

Number Theory

I: Tools and Diophantine Equations

II: Analytic and Modern Methods

by

Henri COHEN

Version of October 28, 2006

This manuscript was typed using $\mathcal{A}\mathcal{M}\mathcal{S}$ - $\mathcal{L}\mathcal{A}\mathcal{T}\mathcal{E}\mathcal{X}$ and the Springer-Verlag `clmono01` macro package.

Preface

This book deals with several aspects of what is now called “explicit number theory,” not including the essential algorithmic aspects, which are for the most part covered by two other books of the author [Coh0] and [Coh1]. The central (although not unique) theme is the solution of Diophantine equations, i.e., equations or systems of polynomial equations that must be solved in integers, rational numbers, or more generally in algebraic numbers. This theme is in particular the central motivation for the modern theory of arithmetic algebraic geometry. We will consider it through three of its most basic aspects.

The first is the *local* aspect: the invention of p -adic numbers and their generalizations by K. Hensel was a major breakthrough, enabling in particular the simultaneous treatment of congruences modulo prime powers. But more importantly, one can do *analysis* in p -adic fields, and this goes much further than the simple definition of p -adic numbers. The local study of equations is usually not very difficult. We start by looking at solutions in *finite fields*, where important theorems such as the Weil bounds and Deligne’s theorem on the Weil conjectures come into play. We then *lift* these solutions to local solutions using *Hensel lifting*.

The second aspect is the *global* aspect: the use of number fields, and in particular of class groups and unit groups. Although local considerations can give a considerable amount of information on Diophantine problems, the “local to global” principles are unfortunately rather rare, and we will see many examples of failure. Concerning the global aspect, we will first require as a prerequisite of the reader that he or she is familiar with the standard basic theory of number fields, up to and including the finiteness of the class group and Dirichlet’s structure theorem for the unit group. This can be found in many textbooks such as [Sam] and [Marc]. Second, and this is less standard, we will always assume that we have at our disposal a computer algebra system (CAS) that is able to compute rings of integers, class and unit groups, generators of principal ideals, and related questions. Such CAS are now very common, for instance *Kash*, *magma*, and *Pari/GP*, to cite the most useful in algebraic number theory.

The third aspect is the theory of zeta and L -functions. This can be considered as a *unifying theme*¹ for the whole subject, and embodies in a beautiful way the local and global aspects of Diophantine problems. Indeed, these functions are defined through the local aspects of the problems, but their analytic behavior is intimately linked to the global aspects. A first example is given by the Dedekind zeta function of a number field, which is defined only through the splitting behavior of the primes, but whose leading term at $s = 0$ contains at the same time explicit information on the unit rank, the class number, the

¹ expression due to Don Zagier

regulator, and the number of roots of unity of the number field. A second very important example, which is one of the most beautiful and important conjectures in the whole of number theory (and perhaps of the whole of mathematics), the Birch and Swinnerton-Dyer conjecture, says that the behavior at $s = 1$ of the L -function of an elliptic curve defined over \mathbb{Q} contains at the same time explicit information on the rank of the group of rational points on the curve, on the regulator, and on the order of the torsion group of the group of rational points, in complete analogy with the case of the Dedekind zeta function. In addition to the purely *analytical* problems, the theory of L -functions contains beautiful results (and conjectures) on *special values*, of which Euler's formula $\sum_{n \geq 1} 1/n^2 = \pi^2/6$ is a special case.

This book can be considered as having four main parts. A first part gives the tools necessary for Diophantine problems: equations over finite fields, number fields, and finally local fields such as \mathfrak{p} -adic fields (Chapters 1, 2, 3, 4, and part of Chapter 5). The emphasis will be mainly on the theory of \mathfrak{p} -adic fields (Chapter 4), since the reader has probably less familiarity with these. Note that we will consider function fields only in Chapter 7, as a tool for proving Hasse's theorem on elliptic curves. An important tool that we will introduce at the end of Chapter 3 is the theory of the Stickelberger ideal over cyclotomic fields, together with the important applications to the Eisenstein reciprocity law, and the Davenport–Hasse relations. Through Eisenstein reciprocity this theory will enable us to prove Wieferich's criterion for the first case of Fermat's last theorem (FLT), and it will also be an essential tool in the proof of Catalan's conjecture given in Chapter 16.

A second part is the study of certain basic Diophantine equations or systems of equations (Chapters 5, 6, 7, and 8). It should be stressed that even though a number of general techniques are available, each Diophantine equation poses a new problem, and it is difficult to know in advance whether it will be easy to solve. Even without mentioning *families* of Diophantine equations such as FLT, the congruent number problem, or Catalan's equation, all of which will be stated below, proving for instance that a specific equation such as $x^3 + y^5 = z^7$ with x, y coprime integers has no solution with $xyz \neq 0$ seems presently out of reach, although it has been proved (based on a deep theorem of Faltings) that there are only finitely many solutions; see [Dar-Gra] and Chapter 14. Note also that it has been shown by Yu. Matiyasevich (after a considerable amount of work by other authors) in answer to Hilbert's tenth problem that there cannot exist a general algorithm for solving Diophantine equations.

