

Algorithms for Computer Algebra

K.O. Geddes

University of Waterloo

S.R. Czapor

Laurentian University

G. Labahn

University of Waterloo



Kluwer Academic Publishers
Boston/Dordrecht/London

CONTENTS

Preface

xv

Chapter 1 Introduction to Computer Algebra

1.1 Introduction	1
1.2 Symbolic versus Numeric Computation	2
1.3 A Brief Historical Sketch	4
1.4 An Example of a Computer Algebra System: MAPLE	11
Exercises	20

Chapter 2 Algebra of Polynomials, Rational Functions, and Power Series

2.1 Introduction	23
2.2 Rings and Fields	23
2.3 Divisibility and Factorization in Integral Domains	26
2.4 The Euclidean Algorithm	32
2.5 Univariate Polynomial Domains	38
2.6 Multivariate Polynomial Domains	46
2.7 The Primitive Euclidean Algorithm	52
2.8 Quotient Fields and Rational Functions	60
2.9 Power Series and Extended Power Series	63
2.10 Relationships among Domains	70
Exercises	73

Chapter 3 Normal Forms and Algebraic Representations

3.1 Introduction	79
3.2 Levels of Abstraction	79
3.3 Normal Form and Canonical Form	80
3.4 Normal Forms for Polynomials	84
3.5 Normal Forms for Rational Functions and Power Series	88
3.6 Data Structures for Multiprecision Integers and Rational Numbers	93
3.7 Data Structures for Polynomials, Rational Functions, and Power Series	96
Exercises	105

Chapter 4 Arithmetic of Polynomials, Rational Functions, and Power Series

4.1 Introduction	111
4.2 Basic Arithmetic Algorithms	112
4.3 Fast Arithmetic Algorithms: Karatsuba's Algorithm	118
4.4 Modular Representations	120
4.5 The Fast Fourier Transform	123
4.6 The Inverse Fourier Transform	128
4.7 Fast Polynomial Multiplication	132
4.8 Computing Primitive N-th Roots of Unity	133
4.9 Newton's Iteration for Power Series Division	136
Exercises	145

Chapter 5 Homomorphisms and Chinese Remainder Algorithms

5.1 Introduction	151
5.2 Intermediate Expression Swell: An Example	151
5.3 Ring Morphisms	153
5.4 Characterization of Morphisms	160
5.5 Homomorphic Images	167
5.6 The Integer Chinese Remainder Algorithm	174
5.7 The Polynomial Interpolation Algorithm	183
5.8 Further Discussion of the Two Algorithms	189
Exercises	196

Chapter 6 Newton's Iteration and the Hensel Construction

6.1 Introduction	205
6.2 P-adic and Ideal-adic Representations	205
6.3 Newton's Iteration for $F(u)=0$	214
6.4 Hensel's Lemma	226
6.5 The Univariate Hensel Lifting Algorithm	232
6.6 Special Techniques for the Non-monic Case	240
6.7 The Multivariate Generalization of Hensel's Lemma	250
6.8 The Multivariate Hensel Lifting Algorithm	260
Exercises	274

Chapter 7 Polynomial GCD Computation

7.1 Introduction	279
7.2 Polynomial Remainder Sequences	280
7.3 The Sylvester Matrix and Subresultants	285
7.4 The Modular GCD Algorithm	300
7.5 The Sparse Modular GCD Algorithm	311
7.6 GCD's using Hensel Lifting: The EZ-GCD Algorithm	314
7.7 A Heuristic Polynomial GCD Algorithm	320
Exercises	331

Chapter 8 Polynomial Factorization

8.1 Introduction	337
8.2 Square-Free Factorization	337
8.3 Square-Free Factorization Over Finite Fields	343
8.4 Berlekamp's Factorization Algorithm	347
8.5 The Big Prime Berlekamp Algorithm	359
8.6 Distinct Degree Factorization	368
8.7 Factoring Polynomials over the Rationals.....	374
8.8 Factoring Polynomials over Algebraic Number Fields	378
Exercises	384

Chapter 9 Solving Systems of Equations

9.1 Introduction	389
9.2 Linear Equations and Gaussian Elimination	390
9.3 Fraction-Free Gaussian Elimination	393
9.4 Alternative Methods for Solving Linear Equations	399
9.5 Nonlinear Equations and Resultants	405
Exercises	422

Chapter 10 Gröbner Bases for Polynomial Ideals

10.1 Introduction	429
10.2 Term Orderings and Reduction	431
10.3 Gröbner Bases and Buchberger's Algorithm	439
10.4 Improving Buchberger's Algorithm	447
10.5 Applications of Gröbner Bases	451
10.6 Additional Applications	462
Exercises	466

Chapter 11 Integration of Rational Functions

11.1 Introduction	473
11.2 Basic Concepts of Differential Algebra	474
11.3 Rational Part of the Integral: Hermite's Method	482
11.4 Rational Part of the Integral: Horowitz' Method	488
11.5 Logarithmic Part of the Integral	492
Exercises	508

Chapter 12 The Risch Integration Algorithm

12.1 Introduction	511
12.2 Elementary Functions	512
12.3 Differentiation of Elementary Functions	519
12.4 Liouville's Principle	523
12.5 The Risch Algorithm for Transcendental Elementary Functions	529
12.6 The Risch Algorithm for Logarithmic Extensions	530
12.7 The Risch Algorithm for Exponential Extensions	547
12.8 Integration of Algebraic Functions	561
Exercises	569
 Notation	 575
 Index	 577