

Hua Loo Keng

# Introduction to Number Theory

Translated from the Chinese by Peter Shiu

With 14 Figures

Springer-Verlag  
Berlin Heidelberg New York 1982

# Table of Contents

|                                                                        |           |
|------------------------------------------------------------------------|-----------|
| List of Frequently Used Symbols . . . . .                              | XVII      |
| <b>Chapter 1. The Factorization of Integers . . . . .</b>              | <b>1</b>  |
| 1.1 Divisibility . . . . .                                             | 1         |
| 1.2 Prime Numbers and Composite Numbers . . . . .                      | 2         |
| 1.3 Prime Numbers . . . . .                                            | 3         |
| 1.4 Integral Modulus . . . . .                                         | 4         |
| 1.5 The Fundamental Theorem of Arithmetic . . . . .                    | 6         |
| 1.6 The Greatest Common Factor and the Least Common Multiple . . . . . | 7         |
| 1.7 The Inclusion-Exclusion Principle . . . . .                        | 10        |
| 1.8 Linear Indeterminate Equations . . . . .                           | 11        |
| 1.9 Perfect Numbers . . . . .                                          | 12        |
| 1.10 Mersenne Numbers and Fermat Numbers . . . . .                     | 14        |
| 1.11 The Prime Power in a Factorial . . . . .                          | 16        |
| 1.12 Integral Valued Polynomials . . . . .                             | 17        |
| 1.13 The Factorization of Polynomials . . . . .                        | 19        |
| Notes . . . . .                                                        | 21        |
| <b>Chapter 2. Congruences . . . . .</b>                                | <b>22</b> |
| 2.1 Definition . . . . .                                               | 22        |
| 2.2 Fundamental Properties of Congruences . . . . .                    | 22        |
| 2.3 Reduced Residue System . . . . .                                   | 23        |
| 2.4 The Divisibility of $2^{n-1} - 1$ by $p^2$ . . . . .               | 24        |
| 2.5 The Function $\phi(n)$ . . . . .                                   | 26        |
| 2.6 Congruences . . . . .                                              | 28        |
| 2.7 The Chinese Remainder Theorem . . . . .                            | 29        |
| 2.8 Higher Degree Congruences . . . . .                                | 31        |
| 2.9 Higher Degree Congruences to a Prime Power Modulus . . . . .       | 32        |
| 2.10 Wolstenholme's Theorem . . . . .                                  | 33        |
| <b>Chapter 3. Quadratic Residues . . . . .</b>                         | <b>35</b> |
| 3.1 Definitions and Euler's Criterion . . . . .                        | 35        |
| 3.2 The Evaluation of Legendre's Symbol . . . . .                      | 36        |
| 3.3 The Law of Quadratic Reciprocity . . . . .                         | 38        |
| 3.4 Practical Methods for the Solutions . . . . .                      | 42        |