The third part (Chapters 9, 10, and 11) deals with the detailed study of analytic objects linked to algebraic number theory: Bernoulli polynomials and numbers, the gamma function, and zeta and L -functions of Dirichlet characters, which are the simplest types of L -functions. In Chapter 11 we also study p -adic analogues of the gamma, zeta, and L -functions, which have come to play an important role in number theory, and in particular the Gross–

Koblitz formula for Morita’s p -adic gamma function. In particular we will see that this formula leads to remarkably simple proofs of Stickelberger’s congruence and the Hasse–Davenport product relation. More general L -functions such as Hecke L -functions for Grössencharacters, Artin L -functions for Galois representations, or L -functions attached to modular forms, elliptic curves, or higher-dimensional objects are mentioned in several places, but a systematic exposition of their properties would be beyond the scope of this book.

Much more sophisticated techniques have been brought to bear on the subject of Diophantine equations, and it is impossible to be exhaustive. Because the author is not an expert in most of these techniques they are not studied in the first three parts of the book. However considering their importance, I have asked a number of much more knowledgeable people to write a few chapters on these techniques, and I have written two myself, and this forms the fourth and last part of the book (Chapters 12 to 16). These chapters have a different flavor from the rest of the book: they are in general not self-contained, are of a higher mathematical sophistication than the rest, and usually have no exercises. Chapter 12, written by Yann Bugeaud, Guillaume Hanrot, and Maurice Mignotte, deals with the applications of Baker’s explicit results on linear forms in logarithms of algebraic numbers, which permit the solution of a large class of Diophantine equations such as Thue equations and norm form equations, and includes some recent spectacular successes. Paradoxically, the similar problems on elliptic curves are considerably less technical, and are studied in detail in Section 8.7. Chapter 13, written by Sylvain Duquesne, deals with the search for rational points on curves of genus greater than or equal to 2, restricting for simplicity to the case of hyperelliptic curves of genus 2 (the case of genus 0, in other words of quadratic forms, is treated in Chapters 5 and 6, and the case of genus 1, essentially of elliptic curves, is treated in Chapters 7 and 8). Chapter 14, written by the author, deals with the so-called super-Fermat equation $x^p + y^q = z^r$, on which several methods have been used, including ordinary algebraic number theory, classical invariant theory, rational points on higher genus curves, and Ribet–Wiles type methods. The only proofs that are included are those coming from algebraic number theory. Chapter 15, written by Samir Siksek, deals with the use of Galois representations, and in particular of Ribet’s level-lowering theorem and Wiles’s and Taylor–Wiles’s theorem proving the modularity conjecture. The main application is to equations of “abc” type, in other words, equations of the form $a + b + c = 0$ with a , b , and c highly composite, the “easiest” application of this method being the proof of FLT. The author of this chapter has tried to hide all the sophisticated mathematics and to present the method as a black box that can be used without completely understanding the underlying theory. Finally Chapter 16, also written by the author, gives the complete proof of Catalan’s conjecture by P. Mihăilescu. It is entirely based on notes of Yu. Bilu, R. Schoof, and especially of J. Boéchat and M. Mischler, and the only reason that it is not self-contained is that it will be necessary to assume

the validity of an important theorem of F. Thaine on the annihilator of the plus part of the class group of cyclotomic fields.

Warnings

Since several mathematical conventions and notation are not the same from one mathematical culture to the next, I have decided to use systematically unambiguous terminology, and when the notation clash, the French notation. Here are the most important:

- We will systematically say that a is strictly greater than b , or greater than or equal to b (or b is strictly less than a , or less than or equal to a), although the English terminology a is greater than b means in fact one of the two (I don't remember which one, and that is one of the main reasons I refuse to use it) and the French terminology means the other. Similarly, positive and negative are ambiguous (does it include the number 0)? Even though the expression “ x is nonnegative” is slightly ambiguous, it is useful, and I *will* allow myself to use it, with the meaning $x \geq 0$.
- Although we will almost never deal with noncommutative fields (which is a contradiction in terms since in principle the word field implies commutativity), we will usually not use the word field alone. Either we will write explicitly commutative (or noncommutative) field, or we will deal with specific classes of fields, such as finite fields, \mathfrak{p} -adic fields, local fields, number fields, etc. . . . , for which commutativity is clear. Note that the “proper” way in English-language texts to talk about noncommutative fields is to call them either skew fields or division algebras. In any case this will not be an issue since the only appearances of skew fields will be in Chapter 2, where we will prove that finite skew fields are commutative, and in Chapter 7 about endomorphism rings of elliptic curves over finite fields.
- The GCD (resp., the LCM) of two integers can be denoted by (a, b) (resp., by $[a, b]$), but to avoid ambiguities, I will systematically use the explicit notation $\gcd(a, b)$ (resp., $\text{lcm}(a, b)$), and similarly when more than two integers are involved.
- An open interval with endpoints a and b is denoted by (a, b) in the English literature, and by $]a, b[$ in the French literature. I will use the French notation, and similarly for half-open intervals $(a, b]$ and $[a, b)$, which I will denote by $]a, b]$ and $[a, b[$. Although it is impossible to change such a well-entrenched notation, I urge my English-speaking readers to realize the dreadful ambiguity of the notation (a, b) , which can either mean the ordered pair (a, b) , the GCD of a and b , or the open interval.
- The trigonometric functions $\sec(x)$ and $\csc(x)$ do not exist in France, so I will not use them. The functions $\tan(x)$, $\cotan(x)$, $\cosh(x)$, $\sinh(x)$, $\tanh(x)$, and $\cotanh(x)$ are denoted respectively $\text{tg}(x)$, $\text{cotg}(x)$, $\text{ch}(x)$,

$\operatorname{sh}(x)$, $\operatorname{th}(x)$, and $\operatorname{coth}(x)$ in France, but for once to bow to the majority I will use the English names.

- $\Re(s)$ and $\Im(s)$ denote the real and imaginary part of the complex number, the notation coming from the standard \TeX macros.

Notation

In addition to the standard notation of number theory we will use the following notation.

- We will often use the practical self-explanatory notation $\mathbb{Z}_{>0}$, $\mathbb{Z}_{\geq 0}$, $\mathbb{Z}_{<0}$, $\mathbb{Z}_{\leq 0}$, and generalizations thereof, which avoid using long wordage. On the other hand I prefer not to use the notation \mathbb{N} (for $\mathbb{Z}_{\geq 0}$, or is it $\mathbb{Z}_{>0}$?).
- If a and b are nonzero integers, we write $\gcd(a, b^\infty)$ for the limit of the ultimately constant sequence $\gcd(a, b^n)$ as $n \rightarrow \infty$. We have of course $\gcd(a, b^\infty) = \prod_{p|\gcd(a,b)} p^{v_p(a)}$, and $a/\gcd(a, b^\infty)$ is the largest divisor of a coprime to b .
- If n is a nonzero integer and $d \mid n$, we write $d \parallel n$ if $\gcd(d, n/d) = 1$. Note that this is *not* the same thing as the condition $d^2 \nmid n$, except if d is prime.
- If $x \in \mathbb{R}$, we denote by $\lfloor x \rfloor$ the largest integer less than or equal to x (the *floor* of x), by $\lceil x \rceil$ the smallest integer greater than or equal to x (the *ceiling* of x , which is equal to $\lfloor x \rfloor + 1$ if and only if $x \notin \mathbb{Z}$), and by $\{x\}$ the nearest integer to x (or one of the two if $x \in 1/2 + \mathbb{Z}$), so that $\lfloor x \rfloor = \lfloor x + 1/2 \rfloor$.
- For any α belonging to a field K of characteristic zero and any $k \in \mathbb{Z}_{\geq 0}$ we set

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!}.$$

In particular if $\alpha \in \mathbb{Z}_{\geq 0}$ we have $\binom{\alpha}{k} = 0$ if $k > \alpha$, and in this case we will set $\binom{\alpha}{k} = 0$ also when $k < 0$. On the other hand $\binom{\alpha}{k}$ is *undetermined* for $k < 0$ if $\alpha \notin \mathbb{Z}_{\geq 0}$.

- Capital italic letters such as K and L will usually denote number fields.
- Capital calligraphic letters such as \mathcal{K} and \mathcal{L} will denote general \mathfrak{p} -adic fields (for specific ones, we write for instance $K_{\mathfrak{p}}$).
- The capital letter \mathbb{Z} indexed by a capital italic or calligraphic letter such as \mathbb{Z}_K , \mathbb{Z}_L , $\mathbb{Z}_{\mathcal{K}}$, etc... will always denote the ring of integers of the corresponding field.
- Capital italic letters such as A , B , C , G , H , S , T , U , V , W , or lowercase italic letters such as f , g , h will usually denote polynomials or formal power series with coefficients in some base ring or field. The coefficient of degree m of these polynomials or power series will be denoted by the corresponding letter indexed by m , such as A_m , B_m , etc... Thus we will always write (for

instance) $A(X) = A_d X^d + A_{d-1} X^{d-1} + \cdots + A_0$, so that the i th elementary symmetric function of the roots is equal to $(-1)^i A_{d-i}/A_d$.

