

# Graduate Texts in Mathematics

Henri Cohen

## Number Theory

Volume I:  
Tools and Diophantine  
Equations

# Table of Contents

---

## Volume I

---

<b>Preface</b> .....	v
<b>1. Introduction to Diophantine Equations</b> .....	1
1.1 Introduction .....	1
1.1.1 Examples of Diophantine Problems .....	1
1.1.2 Local Methods .....	4
1.1.3 Dimensions .....	6
1.2 Exercises for Chapter 1 .....	8

---

## Part I. Tools

---

<b>2. Abelian Groups, Lattices, and Finite Fields</b> .....	11
2.1 Finitely Generated Abelian Groups .....	11
2.1.1 Basic Results .....	11
2.1.2 Description of Subgroups .....	16
2.1.3 Characters of Finite Abelian Groups .....	17
2.1.4 The Groups $(\mathbb{Z}/m\mathbb{Z})^*$ .....	20
2.1.5 Dirichlet Characters .....	25
2.1.6 Gauss Sums .....	30
2.2 The Quadratic Reciprocity Law .....	33
2.2.1 The Basic Quadratic Reciprocity Law .....	33
2.2.2 Consequences of the Basic Quadratic Reciprocity Law .....	36
2.2.3 Gauss's Lemma and Quadratic Reciprocity .....	39
2.2.4 Real Primitive Characters .....	43
2.2.5 The Sign of the Quadratic Gauss Sum .....	45
2.3 Lattices and the Geometry of Numbers .....	50
2.3.1 Definitions .....	50
2.3.2 Hermite's Inequality .....	53
2.3.3 LLL-Reduced Bases .....	55
2.3.4 The LLL Algorithms .....	58
2.3.5 Approximation of Linear Forms .....	60
2.3.6 Minkowski's Convex Body Theorem .....	63

2.4	Basic Properties of Finite Fields . . . . .	65
2.4.1	General Properties of Finite Fields . . . . .	65
2.4.2	Galois Theory of Finite Fields . . . . .	69
2.4.3	Polynomials over Finite Fields . . . . .	71
2.5	Bounds for the Number of Solutions in Finite Fields . . . . .	72
2.5.1	The Chevalley–Warning Theorem . . . . .	72
2.5.2	Gauss Sums for Finite Fields . . . . .	73
2.5.3	Jacobi Sums for Finite Fields . . . . .	79
2.5.4	The Jacobi Sums $J(\chi_1, \chi_2)$ . . . . .	82
2.5.5	The Number of Solutions of Diagonal Equations . . . . .	87
2.5.6	The Weil Bounds . . . . .	90
2.5.7	The Weil Conjectures (Deligne’s Theorem) . . . . .	92
2.6	Exercises for Chapter 2 . . . . .	93
<b>3.</b>	<b>Basic Algebraic Number Theory . . . . .</b>	<b>101</b>
3.1	Field-Theoretic Algebraic Number Theory . . . . .	101
3.1.1	Galois Theory . . . . .	101
3.1.2	Number Fields . . . . .	106
3.1.3	Examples . . . . .	108
3.1.4	Characteristic Polynomial, Norm, Trace . . . . .	109
3.1.5	Noether’s Lemma . . . . .	110
3.1.6	The Basic Theorem of Kummer Theory . . . . .	111
3.1.7	Examples of the Use of Kummer Theory . . . . .	114
3.1.8	Artin–Schreier Theory . . . . .	115
3.2	The Normal Basis Theorem . . . . .	117
3.2.1	Linear Independence and Hilbert’s Theorem 90 . . . . .	117
3.2.2	The Normal Basis Theorem in the Cyclic Case . . . . .	119
3.2.3	Additive Polynomials . . . . .	120
3.2.4	Algebraic Independence of Homomorphisms . . . . .	121
3.2.5	The Normal Basis Theorem . . . . .	123
3.3	Ring-Theoretic Algebraic Number Theory . . . . .	124
3.3.1	Gauss’s Lemma on Polynomials . . . . .	124
3.3.2	Algebraic Integers . . . . .	125
3.3.3	Ring of Integers and Discriminant . . . . .	128
3.3.4	Ideals and Units . . . . .	130
3.3.5	Decomposition of Primes and Ramification . . . . .	132
3.3.6	Galois Properties of Prime Decomposition . . . . .	134
3.4	Quadratic Fields . . . . .	136
3.4.1	Field-Theoretic and Basic Ring-Theoretic Properties . . . . .	136
3.4.2	Results and Conjectures on Class and Unit Groups . . . . .	138
3.5	Cyclotomic Fields . . . . .	140
3.5.1	Cyclotomic Polynomials . . . . .	140
3.5.2	Field-Theoretic Properties of $\mathbb{Q}(\zeta_n)$ . . . . .	144
3.5.3	Ring-Theoretic Properties . . . . .	146
3.5.4	The Totally Real Subfield of $\mathbb{Q}(\zeta_{p^k})$ . . . . .	148

