

# Contents

Preface	ix
Preface to the English Edition	xi
Objectives and Outline of these Books	xiii
Notation	xv
Chapter 0. Introduction	
— Fermat and Number Theory —	1
0.1. Before Fermat	1
0.2. Prime numbers and the sum of two squares	4
0.3. $p = x^2 + 2y^2$ , $p = x^2 + 3y^2, \dots$	6
0.4. Pell's equations	7
0.5. Triangular numbers, quadrangular numbers, pentagonal numbers	8
0.6. Triangular numbers, squares, cubes	10
0.7. Right triangles and elliptic curves	11
0.8. Fermat's Last Theorem	12
Exercises	14
Chapter 1. Rational Points on Elliptic Curves	17
1.1. Fermat and elliptic curves	17
1.2. Group structure of an elliptic curve	25
1.3. Mordell's theorem	30
Summary	43
Exercises	43
Chapter 2. Conics and $p$ -adic Numbers	45
2.1. Conics	45
2.2. Congruence	49
2.3. Conics and quadratic residue symbols	53
2.4. $p$ -adic number fields	58

2.5.	Multiplicative structure of the $p$ -adic number field	69
2.6.	Rational points on conics	74
	Summary	78
	Exercises	78
Chapter 3.	$\zeta$	81
3.1.	Three wonders of the values of the $\zeta$ function	81
3.2.	Values at positive integers	84
3.3.	Values at negative integers	89
	Summary	99
	Exercises	100
Chapter 4.	Algebraic Number Theory	103
4.1.	Method of algebraic number theory	104
4.2.	The heart of algebraic number theory	113
4.3.	The class number formula for imaginary quadratic fields	124
4.4.	Fermat's Last Theorem and Kummer	127
	Summary	132
	Exercises	132
Appendix A.	Rudiments on Dedekind domains	135
A.1.	Definition of a Dedekind domain	135
A.2.	Fractional ideal	136
Answers to Questions		139
Answers to Exercises		145
Index		153