Fundamentals of Number Theory

Emanuel Patterson

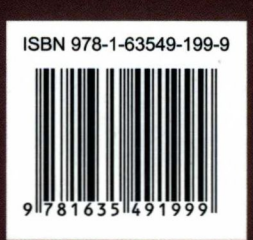
Larsen & Keller

Fundamentals of Number Theory

The branch of pure mathematics that is dedicated to study of integers is called number theory or arithmetic. Number theory studies the properties of prime numbers, rational numbers, and algebraic integers. This book elucidates the concepts and innovative models around prospective developments with respect to number theory. Such selected concepts that redefine this subject have been presented in it. It will provide comprehensive knowledge to the readers. Those in search of information to further their knowledge will be greatly assisted by this textbook. Coherent flow of topics, student-friendly language and extensive use of examples make this book an invaluable source of information.

Emanuel Patterson pursued his PhD. in Number Theory and Geometry form The University of Nottingham, United Kingdom. He has been awarded the "University Excellence in Teaching" award for his excellence in guiding students. Patterson works with various mathematical societies and his work focuses on algebraic integers, analytic number theory and Diophantine geometry. He has presented over 15 papers at international symposiums and conferences.

ISBN 978-1-63549-199-9



Larsen & Keller
www.larsen-keller.com

Patterson Fundamentals of Number Theory Larsen & Keller

Fundamentals of Number Theory

Edited by
Emanuel Patterson

Larsen & Keller
www.larsen-keller.com

Fundamentals of Number Theory
Edited by Emanuel Patterson
ISBN: 978-1-63549-199-9 (Hardback)

Larsen & Keller
Published by Larsen and Keller Education,
5 Penn Plaza,
19th Floor,
New York, NY 10001, USA

Cataloging-in-Publication Data

Fundamentals of number theory / edited by Emanuel Patterson
p. cm.
Includes bibliographical references and index.
ISBN 978-1-63549-199-9
1. Number theory. 2. Algebra. I. Patterson, Emanuel.
QA241 .F86 2017
512.7--dc23

The publisher's policy is to use permanent paper from mills that operate a sustainable forestry policy. Furthermore, the publisher ensures that the text paper and cover boards used have met acceptable environmental accreditation standards.

Printed and bound in China.

For more information regarding Larsen and Keller Education and its products, please visit the publisher's website www.larsen-keller.com

Fundamentals of Number Theory

Preface

The branch of pure mathematics that is dedicated to study of integers is called number theory or arithmetic. Number theory studies the properties of prime numbers, rational numbers, and algebraic integers. This book elucidates the concepts and innovative models around prospective developments with respect to number theory. Such selected concepts that redefine this subject have been presented in it. It will provide comprehensive knowledge to the readers. Those in search of information to further their knowledge will be greatly assisted by this textbook. Coherent flow of topics, student-friendly language and extensive use of examples make this book an invaluable source of information.

To facilitate a deeper understanding of the contents of this book a short introduction of every chapter is written below:

Chapter 1- Number theory is a branch of mathematics that concerns itself with the study of integers. They study prime numbers and also the properties of objects that are made of integers. The chapter on number theory offers an insightful focus, keeping in mind the subject matter.

Chapter 2- The two branches of number theory are analytic number theory and algebraic number theory. Analytic number theory focuses on the methods of mathematical analysis that is used to solve problems that are related to integers. This section is a compilation of the various branch of number theory that forms an integral part of the broader subject matter.

Chapter 3- A number is used to count and measure objects. Apart from counting and measuring, numbers are also used for codes and mathematical abstraction. This chapter also explains theories such as natural numbers, rational numbers, integers, prime numbers, real numbers and complex numbers. This section is an overview of the subject matter incorporating all the major aspects of numbers.

Chapter 4- Fraction represents a part of an entire object or a number. An example of a fraction would be 5/25 and ¾. Unit fraction, dyadic rational, repeating decimal, cyclic number and Egyptian fraction are the aspects elucidated in the following chapter.