Acknowledgments

A large part of the material on local fields has been taken with little change from the remarkable book by Cassels [Cas1], and also from unpublished notes of Jaulent written in 1994. For p -adic analysis, I have also liberally borrowed from work of Robert, in particular his superb GTM volume [Rob1]. For part of the material on elliptic curves I have borrowed from another excellent book by Cassels [Cas2], as well as the treatises of Cremona and Silverman [Cre2], [Sil1], [Sil2], and the introductory book by Silverman–Tate [Sil-Tat]. I have also borrowed from the classical books by Borevich–Shafarevich [Bor-Sha], Serre [Ser1], Ireland–Rosen [Ire-Ros], and Washington [Was]. I would like to thank my former students K. Belabas, C. Delaunay, S. Duquesne, and D. Simon, who have helped me to write specific sections, and my colleagues J.-F. Jaulent and J. Martinet for answering many questions in algebraic number theory. I would also like to thank M. Bennett, J. Cremona, A. Kraus, and F. Rodriguez-Villegas for valuable comments on parts of this book. I want especially like to thank D. Bernardi for his thorough rereading of the first ten chapters of the manuscript, which enabled me to remove a large number of errors, mathematical or otherwise.

It is unavoidable that there still remain errors, typographical or otherwise, and the author would like to hear about them. Please send e-mail to

`Henri.Cohen@math.u-bordeaux1.fr`

Lists of known errors for the author’s books including the present one can be obtained on the author’s home page at the URL

`http://www.math.u-bordeaux1.fr/~cohen/`

Table of Contents

Preface	iii
1. Introduction to Diophantine Equations	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
<hr/>	
Part I. Tools	
<hr/>	
2. Abelian Groups, Lattices, and Finite Fields	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	40
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	56
2.3.4 The LLL Algorithms	59
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	74
2.5.3	Jacobi Sums for Finite Fields	79
2.5.4	The Jacobi Sums $J(\chi_1, \chi_2)$	83
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
3.	Basic Algebraic Number Theory	101
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 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	171
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
4.	p-adic Fields	185
4.1	Absolute Values and Completions	185
4.1.1	Absolute Values	185
4.1.2	Archimedean Absolute Values	186
4.1.3	Non-Archimedean and Ultrametric Absolute Values	190
4.1.4	Ostrowski’s Theorem and the Product Formula	192
4.1.5	Completions	194
4.1.6	Completions of a Number Field	197
4.1.7	Hensel’s Lemmas	201
4.2	Analytic Functions in p-adic Fields	207
4.2.1	Elementary Properties	207
4.2.2	Examples of Analytic Functions	210
4.2.3	Application of the Artin–Hasse Exponential	219
4.2.4	Mahler Expansions	222
4.3	Additive and Multiplicative Structures	226
4.3.1	Concrete Approach	226
4.3.2	Basic Reductions	228
4.3.3	Study of the Groups U_i	231
4.3.4	Study of the Group U_1	234
4.3.5	The Group $K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*2}$	236
4.4	Extensions of p-adic Fields	237
4.4.1	Preliminaries on Local Field Norms	238
4.4.2	Krasner’s Lemma	241
4.4.3	General Results on Extensions	242
4.4.4	Applications of the Cohomology of Cyclic Groups	245
4.4.5	Characterization of Unramified Extensions	251
4.4.6	Properties of Unramified Extensions	253
4.4.7	Totally Ramified Extensions	255
4.4.8	Analytic Representations of p th Roots of Unity	257
4.4.9	Factorizations in Number Fields	260
4.4.10	Existence of the Field \mathbb{C}_p	262
4.4.11	Some Analysis in \mathbb{C}_p	265
4.5	The Theorems of Strassmann and Weierstrass	268

4.5.1	Strassmann's Theorem	268
4.5.2	Krasner Analytic Functions	269
4.5.3	The Weierstrass Preparation Theorem	272
4.5.4	Applications of Strassmann's Theorem	274
4.6	Exercises for Chapter 4	278
5.	Quadratic Forms and Local–Global Principles	287
5.1	Basic Results on Quadratic Forms	287
5.1.1	Basic Properties of Quadratic Modules	288
5.1.2	Contiguous Bases and Witt's Theorem	290
5.1.3	Translations into Results on Quadratic Forms	293
5.2	Quadratic Forms over Finite and Local Fields	296
5.2.1	Quadratic Forms over Finite Fields	296
5.2.2	Definition of the Local Hilbert Symbol	297
5.2.3	Main Properties of the Local Hilbert Symbol	298
5.2.4	Quadratic Forms over \mathbb{Q}_p	302
5.3	Quadratic Forms over \mathbb{Q}	305
5.3.1	Global Properties of the Hilbert Symbol	305
5.3.2	Statement of the Hasse–Minkowski Theorem	307
5.3.3	The Hasse–Minkowski Theorem for $n \leq 2$	308
5.3.4	The Hasse–Minkowski Theorem for $n = 3$	309
5.3.5	The Hasse–Minkowski Theorem for $n = 4$	310
5.3.6	The Hasse–Minkowski Theorem for $n \geq 5$	311
5.4	Consequences of the Hasse–Minkowski Theorem	312
5.4.1	General Results	312
5.4.2	A Result of Davenport and Cassels	313
5.4.3	Universal Quadratic Forms	314
5.4.4	Sums of Squares	316
5.5	The Hasse Norm Principle	320
5.6	The Hasse Principle for Powers	323
5.6.1	A General Theorem on Powers	323
5.6.2	The Hasse Principle for Powers	326
5.7	Some Counterexamples to the Hasse Principle	328
5.8	Exercises for Chapter 5	332