3.6	Stickelberger's Theorem . . . . .	150
3.6.1	Introduction and Algebraic Setting . . . . .	150
3.6.2	Instantiation of Gauss Sums . . . . .	151
3.6.3	Prime Ideal Decomposition of Gauss Sums . . . . .	154
3.6.4	The Stickelberger Ideal . . . . .	160
3.6.5	Diagonalization of the Stickelberger Element . . . . .	163
3.6.6	The Eisenstein Reciprocity Law . . . . .	165
3.7	The Hasse–Davenport Relations . . . . .	170
3.7.1	Distribution Formulas . . . . .	171
3.7.2	The Hasse–Davenport Relations . . . . .	173
3.7.3	The Zeta Function of a Diagonal Hypersurface . . . . .	177
3.8	Exercises for Chapter 3 . . . . .	179
<b>4.</b>	<b>p-adic Fields . . . . .</b>	<b>183</b>
4.1	Absolute Values and Completions . . . . .	183
4.1.1	Absolute Values . . . . .	183
4.1.2	Archimedean Absolute Values . . . . .	184
4.1.3	Non-Archimedean and Ultrametric Absolute Values . . . . .	188
4.1.4	Ostrowski's Theorem and the Product Formula . . . . .	190
4.1.5	Completions . . . . .	192
4.1.6	Completions of a Number Field . . . . .	195
4.1.7	Hensel's Lemmas . . . . .	199
4.2	Analytic Functions in p-adic Fields . . . . .	205
4.2.1	Elementary Properties . . . . .	205
4.2.2	Examples of Analytic Functions . . . . .	208
4.2.3	Application of the Artin–Hasse Exponential . . . . .	217
4.2.4	Mahler Expansions . . . . .	220
4.3	Additive and Multiplicative Structures . . . . .	224
4.3.1	Concrete Approach . . . . .	224
4.3.2	Basic Reductions . . . . .	225
4.3.3	Study of the Groups $U_i$ . . . . .	229
4.3.4	Study of the Group $U_1$ . . . . .	231
4.3.5	The Group $K_p^*/K_p^{*2}$ . . . . .	234
4.4	Extensions of p-adic Fields . . . . .	235
4.4.1	Preliminaries on Local Field Norms . . . . .	235
4.4.2	Krasner's Lemma . . . . .	238
4.4.3	General Results on Extensions . . . . .	239
4.4.4	Applications of the Cohomology of Cyclic Groups . . . . .	242
4.4.5	Characterization of Unramified Extensions . . . . .	249
4.4.6	Properties of Unramified Extensions . . . . .	251
4.4.7	Totally Ramified Extensions . . . . .	253
4.4.8	Analytic Representations of $p$ th Roots of Unity . . . . .	254
4.4.9	Factorizations in Number Fields . . . . .	258
4.4.10	Existence of the Field $\mathbb{C}_p$ . . . . .	260
4.4.11	Some Analysis in $\mathbb{C}_p$ . . . . .	263

4.5	The Theorems of Strassmann and Weierstrass . . . . .	266
4.5.1	Strassmann's Theorem . . . . .	266
4.5.2	Krasner Analytic Functions . . . . .	267
4.5.3	The Weierstrass Preparation Theorem . . . . .	270
4.5.4	Applications of Strassmann's Theorem . . . . .	272
4.6	Exercises for Chapter 4 . . . . .	275
<b>5.</b>	<b>Quadratic Forms and Local-Global Principles . . . . .</b>	<b>285</b>
5.1	Basic Results on Quadratic Forms . . . . .	285
5.1.1	Basic Properties of Quadratic Modules . . . . .	286
5.1.2	Contiguous Bases and Witt's Theorem . . . . .	288
5.1.3	Translations into Results on Quadratic Forms . . . . .	291
5.2	Quadratic Forms over Finite and Local Fields . . . . .	294
5.2.1	Quadratic Forms over Finite Fields . . . . .	294
5.2.2	Definition of the Local Hilbert Symbol . . . . .	295
5.2.3	Main Properties of the Local Hilbert Symbol . . . . .	296
5.2.4	Quadratic Forms over $\mathbb{Q}_p$ . . . . .	300
5.3	Quadratic Forms over $\mathbb{Q}$ . . . . .	303
5.3.1	Global Properties of the Hilbert Symbol . . . . .	303
5.3.2	Statement of the Hasse-Minkowski Theorem . . . . .	305
5.3.3	The Hasse-Minkowski Theorem for $n \leq 2$ . . . . .	306
5.3.4	The Hasse-Minkowski Theorem for $n = 3$ . . . . .	307
5.3.5	The Hasse-Minkowski Theorem for $n = 4$ . . . . .	308
5.3.6	The Hasse-Minkowski Theorem for $n \geq 5$ . . . . .	309
5.4	Consequences of the Hasse-Minkowski Theorem . . . . .	310
5.4.1	General Results . . . . .	310
5.4.2	A Result of Davenport and Cassels . . . . .	311
5.4.3	Universal Quadratic Forms . . . . .	312
5.4.4	Sums of Squares . . . . .	314
5.5	The Hasse Norm Principle . . . . .	318
5.6	The Hasse Principle for Powers . . . . .	321
5.6.1	A General Theorem on Powers . . . . .	321
5.6.2	The Hasse Principle for Powers . . . . .	324
5.7	Some Counterexamples to the Hasse Principle . . . . .	326
5.8	Exercises for Chapter 5 . . . . .	329

