The Queen of Mathematics

A Historically Motivated Guide to Number Theory

Jay R. Goldman
School of Mathematics
University of Minnesota
Minneapolis, Minnesota

A K Peters
Wellesley, Massachusetts
Contents

PART 1: FROM FERMAT TO LEGENDRE

Chapter 1. The Founding Fathers
1. The Beginnings ......................................................... 1
2. Fermat’s Mathematical Background ................................. 5
3. Pythagorean Triples .................................................... 8
Appendix: Properties of the Integers ................................. 11

Chapter 2. Fermat
1. Fermat (1601-1665) ..................................................... 12
2. Infinite Descent .......................................................... 13
3. Fermat’s Last Theorem .................................................. 14
4. Pell’s Equation ........................................................... 17
5. $y^3 = x^2 + k$ ............................................................ 19
6. Sums of Squares ........................................................ 19
7. Perfect Numbers and Fermat’s Little Theorem .................. 21
8. Fermat’s Error .......................................................... 23

Chapter 3. Euler
1. Euler ........................................................................ 24
2. Partitions of a Number ................................................... 27
3. The Beginning of Analytic Number Theory; Prime Numbers, Zeta Functions, Bernoulli Numbers ......................... 30
4. Arithmetic Functions .................................................... 38
5. The Beginning of Algebraic Number Theory ...................... 39

xvii
Chapter 4. From Euler to Lagrange; The Theory of Continued Fractions

1. Introduction ................................................................. 43
2. The Basic Notions: Finite and Infinite Continued Fractions. 44
   The Continued Fraction Algorithm ............................... 48
3. The Early History .................................................... 50
4. The Algebra of Finite Continued Fractions ................... 51
5. The Arithmetic of Finite Continued Fractions ............... 55
6. Infinite Continued Fractions ....................................... 58
7. Diophantine Approximation and Geometry .......... 61
8. Quadratic Irrationalities ............................................. 66
9. Pell’s Equation .......................................................... 71
10. Generalizations .......................................................... 73

Chapter 5. Lagrange

1. Lagrange and His Work ............................................... 76
2. Quadratic Forms .......................................................... 78

Chapter 6. Legendre

1. Legendre ......................................................................... 81
2. Rational Points on Conics .............................................. 82
3. Distribution of Prime Numbers ......................................... 82
4. Quadratic Residues and Quadratic Reciprocity ............. 83

PART 2: GAUSS AND THE DISQUISITIONES ARITHMETICA

Chapter 7. Gauss

1. Gauss and His Work ...................................................... 86
2. An Overview of the Disquisitiones Arithmeticae ........ 94

Chapter 8. Theory of Congruence 1

1. Section I of the Disquisitiones ....................................... 95
2. Residue Classes ............................................................. 99
3. Congruences and Algebraic Structures ....................... 101
4. Applications ................................................................. 103
5. Linear Congruences ....................................................... 107
Chapter 9. Theory of Congruences 2
1. Introduction .................................................. 109
2. Reduced Residue Classes .............................. 109
3. The Structure of $\mathbb{Z}/n\mathbb{Z}$ ......................... 111
4. Polynomial Congruences .......................... 114
5. Polynomial Congruences and Polynomial Functions .... 119
6. Congruences in Several Variables; Chevalley's Theorem ... 121
7. Solutions of Congruences and Solutions of Equations; The Hasse Principle .................. 123

Chapter 10. Primitive Roots and Power Residues
1. Primitive Roots ........................................... 125
2. Indices ...................................................... 127
3. $k^{th}$ Power Residues ............................... 129

Chapter 11. Congruences of the Second Degree
1. Introduction ............................................. 132
2. Elementary Properties of Quadratic Residues ........ 133
3. Gauss's Lemma ........................................... 135
4. Computing $\left( \frac{a}{p} \right)$ .............................. 136
5. Quadratic Reciprocity 1 ................................. 141
6. Quadratic Reciprocity 2 ................................ 145
7. Some History and Other Proofs ....................... 151