Part II. Diophantine Equations

6.	Some Diophantine Equations	337
6.1	Introduction	337
6.1.1	The Use of Finite Fields	337
6.1.2	Local Methods	339
6.1.3	Global Methods	339
6.2	Diophantine Equations of Degree 1	341
6.3	Diophantine Equations of Degree 2	343

6.3.1	The General Homogeneous Equation	343
6.3.2	The Homogeneous Ternary Quadratic Equation	345
6.3.3	Computing a Particular Solution	349
6.3.4	Examples of Homogeneous Ternary Equations	354
6.3.5	The Pell–Fermat Equation $x^2 - Dy^2 = N$	356
6.4	Diophantine Equations of Degree 3	360
6.4.1	Introduction	360
6.4.2	The Equation $ax^3 + by^3 + cz^3 = 0$: Local Solubility . . .	361
6.4.3	The Equation $ax^3 + by^3 + cz^3 = 0$ using Number Fields	363
6.4.4	The Equation $ax^3 + by^3 + cz^3 = 0$ using Elliptic Curves	369
6.4.5	The Equation $x^3 + y^3 + cz^3 = 0$	373
6.4.6	Sums of Two or More Cubes	377
6.4.7	Skolem’s Equations $x^3 + dy^3 = 1$	386
6.4.8	Special Cases of Skolem’s Equations	387
6.4.9	The Equations $y^2 = x^3 \pm 1$ in Rational Numbers	388
6.5	The Equations $ax^4 + by^4 + cz^2 = 0$ and $ax^6 + by^3 + cz^2 = 0$.	390
6.5.1	The Equation $ax^4 + by^4 + cz^2 = 0$: Local Solubility . . .	390
6.5.2	The Equations $x^4 \pm y^4 = z^2$ and $x^4 + 2y^4 = z^2$	392
6.5.3	The Equation $ax^4 + by^4 + cz^2 = 0$ using Elliptic Curves	393
6.5.4	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	408
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	425
6.9	Fermat’s “Last Theorem” $x^n + y^n = z^n$	428
6.9.1	Introduction	428
6.9.2	General Prime n : The First Case	429
6.9.3	Congruence Criteria	429
6.9.4	The Criteria of Wendt and Germain	430
6.9.5	Kummer’s Criterion: Regular Primes	432
6.9.6	The Criteria of Furtwängler and Wieferich	434
6.9.7	General Prime n : The Second Case	436
6.10	An Example of Runge’s Method	439

6.11	First Results on Catalan's Equation	443
6.11.1	Introduction	443
6.11.2	The Theorems of Nagell and Ko Chao	445
6.11.3	Some Lemmas on Binomial Series	446
6.11.4	Proof of Cassels's Theorem 6.11.5	448
6.12	Congruent Numbers	451
6.12.1	Reduction to an Elliptic Curve	451
6.12.2	Use of the Birch and Swinnerton-Dyer Conjecture	452
6.12.3	Tunnell's Theorem	454
6.13	Some Unsolved Diophantine Problems	455
6.14	Exercises for Chapter 6	457
7.	Elliptic Curves	465
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 $x^2 + y^4 = 2z^4$	479
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	499
7.3.6	Reduction of Elliptic Curves over $K_{\mathfrak{p}}$	504
7.3.7	The \mathfrak{p} -adic Filtration for Elliptic Curves over $K_{\mathfrak{p}}$	506
7.4	Exercises for Chapter 7	512
8.	Diophantine Aspects of Elliptic Curves	517
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 ϕ	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 with 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 α	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 . .	556
8.4.1	Rational 3-Torsion Subgroups	557
8.4.2	The Fundamental 3-Isogeny	558
8.4.3	Description of the Image of ϕ	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	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	595
8.6.6	A Complete Example	598
8.7	Computation of Integral Points	599
8.7.1	Introduction	600
8.7.2	An Upper Bound for the Elliptic Logarithm on $E(\mathbb{Z})$.	600
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