---

**Part II. Diophantine Equations**

---

<b>6.</b>	<b>Some Diophantine Equations . . . . .</b>	<b>335</b>
6.1	Introduction . . . . .	335
6.1.1	The Use of Finite Fields . . . . .	335
6.1.2	Local Methods . . . . .	337
6.1.3	Global Methods . . . . .	337
6.2	Diophantine Equations of Degree 1 . . . . .	339

6.3	Diophantine Equations of Degree 2 . . . . .	341
6.3.1	The General Homogeneous Equation . . . . .	341
6.3.2	The Homogeneous Ternary Quadratic Equation . . . . .	343
6.3.3	Computing a Particular Solution . . . . .	347
6.3.4	Examples of Homogeneous Ternary Equations . . . . .	352
6.3.5	The Pell–Fermat Equation $x^2 - Dy^2 = N$ . . . . .	354
6.4	Diophantine Equations of Degree 3 . . . . .	357
6.4.1	Introduction . . . . .	358
6.4.2	The Equation $ax^p + by^p + cz^p = 0$ : Local Solubility . . . . .	359
6.4.3	The Equation $ax^p + by^p + cz^p = 0$ : Number Fields . . . . .	362
6.4.4	The Equation $ax^p + by^p + cz^p = 0$ : Hyperelliptic Curves . . . . .	368
6.4.5	The Equation $x^3 + y^3 + cz^3 = 0$ . . . . .	373
6.4.6	Sums of Two or More Cubes . . . . .	376
6.4.7	Skolem’s Equations $x^3 + dy^3 = 1$ . . . . .	385
6.4.8	Special Cases of Skolem’s Equations . . . . .	386
6.4.9	The Equations $y^2 = x^3 \pm 1$ in Rational Numbers . . . . .	387
6.5	The Equations $ax^4 + by^4 + cz^2 = 0$ and $ax^6 + by^3 + cz^2 = 0$ . . . . .	389
6.5.1	The Equation $ax^4 + by^4 + cz^2 = 0$ : Local Solubility . . . . .	389
6.5.2	The Equations $x^4 \pm y^4 = z^2$ and $x^4 + 2y^4 = z^2$ . . . . .	391
6.5.3	The Equation $ax^4 + by^4 + cz^2 = 0$ : Elliptic Curves . . . . .	392
6.5.4	The Equation $ax^4 + by^4 + cz^2 = 0$ : Special Cases . . . . .	393
6.5.5	The Equation $ax^6 + by^3 + cz^2 = 0$ . . . . .	396
6.6	The Fermat Quartics $x^4 + y^4 = cz^4$ . . . . .	397
6.6.1	Local Solubility . . . . .	398
6.6.2	Global Solubility: Factoring over Number Fields . . . . .	400
6.6.3	Global Solubility: Coverings of Elliptic Curves . . . . .	407
6.6.4	Conclusion, and a Small Table . . . . .	409
6.7	The Equation $y^2 = x^n + t$ . . . . .	410
6.7.1	General Results . . . . .	411
6.7.2	The Case $p = 3$ . . . . .	414
6.7.3	The Case $p = 5$ . . . . .	416
6.7.4	Application of the Bilu–Hanrot–Voutier Theorem . . . . .	417
6.7.5	Special Cases with Fixed $t$ . . . . .	418
6.7.6	The Equations $ty^2 + 1 = 4x^p$ and $y^2 + y + 1 = 3x^p$ . . . . .	420
6.8	Linear Recurring Sequences . . . . .	421
6.8.1	Squares in the Fibonacci and Lucas Sequences . . . . .	421
6.8.2	The Square Pyramid Problem . . . . .	424
6.9	Fermat’s “Last Theorem” $x^n + y^n = z^n$ . . . . .	427
6.9.1	Introduction . . . . .	427
6.9.2	General Prime $n$ : The First Case . . . . .	428
6.9.3	Congruence Criteria . . . . .	429
6.9.4	The Criteria of Wendt and Germain . . . . .	430
6.9.5	Kummer’s Criterion: Regular Primes . . . . .	431

