Number Theory
Algebraic Numbers and Functions

Helmut Koch

Translated by
David Kramer

Graduate Studies in Mathematics
Volume 24
Contents

Preface xiii

Translator’s Note xvi

Notation xvii

List of Symbols xvii

Chapter 1. Introduction 1

1.1. Pythagorean Triples 1

1.2. Pell’s Equation 3

1.3. Fermat’s Last Theorem 4

1.4. Congruences 8

1.5. Public Key Cryptology 11

1.6. Quadratic Residues 12

1.7. Prime Numbers 22

1.8. The Prime Number Theorem 26

1.9. Exercises 31

Chapter 2. The Geometry of Numbers 35

2.1. Binary Quadratic Forms 35

2.2. Complete Decomposable Forms of Degree $n$ 37

2.3. Modules and Orders 39
2.4. Complete Modules in Finite Extensions of $P$ 43
2.5. The Integers of a Quadratic Field 45
2.6. Further Examples of Determining a $\mathbb{Z}$-Basis for the Ring of Integers of a Number Field 46
2.7. The Finiteness of the Class Number 47
2.8. The Group of Units 48
2.9. The Start of the Proof of Dirichlet’s Unit Theorem 50
2.10. The Rank of $I(E)$ 51
2.11. The Regulator of an Order 55
2.12. The Lattice Point Theorem 55
2.13. Minkowski’s Geometry of Numbers 57
2.14. Application to Complete Decomposable Forms 62
2.15. Exercises 64

Chapter 3. Dedekind’s Theory of Ideals 65
3.1. Basic Definitions 66
3.2. The Main Theorem of Dedekind’s Theory of Ideals 68
3.3. Consequences of the Main Theorem 71
3.4. The Converse of the Main Theorem 73
3.5. The Norm of an Ideal 74
3.6. Congruences 76
3.7. Localization 78
3.8. The Decomposition of a Prime Ideal in a Finite Separable Extension 80
3.9. The Class Group of an Algebraic Number Field 84
3.10. Relative Extensions 88
3.11. Geometric Interpretation 93
3.12. Different and Discriminant 94
3.13. Exercises 101
Chapter 4. Valuations

4.1. Fields with Valuation

4.2. Valuations of the Field of Rational Numbers and of a Field of Rational Functions

4.3. Completion

4.4. Complete Fields with Respect to a Discrete Valuation

4.5. Extension of a Valuation of a Complete Field to a Finite Extension

4.6. Finite Extensions of a Complete Field with a Discrete Valuation

4.7. Complete Fields with a Discrete Valuation and Finite Residue Class Field

4.8. Extension of the Valuation of an Arbitrary Field to a Finite Extension

4.9. Arithmetic in the Compositum of Two Field Extensions

4.10. Exercises

Chapter 5. Algebraic Functions of One Variable

5.1. Algebraic Function Fields

5.2. The Places of an Algebraic Function Field

5.3. The Function Space Associated to a Divisor

5.4. Differentials

5.5. Extensions of the Field of Constants

5.6. The Riemann–Roch Theorem

5.7. Function Fields of Genus 0

5.8. Function Fields of Genus 1

5.9. Exercises

Chapter 6. Normal Extensions

6.1. Decomposition Group and Ramification Groups

6.2. A New Proof of Dedekind's Theorem on the Different

6.3. Decomposition of Prime Ideals in an Intermediate Field

6.4. Cyclotomic Fields
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5. The First Case of Fermat’s Last Theorem</td>
<td>184</td>
</tr>
<tr>
<td>6.6. Localization</td>
<td>188</td>
</tr>
<tr>
<td>6.7. Upper Numeration of the Ramification Group</td>
<td>190</td>
</tr>
<tr>
<td>6.8. Kummer Extensions</td>
<td>195</td>
</tr>
<tr>
<td>6.9. Exercises</td>
<td>199</td>
</tr>
<tr>
<td>Chapter 7. L-Series</td>
<td>203</td>
</tr>
<tr>
<td>7.1. From the Riemann $\zeta$-Function to the Hecke $L$-Series</td>
<td>204</td>
</tr>
<tr>
<td>7.2. Normalized Valuations</td>
<td>207</td>
</tr>
<tr>
<td>7.3. Adeles</td>
<td>209</td>
</tr>
<tr>
<td>7.4. Ideles</td>
<td>212</td>
</tr>
<tr>
<td>7.5. Idele Class Group and Ray Class Group</td>
<td>214</td>
</tr>
<tr>
<td>7.6. Hecke Characters</td>
<td>217</td>
</tr>
<tr>
<td>7.7. Analysis on Local Additive Groups</td>
<td>219</td>
</tr>
<tr>
<td>7.8. Analysis on the Adele Group</td>
<td>223</td>
</tr>
<tr>
<td>7.9. The Multiplicative Group of a Local Field</td>
<td>227</td>
</tr>
<tr>
<td>7.10. The Local Functional Equation</td>
<td>230</td>
</tr>
<tr>
<td>7.11. Calculation of $\rho(c)$ for $K = \mathbb{R}$</td>
<td>232</td>
</tr>
<tr>
<td>7.12. Calculation of $\rho(c)$ for $K = \mathbb{C}$</td>
<td>234</td>
</tr>
<tr>
<td>7.13. Computation of the $\rho$-Factors for a Nonarchimedean Field</td>
<td>236</td>
</tr>
<tr>
<td>7.14. Relations Among the $\rho$-Factors</td>
<td>239</td>
</tr>
<tr>
<td>7.15. Analysis on the Idele Group</td>
<td>240</td>
</tr>
<tr>
<td>7.16. Global Zeta Functions</td>
<td>243</td>
</tr>
<tr>
<td>7.17. The Dedekind Zeta Function</td>
<td>247</td>
</tr>
<tr>
<td>7.18. Hecke $L$-Series</td>
<td>251</td>
</tr>
<tr>
<td>7.19. Congruence Zeta Functions</td>
<td>252</td>
</tr>
<tr>
<td>7.20. Exercises</td>
<td>257</td>
</tr>
<tr>
<td>Chapter 8. Applications of Hecke $L$-Series</td>
<td>259</td>
</tr>
<tr>
<td>8.1. The Decomposition of Prime Numbers in Algebraic Number Fields</td>
<td>259</td>
</tr>
<tr>
<td>8.2. The Nonvanishing of the $L$-Series at $s = 1$</td>
<td>262</td>
</tr>
</tbody>
</table>
8.3. The Distribution of Prime Ideals in an Algebraic Number Field 266
8.4. The Generalized Riemann Hypothesis 270
8.5. Exercises 273

