental de la Aritmética . . . 9
- 1.8. Algoritmo de Euclides . . . 10

2. TEORÍA DE CONGRUENCIAS 15
- 2.1. Definición y propiedades . . . 15
- 2.2. El anillo $\mathbb{Z}_m$ . . . 17
- 2.3. El teorema de Euler-Fermat . . . 19
- 2.4. Congruencias lineales . . . 22
- 2.5. Congruencias polinómicas módulo un primo . . . 25
- 2.6. Algoritmo chino de los restos . . . 26

3. LEY DE RECIPROCIDAD CUADRÁTICA 33
- 3.1. Introducción . . . 33
- 3.2. Concepto de resíduo cuadrático . . . 34
- 3.3. El símbolo de Legendre . . . 36
- 3.4. Infinitud de primos en progresiones aritméticas . . . 44
- 3.5. Ley de reciprocidad cuadrática . . . 47
- 3.6. El símbolo de Jacobi . . . 55

4. EL GRUPO DE LAS UNIDADES DE $\mathbb{Z}_m$ 61
- 4.1. Introducción . . . 61
- 4.2. La estructura de $\mathcal{U}(\mathbb{Z}_m)$ para $m = p^e, 2p^e$ con p primo impar 63
- 4.3. La estructura del grupo $\mathcal{U}(\mathbb{Z}_{2^e})$ . . . 66

4.4. El teorema de Carmichael 68

5. ELEMENTOS DISTINGUIDOS DE $\mathcal{U}(\mathbb{Z}_m)$ 73
5.1. Introducción 73
5.2. Resíduos cuadráticos 74
5.3. Idempotentes 75
5.4. Raíces cuadradas de la unidad 76

6. FACTORIZACIÓN 79
6.1. Introducción 79
6.2. Descomposición de un número conocida una raíz cuadrada de la unidad no trivial 79
6.3. Descomposición de un número conocido un idempotente no trivial 81
6.4. Ejemplo 82

7. TEST DETERMINISTAS DE PRIMALIDAD 85
7.1. Introducción 85
7.2. El test de Wilson 87
7.3. Los test de primalidad clásicos 89
7.4. Test de primalidad para primos de Fermat 91
7.5. Algunos test más eficientes de primalidad 94

8. TEST DE PRIMALIDAD BASADOS EN SUCESIONES EN RECURRENCIA 97
8.1. Sucesiones de Lucas 97
8.2. Tests de Lucas y de Morrison 99
8.3. Números de Mersenne 101
8.4. Números perfectos 104

9. TEST PROBABILÍSTICOS DE PRIMALIDAD 109
9.1. El test de Fermat 109
9.2. Números de Carmichael y pseudoprimos 110
9.3. Test de Solavay-Strassen 116
9.4. Test de Miller-Rabin 118
9.5. El teorema de Selfridge 121

10. EL ALGORITMO AKS 131
10.1. Introducción 131
10.2. El algoritmo AKS 132
10.3. Algoritmo AKS revisado 134
10.4. Algoritmo AKS "práctico" 134