## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>ix</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td><strong>Chapter One: Divisibility, Primes, and the Euclidean Algorithm</strong></td>
<td>6</td>
</tr>
<tr>
<td>Results</td>
<td>7</td>
</tr>
<tr>
<td>Divisibility</td>
<td>7</td>
</tr>
<tr>
<td>Primes</td>
<td>10</td>
</tr>
<tr>
<td>The Euclidean Algorithm</td>
<td>13</td>
</tr>
<tr>
<td>The Equation $ax + by = c$</td>
<td>15</td>
</tr>
<tr>
<td>Problems and Solutions</td>
<td>17</td>
</tr>
<tr>
<td>Exercises</td>
<td>32</td>
</tr>
<tr>
<td>Notes, Biographical Sketches, References</td>
<td>35</td>
</tr>
<tr>
<td><strong>Chapter Two: Congruences</strong></td>
<td>39</td>
</tr>
<tr>
<td>Results</td>
<td>40</td>
</tr>
<tr>
<td>Divisibility Tests</td>
<td>42</td>
</tr>
<tr>
<td>Linear Congruences</td>
<td>43</td>
</tr>
<tr>
<td>Techniques for Solving $ax \equiv b \pmod{m}$</td>
<td>44</td>
</tr>
<tr>
<td>The Chinese Remainder Theorem</td>
<td>46</td>
</tr>
<tr>
<td>An Application: Finding the Day of the Week</td>
<td>47</td>
</tr>
<tr>
<td>Problems and Solutions</td>
<td>48</td>
</tr>
<tr>
<td>Exercises</td>
<td>64</td>
</tr>
<tr>
<td>Notes, Biographical Sketches, References</td>
<td>66</td>
</tr>
<tr>
<td><strong>Chapter Three: The Theorems of Fermat, Euler, and Wilson</strong></td>
<td>71</td>
</tr>
<tr>
<td>Results</td>
<td>72</td>
</tr>
<tr>
<td>Fermat's Theorem and Wilson's Theorem</td>
<td>72</td>
</tr>
<tr>
<td>Euler's Theorem and the Euler $\phi$-function</td>
<td>75</td>
</tr>
<tr>
<td>Problems and Solutions</td>
<td>78</td>
</tr>
</tbody>
</table>
## CONTENTS

Exercises 94  
Notes, Biographical Sketches, References 96

### Chapter Four: Polynomial Congruences 101

**Results** 101  
- General Polynomial Congruences 101  
- Solutions of $f(x) \equiv 0 \pmod{p^k}$ 106  
- The Congruence $x^2 \equiv a \pmod{p^k}$ 109  

**Problems and Solutions** 110  

**Exercises** 122  

**Notes, References** 124

### Chapter Five: Quadratic Congruences and the Law of Quadratic Reciprocity 125

**Results** 126  
- General Quadratic Congruences 126  
- The Congruence $x^2 \equiv a \pmod{m}$ 127  
- Quadratic Residues 128  
- The Law of Quadratic Reciprocity 131  

**Problems and Solutions** 137  

**Exercises** 153  

**Notes, Biographical Sketches, References** 155

### Chapter Six: Primitive Roots and Indices 158

**Results** 158  
- The Order of an Integer 158  
- Primitive Roots 160  
- Power Residues and Indices 164  
- The Existence of Primitive Roots 167  

**Problems and Solutions** 169  

**Exercises** 189  

**Notes, Biographical Sketches, References** 191

### Chapter Seven: Prime Numbers 194

**Results** 195  
- The Sieve of Eratosthenes 195  
- Perfect Numbers 196  
- Mersenne Primes 197  
- Fermat Numbers 198  
- The Prime Number Theorem 200  
- Dirichlet’s Theorem 202  
- Goldbach’s Conjecture 203  
- Other Open Problems 204
Chapter Eight: Some Diophantine Equations and
Fermat's Last Theorem 221

Results 222
The Equation $x^2 + y^2 = z^2$ 222
Fermat's Last Theorem 224
Sums of Two Squares 226
Sums of Two Relatively Prime Squares 229
Sums of Four Squares 233
Sums of Three Squares 235
Waring's Problem 236

Problems and Solutions 237
Exercises 263
Notes, Biographical Sketches, References 265

Chapter Nine: Continued Fractions 270

Results 271
Finite Continued Fractions 271
An Application: Solutions of $ax + by = c$ 274
Infinite Continued Fractions 275
The Infinite Continued Fraction of an Irrational Number 276
Periodic Continued Fractions 278
Purely Periodic Continued Fractions 281
Rational Approximations to Irrational Numbers 282
An Application: Calendars 285

Problems and Solutions 286
Exercises 308
Notes, Biographical Sketches, References 310

Chapter Ten: Pell's Equation 314

Results 315
Pell's Equation $x^2 - dy^2 = 1$ 315
The Equation $x^2 - dy^2 = -1$ 322
The Equation $x^2 - dy^2 = N$ 324
Pell's Equation and Sums of Two Squares 325
An Application: Factoring Large Numbers 327

Problems and Solutions 329
Exercises 352
Notes, Biographical Sketches, References 354
Chapter Eleven: The Gaussian Integers and Other Quadratic Extensions 357

Results 358
- The Gaussian Integers 358
- Unique Factorization for Gaussian Integers 361
- The Gaussian Primes 362
- An Application: Gaussian Integers and Sums of Two Squares 363
- Applications of Gaussian Integers to Diophantine Equations 364
- The Integers of \( \mathbb{Q}(\sqrt{d}) \) 365
- Primes of \( \mathbb{Q}(\sqrt{d}) \) and Diophantine Equations 369
- Units of \( \mathbb{Q}(\sqrt{d}) \) 370

Problems and Solutions 372
Exercises 387
Notes, Biographical Sketches, References 388

Appendix 391
- Table of Primes and Their Least Primitive Root 392
- Table of Continued Fraction Expansion of \( \sqrt{d} \) 393

General References 394

Index 398