Contents

Preface xi

1

Introduction 1

1.1 *What is Number Theory 1*
1.2 *Prerequisites 6*
1.3 *How to Use this Book 9*

2

Divisibility and Primes 10

2.1 *Introduction 10*
2.2 *Divisibility 12*
2.3 *The Greatest Common Divisor 17*
2.4 *Unique Factorization 27*
Appendix A *Euler's Proof of the Infinitude of Primes 33*

3

Congruences 39

3.1 *Introduction* 39
3.2 *Basic Properties of Congruences* 43
3.3 *Some Special Congruences* 59
3.4 *Solving Polynomial Congruences, I* 66
3.5 *Solving Polynomial Congruences, II* 78
3.6 *Primitive Roots* 85
3.7 *Congruences—Some Historical Notes* 98

4

The Law of Quadratic Reciprocity 100

4.1 *Introduction* 100
4.2 *Basic Properties of Quadratic Residues* 104
4.3 *The Gauss Lemma* 112
4.4 *The Law of Quadratic Reciprocity* 122
4.5 *Applications to Diophantine Equations* 132

5

Arithmetic Functions 136

5.1 *Introduction* 136
5.2 *Multiplicative Arithmetic Functions* 138
5.3 *The Möbius Inversion Formula* 146
5.4 *Perfect and Amicable Numbers* 152

6

A Few Diophantine Equations 156

6.1 *Introduction* 156
6.2 *The Equation* $x^2 + y^2 = z^2$ 159
6.3 *The Equation* $x^4 + y^4 = z^2$ 162
6.4 *The Equation* $x^2 + y^2 = n$ 165
6.5 *The Equation* $x^2 + y^2 + z^2 + w^2 = n$ 170
6.6 *Pell's Equation* $x^2 - dy^2 = 1$ 174
Appendix B *Diophantine Approximations* 184

Introduction to Chapters 7–11 191

7

The Gaussian Integers 194

7.1 *Introduction 194*
7.2 *The Fundamental Theorem of Arithmetic in the Gaussian Integers 197*
7.3 *The Two Square Problem Revisited 205*

8

Arithmetic in Quadratic Fields 209

8.1 *Introduction 209*
8.2 *Quadratic Fields 210*
8.3 *The Integers of a Quadratic Field 214*
8.4 *Binary Quadratic Forms 219*
8.5 *Modules 223*
8.6 *The Coefficient Ring of a Module 228*
8.7 *The Unit Theorem 234*
8.8 *Computing Elements of a Given Norm in a Module 242*

9

Factorization Theory in Quadratic Fields 249

9.1 *The Failure of Unique Factorization 249*
9.2 *Generalized Congruences and the Norm of a Module 256*
9.3 *Products and Sums of Modules 261*
9.4 *The Fundamental Factorization Theorem 268*
9.5 *The Prime Modules Belonging to $\mathfrak{O}$ 274*
9.6 *Finiteness of the Class Number 282*

10

Applications of the Factorization Theory to Diophantine Equations 290

10.1 *The Diophantine Equation $y^2 = x^3 + k$ 290*
10.2 *Proof of Fermat's Last Theorem for $n = 3$ 295*
10.3 *Norm Form Equations 300*

11

The Representation of Integers by Binary Quadratic Forms 307

11.1 *Equivalence of Forms 307*
11.2 *Strict Similarity of Modules 313*
11.3 *The Correspondence Between Modules and Forms 318*
11.4 *The Representation of Integers by Binary Quadratic Forms 325*
11.5 *Composition Theory for Binary Quadratic Forms 334*

Notation 353

Diophantine Equations 355

Index 357