Chapter 9. Quadratic Number Fields 275
9.1. Quadratic Forms and Orders in Quadratic Number Fields 275
9.2. The Class Number of Imaginary Quadratic Number Fields 282
9.3. Continued Fractions 285
9.4. Periodic Continued Fractions 290
9.5. The Fundamental Unit of an Order of a Real Quadratic Number Field 295
9.6. The Character of a Quadratic Number Field 301
9.7. The Arithmetic Class Number Formula 303
9.8. Computing the Gaussian Sum 310
9.9. Exercises 313

Chapter 10. What Next? 315
10.1. Absolutely Abelian Extensions 316
10.2. The Class Field of the Ray Class Group 317
10.3. Local Class Field Theory 321
10.4. Formulation of Class Field Theory Using Ideles 322
10.5. Exercises 324

Appendix A. Divisibility Theory 325
A.1. Divisibility in Monoids 325
A.2. Principal Ideal Domains 328
A.3. Euclidean Domains 330
A.4. Finitely Generated Modules over a Principal Ideal Domain 331
A.5. Modules over Euclidean Domains 338
A.6. The Arithmetic of Polynomials over Rings 340

Appendix B. Trace, Norm, Different, and Discriminant 341
Preface

In writing this introduction to algebraic number theory I have been guided by several principles.

First, it is my firm conviction that an area of mathematics such as number theory that has developed over a long period of time can be properly studied and understood only if one proceeds through this entire development in abbreviated form, much as an organism recapitulates its evolutionary path in abbreviated form during its embryonic development.

From this I derived the concept of allowing the reader to take part from chapter to chapter in the historical development of number theory. This holds for the first seven chapters, while the last three chapters are devoted primarily to applications and an overview.

Second, it was a discovery of Dedekind and Kronecker in the 1880s that principles that had been developed to study algebraic numbers could also be applied to the theory of algebraic functions. Dedekind wished to provide a firm foundation to Riemannian function theory. Together with H. Weber [DeWe1882] he considered the case of functions whose arguments and values are complex numbers. It later became clear that the theory of Dedekind and Weber could be extended to cover algebraic functions over an arbitrary field of constants. The most complete analogy to algebraic numbers then appears when the field of constants is finite. In fact, we find ourselves in this case in an area of number theory itself, the theory of congruences. Therefore, in this book we shall consider algebraic numbers and functions (of a single variable) together.

Lastly, this book is an introduction only to the extent that an important area of algebraic number theory, class field theory, is considered only
summarily, in the tenth, and last, chapter. Below this threshold the reader should nonetheless be able to embark on a research topic. In particular, the theory of the different and discriminant and the theory of higher ramification groups are explicated in considerable detail.

Corresponding to these three principles the book is constructed as follows: The first chapter discusses some issues of elementary number theory and encompasses the time before the development of the theory of algebraic number fields. There are two exceptions: In Section 1.5 we consider public key cryptology as an example of the application of number theory of the nineteenth century to present-day communications technology, and in Section 1.8 we prove the prime number theorem with methods that reflect the spirit of Cauchy, Riemann, and Chebyshev, though the brevity of our presentation is made possible by simplifications of recent vintage. I wish to thank F. Hirzebruch and D. Zagier for apprising me of these developments in a recent manuscript ([Za1997]).

The second chapter is concerned with the part of algebraic number theory that is applicable to arbitrary orders in algebraic number fields. This corresponds on the one hand to the state of knowledge before Dedekind, and here in particular Dirichlet’s theorem on units has its place. On the other hand, our presentation is not strictly historical; rather, it is suffused with Dedekind’s ideas. Also present here is Minkowski’s geometry of numbers, which provides the chapter its title. Number theory had its beginnings in the study of the rational integers. We therefore begin the second chapter with a discussion of complete forms, which provides the transition from questions about rational integers to questions about algebraic numbers.