|                                                                      |            |
|----------------------------------------------------------------------|------------|
| 3.5 The Number of Roots of a Quadratic Congruence . . . . .          | 44         |
| 3.6 Jacobi's Symbol . . . . .                                        | 44         |
| 3.7 Two Terms Congruences . . . . .                                  | 47         |
| 3.8 Primitive Roots and Indices . . . . .                            | 48         |
| 3.9 The Structure of a Reduced Residue System . . . . .              | 49         |
| <b>Chapter 4. Properties of Polynomials . . . . .</b>                | <b>57</b>  |
| 4.1 The Division of Polynomials . . . . .                            | 57         |
| 4.2 The Unique Factorization Theorem . . . . .                       | 58         |
| 4.3 Congruences . . . . .                                            | 60         |
| 4.4 Integer Coefficient Polynomials . . . . .                        | 61         |
| 4.5 Polynomial Congruences with a Prime Modulus . . . . .            | 62         |
| 4.6 On Several Theorems Concerning Factorizations . . . . .          | 63         |
| 4.7 Double Moduli Congruences . . . . .                              | 64         |
| 4.8 Generalization of Fermat's Theorem . . . . .                     | 65         |
| 4.9 Irreducible Polynomials mod $p$ . . . . .                        | 66         |
| 4.10 Primitive Roots . . . . .                                       | 67         |
| 4.11 Summary . . . . .                                               | 68         |
| <b>Chapter 5. The Distribution of Prime Numbers . . . . .</b>        | <b>70</b>  |
| 5.1 Order of Infinity . . . . .                                      | 70         |
| 5.2 The Logarithm Function . . . . .                                 | 71         |
| 5.3 Introduction . . . . .                                           | 72         |
| 5.4 The Number of Primes is Infinite . . . . .                       | 75         |
| 5.5 Almost All Integers are Composite . . . . .                      | 78         |
| 5.6 Chebyshev's Theorem . . . . .                                    | 79         |
| 5.7 Bertrand's Postulate . . . . .                                   | 82         |
| 5.8 Estimation of a Sum by an Integral . . . . .                     | 85         |
| 5.9 Consequences of Chebyshev's Theorem . . . . .                    | 89         |
| 5.10 The Number of Prime Factors of $n$ . . . . .                    | 94         |
| 5.11 A Prime Representing Function . . . . .                         | 96         |
| 5.12 On Primes in an Arithmetic Progression . . . . .                | 97         |
| Notes . . . . .                                                      | 99         |
| <b>Chapter 6. Arithmetic Functions . . . . .</b>                     | <b>102</b> |
| 6.1 Examples of Arithmetic Functions . . . . .                       | 102        |
| 6.2 Properties of Multiplicative Functions . . . . .                 | 104        |
| 6.3 The Möbius Inversion Formula . . . . .                           | 105        |
| 6.4 The Möbius Transformation . . . . .                              | 107        |
| 6.5 The Divisor Function . . . . .                                   | 111        |
| 6.6 Two Theorems Related to Asymptotic Densities . . . . .           | 113        |
| 6.7 The Representation of Integers as a Sum of Two Squares . . . . . | 115        |
| 6.8 The Methods of Partial Summation and Integration . . . . .       | 120        |
| 6.9 The Circle Problem . . . . .                                     | 122        |
| 6.10 Farey Sequence and Its Applications . . . . .                   | 125        |

|                                                                                                          |            |
|----------------------------------------------------------------------------------------------------------|------------|
| 6.11 Vinogradov's Method of Estimating Sums of Fractional Parts . . . . .                                | 129        |
| 6.12 Application of Vinogradov's Theorem to Lattice Point Problems . . . . .                             | 134        |
| 6.13 $\Omega$ -results . . . . .                                                                         | 138        |
| 6.14 Dirichlet Series . . . . .                                                                          | 143        |
| 6.15 Lambert Series . . . . .                                                                            | 146        |
| Notes . . . . .                                                                                          | 147        |
| <b>Chapter 7. Trigonometric Sums and Characters . . . . .</b>                                            | <b>149</b> |
| 7.1 Representation of Residue Classes . . . . .                                                          | 149        |
| 7.2 Character Functions . . . . .                                                                        | 151        |
| 7.3 Types of Characters . . . . .                                                                        | 156        |
| 7.4 Character Sums . . . . .                                                                             | 159        |
| 7.5 Gauss Sums . . . . .                                                                                 | 162        |
| 7.6 Character Sums and Trigonometric Sums . . . . .                                                      | 169        |
| 7.7 From Complete Sums to Incomplete Sums . . . . .                                                      | 170        |
| 7.8 Applications of the Character Sum $\sum_{a=1}^p \left( x^2 + ax + b \right) \frac{p}{p}$ . . . . .   | 174        |
| 7.9 Tao Problem of the Distribution of Primitive Roots . . . . .                                         | 177        |
| 7.10 Trigonometric Sums Involving Polynomials . . . . .                                                  | 180        |
| Notes . . . . .                                                                                          | 185        |
| <b>Chapter 8. On Several Arithmetic Problems Associated with the Elliptic Modular Function . . . . .</b> | <b>186</b> |
| 8.1 Introduction . . . . .                                                                               | 186        |
| 8.2 The Partition of Integers . . . . .                                                                  | 187        |
| 8.3 Jacobi's Identity . . . . .                                                                          | 188        |
| 8.4 Methods of Representing Partitions . . . . .                                                         | 193        |
| 8.5 Graphical Method for Partitions . . . . .                                                            | 195        |
| 8.6 Estimates for $p(n)$ . . . . .                                                                       | 199        |
| 8.7 The Problem of Sums of Squares . . . . .                                                             | 204        |
| 8.8 Density . . . . .                                                                                    | 210        |
| 8.9 A Summary of the Problem of Sums of Squares . . . . .                                                | 215        |
| <b>Chapter 9. The Prime Number Theorem . . . . .</b>                                                     | <b>217</b> |
| 9.1 Introduction . . . . .                                                                               | 217        |
| 9.2 The Riemann $\zeta$ -Function . . . . .                                                              | 219        |
| 9.3 Several Lemmas . . . . .                                                                             | 222        |
| 9.4 A Tauberian Theorem . . . . .                                                                        | 226        |
| 9.5 The Prime Number Theorem . . . . .                                                                   | 231        |
| 9.6 Selberg's Asymptotic Formula . . . . .                                                               | 233        |
| 9.7 Elementary Proof of the Prime Number Theorem . . . . .                                               | 235        |
| 9.8 Dirichlet's Theorem . . . . .                                                                        | 243        |
| Notes . . . . .                                                                                          | 248        |

