Contents

Preface vii

1 Introduction: The McNugget Problem 1

Part I Integers

2 Induction and the Division Theorem 9
2.1 The Method of Induction 9
2.2 The Tower of Hanoi 15
2.3 The Division Theorem 17

3 The Euclidean Algorithm 23
3.1 Greatest Common Divisors 23
3.2 The Euclidean Algorithm 27
3.3 Bézout's Theorem 31
3.4 An Application of Bézout's Theorem 34
3.5 Diophantine Equations 36

4 Congruences 41
4.1 Congruences 41
4.2 Solving Congruences 46
4.3 Congruence Classes and McNuggets 50

5 Prime Numbers 57
5.1 Prime Numbers and Generalized Induction 57
5.2 Uniqueness of Prime Factorizations 61
5.3 Greatest Common Divisors Revisited 63

6 Rings 69
6.1 Numbers 69
6.2 Number Rings 77
6.3 Fruit Rings 83
6.4 Modular Arithmetic Rings 88
6.5 Congruence Rings 91

7 Euler's Theorem 95
7.1 Units 95
7.2 Roots of Unity 99
7.3 The Theorems of Fermat and Euler 101
7.4 The Euler ϕ-Function 105
7.5 RSA Encryption 110

8 Binomial Coefficients 115
8.1 Pascal's Triangle 115
8.2 The Binomial Theorem 120

Part II Polynomials

9 Polynomials and Roots 127
9.1 Polynomial Equations 127
9.2 Rings of Polynomials 128
9.3 Factoring a Polynomial 130
9.4 The Roots of a Polynomial 133
9.5 Minimal Polynomials 136

10 Polynomials with Real Coefficients 141
10.1 Quadratic Polynomials 141
10.2 Cubic Polynomials 146
10.3 The Discriminant of a Cubic Polynomial 153
10.4 Quartic Polynomials 159
10.5 A Closer Look at Quartic Polynomials 164
10.6 The Discriminant of a Quartic Polynomial 167
10.7 The Fundamental Theorem of Algebra 171

11 Polynomials with Rational Coefficients 177
11.1 Polynomials over $\mathbb{Q}$ 177
11.2 Gauss's Lemma 181
11.3 Eisenstein's Criterion 184
11.4 Polynomials with Coefficients in $\mathbb{F}_p$ 187

12 Polynomial Rings . . . 193
12.1 Unique Factorization for Integers Revisited . . . 193
12.2 The Euclidean Algorithm . . . 196
12.3 Bézout's Theorem . . . 198
12.4 Unique Factorization for Polynomials . . . 199

13 Quadratic Polynomials . . . 201
13.1 Square Roots . . . 201
13.2 The Quadratic Formula . . . 204
13.3 Square Roots in Finite Fields . . . 209
13.4 Quadratic Field Constructions . . . 214

14 Polynomial Congruence Rings . . . 221
14.1 A Construction of New Rings . . . 221
14.2 Polynomial Congruences . . . 226
14.3 Polynomial Congruence Rings . . . 230
14.4 Equations and Congruences with Polynomial Unknowns . . . 233
14.5 Polynomial Congruence Fields . . . 236

Part III All Together Now

15 Euclidean Rings . . . 241
15.1 Factoring Elements in Rings . . . 241
15.2 Euclidean Rings . . . 245
15.3 Unique Factorization . . . 249

16 The Ring of Gaussian Integers . . . 255
16.1 The Irreducible Gaussian Integers . . . 255
16.2 Gaussian Congruence Rings . . . 259
16.3 Fermat's Theorem . . . 262

17 Finite Fields . . . 267
17.1 Primitive Roots . . . 267
17.2 Quadratic Reciprocity . . . 271
17.3 Classification . . . 277

Index . . . 281

http://www.springer.com/978-0-387-40397-7

Integers, Polynomials, and Rings
A Course in Algebra
Irving, R.S.
2004, XVI, 288 p., Hardcover
ISBN: 978-0-387-40397-7