With the third chapter we have finally arrived at Dedekind’s theory of ideals, which we develop in a generality that makes possible the simultaneous treatment of algebraic number fields and function fields.

The valuation-theoretic method of Chapter 4 is a supplement to the ring-theoretic method of Chapter 3.

With the machinery thus developed we present in Chapter 5 the theory of algebraic functions of one variable, basing our presentation principally on H. Hasse’s Zahlentheorie [Ha1949].

In Chapter 6 we consider the decomposition groups and ramification groups of normal extensions and thereby come to the completion of the theory of algebraic number fields of Dedekind and Hilbert. This then makes it possible to treat the important example of cyclotomic fields in an adequate manner. The Kronecker–Weber theorem is presented in the form of a series of exercises. With the upper numeration of Hasse and Herbrand we have reached the mathematics of the 1930s.
Chapter 7 is devoted primarily to a proof of the functional equation for Hecke $L$-series as presented in Tate’s thesis [Ta1950]. This result alone would hardly justify a chapter of such length, since we draw relatively few consequences from it. If I have nevertheless decided to present this in full detail, it is because on the one hand it introduces new methods of proof compared to those of the previous chapters, such as analysis on locally compact abelian groups including Pontryagin duality theory, and on the other hand the methods of Tate’s thesis allow generalizations that are of fundamental significance for the union of number theory and the representation theory of reductive groups (the Langlands conjectures).

Chapter 7 begins with a careful presentation of the relation between idele class groups and ray class groups as well as that between Hecke characters and Grössencharakters. The basic properties of ideles and adeles are proved for number fields and function fields. In proving the functional equation, however, we consider only number fields.

Chapter 8 contains applications of the analytic methods of Chapter 7 to the distribution of prime ideals in algebraic number fields. In the section on generalized Riemann hypotheses we also consider the congruence zeta functions of Artin and F.K. Schmidt. I wish to thank S. Böcherer and R. Schulze-Pillot for supplying me with extended seminar notes by P.K. Draxl on the theorem of Hecke on the distribution of primes in cones, which made possible an essential rounding off of Chapter 8.

Chapter 9 is devoted to quadratic number fields, for which many attributes can be represented more explicitly than in the general case. This holds especially for the computation of the class number and the determination of the fundamental unit. Here we also build bridges between Gauss’s theory of quadratic forms and the theory of orders in quadratic number fields.

Chapter 10 finally provides a glimpse of class field theory.

In writing this book I have had before me the image of a reader who possesses a good knowledge of linear algebra. This must be supplemented by knowledge of field theory, particularly Galois theory, along the lines of what is covered in E. Kunz’s *Algebra*, which has also appeared in Vieweg Verlag’s series “Aufbaukurs Mathematik.” In some ways this book builds directly on Kunz’s *Algebra*, which we have cited at many points. If at the beginning of this book we spoke of an “abbreviated development,” such an abbreviation has been made possible by the developments of modern algebra, which have simplified many a difficult proof by one of the older masters.

In the planning of this book I have had before me as examples the long series of texts on algebraic number theory, above all the books by H. Hasse [Ha1949] and Borevich and Shafarevich [BoSh1966]. The idea for treating
simultaneously the cases of number fields and function fields is to be found in, aside from the above-mentioned books, the books of Eichler [Ei1963], Artin [Ar1967], and Weil [We1967]. For various reasons these books seem to me unsuitable for the beginner.

My colleagues S. Böge, G. Frei, W. Hoffmann, S. Kukkuk, W. Narkiewicz, and F. Nicolae have read drafts of individual chapters of this book and have suggested very valuable improvements and corrections. I offer them my heartfelt thanks, which I offer also to C. Hadan, B. Wüst, and again S. Kukkuk and F. Nicolae for preparing the \TeX files.

Some of the greatest mathematicians of the past—I name here only David Hilbert and Hermann Weyl—have seen in algebraic number theory one of the most outstanding creations of mathematics. The task of this book will have been fulfilled if some of this enthusiasm is transmitted to the reader.

Berlin, March 1997

Translator’s Note

This English translation is generally faithful to the German text, the only changes being the correction of a few small errors and the enlargement of the index. I hope that I have not introduced too many new errors.

The German edition of this book is part of the series Vieweg Studium, Aufbaukurs Mathematik. Thus it was natural for the author to cite as a source for results on abstract algebra the text in the same series by E. Kunz [Ku]. Since this book has appeared only in German, in this edition it has been replaced as a reference by Serge Lang’s Algebra [La], which is known to a worldwide English-language readership. Most of these references are to standard results in field theory. The reader who is familiar with another introductory algebra text, that of van der Waerden [Wa1966, Wa1967], for example, will certainly find the requisite background material for the study of algebraic number theory.

I would like to thank Helmut Koch for his kind assistance with the translation. He answered a large number of queries about notation and terminology and then looked over the entire English manuscript. I would also like to express my gratitude to Walter Neumann and Lawrence Washington for their help with terminology and in clarifying a few sticky points.
Chapter 1

Introduction

The origins of humankind’s interest in numbers are shrouded in the mists of time. The first numbers to impinge themselves on human consciousness were certainly the natural numbers, that is, the elements of the sequence

\[ 1, 2, 3, \ldots \]

It was Kronecker who said, “God created the natural numbers. All else is the work of man.”

