An Invitation to
Modern Number Theory

Steven J. Miller and
Ramin Takloo-Bighash

PRINCETON UNIVERSITY PRESS
PRINCETON AND OXFORD
Contents

Foreword xi

Preface xiii

Notation xix

PART 1. BASIC NUMBER THEORY 1

Chapter 1. Mod $p$ Arithmetic, Group Theory and Cryptography 3
  1.1 Cryptography 3
  1.2 Efficient Algorithms 5
  1.3 Clock Arithmetic: Arithmetic Modulo $n$ 14
  1.4 Group Theory 15
  1.5 RSA Revisited 20
  1.6 Eisenstein's Proof of Quadratic Reciprocity 21

Chapter 2. Arithmetic Functions 29
  2.1 Arithmetic Functions 29
  2.2 Average Order 32
  2.3 Counting the Number of Primes 38

Chapter 3. Zeta and $L$-Functions 47
  3.1 The Riemann Zeta Function 47
  3.2 Zeros of the Riemann Zeta Function 54
  3.3 Dirichlet Characters and $L$-Functions 69

Chapter 4. Solutions to Diophantine Equations 81
  4.1 Diophantine Equations 81
  4.2 Elliptic Curves 85
  4.3 Height Functions and Diophantine Equations 89
  4.4 Counting Solutions of Congruences Modulo $p$ 95
  4.5 Research Projects 105

PART 2. CONTINUED FRACTIONS AND APPROXIMATIONS 107

Chapter 5. Algebraic and Transcendental Numbers 109
5.1 Russell's Paradox and the Banach-Tarski Paradox 109
5.2 Definitions 110
5.3 Countable and Uncountable Sets 112
5.4 Properties of e 118
5.5 Exponent (or Order) of Approximation 124
5.6 Liouville's Theorem 128
5.7 Roth's Theorem 132

Chapter 6. The Proof of Roth's Theorem 137
6.1 Liouville's Theorem and Roth's Theorem 137
6.2 Equivalent Formulation of Roth's Theorem 138
6.3 Roth's Main Lemma 142
6.4 Preliminaries to Proving Roth's Lemma 147
6.5 Proof of Roth's Lemma 155

Chapter 7. Introduction to Continued Fractions 158
7.1 Decimal Expansions 158
7.2 Definition of Continued Fractions 159
7.3 Representation of Numbers by Continued Fractions 161
7.4 Infinite Continued Fractions 167
7.5 Positive Simple Convergents and Convergence 169
7.6 Periodic Continued Fractions and Quadratic Irrationals 170
7.7 Computing Algebraic Numbers' Continued Fractions 177
7.8 Famous Continued Fraction Expansions 179
7.9 Continued Fractions and Approximations 182
7.10 Research Projects 186

PART 3. PROBABILISTIC METHODS AND EQUIDISTRIBUTION 189

Chapter 8. Introduction to Probability 191
8.1 Probabilities of Discrete Events 192
8.2 Standard Distributions 205
8.3 Random Sampling 211
8.4 The Central Limit Theorem 213

Chapter 9. Applications of Probability: Benford's Law and Hypothesis Testing 216
9.1 Benford's Law 216
9.2 Benford's Law and Equidistributed Sequences 218
9.3 Recurrence Relations and Benford's Law 219
9.4 Random Walks and Benford's Law 221
9.5 Statistical Inference 225
9.6 Summary 229

Chapter 10. Distribution of Digits of Continued Fractions 231
10.1 Simple Results on Distribution of Digits 231
10.2 Measure of $\alpha$ with Specified Digits 235
CONTENTS

10.3 The Gauss-Kuzmin Theorem 237
10.4 Dependencies of Digits 244
10.5 Gauss-Kuzmin Experiments 248
10.6 Research Projects 252

Chapter 11. Introduction to Fourier Analysis 255
11.1 Inner Product of Functions 256
11.2 Fourier Series 258
11.3 Convergence of Fourier Series 262
11.4 Applications of the Fourier Transform 268
11.5 Central Limit Theorem 273
11.6 Advanced Topics 276

Chapter 12. \{n^k \alpha\} and Poissonian Behavior 278
12.1 Definitions and Problems 278
12.2 Denseness of \{n^k \alpha\} 280
12.3 Equidistribution of \{n^k \alpha\} 283
12.4 Spacing Preliminaries 288
12.5 Point Masses and Induced Probability Measures 289
12.6 Neighbor Spacings 290
12.7 Poissonian Behavior 291
12.8 Neighbor Spacings of \{n^k \alpha\} 296
12.9 Research Projects 299

PART 4. THE CIRCLE METHOD 301

Chapter 13. Introduction to the Circle Method 303
13.1 Origins 303
13.2 The Circle Method 309
13.3 Goldbach’s Conjecture Revisited 315

14.1 Germain Primes 326
14.2 Preliminaries 328
14.3 The Functions \(F_N(x)\) and \(u(x)\) 331
14.4 Approximating \(F_N(x)\) on the Major Arcs 332
14.5 Integrals over the Major Arcs 338
14.6 Major Arcs and the Singular Series 342
14.7 Number of Germain Primes and Weighted Sums 350
14.8 Exercises 353
14.9 Research Projects 354

PART 5. RANDOM MATRIX THEORY AND \(L\)-FUNCTIONS 357

Chapter 15. From Nuclear Physics to \(L\)-Functions 359
15.1 Historical Introduction 359
15.2 Eigenvalue Preliminaries 364
## CONTENTS

15.3 Semi-Circle Law 368
15.4 Adjacent Neighbor Spacings 374
15.5 Thin Sub-families 377
15.6 Number Theory 383
15.7 Similarities between Random Matrix Theory and $L$-Functions 389
15.8 Suggestions for Further Reading 390

Chapter 16. Random Matrix Theory: Eigenvalue Densities 391
16.1 Semi-Circle Law 391
16.2 Non-Semi-Circle Behavior 398
16.3 Sparse Matrices 402
16.4 Research Projects 403

Chapter 17. Random Matrix Theory: Spacings between Adjacent Eigenvalues 405
17.1 Introduction to the $2 \times 2$ GOE Model 405
17.2 Distribution of Eigenvalues of $2 \times 2$ GOE Model 409
17.3 Generalization to $N \times N$ GOE 414
17.4 Conjectures and Research Projects 418

Chapter 18. The Explicit Formula and Density Conjectures 421
18.1 Explicit Formula 422
18.2 Dirichlet Characters from a Prime Conductor 429
18.3 Summary of Calculations 437

Appendix A. Analysis Review 439
A.1 Proofs by Induction 439
A.2 Calculus Review 442
A.3 Convergence and Continuity 447
A.4 Dirichlet's Pigeon-Hole Principle 448
A.5 Measures and Length 450
A.6 Inequalities 452

Appendix B. Linear Algebra Review 455
B.1 Definitions 455
B.2 Change of Basis 456
B.3 Orthogonal and Unitary Matrices 457
B.4 Trace 458
B.5 Spectral Theorem for Real Symmetric Matrices 459

Appendix C. Hints and Remarks on the Exercises 463

Appendix D. Concluding Remarks 475

Bibliography 476

Index 497