6.9.6	The Criteria of Furtwängler and Wieferich	434
6.9.7	General Prime $n$ : The Second Case	435
6.10	An Example of Runge's Method	439
6.11	First Results on Catalan's Equation	442
6.11.1	Introduction	442
6.11.2	The Theorems of Nagell and Ko Chao	444
6.11.3	Some Lemmas on Binomial Series	446
6.11.4	Proof of Cassels's Theorem 6.11.5	447
6.12	Congruent Numbers	450
6.12.1	Reduction to an Elliptic Curve	451
6.12.2	The Use of the Birch and Swinnerton-Dyer Conjecture	452
6.12.3	Tunnell's Theorem	453
6.13	Some Unsolved Diophantine Problems	455
6.14	Exercises for Chapter 6	456
<b>7.</b>	<b>Elliptic Curves</b>	<b>465</b>
7.1	Introduction and Definitions	465
7.1.1	Introduction	465
7.1.2	Weierstrass Equations	465
7.1.3	Degenerate Elliptic Curves	467
7.1.4	The Group Law	470
7.1.5	Isogenies	472
7.2	Transformations into Weierstrass Form	474
7.2.1	Statement of the Problem	474
7.2.2	Transformation of the Intersection of Two Quadrics	475
7.2.3	Transformation of a Hyperelliptic Quartic	476
7.2.4	Transformation of a General Nonsingular Cubic	477
7.2.5	Example: The Diophantine Equation $x^2 + y^4 = 2z^4$	480
7.3	Elliptic Curves over $\mathbb{C}$ , $\mathbb{R}$ , $k(T)$ , $\mathbb{F}_q$ , and $K_{\mathfrak{p}}$	482
7.3.1	Elliptic Curves over $\mathbb{C}$	482
7.3.2	Elliptic Curves over $\mathbb{R}$	484
7.3.3	Elliptic Curves over $k(T)$	486
7.3.4	Elliptic Curves over $\mathbb{F}_q$	494
7.3.5	Constant Elliptic Curves over $R[[T]]$ : Formal Groups	500
7.3.6	Reduction of Elliptic Curves over $K_{\mathfrak{p}}$	505
7.3.7	The $\mathfrak{p}$ -adic Filtration for Elliptic Curves over $K_{\mathfrak{p}}$	507
7.4	Exercises for Chapter 7	512
<b>8.</b>	<b>Diophantine Aspects of Elliptic Curves</b>	<b>517</b>
8.1	Elliptic Curves over $\mathbb{Q}$	517
8.1.1	Introduction	517
8.1.2	Basic Results and Conjectures	518
8.1.3	Computing the Torsion Subgroup	524
8.1.4	Computing the Mordell–Weil Group	528
8.1.5	The Naïve and Canonical Heights	529

