

J. L. Lehman

Quadratic Ideal Numbers

A Computational Method for Binary Quadratic Forms

DE GRUYTER

Contents

Preface — VII

Acknowledgments — IX

1	Introduction to ideal numbers — 1
1.1	Discriminants and principal polynomials — 1
1.2	Definition of ideal numbers — 3
1.3	Ideal numbers and quadratic polynomials — 5
1.4	Ideal numbers and quadratic forms — 9
1.5	Ideal numbers and quadratic numbers — 12
1.6	Ideal numbers and ideals in quadratic domains — 18
2	Congruence classes of ideal numbers — 21
2.1	Congruence and divisibility of ideal numbers — 21
2.2	Ideal numbers of prime power norm and level zero — 25
2.3	Seeding maps — 30
2.4	Counting congruence classes of ideal numbers — 34
3	Composition of ideal numbers — 39
3.1	Composition of congruence classes — 39
3.2	Prime subgroups of level zero — 43
3.3	Prime kernels of a discriminant — 45
3.4	The kernel of a prime subgroup — 48
3.5	Level subgroups — 51
3.6	Prime subgroups of positive level — 54
4	Classes of ideal numbers — 60
4.1	Equivalence of ideal numbers — 60
4.2	Proper representations by ideal numbers — 64
4.3	Reduction of ideal numbers — 67
4.4	Automorphs of ideal numbers — 71
4.5	The class group of a discriminant — 74
5	Genera of ideal numbers — 78
5.1	The genus group of a discriminant — 78
5.2	Genus equivalence of ideal numbers — 84
5.3	The existence of genera of ideal numbers — 88
5.4	Class groups and genera — 92

6 Ideal numbers of negative discriminant — 96

- 6.1 Reduced ideal numbers of negative discriminant — **96**
- 6.2 Reduced ideal numbers and equivalence — **100**
- 6.3 Class groups of primitive negative discriminant — **103**
- 6.4 Class groups and representations — **106**
- 6.5 Negative Boolean discriminants — **111**
- 6.6 Class groups of arbitrary negative discriminant — **115**

7 Ideal numbers of positive discriminant — 120

- 7.1 Reduced ideal numbers of positive discriminant — **120**
- 7.2 Reduction maps — **124**
- 7.3 Periodicity of reduction maps — **129**
- 7.4 Reduction and equivalence — **133**
- 7.5 The continued fraction of an indefinite ideal number — **137**
- 7.6 Representations of integers by indefinite ideal numbers — **141**
- 7.7 Class group calculations — **143**

A Appendix: Review of number theory — 149

- A.1 Divisibility and congruence — **149**
- A.2 Combinations — **151**
- A.3 Prime factorization — **153**
- A.4 The Euclidean algorithm — **155**
- A.5 Linear equations and congruences — **157**
- A.6 Systems of linear congruences — **160**
- A.7 Quadratic congruences modulo primes — **162**
- A.8 Quadratic reciprocity theorem — **167**

B Appendix: Review of groups — 172

- B.1 Groups and subgroups — **172**
- B.2 Cosets and quotient groups — **175**
- B.3 Finite Abelian groups — **177**

C Appendix: Ideals of quadratic domains — 185

- C.1 Ideals of integral domains — **185**
- C.2 Quadratic domains — **187**
- C.3 Classification of ideals of a quadratic domain — **189**
- C.4 Ideal number expressions for ideals — **193**
- C.5 Complete quadratic domains and their subdomains — **195**
- C.6 Multiplication of ideals of a quadratic domain — **198**
- C.7 Composition of primitive ideals — **203**
- C.8 Equivalence of ideals — **206**
- C.9 Ordered bases of ideals — **207**

C.10 Ideal equivalence and ideal number equivalence — 212

D Appendix: Continued fractions — 215

D.1 Continued fractions of rational numbers — 215

D.2 Convergents — 217

D.3 Infinite continued fractions — 220

D.4 Calculating periodic continued fractions — 222

D.5 Continued fractions and rational approximations — 225

References — 233

Index — 235