Contents

Preface

-1	D 11 1	TN /F /	
	Preliminary	N/I of	homotics

- 1.1 Permutation Groups
- 1.2 Cosets and Quotient Groups
- 1.3 Rings and Euclidean Domains
- 1.4 Finite Fields
- 1.5 Finite Fields with Maple
- 1.6 The Euclidean Algorithm

2 Block Designs

- 2.1 General Properties of Block Designs
- 2.2 Hadamard Matrices
- 2.3 Hadamard Matrices with Maple
- 2.4 Difference Sets
- 2.5 Difference Sets with Maple

3 Error-Correcting Codes

- 3.1 General Properties of Codes
- 3.2 Hadamard Codes
- 3.3 Reed-Muller Codes

- 3.4 Reed-Muller Codes with Maple
- 3.5 Linear Codes
- 3.6 Hamming Codes with Maple

4 BCH Codes

- 4.1 Construction of BCH Codes
- 4.2 Error Correction in BCH Codes
- 4.3 BCH Codes with Maple
 - 4.3.1 Construction of the Generator Polynomial
 - 4.3.2 Error Correction

5 Reed-Solomon Codes

- 5.1 Construction of Reed-Solomon Codes
- 5.2 Error Correction in Reed-Solomon Codes
- 5.3 Proof of Reed-Solomon Error Correction
- 5.4 Binary Reed-Solomon Codes
- 5.5 Reed-Solomon Codes with Maple
 - 5.5.1 Construction of the Codewords
 - 5.5.2 Error Correction
- 5.6 Reed-Solomon Codes in Voyager 2

6 Algebraic Cryptography

- 6.1 Some Elementary Cryptosystems
- 6.2 The Hill Cryptosystem
- 6.3 The Hill Cryptosystem with Maple
- 6.4 Generalizations of the Hill Cryptosystem
- 6.5 The Two-Message Problem

7 The RSA Cryptosystem

7.1 Mathematical Prerequisites

- 7.2 RSA Encryption and Decryption
- 7.3 The RSA Cryptosystem with Maple
- 7.4 A Note on Modular Exponentiation
- 7.5 A Note on Primality Testing
- 7.6 A Note on Integer Factorization
- 7.7 A Note on Digital Signatures
- 7.8 The Diffie-Hellman Key Exchange

8 Elliptic Curve Cryptography

- 8.1 The ElGamal Cryptosystem
- 8.2 The ElGamal Cryptosystem with Maple
- 8.3 Elliptic Curves
- 8.4 Elliptic Curves with Maple
- 8.5 Elliptic Curve Cryptography
- 8.6 Elliptic Curve Cryptography with Maple

9 Polya Theory

- 9.1 Group Actions
- 9.2 Burnside's Theorem
- 9.3 The Cycle Index
- 9.4 The Pattern Inventory
- 9.5 The Pattern Inventory with Maple
- 9.6 Switching Functions
- 9.7 Switching Functions with Maple

Appendices

A Basic Maple Tutorial

- A.1 Introduction to Maple
- A.2 Arithmetic

- A.3 Defining Variables and Functions
- A.4 Algebra
- A.5 Case Sensitivity
- A.6 Help File
- A.7 Arrays and Loops
- A.8 Conditional Statements
- A.9 Maple Procedures

B Some Maple Linear Algebra Commands

C User-Written Maple Procedures

- C.1 Chapter 5 Procedures
- C.2 Chapter 7 Procedures
- C.3 Chapter 8 Procedures
- C.4 Chapter 9 Procedures

Hints and Solutions to Selected Written Exercises