Chapter 5- Some of the arithmetic operations explained in the section are algebraic operation, addition, subtraction, method of complements, multiplication and division. These operations are performed on numbers and variables. The topics elucidated in this chapter are of vital importance and provide a better understanding of arithmetic operations.

Chapter 6- Division algorithm calculates the quotient of two given integers N and D. Division algorithm falls under two major categories which are slow division and fast division. Multiplication algorithm, Euclidean algorithm, greatest common divisor, least common multiple and fundamental theorem of arithmetic are some of the aspects elucidated in the section. The chapter discusses the methods of division and multiplication algorithm in a critical manner providing key analysis to the subject matter.

I owe the completion of this book to the never-ending support of my family, who supported me throughout the project.

Editor

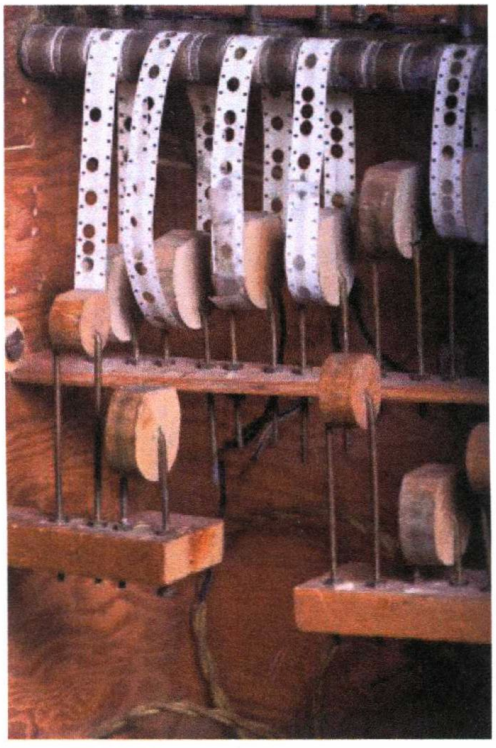
Table of Contents

1

Introduction to Number Theory

Number theory is a branch of mathematics that concerns itself with the study of integers. They study prime numbers and also the properties of objects that are made of integers. The chapter on number theory offers an insightful focus, keeping in mind the subject matter.

Number theory or, in older usage, arithmetic is a branch of pure mathematics devoted primarily to the study of the integers. It is sometimes called "The Queen of Mathematics" because of its foundational place in the discipline. Number theorists study prime numbers as well as the properties of objects made out of integers (e.g., rational numbers) or defined as generalizations of the integers (e.g., algebraic integers).



A Lehmer sieve, which is a primitive digital computer once used for finding primes and solving simple Diophantine equations.

Integers can be considered either in themselves or as solutions to equations (Diophantine geometry). Questions in number theory are often best understood through the study of analytical objects (e.g., the Riemann zeta function) that encode properties of the integers, primes or other number-theoretic objects in some fashion (analytic number theory). One may also study real numbers in relation to rational numbers, e.g., as approximated by the latter (Diophantine approximation).

The older term for number theory is *arithmetic*. By the early twentieth century, it had been superseded by "number theory". (The word "arithmetic" is used by the general public to mean "elemen-

tary calculations"; it has also acquired other meanings in mathematical logic, as in *Peano arithmetic*, and computer science, as in *floating point arithmetic*.) The use of the term *arithmetic* for *number theory* regained some ground in the second half of the 20th century, arguably in part due to French influence. In particular, *arithmetical* is preferred as an adjective to *number-theoretic*.

History

Origins

Dawn of Arithmetic

The first historical find of an arithmetical nature is a fragment of a table: the broken clay tablet Plimpton 322 (Larsa, Mesopotamia, ca. 1800 BCE) contains a list of "Pythagorean triples", i.e., integers (a,b,c) such that $a^2+b^2=c^2$. The triples are too many and too large to have been obtained by brute force. The heading over the first column reads: "The *takiltum* of the diagonal which has been subtracted such that the width..."