Number theory as it was practiced by the ancients has today become a part of algebra by and large, and so we shall not go into the subject as it was practiced in early advanced civilizations and in classical antiquity, and that includes the theorem on the unique prime factorization of natural numbers, which we shall employ in this book without comment.

Likewise, we shall employ congruences among integers: \( a \equiv b \pmod{c} \) means that \( a - b \) is divisible by \( c \).

1.1. Pythagorean Triples

A *Pythagorean triple* is a triple \( x, y, z \) of natural numbers that satisfy the equation

\[ x^2 + y^2 = z^2. \]  \hspace{1cm} (1.1.1)

The smallest example is the triple 3, 4, 5. The name derives from the Pythagorean theorem, which asserts that the sides of a right triangle satisfy equation (1.1.1). In fact, the converse is true: A triangle whose sides satisfy (1.1.1) is a right triangle. This theorem has from time immemorial provided a method of constructing right triangles in the building trade, and it is still used by craftsmen today for this purpose.
Perhaps the earliest known use of Pythagorean triples is to be found inscribed in Babylonian cuneiform on a clay tablet dating from about 1900–1600 B.C.E. (see [We1983], p. 8), which contains fifteen such triples.

It is not difficult to obtain a description of all Pythagorean triples. We shall do this in a way that makes clear the connection with arithmetic geometry, the most modern form of algebraic number theory.

We first observe that there is no solution of (1.1.1) with odd \(x\) and \(y\). Indeed, let \(x\) and \(y\) be a pair of odd numbers. Then \(x^2 \equiv 1 \pmod{8}\), \(y^2 \equiv 1 \pmod{8}\), from which it follows that \(x^2 + y^2 = z^2 \equiv 2 \pmod{8}\). But there is no integer \(z\) such that \(z^2 \equiv 2 \pmod{8}\). Now, if \(x, y, z\) is a Pythagorean triple, then so is \(y, x, z\), and thus without loss of generality we may assume that \(x\) is even. If we rearrange (1.1.1) and divide by \(x\), then we see that (1.1.1) is equivalent to

\[
\zeta^2 - \eta^2 = 1,
\]

where \(\zeta = z/x\) and \(\eta = y/x\) are positive rational numbers. Since \(\zeta^2 - \eta^2 = (\zeta + \eta)(\zeta - \eta)\), we may set

\[
\tau = \zeta + \eta, \quad \frac{1}{\tau} = \zeta - \eta,
\]

and obtain all solutions of (1.1.2) uniquely in the form

\[
\zeta = \frac{1}{2} \left( \tau + \frac{1}{\tau} \right), \quad \eta = \frac{1}{2} \left( \tau - \frac{1}{\tau} \right),
\]

where \(\tau\) is an arbitrary rational number greater than 1. Equation (1.1.3) is a birational map of the affine line onto the hyperbola given in (1.1.2). There is no point on the hyperbola corresponding to the point 0 on the line.

Returning now from (1.1.3) to the Pythagorean triples, we observe that if \(x, y, z\) is a solution of (1.1.1), then so is \(dx, dy, dz\) for every natural number \(d\). Therefore, it suffices to consider only *primitive* solutions of (1.1.1), that is, triples of integers \(x, y, z\) with greatest common divisor equal to 1. We set \(\tau = u/v\), where \(u\) and \(v\) are relatively prime positive integers. Then

\[
\zeta = \frac{u^2 + v^2}{2uv}, \quad \eta = \frac{u^2 - v^2}{2uv}.
\]

If \(u\) and \(v\) are both odd, we obtain the primitive triples of integers

\[
x = uv, \quad y = \frac{u^2 - v^2}{2}, \quad z = \frac{u^2 + v^2}{2}.
\]

However, these are not of interest, since in this case \(x\) is odd, and we have assumed \(x\) even. Therefore, let either \(u\) or \(v\) be even, and note that \(u > v\), since \(\tau > 1\). We then obtain the primitive triples

\[
x = 2uv, \quad y = u^2 - v^2, \quad z = u^2 + v^2.
\]

With this we have proved the following theorem.
Theorem 1.1.1. Let $x, y, z$ be a solution of the equation

$$x^2 + y^2 = z^2$$

in relatively prime integers. Then $x$ or $y$ must be even. On the assumption that $x$ is even, $x, y, z$ has the form

$$x = 2uv, \quad y = u^2 - v^2, \quad z = u^2 + v^2,$$

where $u$ and $v$ are relatively prime natural numbers with $u + v$ odd and $u > v$. Every such pair $u, v$ corresponds to exactly one primitive Pythagorean triple $x, y, z$.

1.2. Pell’s Equation

In 1769 the German playwright Gotthold Ephraim Lessing (1729–1781) was appointed by the Duke of Brunswick to the directorship of the famous Wolfenbüttel library. In 1773 Lessing published a Greek epigram that he had discovered in one of the library’s volumes. The epigram contained a mathematical problem in verse that had been sent by Archimedes (c. 287–212 B.C.E.) to the mathematicians of Alexandria.

Several historians of mathematics have expressed doubt as to whether this epigram can indeed be ascribed to Archimedes. A. Weil, who describes the problem in [We1983], Section 1.9, is of the opinion that all the evidence is for, and none against, Archimedes being indeed the perpetrator.

