

ALGEBRAIC NUMBER THEORY AND FERMAT'S LAST THEOREM

THIRD EDITION

$$x^n + y^n = z^n$$

Ian Stewart • David Tall

Contents

Preface	xi
Index of Notation	xvii
The Origins of Algebraic Number Theory	1
I Algebraic Methods	7
1 Algebraic Background	9
1.1 Rings and Fields	10
1.2 Factorization of Polynomials	13
1.3 Field Extensions	20
1.4 Symmetric Polynomials	22
1.5 Modules	25
1.6 Free Abelian Groups	26
1.7 Exercises	32
2 Algebraic Numbers	35
2.1 Algebraic Numbers	36
2.2 Conjugates and Discriminants	38
2.3 Algebraic Integers	42
2.4 Integral Bases	45
2.5 Norms and Traces	49
2.6 Rings of Integers	51
2.7 Exercises	57

3	Quadratic and Cyclotomic Fields	61
3.1	Quadratic Fields	61
3.2	Cyclotomic Fields	64
3.3	Exercises	69
4	Factorization into Irreducibles	73
4.1	Historical Background	75
4.2	Trivial Factorizations	76
4.3	Factorization into Irreducibles	79
4.4	Examples of Non-Unique Factorization into Irreducibles . .	82
4.5	Prime Factorization	86
4.6	Euclidean Domains	90
4.7	Euclidean Quadratic Fields	91
4.8	Consequences of Unique Factorization	94
4.9	The Ramanujan-Nagell Theorem	96
4.10	Exercises	99
5	Ideals	101
5.1	Historical Background	102
5.2	Prime Factorization of Ideals	105
5.3	The Norm of an Ideal	114
5.4	Nonunique Factorization in Cyclotomic Fields	122
5.5	Exercises	124
II	Geometric Methods	127
6	Lattices	129
6.1	Lattices	129
6.2	The Quotient Torus	132
6.3	Exercises	136
7	Minkowski's Theorem	139
7.1	Minkowski's Theorem	139
7.2	The Two-Squares Theorem	142
7.3	The Four-Squares Theorem	143
7.4	Exercises	144
8	Geometric Representation of Algebraic Numbers	145
8.1	The Space $\mathbf{L}^{st}$	145
8.2	Exercises	149

9	Class-Group and Class-Number	151
9.1	The Class-Group	152
9.2	An Existence Theorem	153
9.3	Finiteness of the Class-Group	157
9.4	How to Make an Ideal Principal	158
9.5	Unique Factorization of Elements in an Extension Ring . .	162
9.6	Exercises	164
III	Number-Theoretic Applications	167
10	Computational Methods	169
10.1	Factorization of a Rational Prime	169
10.2	Minkowski's Constants	172
10.3	Some Class-Number Calculations	176
10.4	Tables	179
10.5	Exercises	180
11	Kummer's Special Case of Fermat's Last Theorem	183
11.1	Some History	183
11.2	Elementary Considerations	186
11.3	Kummer's Lemma	189
11.4	Kummer's Theorem	193
11.5	Regular Primes	196
11.6	Exercises	198
12	The Path to the Final Breakthrough	201
12.1	The Wolfskehl Prize	201
12.2	Other Directions	203
12.3	Modular Functions and Elliptic Curves	205
12.4	The Taniyama–Shimura–Weil Conjecture	206
12.5	Frey's Elliptic Equation	207
12.6	The Amateur who Became a Model Professional	207
12.7	Technical Hitch	210
12.8	Flash of Inspiration	211
12.9	Exercises	212
13	Elliptic Curves	213
13.1	Review of Conics	214
13.2	Projective Space	215
13.3	Rational Conics and the Pythagorean Equation	220
13.4	Elliptic Curves	222
13.5	The Tangent/Secant Process	225

13.6	Group Structure on an Elliptic Curve	226
13.7	Applications to Diophantine Equations	230
13.8	Exercises	233
14	Elliptic Functions	235
14.1	Trigonometry Meets Diophantus	235
14.2	Elliptic Functions	243
14.3	Legendre and Weierstrass	249
14.4	Modular Functions	250
14.5	The Frey Elliptic Curve	256
14.6	The Taniyama–Shimura–Weil Conjecture	257
14.7	Sketch Proof of Fermat’s Last Theorem	261
14.8	Recent Developments	263
14.9	Exercises	268
IV	Appendices	271
A	Quadratic Residues	273
A.1	Quadratic Equations in $\mathbf{Z}_m$	274
A.2	The Units of $\mathbf{Z}_m$	276
A.3	Quadratic Residues	281
A.4	Exercises	290
B	Dirichlet’s Units Theorem	293
B.1	Introduction	293
B.2	Logarithmic Space	294
B.3	Embedding the Unit Group in Logarithmic Space	295
B.4	Dirichlet’s Theorem	296
B.5	Exercises	301
	Bibliography	303
	Index	309