

Contents

Part I Foundational material

1	Introduction	3
1.1	The Pythagorean Theorem	3
1.2	Pythagorean triples	6
1.3	The questions	8
	Exercises	8
	Notes	10
2	Basic number theory	13
2.1	Natural numbers, mathematical induction, and the Well-ordering Principle	13
2.2	Divisibility and prime factorization	14
2.3	The Chinese Remainder Theorem	22
2.4	Euler's Theorem	24
2.5	Polynomials modulo a prime	30
2.6	Digit expansions	32
2.7	Digit expansions of rational numbers	39
2.8	Primitive roots	41
	Exercises	49
	Notes	53
3	Integral solutions to the Pythagorean Equation	59
3.1	Solutions	59
3.2	Geometric method to find solutions	61
3.3	Geometric method to find solutions: Non-Pythagorean examples	65
3.4	Application: $X^4 + Y^4 = Z^4$	70
	Exercises	72
	Notes	73

4	What integers are areas of right triangles?	81
4.1	Congruent numbers	81
4.2	Small numbers	83
4.3	Connection to cubic equations	84
	Exercises	87
	Notes	88
5	What numbers are the edges of a right triangle?	91
5.1	The theorem	91
5.2	Gaussian integers	93
5.3	The proof of Theorem 5.2	95
5.4	Irreducible elements in $\mathbb{Z}[i]$	98
5.5	Proof of Theorem 5.1	99
	Exercises	101
	Notes	102
6	Primes of the form $4k + 1$	105
6.1	Euclid's theorem on the infinitude of primes	105
6.2	Quadratic residues	107
6.3	An application of the Law of Quadratic Reciprocity	112
	Exercises	113
	Notes	115
7	Gauss Sums, Quadratic Reciprocity, and the Jacobi Symbol	119
7.1	Gauss sums and Quadratic Reciprocity	119
7.2	The Jacobi Symbol	124
	Exercises	129
	Notes	130

Part II Advanced Topics

8	Counting Pythagorean triples modulo an integer	133
8.1	The Pythagorean Equation modulo a prime number p	133
8.2	Solutions modulo n for a natural number n	138
	Exercises	145
	Notes	146
9	How many lattice points are there on a circle or a sphere?	151
9.1	The case of two squares	151
9.2	More than two squares	155
9.3	Integral points on arcs	156
	Exercises	162
	Notes	164

10	What about geometry?	165
10.1	Lattices in $\mathbb{R}^n$	165
10.2	Minkowski's Theorem	168
10.3	Sums of two squares	172
10.4	Sums of four squares	173
10.5	Sums of three squares	176
	Exercises	180
	Notes	182
11	Another proof of the four squares theorem	187
11.1	Quaternions	187
11.2	Matrix representation	189
11.3	Four squares	190
	Exercises	192
	Notes	193
12	Quadratic forms and sums of squares	195
12.1	Quadratic forms with integral coefficients	195
12.2	Binary forms	200
12.3	Ternary forms	203
12.4	Three squares	206
	Exercises	208
	Notes	209
13	How many Pythagorean triples are there?	211
13.1	The asymptotic formula	211
13.2	The computation of C_2	217
	Exercises	220
	Notes	223
14	How are rational points distributed, really?	227
14.1	The real line	227
14.2	The unit circle	240
	Exercises	243
	Notes	245
	Appendix A: Background	247
	Appendix B: Algebraic integers	255
	Appendix C: SageMath	261
	References	271
	Index	277