

---

# Contents

<b>Preface</b> .....	vii
<b>1 Introduction</b> .....	1
1.1 Diophantine Equations .....	1
1.2 The Pell Equation .....	3
1.3 Representation of All Solutions .....	8
1.4 The Lucas Functions .....	13
<b>2 Early History of the Pell Equation</b> .....	19
2.1 The Cattle Problem of Archimedes .....	19
2.2 Further Contributions of the Greeks .....	24
2.3 The Indian Mathematicians .....	31
2.4 Fermat and His Successors .....	36
<b>3 Continued Fractions</b> .....	43
3.1 General Continued Fractions .....	43
3.2 Simple Continued Fractions .....	47
3.3 Simple Continued Fractions of Quadratic Irrationals .....	53
3.4 Some Special Results .....	63
<b>4 Quadratic Number Fields</b> .....	75
4.1 Algebraic Numbers .....	75
4.2 Modules and Orders of $\mathbb{K}$ .....	78
4.3 The Units of $\mathcal{O}$ .....	81
4.4 The Ideals of $\mathcal{O}$ .....	83
4.5 Equivalence and Norms .....	88
4.6 Divisibility and Prime Ideals .....	93
<b>5 Ideals and Continued Fractions</b> .....	97
5.1 Reduced Ideals of $\mathcal{O}$ .....	97
5.2 Reduction Algorithms .....	104

5.3	Reduced Ideals When $\Delta > 0$ .....	109
5.4	Ideal Products and NUCOMP .....	116
<b>6</b>	<b>Some Special Pell Equations</b> .....	125
6.1	Introduction .....	125
6.2	Continued Fractions .....	128
6.3	Schinzel's Families .....	134
6.4	Creepers and Kreepers .....	140
6.5	Yamamoto's Results .....	145
<b>7</b>	<b>The Ideal Class Group</b> .....	153
7.1	Introduction .....	153
7.2	The Cohen-Lenstra Heuristics .....	157
7.2.1	Imaginary Quadratic Fields .....	157
7.2.2	Real Quadratic Fields .....	164
7.3	The 2-Sylow Subgroup .....	169
7.4	Infrastructure .....	172
<b>8</b>	<b>The Analytic Class Number Formula</b> .....	185
8.1	Dirichlet Characters .....	185
8.2	Primitive Characters .....	191
8.3	The $L$ -Function .....	194
8.4	Ideal Density .....	197
8.5	The Class Number Formula .....	202
<b>9</b>	<b>Some Additional Analytic Results</b> .....	209
9.1	More on Gauss Sums .....	209
9.2	A Closed Formula for $h_{\mathbb{K}}$ .....	212
9.3	The Riemann Zeta-Function .....	217
9.4	The Euler Product for $L(1, \chi)$ .....	222
9.5	Bounds on $L(1, \chi)$ .....	226
<b>10</b>	<b>Some Computational Techniques</b> .....	237
10.1	Introduction .....	237
10.2	Computing the Regulator .....	238
10.3	Computing the Class Number .....	245
10.4	Computing the Class Group .....	253
10.5	Numerical Results .....	256
10.5.1	Imaginary Quadratic Fields .....	257
10.5.2	Real Quadratic Fields .....	260
<b>11</b>	<b><math>(f, p)</math> Representations of <math>\mathcal{O}</math>-ideals</b> .....	265
11.1	Basic Concepts and Definitions .....	265
11.2	$w$ -Near Representations .....	270
11.3	Exponentiation of Ideals and Computation of $\mathfrak{a}[x]$ .....	275

<b>12 Compact Representations</b>	285
12.1 Compact Representation of $\theta_j$	285
12.2 Compact Representation of Quadratic Integers	290
12.3 The Arithmetic of Compact Representations	297
<b>13 The Subexponential Method</b>	307
13.1 Introduction	307
13.2 Solving the Discrete Logarithm Problem in $Cl_\Delta$	308
13.3 Computing the Class Number and Class Group	316
13.4 Computing the Regulator	322
13.5 Principality Testing	331
13.6 Complexity	333
13.7 Practical Improvements	337
13.7.1 Improvements to the Random Exponents Method	337
13.7.2 The Large Prime Variation	338
13.7.3 Parallelism	340
13.7.4 Computing Relations Using Sieving	340
13.7.5 Self-initialization	342
13.8 Computational Results	345
13.9 Open Problems and Further Improvements	348
<b>14 Applications to Cryptography</b>	353
14.1 Introduction	353
14.2 The Pell Equation in a Public-Key Cryptosystem	355
14.3 Cryptography in Imaginary Quadratic Fields	360
14.3.1 Cryptographic Protocols	363
14.3.2 Efficiency	363
14.4 Cryptography in Real Quadratic Fields	364
14.4.1 Security	369
14.4.2 Efficiency	373
14.4.3 Other Cryptosystems	374
14.5 Cryptosystems in Non-Maximal Quadratic Orders	374
14.5.1 NICE	376
14.5.2 REAL-NICE	378
14.5.3 Trapdoor Discrete Logarithm Computation	380
<b>15 Unconditional Verification of the Regulator and the Class Number</b>	387
15.1 Introduction	387
15.2 Some Preliminary Results	388
15.3 The Algorithm and Some Implementation Issues	393
15.4 The Class Number	399

<b>16</b>	<b>Principal Ideal Testing in <math>\mathcal{O}</math></b>	405
16.1	Introduction	405
16.2	Another Approach to Problem <b>P</b>	410
16.3	The Equation $X^2 - DY^2 = N$	415
<b>17</b>	<b>Conclusion</b>	423
17.1	A More General Equation	423
17.2	Other Generalizations of the Pell Equation	426
17.3	Some Questions	432
<b>Appendix</b>		439
A.1	NUCOMP	439
A.2	NUMULT	446
A.3	Theoretical Background for WNEAR	449
A.4	WNEAR	454
<b>References</b>		461
<b>Index</b>		489



<http://www.springer.com/978-0-387-84922-5>

Solving the Pell Equation

Jacobson, M.; Williams, H.

2009, XX, 495 p., Hardcover

ISBN: 978-0-387-84922-5