|                                                                                          |     |
|------------------------------------------------------------------------------------------|-----|
| <b>Chapter 10. Continued Fractions and Approximation Methods</b> . . . . .               | 259 |
| 10.1 Simple Continued Fractions . . . . .                                                | 259 |
| 10.2 The Uniqueness of a Continued Fraction Expansion . . . . .                          | 252 |
| 10.3 The Best Approximation . . . . .                                                    | 254 |
| 10.4 Hurwitz's Theorem . . . . .                                                         | 255 |
| 10.5 The Equivalence of Real Numbers . . . . .                                           | 257 |
| 10.6 Periodic Continued Fractions . . . . .                                              | 260 |
| 10.7 Legendre's Criterion . . . . .                                                      | 261 |
| 10.8 Quadratic Indeterminate Equations . . . . .                                         | 262 |
| 10.9 Pell's Equation . . . . .                                                           | 264 |
| 10.10 Chebyshev's Theorem and Khintchine's Theorem . . . . .                             | 266 |
| 10.11 Uniform Distributions and the Uniform Distribution of $n\theta \pmod{1}$ . . . . . | 269 |
| 10.12 Criteria for Uniform Distributions . . . . .                                       | 270 |
| <br><b>Chapter 11. Indeterminate Equations</b> . . . . .                                 | 276 |
| 11.1 Introduction . . . . .                                                              | 276 |
| 11.2 Linear Indeterminate Equations . . . . .                                            | 276 |
| 11.3 Quadratic Indeterminate Equations . . . . .                                         | 278 |
| 11.4 The Solution to $ax^2 + bxy + cy^2 = h$ . . . . .                                   | 278 |
| 11.5 Method of Solution . . . . .                                                        | 283 |
| 11.6 Generalization of Soong Go's Theorem . . . . .                                      | 286 |
| 11.7 Fermat's Conjecture . . . . .                                                       | 288 |
| 11.8 Markoff's Equation . . . . .                                                        | 288 |
| 11.9 The Equation $x^3 + y^3 + z^3 + w^3 = 0$ . . . . .                                  | 290 |
| 11.10 Rational Points on a Cubic Surface . . . . .                                       | 293 |
| Notes . . . . .                                                                          | 299 |
| <br><b>Chapter 12. Binary Quadratic Forms</b> . . . . .                                  | 309 |
| 12.1 The Partitioning of Binary Quadratic Forms into Classes . . . . .                   | 309 |
| 12.2 The Finiteness of the Number of Classes . . . . .                                   | 302 |
| 12.3 Kronecker's Symbol . . . . .                                                        | 304 |
| 12.4 The Number of Representations of an Integer by a Form . . . . .                     | 307 |
| 12.5 The Equivalence of Forms mod $q$ . . . . .                                          | 309 |
| 12.6 The Character System for a Quadratic Form and the Genus . . . . .                   | 314 |
| 12.7 The Convergence of the Series $K(\theta)$ . . . . .                                 | 317 |
| 12.8 The Number of Lattice Points Inside a Hyperbola and an Ellipse . . . . .            | 318 |
| 12.9 The Limiting Average . . . . .                                                      | 318 |
| 12.10 The Class Number: An Analytic Expression . . . . .                                 | 321 |
| 12.11 The Fundamental Discriminants . . . . .                                            | 322 |
| 12.12 The Class Number Formula . . . . .                                                 | 323 |
| 12.13 The Least Solution to Pell's Equation . . . . .                                    | 326 |
| 12.14 Several Lemmas . . . . .                                                           | 329 |
| 12.15 Siegel's Theorem . . . . .                                                         | 331 |
| Notes . . . . .                                                                          | 337 |

