

# Contents

<b>Preface</b>	<b>V</b>
<b>1 Introduction and Philosophy</b>	<b>1</b>
1.1 A Historical Overview . . . . .	1
1.2 Pars pro toto . . . . .	3
1.3 Chinese Remainder Theorem: A First Formulation . . . . .	5
1.4 CRT in the Hands of Old Mathematicians . . . . .	8
1.5 CRT in Applications: the Three C's . . . . .	10
<b>2 Chinese Remainder Algorithm</b>	<b>13</b>
2.1 Historical Development . . . . .	13
2.2 Chinese Remainder Algorithms . . . . .	22
2.3 Chinese Remainder Theorem . . . . .	24
2.4 A Generalized CRA . . . . .	25
2.5 Another Generalized CRT . . . . .	29
<b>3 In Modular Computations</b>	<b>33</b>
3.1 Modular Computation Based on CRA . . . . .	33
3.2 A Modular Approach to Multiplication . . . . .	38
3.3 Computing Exact Polynomial Resultants . . . . .	47
3.4 Other Applications in Symbolic Computations . . . . .	58
3.5 CRA and Homomorphic Image Computing . . . . .	59
3.6 Information and CRT . . . . .	62
<b>4 In Algorithmics</b>	<b>65</b>
4.1 Divide-and-Conquer Techniques . . . . .	66
4.2 Polynomial Interpolation over Fields . . . . .	68
4.3 Polynomial Interpolation over $\mathbf{Z}/(m)$ . . . . .	71
4.4 Shift-Register Synthesis over $\mathbf{Z}/(m)$ . . . . .	74
4.5 Common Primitive Roots . . . . .	80
4.6 From One- to Multi-dimension . . . . .	82

4.7	A Modular Algorithm for Cyclic Convolution . . . . .	85
4.8	A Fast Algorithm for Cyclic Convolution . . . . .	87
4.9	Fast Fourier Transform and CRT . . . . .	90
<b>5</b>	<b>In Bridging Computations</b>	<b>95</b>
5.1	A Main Bridge . . . . .	95
5.2	Solving Equations over $\mathbf{Z}/(m)$ . . . . .	97
5.3	Number of Roots of Equations over $\mathbf{Z}/(m)$ . . . . .	99
5.4	Computing Fixed Points . . . . .	101
5.5	Bridging Divisions of Polynomials . . . . .	105
5.6	Permutation Polynomials of $\mathbf{Z}/(m)$ . . . . .	106
<b>6</b>	<b>In Coding Theory</b>	<b>113</b>
6.1	Basics of Block Codes . . . . .	114
6.2	Redundant Residue Codes . . . . .	120
6.3	Reed-Solomon Codes . . . . .	122
6.4	Redundant Residue Codes of Degree 2 . . . . .	128
6.5	Bossen-Yau Codes . . . . .	131
6.6	Generalized Redundant Residue Codes . . . . .	141
6.7	Restricted GRR Codes . . . . .	146
6.8	A Class of Arithmetic Residue Codes . . . . .	147
<b>7</b>	<b>In Cryptography</b>	<b>157</b>
7.1	Secret Sharing and CRT . . . . .	157
7.2	Secret Sharing and Codes . . . . .	165
7.3	CRT and Stream Ciphering . . . . .	171
7.4	CRA and Knapsack Problems . . . . .	175
7.5	Public-Key Systems via CRT . . . . .	179
<b>A</b>	<b>Tutorial in Information Theory</b>	<b>185</b>
<b>B</b>	<b>Tutorial in Algebra</b>	<b>193</b>
<b>C</b>	<b>List of Mathematical Symbols</b>	<b>201</b>
	<b>Bibliography</b>	<b>203</b>
	<b>Index</b>	<b>211</b>