Contents

List of Symbols xi

Preface xv

Introduction xvii

1 Background from Algebraic Number Theory. 1
1.1 Quadratic Fields: Integers and Units 4
1.2 The Arithmetic of Ideals in Quadratic Fields 9
1.3 The Class Group and Class Number 14
1.4 Reduced Ideals 19
1.5 Quadratic Orders 23
1.6 Powerful Numbers: An Application of Real Quadratics 30

2 Continued Fractions Applied to Quadratic Fields. 41
2.1 Continued Fractions and Real Quadratics: The Infrastructure . . . 41
2.2 The Continued Fraction Analogue for Complex Quadratics 63

3 Diophantine Equations and Class Numbers. 67
3.1 Class Numbers and Complex Quadratics 67
3.2 Real Quadratics and Diophantine Equations 77
3.3 Reduced Ideals and Diophantine Equations 87
3.4 Class Numbers and Real Quadratics 92
3.5 Halfway to a Solution 96

4 Prime-Producing Polynomials. 105
4.1 Complex Prime-Producers 105
4.2 Real Prime-Producers 129
4.3 Density of Primes 145

5 Class Numbers: Criteria and Bounds. 149
5.1 Factoring Rabinowitsch 149
5.2 Class Number One Criteria 158
5.3 Class Number Bounds via the Divisor Function 163
5.4 The GRH: Relevance of the Riemann Hypothesis 172

6 Ambiguous Ideals. 187
6.1 Ambiguous Cycles in Real Orders: The Palindromic Index 187
6.2 Exponent Two 199

7 Influence of the Infrastructure. **223**
7.1 Quadratic Residue Covers 223
7.2 Consecutive Powers 232

8 Algorithms. **235**
8.1 Computation of the Class Number of a Real Quadratic Field 235
8.2 Cryptology 257
8.3 Implications of Computational Mathematics for the Philosophy of Mathematics 266

APPENDIX A: Tables. **271**
Table A1: This is a list of all positive fundamental radicands with class number $h_\Delta = 1$ and period length ℓ, of the simple continued fraction expansion of the principal class, less than 24, known to be unconditionally complete whereas Table A1 is complete with one GRH-ruled out exception, as are Tables A2–A4, A6–A7 and A9 271
Table A2: This is a subset of Table A1 with $D \equiv 1 \pmod 8$ 273
Table A3: $h_\Delta = 2$ for fundamental radicands $D > 0$ with $\ell \leq 24$ 274
Table A4: This is a list of all fundamental radicands of ERD-type with class groups of exponent 2, broken down into three parts depending on congruence modulo 4 of the radicand 278
Table A5: This three-part table is an illustration of a computer run done for the proof of Theorem 6.2.2 281
Table A6: This is a list of all fundamental radicands $D > 0$ of ERD-type having no split primes less than the Minkowski bound 283
Table A7: This is a complete list of all fundamental radicands $D > 0$ with $n_\Delta \neq 0$ (see Exercise 3.2.11) and associated regulators, such that the class number is 1 284
Table A8: This is a list of all fundamental discriminants $\Delta \equiv 1 \pmod 8$ of ERD-type with class number less than 24, and is known to be unconditionally complete 285
Table A9: This table lists all fundamental discriminants of ERD-type with class number 2 286

APPENDIX B: Fundamental Units of Real Quadratic Fields.
This list is broken up into three parts according to congruence modulo 4 of fundamental radicands less than $2 \cdot 10^3$ 287

APPENDIX C: Class Numbers of Real Quadratic Fields.
This table is presented in matrix form with each entry describing a specified class number together with the norm of the fundamental unit with radicands less than 10^4 313

APPENDIX D: Class Numbers of Complex Quadratic Fields (and their class group structure).
This is a table of fundamental radicands $D < 0$ for $|D| < 2 \cdot 10^3$, together with h_Δ and the class group structure as a product of cyclic groups 335

APPENDIX E: A Gazetteer of Forms
We give an overview of the classical theory of binary quadratic forms and the interrelationships with ideal theory 347

APPENDIX F: Analytic Considerations
This provides background facts from analytic number theory. In particular this gives a brief overview of the required material for Chapter Five, section four 355

BIBLIOGRAPHY. **359**

INDEX. **383**