|                                                                         |     |
|-------------------------------------------------------------------------|-----|
| <b>Chapter 13. Unimodular Transformations</b> . . . . .                 | 338 |
| 13.1 The Complex Plane . . . . .                                        | 338 |
| 13.2 Properties of the Bilinear Transformation . . . . .                | 339 |
| 13.3 Geometric Properties of the Bilinear Transformation . . . . .      | 342 |
| 13.4 Real Transformations . . . . .                                     | 344 |
| 13.5 Unimodular Transformations . . . . .                               | 348 |
| 13.6 The Fundamental Region . . . . .                                   | 350 |
| 13.7 The Net of the Fundamental Region . . . . .                        | 354 |
| 13.8 The Structure of the Modular Group . . . . .                       | 355 |
| 13.9 Positive Definite Quadratic Forms . . . . .                        | 356 |
| 13.10 Indefinite Quadratic Forms . . . . .                              | 358 |
| 13.11 The Least Value of an Indefinite Quadratic Form . . . . .         | 361 |
| <b>Chapter 14. Integer Matrices and Their Applications</b> . . . . .    | 365 |
| 14.1 Introduction . . . . .                                             | 365 |
| 14.2 The Product of Matrices . . . . .                                  | 371 |
| 14.3 The Number of Generators for Modular Matrices . . . . .            | 377 |
| 14.4 Left Association . . . . .                                         | 382 |
| 14.5 Invariant Factors and Elementary Divisors . . . . .                | 384 |
| 14.6 Applications . . . . .                                             | 387 |
| 14.7 Matrix Factorizations and Standard Prime Matrices . . . . .        | 389 |
| 14.8 The Greatest Common Factor and the Least Common Multiple . . . . . | 394 |
| 14.9 Linear Modules . . . . .                                           | 399 |
| <b>Chapter 15. <math>p</math>-adic Numbers</b> . . . . .                | 405 |
| 15.1 Introduction . . . . .                                             | 405 |
| 15.2 The Definition of a Valuation . . . . .                            | 408 |
| 15.3 The Partitioning of Valuations into Classes . . . . .              | 410 |
| 15.4 Archimedean Valuations . . . . .                                   | 411 |
| 15.5 Non-Archimedean Valuations . . . . .                               | 412 |
| 15.6 The $p$ -Extension of the Rationals . . . . .                      | 415 |
| 15.7 The Completeness of the Extension . . . . .                        | 417 |
| 15.8 The Representation of $p$ -adic Numbers . . . . .                  | 417 |
| 15.9 Application . . . . .                                              | 421 |
| <b>Chapter 16. Introduction to Algebraic Number Theory</b> . . . . .    | 423 |
| 16.1 Algebraic Numbers . . . . .                                        | 423 |
| 16.2 Algebraic Number Fields . . . . .                                  | 424 |
| 16.3 Basis . . . . .                                                    | 425 |
| 16.4 Integral Basis . . . . .                                           | 427 |
| 16.5 Divisibility . . . . .                                             | 430 |
| 16.6 Ideals . . . . .                                                   | 431 |
| 16.7 Unique Factorization Theorem for Ideals . . . . .                  | 433 |
| 16.8 Basis for Ideals . . . . .                                         | 436 |
| 16.9 Congruent Relations . . . . .                                      | 437 |