The Plimpton 322 tablet

The table's layout suggests that it was constructed by means of what amounts, in modern language, to the identity

$$\left(\frac{1}{2}\left(x-\frac{1}{x}\right)\right)^2+1=\left(\frac{1}{2}\left(x+\frac{1}{x}\right)\right)^2,$$

which is implicit in routine Old Babylonian exercises. If some other method was used, the triples were first constructed and then reordered by c/a, presumably for actual use as a "table", i.e., with a view to applications.

It is not known what these applications may have been, or whether there could have been any; Babylonian astronomy, for example, truly flowered only later. It has been suggested instead that the table was a source of numerical examples for school problems.

While Babylonian number theory—or what survives of Babylonian mathematics that can be called thus—consists of this single, striking fragment, Babylonian algebra (in the secondary-school sense of "algebra") was exceptionally well developed. Late Neoplatonic sources state that Pythagoras learned mathematics from the Babylonians. Much earlier sources state that Thales and Pythagoras traveled and studied in Egypt.

Euclid IX 21—34 is very probably Pythagorean; it is very simple material ("odd times even is even", "if an odd number measures [= divides] an even number, then it also measures [= divides] half of it"), but it is all that is needed to prove that $\sqrt{2}$ is irrational. Pythagorean mystics gave great importance to the odd and the even. The discovery that $\sqrt{2}$ is irrational is credited to the early Pythagoreans (pre-Theodorus). By revealing (in modern terms) that numbers could be irrational, this discovery seems to have provoked the first foundational crisis in mathematical history; its proof or its divulgation are sometimes credited to Hippasus, who was expelled or split from the Pythagorean sect. This forced a distinction between *numbers* (integers and the rationals—the subjects of arithmetic), on the one hand, and *lengths* and *proportions* (which we would identify with real numbers, whether rational or not), on the other hand.

The Pythagorean tradition spoke also of so-called polygonal or figurate numbers. While square numbers, cubic numbers, etc., are seen now as more natural than triangular numbers, pentagonal numbers, etc., the study of the sums of triangular and pentagonal numbers would prove fruitful in the early modern period (17th to early 19th century).

We know of no clearly arithmetical material in ancient Egyptian or Vedic sources, though there is some algebra in both. The Chinese remainder theorem appears as an exercise in Sun Zi's *Suan Ching*, also known as *The Mathematical Classic of Sun Zi* (3rd, 4th or 5th century CE.) (There is one important step glossed over in Sun Zi's solution: it is the problem that was later solved by Āryabhata's *kuṭṭaka*)

There is also some numerical mysticism in Chinese mathematics, but, unlike that of the Pythagoreans, it seems to have led nowhere. Like the Pythagoreans' perfect numbers, magic squares have passed from superstition into recreation.

Classical Greece and The Early Hellenistic Period

Aside from a few fragments, the mathematics of Classical Greece is known to us either through the reports of contemporary non-mathematicians or through mathematical works from the early Hellenistic period. In the case of number theory, this means, by and large, *Plato* and *Euclid*, respectively.

Plato had a keen interest in mathematics, and distinguished clearly between arithmetic and calculation. (By *arithmetic* he meant, in part, theorising on number, rather than what *arithmetic* or *number theory* have come to mean.) It is through one of Plato's dialogues—namely, *Theaetetus*—that we know that Theodorus had proven that $\sqrt{3}, \sqrt{5}, \ldots, \sqrt{17}$ are irrational. Theaetetus was, like Plato, a disciple of Theodorus's; he worked on distinguishing different kinds of incommensurables, and was thus arguably a pioneer in the study of number systems. (Book X of Euclid's Elements is described by Pappus as being largely based on Theaetetus's work.)