8.2	Description of 2-Descent with Rational 2-Torsion . . . . .	532
8.2.1	The Fundamental 2-Isogeny . . . . .	532
8.2.2	Description of the Image of $\phi$ . . . . .	534
8.2.3	The Fundamental 2-Descent Map . . . . .	535
8.2.4	Practical Use of 2-Descent with 2-Isogenies . . . . .	538
8.2.5	Examples of 2-Descent using 2-Isogenies . . . . .	542
8.2.6	An Example of Second Descent . . . . .	546
8.3	Description of General 2-Descent . . . . .	548
8.3.1	The Fundamental 2-Descent Map . . . . .	548
8.3.2	The $T$ -Selmer Group of a Number Field . . . . .	550
8.3.3	Description of the Image of $\alpha$ . . . . .	552
8.3.4	Practical Use of 2-Descent in the General Case . . . . .	554
8.3.5	Examples of General 2-Descent . . . . .	555
8.4	Description of 3-Descent with Rational 3-Torsion Subgroup . . . . .	557
8.4.1	Rational 3-Torsion Subgroups . . . . .	557
8.4.2	The Fundamental 3-Isogeny . . . . .	558
8.4.3	Description of the Image of $\phi$ . . . . .	560
8.4.4	The Fundamental 3-Descent Map . . . . .	563
8.5	The Use of $L(E, s)$ . . . . .	564
8.5.1	Introduction . . . . .	564
8.5.2	The Case of Complex Multiplication . . . . .	565
8.5.3	Numerical Computation of $L^{(r)}(E, 1)$ . . . . .	572
8.5.4	Computation of $\Gamma_r(1, x)$ for Small $x$ . . . . .	575
8.5.5	Computation of $\Gamma_r(1, x)$ for Large $x$ . . . . .	580
8.5.6	The Famous Curve $y^2 + y = x^3 - 7x + 6$ . . . . .	582
8.6	The Heegner Point Method . . . . .	584
8.6.1	Introduction and the Modular Parametrization . . . . .	584
8.6.2	Heegner Points and Complex Multiplication . . . . .	586
8.6.3	The Use of the Theorem of Gross-Zagier . . . . .	589
8.6.4	Practical Use of the Heegner Point Method . . . . .	591
8.6.5	Improvements to the Basic Algorithm, in Brief . . . . .	596
8.6.6	A Complete Example . . . . .	598
8.7	Computation of Integral Points . . . . .	600
8.7.1	Introduction . . . . .	600
8.7.2	An Upper Bound for the Elliptic Logarithm on $E(\mathbb{Z})$ . . . . .	601
8.7.3	Lower Bounds for Linear Forms in Elliptic Logarithms . . . . .	603
8.7.4	A Complete Example . . . . .	605
8.8	Exercises for Chapter 8 . . . . .	607
	<b>Bibliography</b> . . . . .	615
	<b>Index of Notation</b> . . . . .	625
	<b>Index of Names</b> . . . . .	633
	<b>General Index</b> . . . . .	639



# Graduate Texts in Mathematics

Henri Cohen

## Number Theory

Volume II:  
Analytic and Modern  
Tools

---

**Volume II**


---

<b>Preface</b> .....	v
----------------------	---

---

**Part III. Analytic Tools**


---

<b>9. Bernoulli Polynomials and the Gamma Function</b> .....	3
9.1 Bernoulli Numbers and Polynomials .....	3
9.1.1 Generating Functions for Bernoulli Polynomials .....	3
9.1.2 Further Recurrences for Bernoulli Polynomials .....	10
9.1.3 Computing a Single Bernoulli Number .....	14
9.1.4 Bernoulli Polynomials and Fourier Series .....	16
9.2 Analytic Applications of Bernoulli Polynomials .....	19
9.2.1 Asymptotic Expansions .....	19
9.2.2 The Euler–MacLaurin Summation Formula .....	21
9.2.3 The Remainder Term and the Constant Term .....	25
9.2.4 Euler–MacLaurin and the Laplace Transform .....	27
9.2.5 Basic Applications of the Euler–MacLaurin Formula ..	31
9.3 Applications to Numerical Integration .....	35
9.3.1 Standard Euler–MacLaurin Numerical Integration ....	36
9.3.2 The Basic Tanh–Sinh Numerical Integration Method ..	37
9.3.3 General Doubly Exponential Numerical Integration ...	39
9.4 $\chi$ -Bernoulli Numbers, Polynomials, and Functions .....	43
9.4.1 $\chi$ -Bernoulli Numbers and Polynomials .....	43
9.4.2 $\chi$ -Bernoulli Functions .....	46
9.4.3 The $\chi$ -Euler–MacLaurin Summation Formula .....	50
9.5 Arithmetic Properties of Bernoulli Numbers .....	52
9.5.1 $\chi$ -Power Sums .....	52
9.5.2 The Generalized Clausen–von Staudt Congruence ....	61
9.5.3 The Voronoi Congruence .....	64
9.5.4 The Kummer Congruences .....	67
9.5.5 The Almkvist–Meurman Theorem .....	70
9.6 The Real and Complex Gamma Functions .....	71
9.6.1 The Hurwitz Zeta Function .....	71
9.6.2 Definition of the Gamma Function .....	77
9.6.3 Preliminary Results for the Study of $\Gamma(s)$ .....	81
9.6.4 Properties of the Gamma Function .....	84
9.6.5 Specific Properties of the Function $\psi(s)$ .....	95
9.6.6 Fourier Expansions of $\zeta(s, x)$ and $\log(\Gamma(x))$ .....	100
9.7 Integral Transforms .....	103
9.7.1 Generalities on Integral Transforms .....	104
9.7.2 The Fourier Transform .....	104
9.7.3 The Mellin Transform .....	107

