

## CONTENTS

<b>Series Editor's Preface</b>	<b>ix</b>
<b>Preface</b>	<b>x</b>
<b>Acknowledgements</b>	<b>xi</b>
<b>Notations</b>	<b>ix</b>
<b>Introduction</b>	<b>1</b>
<b>Chapter 1. Polynomial Factorization</b>	<b>7</b>
1. Univariate factorization	7
2. Multivariate factorization	16
3. Other polynomial decompositions	20
<b>Chapter 2. Finding irreducible and primitive polynomials</b>	<b>21</b>
1. Construction of irreducible polynomials	21
2. Construction of primitive polynomials	27
<b>Chapter 3. The distribution of irreducible and primitive polynomials</b>	<b>30</b>
1. Distribution of irreducible and primitive polynomials	30
2. Irreducible and primitive polynomials of a given height and weight	42
3. Sparse polynomials	46
4. Applications to algebraic number fields	47
<b>Chapter 4. Bases and computation in finite fields</b>	<b>49</b>
1. Construction of some special bases for finite fields	49
2. Discrete logarithm and Zech's logarithm	54
3. Polynomial multiplication and multiplicative complexity in finite fields	56
4. Other algorithms in finite fields	64
<b>Chapter 5. Coding theory and algebraic curves</b>	<b>72</b>
1. Codes and points on algebraic curves	72
2. Codes and exponential sums	86
3. Codes and lattice packings and coverings	92
<b>Chapter 6. Elliptic curves</b>	<b>99</b>
1. Some general properties	99
2. Distribution of primitive points on elliptic curves	105

<b>Chapter 7. Recurrent sequences in finite fields and cyclic linear codes</b>	<b>109</b>
1. Distribution of values of recurrent sequences	109
2. Applications of recurrent sequences	113
3. Cyclic codes and recurrent sequences	116
<b>Chapter 8. Finite fields and discrete mathematics</b>	<b>122</b>
1. Cryptography and permutation polynomials	122
2. Graph theory, combinatorics, Boolean functions	129
3. Enumeration problems in finite fields	136
<b>Chapter 9. Congruences</b>	<b>139</b>
1. Optimal coefficients and pseudo-random numbers	139
2. Residues of exponential functions	143
3. Modular arithmetic	148
4. Other applications	150
<b>Chapter 10. Some related problems</b>	<b>153</b>
1. Integer factorization, primality testing and the greatest common divisor	153
2. Computational algebraic number theory	155
3. Algebraic complexity theory	156
4. Polynomials with integer coefficients	<b>158</b>
<b>Appendix 1</b>	<b>161</b>
<b>Appendix 2</b>	<b>164</b>
<b>Appendix 3</b>	<b>165</b>
<b>Addendum</b>	<b>166</b>
<b>References</b>	<b>191</b>
<b>Index</b>	<b>238</b>