

Duncan A. Buell

Binary Quadratic Forms

Classical Theory and
Modern Computations



Springer-Verlag
New York Berlin Heidelberg
London Paris Tokyo Hong Kong

Contents

Preface	v
1 Elementary Concepts	1
2 Reduction of Positive Definite Forms	13
3 Indefinite Forms	21
3.1 Reduction, Cycles	21
3.2 Automorphs, Pell's Equation	31
3.3 Continued Fractions and Indefinite Forms	35
4 The Class Group	49
4.1 Representation and Genera	49
4.2 Composition Algorithms	55
4.3 Generic Characters Revisited	66
4.4 Representation of Integers	74
5 Miscellaneous Facts	77
5.1 Class Number Computations	77
5.2 Extreme Cases and Asymptotic Results	81
6 Quadratic Number Fields	87
6.1 Basic Algebraic Definitions	87
6.2 Algebraic Numbers and Quadratic Fields	89
6.3 Ideals in Quadratic Fields	94
6.4 Binary Quadratic Forms and Classes of Ideals	103
6.5 History	107

7	Composition of Forms	109
7.1	Nonfundamental Discriminants	109
7.2	The General Problem of Composition	120
7.3	Composition in Different Orders	129
8	Miscellaneous Facts II	135
8.1	The Cohen-Lenstra Heuristics	137
8.2	Decomposing Class Groups	141
8.3	Specifying Subgroups of Class Groups	147
8.3.1	Congruence Conditions	147
8.3.2	Exact and Exotic Groups	153
9	The 2-Sylow Subgroup	159
9.1	Classical Results on the Pell Equation	162
9.2	Modern Results	170
9.3	Reciprocity Laws	183
9.4	Special References for Chapter 9	185
10	Factoring with Binary Quadratic Forms	191
10.1	Classical Methods	191
10.2	SQUFOF	197
10.3	CLASNO	202
10.4	SPAR	206
10.4.1	Pollard $p - 1$	206
10.4.2	SPAR	208
10.5	CFRAC	209
10.6	A General Analysis	212
	Bibliography	213
	Appendix 1: Tables, Negative Discriminants	223
	Appendix 2: Tables, Positive Discriminants	235
	Index	245