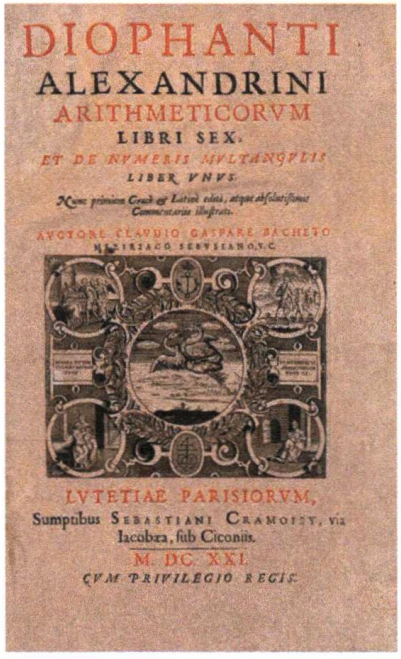
Euclid devoted part of his *Elements* to prime numbers and divisibility, topics that belong unambiguously to number theory and are basic to it (Books VII to IX of Euclid's Elements). In particular, he gave an algorithm for computing the greatest common divisor of two numbers (the Euclidean algorithm; *Elements*, Prop. VII.2) and the first known proof of the infinitude of primes (*Elements*, Prop. IX.20).

In 1773, Lessing published an epigram he had found in a manuscript during his work as a librarian; it claimed to be a letter sent by Archimedes to Eratosthenes. The epigram proposed what has

become known as Archimedes' cattle problem; its solution (absent from the manuscript) requires solving an indeterminate quadratic equation (which reduces to what would later be misnamed Pell's equation). As far as we know, such equations were first successfully treated by the Indian school. It is not known whether Archimedes himself had a method of solution.

Diophantus

Very little is known about Diophantus of Alexandria; he probably lived in the third century CE, that is, about five hundred years after Euclid. Six out of the thirteen books of Diophantus's *Arithmetica* survive in the original Greek; four more books survive in an Arabic translation. The *Arithmetica* is a collection of worked-out problems where the task is invariably to find rational solutions to a system of polynomial equations, usually of the form $f(x,y)=z^2$ or $f(x,y,z)=w^2$ $f(x_1,x_2,x_3)=0$. Thus, nowadays, we speak of *Diophantine equations* when we speak of polynomial equations to which rational or integer solutions must be found.


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
AVCTORE CLAVDIO GASPARE BACHETO
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via
Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

Title page of the 1621 edition of Diophantus' *Arithmetica*, translated into Latin by Claude Gaspard Bachet de Méziriac.

One may say that Diophantus was studying rational points — i.e., points whose coordinates are rational — on curves and algebraic varieties; however, unlike the Greeks of the Classical period, who did what we would now call basic algebra in geometrical terms, Diophantus did what we would now call basic algebraic geometry in purely algebraic terms. In modern language, what Diophantus did was to find rational parametrizations of varieties; that is, given an equation of the form (say) $f(x_1,x_2,x_3)=0$, his aim was to find (in essence) three rational functions g_1,g_2,g_3 such that, for all values of r and s,, setting $x_i=g_i(r,s)$ for $i=1,2,3$ gives a solution to $f(x_1,x_2,x_3)=0$.

Diophantus also studied the equations of some non-rational curves, for which no rational parametrisation is possible. He managed to find some rational points on these curves (elliptic curves, as it happens, in what seems to be their first known occurrence) by means of what amounts to a tangent construction: translated into coordinate geometry (which did not exist in Diophantus's time), his method would be visualised as drawing a tangent to a curve at a known rational point, and then finding the other point of intersection of the tangent with the curve; that other point is

a new rational point. (Diophantus also resorted to what could be called a special case of a secant construction.)

While Diophantus was concerned largely with rational solutions, he assumed some results on integer numbers, in particular that every integer is the sum of four squares (though he never stated as much explicitly).