Archimedes’ problem leads in any event to a so-called Pell’s equation, that is, an equation of the form

$$x^2 - Dy^2 = 1 \quad (1.2.1)$$

with $D \in \mathbb{N}$ (with certain restrictions). The smallest solution to Archimedes’ problem is on the order of $10^{103275}$. If Archimedes indeed possessed a general method of solving (1.2.1) in integers $x, y$, for which, to be sure, there is no evidence, then such a method would be the deepest result of classical number theory.

Pierre de Fermat (1601–1665) posed the problem of solving equation (1.2.1) to several of his mathematical correspondents, and in doing so stated that he himself was in possession of a general method of solution. In a letter to Frenicle written in 1657 he suggests solving the problem with the values $D = 61$ and $D = 109$, so that “the solution not cost too much effort.” In fact, in these cases the smallest solutions are respectively $x = 1766319049, y = 226153980$, and $x = 158070671986249, y = 15140424455100$. Fermat never published his method for solving Pell’s equation. The method usually employed today—an algorithm employing continued fractions—was given in complete and satisfactory form by Lagrange. We will present this method in Sections 9.3–9.5.
1.3. Fermat’s Last Theorem

A. Weil writes in [We1983], page 1, that modern number theory was born twice, the first birth occurring between 1621 and 1636, when Fermat acquired a copy of Diophantus’s book on number theory with a Latin translation and commentary by Bachet, which the latter had published in 1621.

The Greek mathematician Diophantus (third century c.e.) created the most extensive ancient work on number theory. The objects he studied were primarily integral and rational solutions of polynomial equations.

Among the many annotations that Fermat penned into the margin of his copy of Diophantus, the most famous is that in which he noted that he had discovered a marvelous proof of a certain Diophantine problem, but that alas, the margin was too small to contain it. In today’s notation, Fermat’s assertion was that there is no solution to the equation

\[ x^n + y^n = z^n \]  \hspace{1cm} (1.3.1)

in natural numbers \(x, y, z\) when the exponent \(n\) is greater than 2. This conjecture, known as Fermat’s last theorem, was first proved in 1994 by A. Wiles [Wi1995] and R. Taylor [TaWi1995]. Their proof made use of a significant portion of the mathematical developments of the nineteenth and twentieth centuries. Beginning with Euler (1707–1783), who gave a proof for the case \(n = 3\), Fermat’s conjecture was a grail pursued by many mathematicians. We shall return to Fermat’s last theorem later in this book.

Let \(k, l, m\) be natural numbers that are divisors of \(n\). Then from the insolvability of the equation

\[ x^k + y^l = z^m \]

in natural numbers follows the insolvability of (1.3.1). In particular, to prove Fermat’s last theorem it suffices to show that (1.3.1) has no solution for \(n = 4\) or \(n\) an odd prime.

Today, the prevailing opinion is that Fermat could, in fact, prove only the case \(n = 4\). (See [We1983], pp. 75–77, for a careful analysis.) More precisely, he proved the following theorem.

**Theorem 1.3.1.** The equation

\[ x^4 + y^4 = z^2 \]  \hspace{1cm} (1.3.2)

has no solution in natural numbers \(x, y, z\).

**Proof.** Let \(x, y, z\) be such a solution. Then by Theorem 1.1.1, \(x^2, y^2, z\), and \(z\) are of the form

\[ x^2 = 2uvd, \quad y^2 = (u^2 - v^2)d, \quad z = (u^2 + v^2)d, \]
where \( u \) and \( v \) are relatively prime integers with \( u > v \) and with \( u + v \) odd. Since \( 2uv \) and \( u^2 - v^2 \) are relatively prime, any prime divisor \( p \) of \( d \) cannot be contained in both of these numbers. Therefore, such a \( p \) must appear as a factor of \( d \) an even number of times. It follows, then, that there exist \( x, y \) satisfying (1.3.2) with \( d = 1 \). Therefore, we have the equation

\[
v^2 + y^2 = u^2 \tag{1.3.3}
\]

with relatively prime numbers \( u, y, v \). Since \( y \) is odd, \( v \) must be even. Again by Theorem 1.1.1 there are relatively prime integers \( s \) and \( t \) with \( s > t \) and with \( s + t \) odd, and we have

\[
v = 2st, \quad y = s^2 - t^2, \quad u = s^2 + t^2.
\]

It follows that

\[
x^2 = 2uv = 4st(s^2 + t^2). \tag{1.3.4}
\]

Since \( 2st \) and \( s^2 + t^2 \) are relatively prime, we may conclude from (1.3.4) that \( s, t, \) and \( s^2 + t^2 \) are perfect squares, say

\[
s = f^2, \quad t = g^2, \quad s^2 + t^2 = h^2.
\]

We have thus arrived at the equation

\[
f^4 + g^4 = h^2
\]

with

\[
0 < h < h^2 = u < z.
\]

Thus we have found a solution of (1.3.2) that is smaller than the original solution. If we were to carry out this technique on the solution obtained, we would obtain a yet smaller solution of (1.3.2), and continuing in this fashion, we could obtain an arbitrarily long sequence of solutions each with a smaller (positive) value of \( z \). From this contradiction we conclude the insolvability of (1.3.2).

Fermat called this method of proof \textit{infinite descent}.