9.7.4	The Laplace Transform .....	108
9.8	Bessel Functions .....	109
9.8.1	Definitions .....	109
9.8.2	Integral Representations and Applications .....	113
9.9	Exercises for Chapter 9 .....	118
<b>10.</b>	<b>Dirichlet Series and <math>L</math>-Functions</b> .....	<b>151</b>
10.1	Arithmetic Functions and Dirichlet Series .....	151
10.1.1	Operations on Arithmetic Functions .....	152
10.1.2	Multiplicative Functions .....	154
10.1.3	Some Classical Arithmetical Functions .....	155
10.1.4	Numerical Dirichlet Series .....	160
10.2	The Analytic Theory of $L$ -Series .....	162
10.2.1	Simple Approaches to Analytic Continuation .....	163
10.2.2	The Use of the Hurwitz Zeta Function $\zeta(s, x)$ .....	168
10.2.3	The Functional Equation for the Theta Function .....	169
10.2.4	The Functional Equation for Dirichlet $L$ -Functions .....	172
10.2.5	Generalized Poisson Summation Formulas .....	177
10.2.6	Voronoi's Error Term in the Circle Problem .....	182
10.3	Special Values of Dirichlet $L$ -Functions .....	186
10.3.1	Basic Results on Special Values .....	186
10.3.2	Special Values of $L$ -Functions and Modular Forms .....	193
10.3.3	The Pólya-Vinogradov Inequality .....	198
10.3.4	Bounds and Averages for $L(\chi, 1)$ .....	200
10.3.5	Expansions of $\zeta(s)$ Around $s = k \in \mathbb{Z}_{\leq 1}$ .....	205
10.3.6	Numerical Computation of Euler Products and Sums .....	208
10.4	Epstein Zeta Functions .....	210
10.4.1	The Nonholomorphic Eisenstein Series $G(\tau, s)$ .....	211
10.4.2	The Kronecker Limit Formula .....	213
10.5	Dirichlet Series Linked to Number Fields .....	216
10.5.1	The Dedekind Zeta Function $\zeta_K(s)$ .....	216
10.5.2	The Dedekind Zeta Function of Quadratic Fields .....	219
10.5.3	Applications of the Kronecker Limit Formula .....	223
10.5.4	The Dedekind Zeta Function of Cyclotomic Fields .....	230
10.5.5	The Nonvanishing of $L(\chi, 1)$ .....	235
10.5.6	Application to Primes in Arithmetic Progression .....	237
10.5.7	Conjectures on Dirichlet $L$ -Functions .....	238
10.6	Science Fiction on $L$ -Functions .....	239
10.6.1	Local $L$ -Functions .....	239
10.6.2	Global $L$ -Functions .....	241
10.7	The Prime Number Theorem .....	245
10.7.1	Estimates for $\zeta(s)$ .....	246
10.7.2	Newman's Proof .....	250
10.7.3	Iwaniec's Proof .....	254
10.8	Exercises for Chapter 10 .....	258

<b>11. <math>p</math>-adic Gamma and <math>L</math>-Functions</b> . . . . .	275
11.1 Generalities on $p$ -adic Functions . . . . .	275
11.1.1 Methods for Constructing $p$ -adic Functions . . . . .	275
11.1.2 A Brief Study of Volkenborn Integrals . . . . .	276
11.2 The $p$ -adic Hurwitz Zeta Functions . . . . .	280
11.2.1 Teichmüller Extensions and Characters on $\mathbb{Z}_p$ . . . . .	280
11.2.2 The $p$ -adic Hurwitz Zeta Function for $x \in \mathbb{C}\mathbb{Z}_p$ . . . . .	281
11.2.3 The Function $\zeta_p(s, x)$ Around $s = 1$ . . . . .	288
11.2.4 The $p$ -adic Hurwitz Zeta Function for $x \in \mathbb{Z}_p$ . . . . .	290
11.3 $p$ -adic $L$ -Functions . . . . .	300
11.3.1 Dirichlet Characters in the $p$ -adic Context . . . . .	300
11.3.2 Definition and Basic Properties of $p$ -adic $L$ -Functions . . . . .	301
11.3.3 $p$ -adic $L$ -Functions at Positive Integers . . . . .	305
11.3.4 $\chi$ -Power Sums Involving $p$ -adic Logarithms . . . . .	310
11.3.5 The Function $L_p(\chi, s)$ Around $s = 1$ . . . . .	317
11.4 Applications of $p$ -adic $L$ -Functions . . . . .	319
11.4.1 Integrality and Parity of $L$ -Function Values . . . . .	319
11.4.2 Bernoulli Numbers and Regular Primes . . . . .	324
11.4.3 Strengthening of the Almkvist–Meurman Theorem . . . . .	326
11.5 $p$ -adic Log Gamma Functions . . . . .	329
11.5.1 Diamond’s $p$ -adic Log Gamma Function . . . . .	330
11.5.2 Morita’s $p$ -adic Log Gamma Function . . . . .	336
11.5.3 Computation of some $p$ -adic Logarithms . . . . .	346
11.5.4 Computation of Limits of some Logarithmic Sums . . . . .	356
11.5.5 Explicit Formulas for $\psi_p(r/m)$ and $\psi_p(\chi, r/m)$ . . . . .	359
11.5.6 Application to the Value of $L_p(\chi, 1)$ . . . . .	361
11.6 Morita’s $p$ -adic Gamma Function . . . . .	364
11.6.1 Introduction . . . . .	364
11.6.2 Definitions and Basic Results . . . . .	365
11.6.3 Main Properties of the $p$ -adic Gamma Function . . . . .	369
11.6.4 Mahler–Dwork Expansions Linked to $\Gamma_p(x)$ . . . . .	375
11.6.5 Power Series Expansions Linked to $\Gamma_p(x)$ . . . . .	378
11.6.6 The Jacobstahl–Kazandzidis Congruence . . . . .	380
11.7 The Gross–Koblitz Formula and Applications . . . . .	383
11.7.1 Statement and Proof of the Gross–Koblitz Formula . . . . .	383
11.7.2 Application to $L'_p(\chi, 0)$ . . . . .	389
11.7.3 Application to the Stickelberger Congruence . . . . .	390
11.7.4 Application to the Hasse–Davenport Product Relation . . . . .	392
11.8 Exercises for Chapter 11 . . . . .	395