Āryabhata, Brahmagupta, Bhāskara

While Greek astronomy probably influenced Indian learning, to the point of introducing trigonometry, it seems to be the case that Indian mathematics is otherwise an indigenous tradition; in particular, there is no evidence that Euclid's Elements reached India before the 18th century.

Āryabhata (476–550 CE) showed that pairs of simultaneous congruences $n \equiv a_1 \bmod m_1$, $n \equiv a_2 \bmod m_2$ could be solved by a method he called *kuṭṭaka*, or *pulveriser*; this is a procedure close to (a generalisation of) the Euclidean algorithm, which was probably discovered independently in India. Āryabhata seems to have had in mind applications to astronomical calculations.

Brahmagupta (628 CE) started the systematic study of indefinite quadratic equations—in particular, the misnamed Pell equation, in which Archimedes may have first been interested, and which did not start to be solved in the West until the time of Fermat and Euler. Later Sanskrit authors would follow, using Brahmagupta's technical terminology. A general procedure (the chakravala, or "cyclic method") for solving Pell's equation was finally found by Jayadeva (cited in the eleventh century; his work is otherwise lost); the earliest surviving exposition appears in Bhāskara II's Bīja-gaṇita (twelfth century).

Indian mathematics remained largely unknown in Europe until the late eighteenth century; Brahmagupta and Bhāskara's work was translated into English in 1817 by Henry Colebrooke.

Arithmetic in The Islamic Golden Age

Al-Haytham seen by the West: frontispice of *Selenographia*, showing Alhasen [*sic*] representing knowledge through reason, and Galileo representing knowledge through the senses.

In the early ninth century, the caliph Al-Ma'mun ordered translations of many Greek mathematical works and at least one Sanskrit work (the *Sindhind*, which may or may not be Brahmagupta's Brāhmasphuṭasiddhānta). Diophantus's main work, the *Arithmetica*, was translated into Arabic by Qusta ibn Luqa (820–912). Part of the treatise *al-Fakhri* (by al-Karajī, 953 – ca. 1029) builds on it to some extent. According to Rashed Roshdi, Al-Karajī's contemporary Ibn al-Haytham knew what would later be called Wilson's theorem.

Western Europe in The Middle Ages

Other than a treatise on squares in arithmetic progression by Fibonacci — who lived and studied in north Africa and Constantinople during his formative years, ca. 1175–1200 — no number theory to speak of was done in western Europe during the Middle Ages. Matters started to change in Europe in the late Renaissance, thanks to a renewed study of the works of Greek antiquity. A catalyst was the textual emendation and translation into Latin of Diophantus's *Arithmetica* (Bachet, 1621, following a first attempt by Xylander, 1575).

Early Modern Number Theory

Fermat

Pierre de Fermat (1601–1665) never published his writings; in particular, his work on number theory is contained almost entirely in letters to mathematicians and in private marginal notes. He wrote down nearly no proofs in number theory; he had no models in the area. He did make repeated use of mathematical induction, introducing the method of infinite descent.

Pierre de Fermat

One of Fermat's first interests was perfect numbers (which appear in Euclid, *Elements* IX) and amicable numbers; this led him to work on integer divisors, which were from the beginning among the subjects of the correspondence (1636 onwards) that put him in touch with the mathematical community of the day. He had already studied Bachet's edition of Diophantus carefully; by 1643, his interests had shifted largely to Diophantine problems and sums of squares (also treated by Diophantus).

