
Contents

1	The Euclidean algorithm, the Chinese remainder theorem and interpolation	1
1.1	The Euclidean algorithm	1
1.2	The Chinese remainder theorem and Lagrange numbers	5
1.2.1	Computing L_k and u (Lagrange's method)	11
1.2.2	Computing u (Newton's method)	14
1.3	Polynomials	16
1.4	Polynomial interpolation	26
1.4.1	Lagrange's method	26
1.4.2	Newton's method	30
1.4.3	Divided differences	33
1.5	Applications	34
	References	38
2	p-adic series expansions	39
2.1	Expansions of rational numbers	39
2.2	Expansions of algebraic numbers	50
2.3	Newton's method	53
2.4	Series expansion of rational functions	56
2.5	Linear recurrence relations	62
	References	64
3	The resultant	65
3.1	Applications	73
	References	85
4	Factoring polynomials	87
4.1	Kronecker's method	87
4.2	Irreducibility criteria	90
4.3	Finite fields and polynomials	92
4.4	Cyclotomic polynomials	102

4.5	Modular greatest common divisors	106
4.6	Square-free form of a polynomial	108
4.7	The Möbius function	111
4.8	Berlekamp's method	115
4.8.1	Reducing the calculation of the gcds: the Zassenhaus-Cantor method	123
4.8.2	Reducing the calculations of the gcds: the method of the resultant	124
4.8.3	The characteristic polynomial of matrix Q	126
4.8.4	The powers of matrix Q	127
4.9	Hensel's lemma	128
4.9.1	Hensel's lemma for more than two factors	131
4.10	Factorisation over the integers	133
4.10.1	Upper bounds for the coefficients of a factor	134
4.11	Factorisations in an extension	137
	References	139
5	The discrete Fourier transform	141
5.1	Roots of unity	141
5.1.1	Interpolation at the roots of unity	142
5.2	Convolution	147
5.3	Circulant matrices	150
5.4	The Fast Fourier transform	153
5.5	$n \log n$ complexity	157
	References	158
5.6	Appendix	158
5.6.1	Group algebras	158
5.6.2	Cyclic groups	160
5.6.3	The character group	162
5.6.4	The algebra of an Abelian group	165
	References	171
	Index	173