Table of Contents

1. **Introduction** 1

2. **Overview** 7
   - 2.1 Outline 12
   - 2.2 Statement of Main Results 13
   - 2.3 References and Related Works 21
   - 2.4 Open Problems 24

3. **Technical Prerequisites** 27
   - 3.1 Subresultants and the Euclidean Algorithm 28
   - 3.2 The Cost of Arithmetic 33

4. **Change of Basis** 41
   - 4.1 Computing Taylor Shifts 42
   - 4.2 Conversion to Falling Factorials 49
   - 4.3 Fast Multiplication in the Falling Factorial Basis 57

5. **Modular Squarefree and Greatest Factorial Factorization** 61
   - 5.1 Squarefree Factorization 61
   - 5.2 Greatest Factorial Factorization 68

6. **Modular Hermite Integration** 79
   - 6.1 Small Primes Modular Algorithm 80
   - 6.2 Prime Power Modular Algorithm 85
   - 6.3 Implementation 87

7. **Computing All Integral Roots of the Resultant** 97
   - 7.1 Application to Hypergeometric Summation 103
   - 7.2 Computing All Integral Roots Via Factoring 109
   - 7.3 Application to Hyperexponential Integration 112
   - 7.4 Modular LRT Algorithm 116

8. **Modular Algorithms for the Gosper-Petkovšek Form** 121
   - 8.1 Modular GP′-Form Computation 134

9. Polynomial Solutions of Linear First Order Equations 149
9.1 The Method of Undetermined Coefficients 155
9.2 Brent and Kung's Algorithm for Linear Differential Equations 158
9.3 Rothstein's SPDE Algorithm 161
9.4 The ABP Algorithm 165
9.5 A Divide-and-Conquer Algorithm: Generic Case 169
9.6 A Divide-and-Conquer Algorithm: General Case 174
9.7 Barkatou's Algorithm for Linear Difference Equations 179
9.8 Modular Algorithms 180

10. Modular Gosper and Almkvist & Zeilberger Algorithms 195
10.1 High Degree Examples 198

References 207

Index 217

List of Figures and Tables

2.1 Algorithm dependency graph 14

3.1 The dth submatrix of the Sylvester matrix 29

4.1 Running times for shift by 1 with classical arithmetic 44
4.2 Running times for Taylor shift with classical arithmetic 45
4.3 Running times for Taylor shift with classical arithmetic 45
4.4 Running times for Taylor shift with fast arithmetic 48
4.5 Running times for Taylor shift with fast arithmetic 48
4.6 Comparison of running times for Taylor shift 49
4.7 Cost estimates for polynomial basis conversion 57

6.1 Timings for the 1st series with small primes Hermite integration 90
6.2 Timings for the 2nd series with small primes Hermite integration 91
6.3 Timings for the 3rd series with small primes Hermite integration 92
6.4 Timings for the 1st series with prime power Hermite integration 93
6.5 Timings for the 2nd series with prime power Hermite integration 94
6.6 Timings for the 3rd series with prime power Hermite integration 95

9.1 The linear system $Lu = c$ with respect to the monomial basis. 166
9.2 Cost estimates for polynomial solutions of first order equations 192
9.3 Cost estimates for modular algorithms solving first order equations 192

List of Algorithms

3.4 Monic Extended Euclidean Algorithm 29
4.7 Small primes modular Taylor shift 48
4.18 Modular conversion from $\mathcal{M}$ to $\mathcal{M}_{\mathbf{b}}$ 55
4.19 Modular conversion from $\mathcal{M}_{\mathbf{b}}$ to $\mathcal{M}$ 55
4.23 Evaluation in the falling factorial basis 58
4.25 Interpolation in the falling factorial basis 58
5.2 Yun's squarefree factorization 61
5.6 Small primes modular squarefree factorization 63
5.12 Prime power modular squarefree factorization 67
5.18 Gff computation 70
5.20 Gff computation à la Yun 71
5.24 Small primes modular gff computation 74
6.4 Small primes modular Hermite integration 83
6.9 Prime power modular Hermite integration 85
7.2 Modular bivariate EEA 98
7.12 Prime power modular integral root distances 104
7.20 Prime power modular Man & Wright algorithm 109
7.25 Small primes modular integral residues 113
7.29 Small primes modular LRT algorithm 117
8.2 Gosper-Petkovšek form 121
8.6 Small primes modular shift gcd 123
8.12 Small primes modular Gosper-Petkovšek form 126
8.26 GP′-refinement computation 137
8.28 GP′-form computation 139
8.32 Small primes modular GP′-refinement 140
8.37 Prime power modular GP′-refinement 144
9.12 Method of undetermined coefficients: part I 155
9.15 Method of undetermined coefficients: part II 157
9.20 Brent & Kung's algorithm 159
9.23 Rothstein's SPDE algorithm 162
9.25 Rothstein's SPDE algorithm for difference equations 163
9.27 ABP algorithm for first order differential equations 165
9.31 ABP algorithm for first order difference equations 168
9.35 Difference divide & conquer: generic case 171

9.38 Differential divide & conquer: generic case 173
9.41 Difference divide & conquer: general case 175
9.44 Differential divide & conquer: general case 178
9.46 Barkatou's algorithm 179
9.56 Modular Brent & Kung / ABP algorithm 183
9.60 Modular Barkatou algorithm 187
9.64 Modular difference divide & conquer 189
9.67 Modular differential divide & conquer 191
10.1 Modular Gosper algorithm 195
10.4 Modular Almkvist & Zeilberger algorithm 196