Fermat's achievements in arithmetic include:

- Fermat's little theorem (1640), stating that, if a is not divisible by a prime p, then $a^{p-1} \equiv 1 \bmod p$.
- If a and b are coprime, then $a^2 + b^2$ is not divisible by any prime congruent to −1 modulo 4; and every prime congruent to 1 modulo 4 can be written in the form $a^2 + b^2$. These two statements also date from 1640; in 1659, Fermat stated to Huygens that he had proven the latter statement by the method of infinite descent. Fermat and Frenicle also did some work (some of it erroneous) on other quadratic forms.
- Fermat posed the problem of solving $x^2 - Ny^2 = 1$ as a challenge to English mathematicians (1657). The problem was solved in a few months by Wallis and Brouncker. Fermat considered their solution valid, but pointed out they had provided an algorithm without a proof (as had Jayadeva and Bhaskara, though Fermat would never know this.) He states that a proof can be found by descent.
- Fermat developed methods for (doing what in our terms amounts to) finding points on curves of genus 0 and 1. As in Diophantus, there are many special procedures and what amounts to a tangent construction, but no use of a secant construction.
- Fermat states and proves (by descent) in the appendix to *Observations on Diophantus* (Obs. XLV) that $x^4 + y^4 = z^4$ has no non-trivial solutions in the integers. Fermat also mentioned to his correspondents that $x^3 + y^3 = z^3$ has no non-trivial solutions, and that this could be proven by descent. The first known proof is due to Euler (1753; indeed by descent).

Fermat's claim ("Fermat's last theorem") to have shown there are no solutions to $x^n + y^n = z^n$ for all $n \geq 3$ (the only known proof of which is beyond his methods) appears only in his annotations on the margin of his copy of Diophantus; he never claimed this to others and thus would have had no need to retract it if he found any mistake in his supposed proof.

Euler

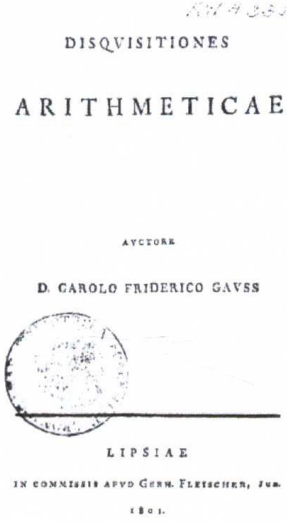
Leonhard Euler

The interest of Leonhard Euler (1707–1783) in number theory was first spurred in 1729, when a friend of his, the amateur Goldbach, pointed him towards some of Fermat's work on the subject.

This has been called the "rebirth" of modern number theory, after Fermat's relative lack of success in getting his contemporaries' attention for the subject. Euler's work on number theory includes the following:

- *Proofs for Fermat's statements.* This includes Fermat's little theorem (generalised by Euler to non-prime moduli); the fact that $p = x^2 + y^2$ if and only if $p \equiv 1 \bmod 4$; initial work towards a proof that every integer is the sum of four squares (the first complete proof is by Joseph-Louis Lagrange (1770), soon improved by Euler himself); the lack of non-zero integer solutions to $x^4 + y^4 = z^2$ (implying the case $n=4$ of Fermat's last theorem, the case $n=3$ of which Euler also proved by a related method).
- *Pell's equation*, first misnamed by Euler. He wrote on the link between continued fractions and Pell's equation.
- *First steps towards analytic number theory.* In his work of sums of four squares, partitions, pentagonal numbers, and the distribution of prime numbers, Euler pioneered the use of what can be seen as analysis (in particular, infinite series) in number theory. Since he lived before the development of complex analysis, most of his work is restricted to the formal manipulation of power series. He did, however, do some very notable (though not fully rigorous) early work on what would later be called the Riemann zeta function.
- *Quadratic forms.* Following Fermat's lead, Euler did further research on the question of which primes can be expressed in the form $x^2 + Ny^2$, some of it prefiguring quadratic reciprocity.
- *Diophantine equations.* Euler worked on some Diophantine equations of genus 0 and 1. In particular, he studied Diophantus's work; he tried to systematise it, but the time was not yet ripe for such an endeavour – algebraic geometry was still in its infancy. He did notice there was a connection between Diophantine problems and elliptic integrals, whose study he had himself initiated.

Lagrange, Legendre and Gauss


DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, JUN.

Carl Friedrich Gauss's Disquisitiones Arithmeticae, first edition