Chapter 12. Binary Quadratic Forms 1: Arithmetic Theory
1. Introduction ............................................. 155
2. Equivalence of Forms .................................. 156
3. Matrix Notation and the Discriminant ................ 157
4. Reduced Forms and the Number of Classes ........... 159
5. Representation and Equivalence ....................... 162
6. Representations and Quadratic Residues ................ 163
7. Proper Equivalence ..................................... 166
8. Definite and Indefinite Forms ......................... 167
9. Positive Definite Forms ................................ 169
10. Primitive Forms and the Class Number ............... 171
Chapter 13. Binary Quadratic Forms 2: Geometric Theory
1. Introduction ................................................. 174
2. The Roots of a Form ........................................ 175
3. Positive Definite Forms and the Upper Half Plane ......... 178
4. Linear Fractional Transformations .......................... 181
5. The Fundamental Domain .................................. 182
6. Forms and the Upper Half Plane Revisited ............... 190
7. Automorphs and the Number of Representations .......... 191
8. Indefinite Forms, $D > 0$ .................................... 195
   Reduction ....................................................... 195
   Automorphs and Representations ............................ 196
   Geometric Methods ......................................... 196
9. Composition of Forms ....................................... 198
10. Genus ......................................................... 201
11. Sections V and VI of the Disquisitiones .................. 202

Chapter 14. Cyclotomy
1. Introduction to Section VII of the Disquisitiones .......... 203
2. Constructibility and the Theory of Equations .............. 206
3. The 5-gon and Gaussian Periods ............................. 209
4. Back to Quadratic Reciprocity ................................ 212
5. Numbers of Solutions of Congruences;
   Equations over Finite Fields ............................... 220
6. Final Remarks on the Disquisitiones ...................... 221

PART 3: ALGEBRAIC NUMBER THEORY

Chapter 15. Algebraic Number Theory 1: The Gaussian
   Integers and Biquadratic Reciprocity
1. Gauss and Biquadratic Reciprocity .......................... 223
2. The Gaussian Integers ....................................... 227
   Back to the Two Square Problem ........................... 230
3. Congruence and the Law of Biquadratic Reciprocity ....... 232
4. The Zeta Function and L Function of $\mathbb{Z}[i]$ .......... 236
Chapter 16. Algebraic Number Theory 2: Algebraic Numbers and Quadratic Fields
1. The Development of Algebraic Number Theory ............... 241
2. Algebraic Integers ........................................ 250
3. Quadratic Fields ........................................... 252
4. Quadratic Integers ......................................... 254
5. Geometric Representation; Divisibility and Units .......... 257
6. Factorization in Quadratic Fields ......................... 260
7. Euclidean Domains and Unique Factorization .......... 261
8. Non-Unique Factorization and Ideals .................... 264

Chapter 17. Algebraic Number Theory 3: Ideals in Quadratic Fields
1. Arithmetic of Ideals in $I_d$ ............................... 267
2. Lattices and Ideals ......................................... 270
Appendix: Lattices ........................................... 274
3. More Arithmetic of Ideals .................................. 275
4. Unique Factorization of Ideals ............................ 278
5. Applications of Unique Factorization ..................... 281
   Divisibility and Diophantine Equations .................. 281
   Unique Factorization Domains ............................ 282
6. The Factorization of Rational Primes ..................... 282
7. Class Structure and the Class Number .................... 284
8. Finiteness of the Class Number; Norm of an Ideal .... 289
9. Bases and Discriminants .................................. 292
10. The Correspondence between Forms and Fields ........ 294
11. Applications of the Correspondence ..................... 299
   Class Numbers ............................................. 299
   Units and Automorphs of Forms .......................... 300
   The Class Group, Composition of Forms, and the Representation of Numbers by Forms .................. 301
12. Factorization of Rational Primes Revisited ............ 301
13. General Reciprocity Laws ................................ 307
Appendix: Dirichlet and 19th-Century Number Theory .... 309
PART 4: ARITHMETIC ON CURVES