---

**Part IV. Modern Tools**


---

<b>12. Applications of Linear Forms in Logarithms</b> . . . . .	411
12.1 Introduction . . . . .	411
12.1.1 Lower Bounds . . . . .	411
12.1.2 Applications to Diophantine Equations and Problems . . . . .	413
12.1.3 A List of Applications . . . . .	414
12.2 A Lower Bound for $ 2^m - 3^n $ . . . . .	415
12.3 Lower Bounds for the Trace of $\alpha^n$ . . . . .	418
12.4 Pure Powers in Binary Recurrent Sequences . . . . .	420
12.5 Greatest Prime Factors of Terms of Some Recurrent Sequences . . . . .	421
12.6 Greatest Prime Factors of Values of Integer Polynomials . . . . .	422
12.7 The Diophantine Equation $ax^n - by^n = c$ . . . . .	423
12.8 Simultaneous Pell Equations . . . . .	424
12.8.1 General Strategy . . . . .	424
12.8.2 An Example in Detail . . . . .	425
12.8.3 A General Algorithm . . . . .	426
12.9 Catalan's Equation . . . . .	428
12.10 Thue Equations . . . . .	430
12.10.1 The Main Theorem . . . . .	430
12.10.2 Algorithmic Aspects . . . . .	432
12.11 Other Classical Diophantine Equations . . . . .	436
12.12 A Few Words on the Non-Archimedean Case . . . . .	439
<b>13. Rational Points on Higher-Genus Curves</b> . . . . .	441
13.1 Introduction . . . . .	441
13.2 The Jacobian . . . . .	442
13.2.1 Functions on Curves . . . . .	443
13.2.2 Divisors . . . . .	444
13.2.3 Rational Divisors . . . . .	445
13.2.4 The Group Law: Cantor's Algorithm . . . . .	446
13.2.5 The Group Law: The Geometric Point of View . . . . .	448
13.3 Rational Points on Hyperelliptic Curves . . . . .	449
13.3.1 The Method of Dem'yanenko–Manin . . . . .	449
13.3.2 The Method of Chabauty–Coleman . . . . .	452
13.3.3 Explicit Chabauty According to Flynn . . . . .	453
13.3.4 When Chabauty Fails . . . . .	455
13.3.5 Elliptic Curve Chabauty . . . . .	456
13.3.6 A Complete Example . . . . .	459