The second birth of modern number theory took place, according to Weil, on the first of December, 1729, when Euler, who was in St. Petersburg, received a letter from his friend Goldbach, who was in Moscow. In this letter Goldbach asked Euler’s opinion of Fermat’s assertion that every integer of the form \( 2^{2^n} + 1 \) is a prime number. On 4 June 1730 Euler wrote in reply that he had just been reading Fermat and had been deeply impressed with several of his number-theoretic assertions. Euler proved some of these assertions and disproved others.

At this point we shall note something about prime numbers of the form \( 2^m + 1 \), which as a result of the above-mentioned assertion of Fermat are known as \textit{Fermat primes}. Such prime numbers play a role in the division
of the circle with straightedge and compass (see, for example, [Wa1966], §65).

**Proposition 1.3.2.** Let $2^m + 1$ be a prime number. Then $m$ is a power of 2.

**Proof.** For an odd natural number $h$ and an integer $a$ one has

$$a^h + 1 = (a + 1)(a^{h-1} - a^{h-2} + \ldots + 1).$$

From this the theorem follows. \qed

The number $2^{2^n} + 1$ is prime for $n = 0, 1, 2, 3, 4$. Euler discovered that $2^{32} + 1$ contains the prime factor 641. He proved the following theorem.

**Theorem 1.3.3.** Let $p$ be a prime divisor of $2^{2^n} + 1$. Then $2^{n+1}$ is a divisor of $p - 1$.

**Proof.** We shall make use of Fermat’s little theorem, equation (1.4.3), in the following group-theoretic formulation: Let $a$ be an integer relatively prime to $p$. Then the order of the equivalence class $\bar{a}$ in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ is a divisor of the order $p - 1$ of this group.

The order of 2 is $2^{n+1}$, since by

$$2^{2^n} \equiv -1 \pmod{p} \quad (1.3.5)$$

one has $2^{2^{n+1}} \equiv 1 \pmod{p}$, that is, the order of 2 is a divisor of $2^{n+1}$, and on account of (1.3.5), the order of 2 is equal to $2^{n+1}$. \qed

Now let $p$ be a prime divisor of $2^{32} + 1$. Then by Theorem 1.3.3, $p$ has the form $p = 64m + 1$. For $m \equiv 2 \pmod{3}$ we have that $64m + 1$ is divisible by 3, and for $m \equiv 1 \pmod{5}$ it is divisible by 5. The primes in question are therefore

$$p = 193, \ 257, \ 449, \ 577, \ 641, \ \ldots,$$

and 641 is a divisor of $2^{32} + 1$.

There are no other known Fermat primes (see [Ri1995], pp. 83–90).

Euler gave the first proof of Fermat’s last theorem for the case $n = 3$. However, there was a flaw in this proof, and even after the flaw was corrected the proof remained rather complicated. There is another proof, due to Carl Friedrich Gauss (1777–1855). This proof is of particular interest in that instead of ordinary integers Gauss uses the Eisenstein numbers $a + \zeta b$ with $a, b \in \mathbb{Z}$, $\zeta = (-1 + \sqrt{-3})/2$ and proves Fermat’s last theorem for such numbers. It may be that this success led Gauss to make a disparaging remark about Fermat’s conjecture, which is contained in a letter of 21 March 1816 to Olbers (Gauss, Werke XI, 75–76, Teubner 1917) in reference to a prize problem proposed by the Paris Académie.
At this point we shall content ourselves with a partial result.

**Theorem 1.3.4.** There are no natural numbers \( x, y, z \) that are relatively prime to 3 and that satisfy the congruence

\[
x^3 + y^3 \equiv z^3 \pmod{9}.
\]

**Proof.** Let \( x, y, z \) be such numbers. From

\[
x^3 + y^3 \equiv z^3 \pmod{3}
\]

follows \( x + y \equiv z \pmod{3} \), and thus \( z \) has the form

\[
z = x + y + 3n
\]

with \( n \in \mathbb{Z} \). From this follows

\[
x^3 + y^3 \equiv (x + y + 3n)^3 \equiv x^3 + y^3 + 3x^2y + 3xy^2 \pmod{9}.
\]

Thus we may conclude that

\[
3xy(x + y) \equiv 0 \pmod{9},
\]

whence

\[
xyz \equiv 0 \pmod{3}.
\]

\(\square\)

The statement that (1.3.1) has no solution in natural numbers \( x, y, z \) relatively prime to \( n \) is known as the *first case* of Fermat’s last theorem. The statement that (1.3.1) has no solution in natural numbers \( x, y, z \) not all relatively prime to \( n \) is known as the *second case* of Fermat’s last theorem.

