

# An Introduction to the Theory of Numbers

## FIFTH EDITION

**Ivan Niven**

*University of Oregon*

**Herbert S. Zuckerman**

*University of Washington*

**Hugh L. Montgomery**

*University of Michigan*



**John Wiley & Sons, Inc.**

New York • Chichester • Brisbane • Toronto • Singapore

# Contents

|                                                    |            |
|----------------------------------------------------|------------|
| <b>Notation</b>                                    | <b>xi</b>  |
| <b>1 Divisibility</b>                              | <b>1</b>   |
| 1.1 Introduction                                   | 1          |
| 1.2 Divisibility                                   | 4          |
| 1.3 Primes                                         | 20         |
| 1.4 The Binomial Theorem                           | 35         |
| Notes on Chapter 1                                 | 44         |
| <b>2 Congruences</b>                               | <b>47</b>  |
| 2.1 Congruences                                    | 47         |
| 2.2 Solutions of Congruences                       | 60         |
| 2.3 The Chinese Remainder Theorem                  | 64         |
| 2.4 Techniques of Numerical Calculation            | 74         |
| 2.5 Public-Key Cryptography                        | 84         |
| 2.6 Prime Power Moduli                             | 86         |
| 2.7 Prime Modulus                                  | 91         |
| 2.8 Primitive Roots and Power Residues             | 97         |
| 2.9 Congruences of Degree Two, Prime Modulus       | 110        |
| 2.10 Number Theory from an Algebraic Viewpoint     | 115        |
| 2.11 Groups, Rings, and Fields                     | 121        |
| Notes on Chapter 2                                 | 128        |
| <b>3 Quadratic Reciprocity and Quadratic Forms</b> | <b>131</b> |
| 3.1 Quadratic Residues                             | 131        |
| 3.2 Quadratic Reciprocity                          | 137        |
| 3.3 The Jacobi Symbol                              | 142        |
| 3.4 Binary Quadratic Forms                         | 150        |

|          |                                                     |            |
|----------|-----------------------------------------------------|------------|
| 3.5      | Equivalence and Reduction of Binary Quadratic Forms | 155        |
| 3.6      | Sums of Two Squares                                 | 163        |
| 3.7      | Positive Definite Binary Quadratic Forms            | 170        |
|          | Notes on Chapter 3                                  | 176        |
| <b>4</b> | <b>Some Functions of Number Theory</b>              | <b>180</b> |
| 4.1      | Greatest Integer Function                           | 180        |
| 4.2      | Arithmetic Functions                                | 188        |
| 4.3      | The Möbius Inversion Formula                        | 193        |
| 4.4      | Recurrence Functions                                | 197        |
| 4.5      | Combinatorial Number Theory                         | 206        |
|          | Notes on Chapter 4                                  | 211        |
| <b>5</b> | <b>Some Diophantine Equations</b>                   | <b>212</b> |
| 5.1      | The Equation $ax + by = c$                          | 212        |
| 5.2      | Simultaneous Linear Equations                       | 219        |
| 5.3      | Pythagorean Triangles                               | 231        |
| 5.4      | Assorted Examples                                   | 234        |
| 5.5      | Ternary Quadratic Forms                             | 240        |
| 5.6      | Rational Points on Curves                           | 249        |
| 5.7      | Elliptic Curves                                     | 261        |
| 5.8      | Factorization Using Elliptic Curves                 | 281        |
| 5.9      | Curves of Genus Greater Than 1                      | 288        |
|          | Notes on Chapter 5                                  | 289        |
| <b>6</b> | <b>Farey Fractions and Irrational Numbers</b>       | <b>297</b> |
| 6.1      | Farey Sequences                                     | 297        |
| 6.2      | Rational Approximations                             | 301        |
| 6.3      | Irrational Numbers                                  | 307        |
| 6.4      | The Geometry of Numbers                             | 312        |
|          | Notes on Chapter 6                                  | 322        |
| <b>7</b> | <b>Simple Continued Fractions</b>                   | <b>325</b> |
| 7.1      | The Euclidean Algorithm                             | 325        |
| 7.2      | Uniqueness                                          | 327        |
| 7.3      | Infinite Continued Fractions                        | 329        |
| 7.4      | Irrational Numbers                                  | 334        |
| 7.5      | Approximations to Irrational Numbers                | 336        |

|           |                                                                     |            |
|-----------|---------------------------------------------------------------------|------------|
| 7.6       | Best Possible Approximations                                        | 341        |
| 7.7       | Periodic Continued Fractions                                        | 344        |
| 7.8       | Pell's Equation                                                     | 351        |
| 7.9       | Numerical Computation                                               | 358        |
|           | Notes on Chapter 7                                                  | 359        |
| <b>8</b>  | <b>Primes and Multiplicative Number Theory</b>                      | <b>360</b> |
| 8.1       | Elementary Prime Number Estimates                                   | 360        |
| 8.2       | Dirichlet Series                                                    | 374        |
| 8.3       | Estimates of Arithmetic Functions                                   | 389        |
| 8.4       | Primes in Arithmetic Progressions                                   | 401        |
|           | Notes on Chapter 8                                                  | 406        |
| <b>9</b>  | <b>Algebraic Numbers</b>                                            | <b>409</b> |
| 9.1       | Polynomials                                                         | 410        |
| 9.2       | Algebraic Numbers                                                   | 414        |
| 9.3       | Algebraic Number Fields                                             | 419        |
| 9.4       | Algebraic Integers                                                  | 424        |
| 9.5       | Quadratic Fields                                                    | 425        |
| 9.6       | Units in Quadratic Fields                                           | 428        |
| 9.7       | Primes in Quadratic Fields                                          | 429        |
| 9.8       | Unique Factorization                                                | 431        |
| 9.9       | Primes in Quadratic Fields Having the Unique Factorization Property | 433        |
| 9.10      | The Equation $x^3 + y^3 = z^3$                                      | 441        |
|           | Notes on Chapter 9                                                  | 445        |
| <b>10</b> | <b>The Partition Function</b>                                       | <b>446</b> |
| 10.1      | Partitions                                                          | 446        |
| 10.2      | Ferrers Graphs                                                      | 448        |
| 10.3      | Formal Power Series, Generating Functions, and Euler's Identity     | 452        |
| 10.4      | Euler's Formula; Bounds on $p(n)$                                   | 457        |
| 10.5      | Jacobi's Formula                                                    | 463        |
| 10.6      | A Divisibility Property                                             | 467        |
|           | Notes on Chapter 10                                                 | 471        |
| <b>11</b> | <b>The Density of Sequences of Integers</b>                         | <b>472</b> |
| 11.1      | Asymptotic Density                                                  | 473        |
| 11.2      | Schnirelmann Density and the $\alpha\beta$ Theorem                  | 476        |
|           | Notes on Chapter 11                                                 | 481        |

|                                                  |                |
|--------------------------------------------------|----------------|
| <b>Appendices</b>                                | <b>482</b>     |
| A.1 The Fundamental Theorem of Algebra           | 482            |
| A.2 Symmetric Functions                          | 484            |
| A.3 A Special Value of the Riemann Zeta Function | 490            |
| A.4 Linear Recurrences                           | 493            |
| <br><b>General References</b>                    | <br><b>500</b> |
| <b>Hints</b>                                     | <b>503</b>     |
| <b>Answers</b>                                   | <b>512</b>     |
| <b>Index</b>                                     | <b>522</b>     |