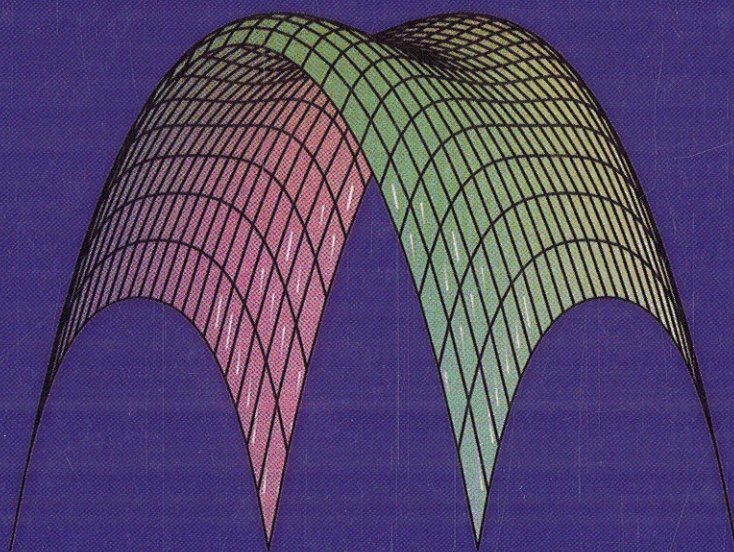


DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor KENNETH H. ROSEN

Advanced Number Theory with Applications



Richard A. Mollin



CRC Press

Taylor & Francis Group

A CHAPMAN & HALL BOOK

Contents

Preface.....	ix
About the Author.....	xiii
1 Algebraic Number Theory and Quadratic Fields	1
1.1 Algebraic Number Fields	1
1.2 The Gaussian Field	18
1.3 Euclidean Quadratic Fields	32
1.4 Applications of Unique Factorization	47
2 Ideals	55
2.1 The Arithmetic of Ideals in Quadratic Fields	55
2.2 Dedekind Domains	67
2.3 Application to Factoring	88
3 Binary Quadratic Forms	97
3.1 Basics	97
3.2 Composition and the Form Class Group	105
3.3 Applications via Ambiguity	118
3.4 Genus	129
3.5 Representation	148
3.6 Equivalence Modulo p	155
4 Diophantine Approximation	159
4.1 Algebraic and Transcendental Numbers	159
4.2 Transcendence	171
4.3 Minkowski's Convex Body Theorem	182
5 Arithmetic Functions	191
5.1 The Euler–Maclaurin Summation Formula	191
5.2 Average Orders	208
5.3 The Riemann ζ -function	218

6	Introduction to p-Adic Analysis	229
6.1	Solving Modulo p^n	229
6.2	Introduction to Valuations	233
6.3	Non-Archimedean vs. Archimedean Valuations	240
6.4	Representation of p -Adic Numbers	243
7	Dirichlet: Characters, Density, and Primes in Progression	247
7.1	Dirichlet Characters	247
7.2	Dirichlet's L -Function and Theorem	252
7.3	Dirichlet Density	263
8	Applications to Diophantine Equations	271
8.1	Lucas–Lehmer Theory	271
8.2	Generalized Ramanujan–Nagell Equations	276
8.3	Bachet's Equation	282
8.4	The Fermat Equation	286
8.5	Catalan and the ABC Conjecture	294
9	Elliptic Curves	301
9.1	The Basics	301
9.2	Mazur, Siegel, and Reduction	310
9.3	Applications: Factoring & Primality Testing	317
9.4	Elliptic Curve Cryptography (ECC)	326
10	Modular Forms	331
10.1	The Modular Group	331
10.2	Modular Forms and Functions	336
10.3	Applications to Elliptic Curves	347
10.4	Shimura–Taniyama–Weil & FLT	353
	Appendix: Sieve Methods	369
	Bibliography	393
	Solutions to Odd-Numbered Exercises	401
	Index: List of Symbols	451
	Index: Subject	453