At the age of twenty, Peter Gustav Lejeune Dirichlet (1805–1859), then a student in Paris, was able, with some amplification from the seventy-four-year-old Legendre, to prove Fermat’s last theorem for the case \( n = 5 \) \([Di1828]\), while Lamé \([La1839]\) proved it for the case \( n = 7 \). Significant progress was made by Kummer with his theory of *ideal numbers* for rings that arise as extensions of \( \mathbb{Z} \) through the adjunction of a primitive \( p \)th root of unity (\([Ku1850]\)). Kummer achieved extremely deep results, results that lead directly into the heart of algebraic number theory and the full consequences of which were not fully appreciated until the 1960s. On the other hand, they comprise, according to our present understanding, a special case of the general theory of algebraic number fields, which was developed above all by Dedekind. We shall investigate Dedekind’s theory in Chapter 3 and not reach Kummer’s results until Chapter 6.
1.4. Congruences

For an arbitrary ring $\Lambda$ and ideal $\mathfrak{A}$ of $\Lambda$ we define the congruence of $a$ and $b$ modulo $\mathfrak{A}$ in $\Lambda$, denoted by

$$a \equiv b \pmod {\mathfrak{A}},$$

by saying that $a$ and $b$ are congruent modulo $\mathfrak{A}$ whenever $a - b$ belongs to $\mathfrak{A}$. This is an equivalence relation, and it is compatible with addition and multiplication in $\Lambda$. Calculation with congruences modulo $\mathfrak{A}$ is equivalent to calculation in the quotient ring $\Lambda/\mathfrak{A}$ ([La], Section 2.1).

If $\Lambda$ is a principal ideal domain, then one writes instead of $a \equiv b \pmod {mA}$ the simpler

$$a \equiv b \pmod {m}.$$

In the following we shall restrict our attention to the ring of integers $\mathbb{Z}$.

The notion of congruence was introduced by Gauss in [Ga1801], where we find the simplest laws governing congruences, some of which go back to Euler. An important result in [Ga1801] is a proof of the law of reciprocity for quadratic residues. In the section after the following one we shall present a proof, similar to one given by Gauss, that rests on Gaussian sums over finite fields. In this section we shall concern ourselves with the general structure of residue class rings $\mathbb{Z}/n\mathbb{Z}$ for a natural number $n$ with prime factorization

$$n = p_1^{m_1} \cdots p_s^{m_s}.$$

By the Chinese remainder theorem (Proposition A.2.2) we have the following decomposition of $\mathbb{Z}/n\mathbb{Z}$ into a direct sum of rings:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{m_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_s^{m_s}\mathbb{Z}. \quad (1.4.1)$$

We are interested in the group of units $(\mathbb{Z}/n\mathbb{Z})^\times$ of $\mathbb{Z}/n\mathbb{Z}$.

**Proposition 1.4.1.** An equivalence class $\bar{a}$ of $\mathbb{Z}/n\mathbb{Z}$ belongs to $(\mathbb{Z}/n\mathbb{Z})^\times$ if and only if $a$ is relatively prime to $n$.

**Proof.** Let $a$ be relatively prime to $n$. Then there exist $x, y \in \mathbb{Z}$ with

$$1 = ax + ny.$$

It follows that $\bar{1} = \bar{a}\bar{x}$, that is, $\bar{a}$ belongs to $(\mathbb{Z}/n\mathbb{Z})^\times$.

Conversely, let $\bar{a}$ be an element of $(\mathbb{Z}/n\mathbb{Z})^\times$. Then there exists an equivalence $\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$ with

$$\bar{1} = \bar{a}\bar{b}.$$
1.4. Congruences

It follows that 1 lies in the ideal generated by \( a \) and \( n \), that is, \( a \) and \( n \) are relatively prime.

The equivalence classes in \((\mathbb{Z}/n\mathbb{Z})^\times\) are known as **prime residue classes**.

Let \( \varphi(n) \) denote the number of classes in \((\mathbb{Z}/n\mathbb{Z})^\times\). Since in a finite group \( G \) of order \( h \) the relation

\[ x^h = 1 \]

holds for all \( x \) in \( G \), it follows that

\[ a^{\varphi(n)} \equiv 1 \pmod{n} \quad (1.4.2) \]

for all \( a \) in \( \mathbb{Z} \) relatively prime to \( n \). This is Euler’s generalization of Fermat’s little theorem:

\[ a^p \equiv a \pmod{p} \quad (1.4.3) \]

for all \( a \) and a prime number \( p \). Equation (1.4.3) follows from (1.4.2) for \( a \) not divisible by \( p \). But for multiples of \( p \), (1.4.3) is trivial.

From (1.4.1) we have

\[ (\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{m_1}\mathbb{Z})^\times \oplus \cdots \oplus (\mathbb{Z}/p_s^{m_s}\mathbb{Z})^\times, \]

whence follows

\[ \varphi(n) = \varphi(p_1^{m_1}) \cdots \varphi(p_s^{m_s}). \]

Furthermore, a residue class \( \bar{a} \in \mathbb{Z}/p^m\mathbb{Z} \) is uniquely defined by a representative \( a \) with \( 0 \leq a < p^m \). The class \( \bar{a} \) belongs to \((\mathbb{Z}/p^m\mathbb{Z})^\times\) when \( a \) is not divisible by \( p \). The number of such numbers \( a \) is equal to \( p^m - p^{m-1} \). Thus we have

\[ \varphi(p^m) = p^m - p^{m-1} \]

and

\[ \varphi(n) = n \cdot \left( 1 - \frac{1}{p_1} \right) \cdots \left( 1 - \frac{1}{p_s} \right). \quad (1.4.4) \]

We would now like to investigate the structure of \((\mathbb{Z}/p^m\mathbb{Z})^\times\).

For \( m = 1 \) we have that \( \mathbb{Z}/p\mathbb{Z} \) is a field. Therefore, \((\mathbb{Z}/p\mathbb{Z})^\times\) is a cyclic group of order \( p - 1 \) ([La], Section 7.5).