Part III. Analytic Methods

9.	Bernoulli Polynomials and the Gamma Function	617
9.1	Bernoulli Numbers and Polynomials	617
9.1.1	Generating Functions for Bernoulli Polynomials	617
9.1.2	Further Recursions for Bernoulli Polynomials	624
9.1.3	Computing a Single Bernoulli Number	629
9.1.4	Bernoulli Polynomials and Fourier Series	630

9.2	Analytic Applications of Bernoulli Polynomials	633
9.2.1	Asymptotic Expansions	634
9.2.2	The Euler–MacLaurin Summation Formula	635
9.2.3	The Remainder Term and the Constant Term	639
9.2.4	Euler–MacLaurin and the Laplace Transform	642
9.2.5	Basic Applications of the Euler–MacLaurin Formula	645
9.3	Applications to Numerical Integration	650
9.3.1	Standard Euler–MacLaurin Numerical Integration	650
9.3.2	The Basic Tanh–Sinh Numerical Integration Method	652
9.3.3	General Double Exponential Numerical Integration	654
9.4	χ -Bernoulli Numbers, Polynomials, and Functions	657
9.4.1	χ -Bernoulli Numbers and Polynomials	658
9.4.2	χ -Bernoulli Functions	661
9.4.3	The χ -Euler–MacLaurin Summation Formula	664
9.5	Arithmetic Properties of Bernoulli Numbers	667
9.5.1	χ -Power Sums	667
9.5.2	The Generalized Clausen–von Staudt Congruence	675
9.5.3	The Voronoi Congruence	678
9.5.4	The Kummer Congruences	681
9.5.5	The Almkvist–Meurman Theorem	683
9.6	The Real and Complex Gamma Function	685
9.6.1	The Hurwitz Zeta Function	685
9.6.2	Definition of the Gamma Function	691
9.6.3	Preliminary Results for the Study of $\Gamma(s)$	695
9.6.4	Properties of the Gamma Function	698
9.6.5	Specific Properties of the function $\psi(s)$	708
9.6.6	Fourier Expansions of $\zeta(s, x)$ and $\log(\Gamma(x))$	713
9.7	Integral Transforms	716
9.7.1	Generalities on Integral Transforms	717
9.7.2	The Fourier Transform	718
9.7.3	The Mellin Transform	720
9.7.4	The Laplace Transform	722
9.8	Bessel Functions	723
9.8.1	Definitions	723
9.8.2	Integral Representations and Applications	726
9.9	Exercises for Chapter 9	731
10.	Dirichlet Series and L-Functions	763
10.1	Arithmetic Functions and Dirichlet Series	763
10.1.1	Operations on Arithmetic Functions	764
10.1.2	Multiplicative Functions	766
10.1.3	Some Classical Arithmetical Functions	767
10.1.4	Numerical Dirichlet Series	772
10.2	The Analytic Theory of L -Series	774
10.2.1	Simple Approaches to Analytic Continuation	775

10.2.2	The Use of the Hurwitz Zeta Function $\zeta(s, x)$	779
10.2.3	The Functional Equation for the Theta Function	781
10.2.4	The Functional Equation for Dirichlet L -Functions	784
10.2.5	Generalized Poisson Summation Formulas	789
10.2.6	Voronoi's Error Term in the Circle Problem	794
10.3	Special Values of Dirichlet L -Functions	798
10.3.1	Basic Results on Special Values	798
10.3.2	Special Values of L -Functions and Modular Forms	805
10.3.3	The Polya–Vinogradov Inequality	810
10.3.4	Bounds and Averages for $L(\chi, 1)$	812
10.3.5	Expansions of $\zeta(s)$ Around $s = k \in \mathbb{Z}_{\leq 1}$	817
10.3.6	Numerical Computation of Euler Products and Sums	820
10.4	Epstein Zeta Functions	823
10.4.1	The Nonholomorphic Eisenstein Series $G(\tau, s)$	823
10.4.2	The Kronecker Limit Formula	826
10.5	Dirichlet Series Linked to Number Fields	828
10.5.1	The Dedekind Zeta Function $\zeta_K(s)$	828
10.5.2	The Dedekind Zeta Function of Quadratic Fields	831
10.5.3	Applications of the Kronecker Limit Formula	835
10.5.4	The Dedekind Zeta Function of Cyclotomic Fields	843
10.5.5	The Nonvanishing of $L(\chi, 1)$	848
10.5.6	Application to Primes in Arithmetic Progression	850
10.5.7	Conjectures on Dirichlet L -Functions	851
10.6	Science-Fiction on L -Functions	852
10.6.1	Local L -Functions	852
10.6.2	Global L -Functions	853
10.7	The Prime Number Theorem	858
10.7.1	Estimates for $\zeta(s)$	858
10.7.2	Newman's Proof	863
10.7.3	Iwaniec's Proof	867
10.8	Exercises for Chapter 10	871
11.	p-adic Gamma and L-Functions	887
11.1	Generalities on p -adic Functions	887
11.1.1	Methods for Constructing p -adic Functions	887
11.1.2	A Brief Study of Volkenborn Integrals	888
11.2	The p -adic Hurwitz Zeta functions	892
11.2.1	Teichmüller Extensions and Characters on \mathbb{Z}_p	892
11.2.2	The p -adic Hurwitz Zeta Function for $x \in \mathbb{C}\mathbb{Z}_p$	893
11.2.3	The Function $\zeta_p(s, x)$ Around $s = 1$	900
11.2.4	The p -adic Hurwitz Zeta Function for $x \in \mathbb{Z}_p$	902
11.3	p -adic L -Functions	912
11.3.1	Dirichlet Characters in the p -adic Context	912
11.3.2	Definition and Basic Properties of p -adic L -Functions	913
11.3.3	p -adic L -Functions at Positive Integers	917