Chapter 18. Arithmetic on Curves 1: Rational Points and Plane Algebraic Curves

1. Introduction ......................................................... 311
2. Lines ........................................................................ 313
3. Conics ....................................................................... 314
4. Cubics and the Geometric Form of Mordell's Theorem .......... 319
5. The Need for Projective Geometry .................................. 322
6. The Real Projective Plane; Homogeneous Coordinates ............ 326
   The Real Projective Plane and its Models .................................. 326
   Homogeneous Coordinates ............................................. 330
7. Algebraic Curves in the Projective Plane ............................ 331
8. Geometry Over a Field; Higher Dimensions and Duality ....... 337
   General Fields .......................................................... 337
   Higher Dimensions .................................................... 339
   Duality ..................................................................... 339

Chapter 19. Arithmetic on Curves 2: Rational Points and Elliptic Curves

1. Introduction .................................................................. 343
2. Intersection of Curves; Bezout's Theorem .......................... 343
3. The Group Law and the Algebraic Form of Mordell's Theorem .... 348
4. Birational Equivalence; Weierstrass Normal Form ............... 350
5. Singular Points and the Genus ....................................... 355
6. Elliptic Curves and the Group Law .................................. 360
7. Elliptic Functions and Elliptic Curves ............................... 368
8. Complex Points of Finite Order ...................................... 372
9. The Early History ..................................................... 373

Chapter 20. Arithmetic on Curves 3: The Twentieth Century

1. From Poincaré to Weil ............................................... 383
2. Points of Finite Order; The Lutz–Nagell Theorem ............... 388
3. The Easy Part of the Theorem ....................................... 390
4. The Hard Part of the Theorem ...................................... 391
5. Mordell's Theorem; An Outline of the Proof ..................... 399
6. Some Preliminary Results ........................................... 402
7. The Height Function ................................................ 404
8. The Weak Mordell–Weil Theorem ................................. 409
9. Equations over Finite Fields; the Zeta and
   L Functions of a Curve ........................................... 413
10. Complex Multiplication ............................................ 416

PART 5: MISCELLANEOUS TOPICS

Chapter 21. Irrational and Transcendental Numbers,
Diophantine Approximation
1. The Early History .................................................. 418
2. From Euler to Dirichlet ........................................... 419
3. Liouville to Hilbert; The Beginning of Transcendental
   Number Theory ...................................................... 423
4. Simultaneous Approximation; Kronecker’s Theorem ........ 431
5. Thue: Diophantine Approximation and
   Diophantine Equations ........................................... 432
6. The 20th Century ................................................... 436
7. Other Results and Problems ...................................... 438
8. The Literature ....................................................... 439

Chapter 22. Geometry of Numbers
1. The Motivating Problem; Quadratic Forms ..................... 440
2. Minkowski’s Fundamental Theorem ............................... 443
3. Minkowski’s Theorem for Lattices ............................... 448
   Lattices .............................................................. 448
   Change of Basis .................................................... 451
   Minkowski’s Theorem Reformulated ............................. 452
4. Back to Quadratic Forms .......................................... 452
5. Sums of Two and Four Squares .................................. 454
6. Linear Forms ........................................................ 457
7. Sums and Products of Linear Forms; The Octahedron ........ 459
8. Gauge Functions; The Equation of a Convex Body ............ 463
9. Successive Minima ................................................... 468
10. Other Directions .................................................... 469
xxiv Contents

Chapter 23. p-adic Numbers and Valuations
1. History ................................................................. 470
2. The $p$-adic Numbers; An Informal Introduction .......... 471
3. The Formal Development .................................. 478
4. Convergence ....................................................... 482
5. Congruences and $p$-adic Numbers ......................... 487
6. Hasse’s Principle; The Hasse-Minkowski Theorem ....... 489
7. Valuations and Algebraic Number Theory ................. 493

Bibliography ................................................................ 497

Index ........................................................................ 517