An integer \( g \) with the property that \( \bar{g} \) is a generator of \((\mathbb{Z}/p\mathbb{Z})^\times\) is called a **primitive root** modulo \( p \).

Let us take \( p = 17 \) as an example. We may choose \( g = 3 \) as a primitive root. In fact, \( 3^8 \equiv -1 \pmod{17} \).

To solve the equation

\[ x^n \equiv a \pmod{p} \]
with \( n \) relatively prime to \( p - 1 \) and \( a \) relatively prime to \( p \), we fix an \( n' \) with
\[
nn' \equiv 1 \pmod{p-1}.
\]
Then we have
\[
x \equiv a^{n'} \pmod{p}.
\]

We now consider congruences modulo a prime power. We have the following proposition.

**Proposition 1.4.2.** Let \( p \) be a prime number different from 2. Then the group \( (\mathbb{Z}/p^m\mathbb{Z})^\times \) is cyclic of order \((p - 1)p^{m-1}\). The class of \( 1 + p \) has order \( p^{m-1} \) in \((\mathbb{Z}/p^m\mathbb{Z})^\times \). There is a primitive root modulo \( p \) whose class in \((\mathbb{Z}/p^m\mathbb{Z})^\times \) has order \( p - 1 \).

**Proof.** By mathematical induction over \( i = 0, 1, \ldots \) one establishes
\[
(1 + p)^{p^i} \equiv 1 + p^{i+1} \pmod{p^{i+2}}. \tag{1.4.5}
\]
From this it follows that
\[
(1 + p)^{p^{m-2}} \equiv 1 + p^{m-1} \pmod{p^m}
\]
and
\[
(1 + p)^{p^{m-1}} \equiv 1 \pmod{p^m}.
\]
Thus the class of \( 1 + p \) has order \( p^{m-1} \). It follows that the group \((\mathbb{Z}/p^m\mathbb{Z})^\times \) is cyclic.

Let \( g \) be a primitive root modulo \( p \). Then \( g' = g^{p^{m-1}} \) is likewise a primitive root, since
\[
g^{p^{m-1}} \equiv g \pmod{p}.
\]
Furthermore,
\[
g^{p^{m-1}} = g^{(p-1)p^{m-1}} \equiv 1 \pmod{p^m}.
\]

The congruence (1.4.5) does not hold for \( p = 2 \). For example, \( 3^2 \equiv 1 \pmod{8} \). Instead of (1.4.5) one has
\[
(1 + 4)^{2^i} \equiv 1 + 2^{i+2} \pmod{2^{i+3}}.
\]
We thus have the following proposition.

**Proposition 1.4.3.** For \( m \geq 3 \) the group \((\mathbb{Z}/2^m\mathbb{Z})^\times \) is a direct product of subgroups generated by the classes of \(-1 \) and \( 5 \). In particular, the order of the class of \( 5 \) in \((\mathbb{Z}/2^m\mathbb{Z})^\times \) is equal to \( 2^{m-2} \).
1.5. Public Key Cryptology

As an application we shall investigate “public key cryptology,” which is based on the present state of computational algorithms for factoring large numbers in a reasonable amount of time.

Let $M$ be a collection of individuals who wish to exchange coded information, where a given message should be able to be decoded only by the person to whom it is addressed.

To this end each participant $a \in M$ chooses a number $n_a$ that is the product of two prime numbers $p_a$ and $q_a$. The integer $n_a$ is available in a directory. However, the factorization $n_a = p_a q_a$ is known only to $a$. The directory entry for $a$ contains, in addition to $n_a$, a number $t_a$ chosen to be relatively prime to $\varphi(n_a)$.

The message to be sent is encoded by a public key into one or more natural numbers that are smaller than $n_a$.

A participant $b$ who wishes to send to $a$ a message encoded by the number $h$ sends $a$ the number $g \equiv h^{t_a} \pmod{n_a}$.

Only $a$ knows the number $u_a$ such that

$$t_a u_a \equiv 1 \pmod{\varphi(n_a)},$$

since to obtain it one must know the factorization $n_a = p_a \cdot q_a$.

Now $a$ computes $h$ by

$$g^{u_a} \equiv h^{t_a u_a} \equiv h \pmod{n_a}.$$

The last congruence is a result of the following lemma.

**Lemma 1.5.1.** Let $n = pq$ with unequal prime numbers $p$ and $q$. Furthermore, let $m$ be an integer with

$$m \equiv 1 \pmod{\varphi(n)}.$$ 

Then

$$h^m \equiv h \pmod{n}$$

for every integer $h$.

**Proof.** If $h$ is relatively prime to $n$, then the lemma follows from (1.4.2). If $h$ is divisible by $n$, then the result is trivial. Therefore, let $h$ be divisible by $p$ but not by $q$. Then

$$h^{q-1} \equiv 1 \pmod{q},$$

whence

$$h^{m-1} \equiv 1 \pmod{q}.$$
We multiply this congruence by $h$, thereby obtaining
\[ h^m \equiv h \pmod{qh} \]
and with it
\[ h^m \equiv h \pmod{n}. \]
The case where $h$ is divisible by $q$ but not by $p$ is handled the same way. □