Contents

Preface **ix**

1 Elementary Number Theory **1**
1.1 Divisibility . . . 1
1.2 Primes and factorization . . . 6
1.3 Congruences . . . 11
1.4 Solving congruences . . . 15
1.5 Theorems of Fermat and Euler . . . 20
1.6 RSA cryptosystem . . . 28

2 Groups **33**
2.1 Definition of a group . . . 33
2.2 Examples of groups . . . 34
2.3 Subgroups . . . 43
2.4 Cosets and Lagrange's Theorem . . . 49

3 Rings **55**
3.1 Definition of a ring . . . 55
3.2 Subrings and ideals . . . 61
3.3 Ring homomorphisms . . . 63
3.4 Integral domains . . . 65

4 Fields **67**
4.1 Definition and basic properties of a field . . . 67

5 Finite Fields **73**
5.1 Number of elements in a finite field . . . 73
5.2 How to construct finite fields . . . 75
5.3 Properties of finite fields . . . 82
5.4 Polynomials over finite fields . . . 86
5.5 Permutation polynomials . . . 89
5.6 Applications . . . 91
5.6.1 Orthogonal Latin squares . . . 91
5.6.2 Diffie/Hellman key exchange . . . 94

6 Vector Spaces **99**
6.1 Definition and examples 99
6.2 Basic properties of vector spaces 103
6.3 Subspaces 109

7 Polynomials **111**
7.1 Basics 111
7.2 Unique factorization 115
7.3 Polynomials over the real and complex numbers 117
7.4 Root formulas 118

8 Linear Codes **127**
8.1 Basics 129
8.2 Hamming codes 132
8.3 Encoding 134
8.4 Decoding 137
8.5 Further study 143
8.6 Exercises 145

9 Appendix **149**
9.1 Mathematical induction 149
9.2 Well-ordering Principle 152
9.3 Sets 154
9.4 Functions 158
9.5 Permutations 160
9.6 Matrices 163
9.7 Complex numbers 165

10 Hints and Partial Solutions to Selected Exercises **167**

Bibliography **195**

Index **199**