

# The Theory of Numbers

---

A TEXT AND SOURCE BOOK OF PROBLEMS

---

Andrew Adler

John E. Coury

*The University of British Columbia*



**Jones and Bartlett Publishers**

*Sudbury, Massachusetts*

**Boston    London    Singapore**

# Contents

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

Exercises	94	
Notes, Biographical Sketches, References	96	
<b>Chapter Four: Polynomial Congruences</b>		<b>101</b>
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	
<b>Chapter Five: Quadratic Congruences and the Law of Quadratic Reciprocity</b>		<b>125</b>
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	
<b>Chapter Six: Primitive Roots and Indices</b>		<b>158</b>
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	
<b>Chapter Seven: Prime Numbers</b>		<b>194</b>
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	

Problems and Solutions	205
Exercises	216
Notes, Biographical Sketches, References	217
<b>Chapter Eight: Some Diophantine Equations and Fermat's Last Theorem</b>	<b>221</b>
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
<b>Chapter Nine: Continued Fractions</b>	<b>270</b>
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
<b>Chapter Ten: Pell's Equation</b>	<b>314</b>
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

<b>Chapter Eleven: The Gaussian Integers and Other Quadratic Extensions</b>	<b>357</b>
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 $Q(\sqrt{d})$	365
Primes of $Q(\sqrt{d})$ and Diophantine Equations	369
Units of $Q(\sqrt{d})$	370
Problems and Solutions	372
Exercises	387
Notes, Biographical Sketches, References	388
 <b>Appendix</b>	 <b>391</b>
Table of Primes and Their Least Primitive Root	392
Table of Continued Fraction Expansion of $\sqrt{d}$	393
 <b>General References</b>	 <b>394</b>
 <b>Index</b>	 <b>398</b>