

---

---

---

# Contents

<b>1</b>	<b>Euclid's Algorithm</b>	<b>1</b>
1.1	Euclidean Algorithm . . . . .	3
1.2	Diophantine Approximations . . . . .	6
1.3	Continued Fractions . . . . .	8
1.4	Diophantine Equations . . . . .	9
<b>2</b>	<b>Continued Fractions</b>	<b>11</b>
2.1	Basics . . . . .	12
2.2	Matrix Representation . . . . .	16
2.3	Continuant Representation . . . . .	18
2.4	Continued Fractions of Quadratics . . . . .	19
2.5	Approximation Properties . . . . .	30
2.6	Continued Fraction Arithmetic . . . . .	34
<b>3</b>	<b>Diophantine Equations</b>	<b>41</b>
3.1	Two Variable Linear Diophantine Equations . . . . .	42
3.2	General Linear Diophantine Equations . . . . .	45
3.3	Pell's Equation . . . . .	50
3.4	Fermat's Last Theorem . . . . .	51

<b>4</b>	<b>Lattice Techniques</b>	<b>57</b>
4.1	Lattice Fundamentals . . . . .	58
4.2	Minkowski Convex Body Theorem . . . . .	64
4.3	Reduced Bases . . . . .	66
4.4	Finding Numerical Relationships . . . . .	71
<b>5</b>	<b>Arithmetic Functions</b>	<b>73</b>
5.1	Arithmetic Functions . . . . .	73
5.2	Asymptotic Behavior of Arithmetic Functions . . . . .	77
5.3	Distribution of Primes . . . . .	80
5.4	Bertrand's Postulate . . . . .	81
<b>6</b>	<b>Residue Rings</b>	<b>85</b>
6.1	Basic Properties of $\mathbb{Z}/m\mathbb{Z}$ . . . . .	86
6.2	Chinese Remainder Theorem . . . . .	88
6.3	Multiplicative Structure of $\mathbb{Z}/m\mathbb{Z}$ . . . . .	90
6.4	Quadratic Reciprocity . . . . .	92
6.5	Algebraic Extensions of $\mathbb{F}_p$ . . . . .	96
6.6	$p$ -adic Numbers . . . . .	98
6.7	Cryptosystems . . . . .	101
6.8	Sums of Squares . . . . .	104
<b>7</b>	<b>Polynomial Arithmetic</b>	<b>107</b>
7.1	Generalities . . . . .	108
7.2	Polynomial Addition . . . . .	110
7.3	Polynomial Multiplication . . . . .	113
7.4	Fast Polynomial Algorithms . . . . .	116
7.5	Polynomial Exponentiation . . . . .	120
7.6	Polynomial Substitution . . . . .	123
<b>8</b>	<b>Polynomial GCD's: Classical Algorithms</b>	<b>125</b>
8.1	Generalities . . . . .	126
8.2	GCD of Several Quantities . . . . .	127
8.3	Polynomial Contents . . . . .	128
8.4	Coefficient Growth . . . . .	130
8.5	Pseudo-Quotients . . . . .	132
8.6	Subresultant Polynomial Remainder Sequence . . . . .	134
<b>9</b>	<b>Polynomial Elimination</b>	<b>137</b>
9.1	Symmetric Functions . . . . .	138
9.2	Polynomial Resultants . . . . .	141
9.3	Subresultants . . . . .	149
9.4	Elimination Examples . . . . .	151

<b>10 Formal Power Series</b>	<b>157</b>
10.1 Introduction . . . . .	158
10.2 Power Series Arithmetic . . . . .	161
10.3 Power Series Exponentiation . . . . .	165
10.4 Composition of Formal Power Series . . . . .	167
10.5 Reversion of Power Series . . . . .	171
<b>11 Bounds on Polynomials</b>	<b>173</b>
11.1 Heights of Polynomials . . . . .	174
11.2 Uniform Coefficient Bounds . . . . .	175
11.3 Weighted Coefficient Bounds . . . . .	180
11.4 Size of a Polynomial's Zeroes . . . . .	181
11.5 Discriminants and Zero Separation . . . . .	182
<b>12 Zero Equivalence Testing</b>	<b>189</b>
12.1 Probabilistic Techniques . . . . .	191
12.2 Deterministic Results . . . . .	195
12.3 Negative Results . . . . .	203
<b>13 Univariate Interpolation</b>	<b>207</b>
13.1 Vandermonde Matrices . . . . .	208
13.2 Lagrange Interpolation . . . . .	214
13.3 Newton Interpolation . . . . .	215
13.4 Fast Fourier Transform . . . . .	218
13.5 Abstract Interpolation . . . . .	226
<b>14 Multivariate Interpolation</b>	<b>231</b>
14.1 Multivariate D�ense Interpolation . . . . .	232
14.2 Probabilistic Sparse Interpolation . . . . .	233
14.3 Deterministic Sparse Interpolation with Degree Bounds . . . . .	242
14.4 Deterministic Sparse Interpolation without Degree Bounds . . . . .	243
<b>15 Polynomial GCD's: Interpolation Algorithms</b>	<b>247</b>
15.1 Heuristic GCD . . . . .	248
15.2 Univariate Polynomials over $\mathbb{Z}$ . . . . .	251
15.3 Multivariate Polynomials . . . . .	254
<b>16 Hensel Algorithms</b>	<b>261</b>
16.1 $m$ -adic Completions . . . . .	262
16.2 One Dimensional Iteration . . . . .	264
16.3 Multidimensional Iteration . . . . .	270
16.4 Hensel's Lemma . . . . .	275
16.5 Generalizations of Hensel's Lemma . . . . .	278
16.6 Zassenhaus' Formulation of Hensel's Lemma . . . . .	281

<b>17 Sparse Hensel Algorithms</b>	<b>285</b>
17.1 Heuristic Presentation . . . . .	287
17.2 Formal Presentation . . . . .	289
<b>18 Factoring over Finite Fields</b>	<b>293</b>
18.1 Square Free Decomposition . . . . .	294
18.2 Distinct Degree Factorization . . . . .	296
18.3 Finding Linear Factors . . . . .	297
18.4 Cantor-Zassenhaus Algorithm . . . . .	299
<b>19 Irreducibility of Polynomials</b>	<b>303</b>
19.1 Deterministic Irreducibility Testing . . . . .	304
19.2 Counting Prime Factors . . . . .	307
19.3 Hilbert Irreducibility Theorem . . . . .	309
19.4 Bertini's Theorem . . . . .	312
<b>20 Univariate Factorization</b>	<b>321</b>
20.1 Reductions . . . . .	322
20.2 Simple Algorithm . . . . .	322
20.3 Asymptotically Good Algorithms . . . . .	324
<b>21 Multivariate Factorization</b>	<b>329</b>
21.1 General Reductions . . . . .	330
21.2 Lifting Multivariate Factorizations . . . . .	332
21.3 Leading Coefficient Determination . . . . .	334
21.4 Multivariate Polynomials over $\mathbb{Q}$ . . . . .	338
21.5 Bivariate Polynomials over Fields . . . . .	339
<b>List of symbols</b>	<b>341</b>
<b>Bibliography</b>	<b>343</b>
<b>Index</b>	<b>357</b>