<b>14. The Super-Fermat Equation</b> .....	463
14.1 Preliminary Reductions .....	463
14.2 The Dihedral Cases $(2, 2, r)$ .....	465
14.2.1 The Equation $x^2 - y^2 = z^r$ .....	465
14.2.2 The Equation $x^2 + y^2 = z^r$ .....	466
14.2.3 The Equations $x^2 + 3y^2 = z^3$ and $x^2 + 3y^2 = 4z^3$ .....	466
14.3 The Tetrahedral Case $(2, 3, 3)$ .....	467
14.3.1 The Equation $x^3 + y^3 = z^2$ .....	467
14.3.2 The Equation $x^3 + y^3 = 2z^2$ .....	470
14.3.3 The Equation $x^3 - 2y^3 = z^2$ .....	472
14.4 The Octahedral Case $(2, 3, 4)$ .....	473
14.4.1 The Equation $x^2 - y^4 = z^3$ .....	473
14.4.2 The Equation $x^2 + y^4 = z^3$ .....	475
14.5 Invariants, Covariants, and Dessins d'Enfants .....	477
14.5.1 Dessins d'Enfants, Klein Forms, and Covariants .....	478
14.5.2 The Icosahedral Case $(2, 3, 5)$ .....	479
14.6 The Parabolic and Hyperbolic Cases .....	481
14.6.1 The Parabolic Case .....	481
14.6.2 General Results in the Hyperbolic Case .....	482
14.6.3 The Equations $x^4 \pm y^4 = z^3$ .....	484
14.6.4 The Equation $x^4 + y^4 = z^5$ .....	485
14.6.5 The Equation $x^6 - y^4 = z^2$ .....	486
14.6.6 The Equation $x^4 - y^6 = z^2$ .....	487
14.6.7 The Equation $x^6 + y^4 = z^2$ .....	488
14.6.8 Further Results .....	489
14.7 Applications of Mason's Theorem .....	490
14.7.1 Mason's Theorem .....	491
14.7.2 Applications .....	492
14.8 Exercises for Chapter 14 .....	493
<b>15. The Modular Approach to Diophantine Equations</b> .....	495
15.1 Newforms .....	495
15.1.1 Introduction and Necessary Software Tools .....	495
15.1.2 Newforms .....	496
15.1.3 Rational Newforms and Elliptic Curves .....	497
15.2 Ribet's Level-Lowering Theorem .....	498
15.2.1 Definition of "Arises From" .....	498
15.2.2 Ribet's Level-Lowering Theorem .....	499
15.2.3 Absence of Isogenies .....	501
15.2.4 How to use Ribet's Theorem .....	503
15.3 Fermat's Last Theorem and Similar Equations .....	503
15.3.1 A Generalization of FLT .....	504
15.3.2 $E$ Arises from a Curve with Complex Multiplication ..	505
15.3.3 End of the Proof of Theorem 15.3.1 .....	506
15.3.4 The Equation $x^2 = y^p + 2^r z^p$ for $p \geq 7$ and $r \geq 2$ .....	507

15.3.5	The Equation $x^2 = y^p + z^p$ for $p \geq 7$ . . . . .	509
15.4	An Occasional Bound for the Exponent . . . . .	509
15.5	An Example of Serre–Mazur–Kraus . . . . .	511
15.6	The Method of Kraus . . . . .	514
15.7	“Predicting Exponents of Constants” . . . . .	517
15.7.1	The Diophantine Equation $x^2 - 2 = y^p$ . . . . .	517
15.7.2	Application to the SMK Equation . . . . .	521
15.8	Recipes for Some Ternary Diophantine Equations . . . . .	522
15.8.1	Recipes for Signature $(p, p, p)$ . . . . .	523
15.8.2	Recipes for Signature $(p, p, 2)$ . . . . .	524
15.8.3	Recipes for Signature $(p, p, 3)$ . . . . .	526
<b>16.</b>	<b>Catalan’s Equation</b> . . . . .	<b>529</b>
16.1	Mihăilescu’s First Two Theorems . . . . .	529
16.1.1	The First Theorem: Double Wieferich Pairs . . . . .	530
16.1.2	The Equation $(x^p - 1)/(x - 1) = py^q$ . . . . .	532
16.1.3	Mihăilescu’s Second Theorem: $p \mid h_q^-$ and $q \mid h_p^-$ . . . . .	536
16.2	The + and – Subspaces and the Group $S$ . . . . .	537
16.2.1	The + and – Subspaces . . . . .	538
16.2.2	The Group $S$ . . . . .	540
16.3	Mihăilescu’s Third Theorem: $p < 4q^2$ and $q < 4p^2$ . . . . .	542
16.4	Mihăilescu’s Fourth Theorem: $p \equiv 1 \pmod{q}$ or $q \equiv 1 \pmod{p}$ . . . . .	547
16.4.1	Preliminaries on Commutative Algebra . . . . .	547
16.4.2	Preliminaries on the Plus Part . . . . .	549
16.4.3	Cyclotomic Units and Thaine’s Theorem . . . . .	552
16.4.4	Preliminaries on Power Series . . . . .	554
16.4.5	Proof of Mihăilescu’s Fourth Theorem . . . . .	557
16.4.6	Conclusion: Proof of Catalan’s Conjecture . . . . .	560
	<b>Bibliography</b> . . . . .	<b>561</b>
	<b>Index of Notation</b> . . . . .	<b>571</b>
	<b>Index of Names</b> . . . . .	<b>579</b>
	<b>General Index</b> . . . . .	<b>585</b>