11.3.4	χ -Power Sums Involving p -adic Logarithms	922
11.3.5	The Function $L_p(\chi, s)$ Around $s = 1$	928
11.4	Applications of p -adic L -Functions	931
11.4.1	Integrality and Parity of L -Function Values	931
11.4.2	Bernoulli Numbers and Regular Primes	935
11.4.3	Strengthening of the Almkvist–Meurman Theorem	938
11.5	p -adic Log Gamma Functions	940
11.5.1	Diamond’s p -adic Log Gamma Function	941
11.5.2	Morita’s p -adic Log Gamma Function	947
11.5.3	Computation of some p -adic Logarithms	957
11.5.4	Computation of Limits of some Logarithmic Sums	967
11.5.5	Explicit Formulas for $\psi_p(r/m)$ and $\psi_p(\chi, r/m)$	970
11.5.6	Application to The Value of $L_p(\chi, 1)$	973
11.6	Morita’s p -adic Gamma Function	976
11.6.1	Introduction	976
11.6.2	Definitions and Basic Results	976
11.6.3	Main Properties of the p -adic Gamma Function	981
11.6.4	Mahler–Dwork Expansions Linked to $\Gamma_p(x)$	986
11.6.5	Power Series Expansions Linked to $\Gamma_p(x)$	989
11.6.6	The Jacobstahl–Kazandzidis Congruence	992
11.7	The Gross–Koblitz Formula and Applications	995
11.7.1	Statement and Proof of the Gross–Koblitz Formula	995
11.7.2	Application to $L'_p(\chi, 0)$	1000
11.7.3	Application to the Stickelberger Congruence	1001
11.7.4	Application to the Hasse–Davenport Product Relation	1003
11.8	Exercises for Chapter 11	1007

Part IV. Modern Methods

12.	Applications of Linear Forms in Logarithms	1021
12.1	Introduction	1021
12.1.1	Lower Bounds	1021
12.1.2	Applications to Diophantine Equations and Problems	1023
12.1.3	A List of Applications	1024
12.2	A Lower Bound for $ 2^m - 3^n $	1025
12.3	Lower Bounds for the Trace of α^n	1029
12.4	Pure Powers in Binary Recursive Sequences	1030
12.5	Greatest Prime Factors of Terms of Some Recursive Sequences	1031
12.6	Greatest Prime Factors of Values of Integer Polynomials	1032
12.7	The Diophantine Equation $ax^n - by^n = c$	1033
12.8	Simultaneous Pell Equations	1034
12.8.1	General Strategy	1034
12.8.2	An Example in Detail	1035

