

# CONTENTS

<b>Preface</b>	<b>ix</b>
<b>Acknowledgments</b>	<b>xi</b>
<b>Notation</b>	<b>xiii</b>
<b>Introduction</b>	<b>1</b>
<b>Links flowchart</b>	<b>13</b>
<b>Chapter 1. Polynomial Factorization</b>	<b>17</b>
1. Univariate factorization	17
2. Counting the number of points on curves and varieties and multivariate factorization	34
3. Other polynomial decompositions	42
<b>Chapter 2. Finding Irreducible and Primitive Polynomials</b>	<b>45</b>
1. Construction of irreducible polynomials	45
2. Construction of primitive polynomials and generating sets	52
<b>Chapter 3. The Distribution of Irreducible, Primitive and Other Special Polynomials and Matrices</b>	<b>65</b>
1. Irreducible, primitive and other special polynomials and matrices of special form	65
2. Irreducible and primitive polynomials of small height and weight	86
3. Sparse polynomials	91
4. Applications to algebraic number fields	97

<b>Chapter 4. Bases and Computation in Finite Fields</b>	<b>99</b>
1. Construction of some special bases for finite fields	99
2. Discrete logarithm and Zech's logarithm	112
3. Polynomial multiplication and multiplicative complexity in finite fields	117
4. Linear algebra, polynomial interpolation and other algorithms in finite fields	127
<b>Chapter 5. Coding Theory and Algebraic Curves</b>	<b>149</b>
1. Codes and points on algebraic curves	149
2. Codes and exponential sums	185
3. Codes and lattice packings and coverings	205
<b>Chapter 6. Elliptic Curves</b>	<b>215</b>
1. Some general properties	215
2. Finding the group structure of elliptic curves	231
<b>Chapter 7. Recurrence Sequences in Finite Fields and Cyclic Linear Codes</b>	<b>239</b>
1. Distribution of values of recurrence sequences	239
2. Applications of recurrence sequences	245
3. BCH and other cyclic linear codes and recurrence sequences	255
<b>Chapter 8. Finite Fields and Discrete Mathematics</b>	<b>265</b>
1. Cryptography, pseudo-random numbers, and permutation polynomials	265
2. Permutation polynomials and other polynomial mappings	282
3. Graph theory, Boolean functions, combinatorial configurations, and integration nets	297
4. Enumeration problems in finite fields	319
<b>Chapter 9. Congruences</b>	<b>325</b>
1. Optimal coefficients and pseudo-random numbers	325
2. Residues of exponential functions	329
3. Modular arithmetic	345
4. Other applications	349
<b>Chapter 10. Some Related Problems</b>	<b>361</b>
1. Integer factorization, primality testing, and the greatest common divisor	361

2. Computational algebraic number theory	372
3. Algebraic complexity theory	376
4. Polynomials with integer coefficients	387
<b>Appendix 1</b>	<b>403</b>
<b>Appendix 2</b>	<b>405</b>
<b>Appendix 3</b>	<b>407</b>
<b>References</b>	<b>409</b>
<b>Index</b>	<b>525</b>