|                                                                                    |            |
|------------------------------------------------------------------------------------|------------|
| 16.10 Prime Ideals . . . . .                                                       | 438        |
| 16.11 Units . . . . .                                                              | 441        |
| 16.12 Ideal Classes . . . . .                                                      | 441        |
| 16.13 Quadratic Fields and Quadratic Forms . . . . .                               | 442        |
| 16.14 Genus . . . . .                                                              | 445        |
| 16.15 Euclidean Fields and Simple Fields . . . . .                                 | 447        |
| 16.16 Lucas's Criterion for the Determination of Mersenne Primes . . . . .         | 449        |
| 16.17 Indeterminate Equations . . . . .                                            | 450        |
| 16.18 Tables . . . . .                                                             | 454        |
| Notes . . . . .                                                                    | 473        |
| <b>Chapter 17. Algebraic Numbers and Transcendental Numbers . . . . .</b>          | <b>474</b> |
| 17.1 The Existence of Transcendental Numbers . . . . .                             | 474        |
| 17.2 Liouville's Theorem and Examples of Transcendental Numbers . . . . .          | 476        |
| 17.3 Roth's Theorem on Rational Approximations to Algebraic Numbers . . . . .      | 478        |
| 17.4 Application of Roth's Theorem . . . . .                                       | 478        |
| 17.5 Application of Thue's Theorem . . . . .                                       | 480        |
| 17.6 The Transcendence of $e$ . . . . .                                            | 483        |
| 17.7 The Transcendence of $\pi$ . . . . .                                          | 486        |
| 17.8 Hilbert's Seventh Problem . . . . .                                           | 488        |
| 17.9 Gelfond's Proof . . . . .                                                     | 490        |
| Notes . . . . .                                                                    | 493        |
| <b>Chapter 18. Waring's Problem and the Problem of Prouhet and Tarry . . . . .</b> | <b>494</b> |
| 18.1 Introduction . . . . .                                                        | 494        |
| 18.2 Lower Bounds for $g(k)$ and $G(k)$ . . . . .                                  | 494        |
| 18.3 Cauchy's Theorem . . . . .                                                    | 496        |
| 18.4 Elementary Methods . . . . .                                                  | 499        |
| 18.5 The Easier Problem of Positive and Negative Signs . . . . .                   | 503        |
| 18.6 Equal Power Sums Problem . . . . .                                            | 505        |
| 18.7 The Problem of Prouhet and Tarry . . . . .                                    | 507        |
| 18.8 Continuation . . . . .                                                        | 511        |
| <b>Chapter 19. Schnirelmann Density . . . . .</b>                                  | <b>514</b> |
| 19.1 The Definition of Density and its History . . . . .                           | 514        |
| 19.2 The Sum of Squares and its Density . . . . .                                  | 515        |
| 19.3 The Goldbach-Schnirelmann Theorem . . . . .                                   | 518        |
| 19.4 Selberg's Inequality . . . . .                                                | 519        |
| 19.5 The Proof of the Goldbach-Schnirelmann Theorem . . . . .                      | 525        |
| 19.6 The Waring-Hilbert Theorem . . . . .                                          | 528        |
| 19.7 The Proof of the Waring-Hilbert Theorem . . . . .                             | 530        |
| Notes . . . . .                                                                    | 534        |

|                                                       |     |
|-------------------------------------------------------|-----|
| <b>Chapter 20. The Geometry of Numbers.</b>           | 535 |
| 20.1 The Two Dimensional Situation                    | 535 |
| 20.2 The Fundamental Theorem of Minkowski.            | 538 |
| 20.3 Linear Forms                                     | 540 |
| 20.4 Positive Definite Quadratic Forms                | 542 |
| 20.5 Products of Linear Forms                         | 543 |
| 20.6 Method of Simultaneous Approximations            | 546 |
| 20.7 Minkowski's Inequality                           | 547 |
| 20.8 The Average Value of the Product of Linear Forms | 554 |
| 20.9 Tchebotaref's Theorem                            | 556 |
| 20.10 Applications to Algebraic Number Theory         | 558 |
| 20.11 The Least Value for $ A $                       | 561 |
| <b>Bibliography</b>                                   | 565 |
| <b>Index</b>                                          | 569 |