12.8.3	A General Algorithm	1037
12.9	Catalan's Equation	1039
12.10	Thue Equations	1040
12.10.1	The Main Theorem	1040
12.10.2	Algorithmic Aspects	1043
12.11	Other Classical Diophantine Equations	1047
12.12	A Few Words on the Non-Archimedean Case	1049
13.	Rational Points on Higher Genus Curves	1051
13.1	Introduction	1051
13.2	The Jacobian	1052
13.2.1	Functions on Curves	1053
13.2.2	Divisors	1054
13.2.3	Rational Divisors	1055
13.2.4	The Group Law: Cantor's Algorithm	1056
13.2.5	The Group Law: the Geometric Point of View	1058
13.3	Rational Points on Hyperelliptic Curves	1060
13.3.1	The Method of Dem'janenko–Manin	1060
13.3.2	The Method of Chabauty–Coleman	1062
13.3.3	Explicit Chabauty According to Flynn	1064
13.3.4	When Chabauty Fails	1065
13.3.5	Elliptic Curve Chabauty	1067
13.3.6	A Complete Example	1070
14.	The Super-Fermat Equation	1075
14.1	Preliminary Reductions	1075
14.2	The Dihedral Cases $(2, 2, r)$	1077
14.2.1	The Equation $x^2 - y^2 = z^r$	1077
14.2.2	The Equation $x^2 + y^2 = z^r$	1078
14.2.3	The Equations $x^2 + 3y^2 = z^3$ and $x^2 + 3y^2 = 4z^3$	1078
14.3	The Tetrahedral Case $(2, 3, 3)$	1079
14.3.1	The Equation $x^3 + y^3 = z^2$	1079
14.3.2	The Equation $x^3 + y^3 = 2z^2$	1082
14.3.3	The Equation $x^3 - 2y^3 = z^2$	1084
14.4	The Octahedral Case $(2, 3, 4)$	1085
14.4.1	The Equation $x^2 - y^4 = z^3$	1086
14.4.2	The Equation $x^2 + y^4 = z^3$	1088
14.5	Invariants, Covariants, and Dessins d'Enfants	1090
14.5.1	Dessins d'Enfants, Klein Forms, and Covariants	1090
14.5.2	The Icosahedral Case $(2, 3, 5)$	1092
14.6	The Parabolic and Hyperbolic Cases	1094
14.6.1	The Parabolic Case	1094
14.6.2	General Results in the Hyperbolic Case	1094
14.6.3	The Equations $x^4 \pm y^4 = z^3$	1097
14.6.4	The Equation $x^4 + y^4 = z^5$	1098

14.6.5	The Equation $x^6 - y^4 = z^2$	1099
14.6.6	The Equation $x^4 - y^6 = z^2$	1099
14.6.7	The Equation $x^6 + y^4 = z^2$	1101
14.6.8	Further Results	1101
14.7	Applications of Mason's Theorem.....	1103
14.7.1	Mason's Theorem	1103
14.7.2	Applications	1104
14.8	Exercises for Chapter 14	1105
15.	The Modular Approach to Diophantine Equations	1107
15.1	Newforms	1107
15.1.1	Introduction and Necessary Software Tools	1107
15.1.2	Newforms	1108
15.1.3	Rational Newforms and Elliptic Curves	1109
15.2	Ribet's Level-Lowering Theorem.....	1110
15.2.1	Definition of "Arises From"	1110
15.2.2	Ribet's Level-Lowering Theorem	1111
15.2.3	Absence of Isogenies	1113
15.2.4	How to use Ribet's Theorem	1115
15.3	Fermat's Last Theorem and Similar Equations	1115
15.3.1	A Generalization of FLT	1116
15.3.2	E Arises from a Curve with Complex Multiplication ..	1117
15.3.3	End of the Proof of Theorem 15.3.1	1118
15.3.4	The Equation $x^2 = y^p + 2^r z^p$ for $p \geq 7$ and $r \geq 2$	1119
15.3.5	The Equation $x^2 = y^p + z^p$ for $p \geq 7$	1121
15.4	An Occasional Bound for the Exponent	1121
15.5	An Example of Serre–Mazur–Kraus	1123
15.6	The Method of Kraus	1126
15.7	"Predicting Exponents of Constants"	1129
15.7.1	The Diophantine Equation $x^2 - 2 = y^p$	1129
15.7.2	Application to the SMK Equation	1133
15.8	Recipes for Some Ternary Diophantine Equations.....	1134
15.8.1	Recipes for Signature (p, p, p)	1135
15.8.2	Recipes for Signature $(p, p, 2)$	1136
15.8.3	Recipes for Signature $(p, p, 3)$	1138
16.	Catalan's Equation	1141
16.1	Mihăilescu's First Two Theorems.....	1141
16.1.1	The First Theorem: Double Wieferich Pairs.....	1142
16.1.2	The Equation $(x^p - 1)/(x - 1) = py^q$	1144
16.1.3	Mihăilescu's Second Theorem: $p \mid h_q^-$ and $q \mid h_p^-$	1148
16.2	The $+$ and $-$ Subspaces and the Group S	1149
16.2.1	The $+$ and $-$ Subspaces.....	1150
16.2.2	The Group S	1152
16.3	Mihăilescu's Third Theorem: $p < 4q^2$ and $q < 4p^2$	1154

16.4 Mihăilescu's Fourth Theorem: $p \equiv 1 \pmod{q}$ or $q \equiv 1 \pmod{p}$	1159
16.4.1 Preliminaries on Commutative Algebra	1159
16.4.2 Preliminaries on the Plus Part	1161
16.4.3 Cyclotomic Units and Thaine's Theorem	1164
16.4.4 Preliminaries on Power Series	1166
16.4.5 Proof of Mihăilescu's Fourth Theorem	1169
16.4.6 Conclusion: Proof of Catalan's Conjecture	1172
Bibliography	1173
Index of Notation	1182
Index of Names	1182
General Index	1189