国外数学名著系列

（影印版）78

Graham Everest　Thomas Ward

An Introduction to Number Theory

数论导引

科学出版社

国外数学名著系列(影印版) 78

An Introduction to Number Theory

数论导引

Graham Everest Thomas Ward

科学出版社

北京

图字：01-2011-3333

图书在版编目(CIP)数据

数论导引= An Introduction to Number Theory /(英)埃弗里斯特(Everest, G.)等编著. —影印版. —北京: 科学出版社, 2011

(国外数学名著系列; 78)

ISBN 978-7-03-031386-7

I. ①数… II. ①埃… ②沃… III. ①数论-英文 IV. ①O156

中国版本图书馆 CIP 数据核字(2011) 第 105002 号

责任编辑:赵彦超 徐园园/责任印刷:钱玉芬/封面设计:陈 敬

科学出版社 出版
北京东黄城根北街16号
邮政编码:100717
http://www.sciencep.com
双青印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2011 年 6 月第 一 版 开本：B5(720 × 1000)
2011 年 6 月第一次印刷 印张：19 1/2
印数: 1—2 000 字数：370 000
定价：76.00 元
(如有印装质量问题，我社负责调换)

《国外数学名著系列》(影印版)序

要使我国的数学事业更好地发展起来，需要数学家淡泊名利并付出更艰苦地努力。另一方面，我们也要从客观上为数学家创造更有利的发展数学事业的外部环境，这主要是加强对数学事业的支持与投资力度，使数学家有较好的工作与生活条件，其中也包括改善与加强数学的出版工作。

从出版方面来讲，除了较好较快地出版我们自己的成果外，引进国外的先进出版物无疑也是十分重要与必不可少的。从数学来说，施普林格(Springer)出版社至今仍然是世界上最具权威的出版社。科学出版社影印一批他们出版的好的新书，使我国广大数学家能以较低的价格购买，特别是在边远地区工作的数学家能普遍见到这些书，无疑是对推动我国数学的科研与教学十分有益的事。

这次科学出版社购买了版权，一次影印了 23 本施普林格出版社出版的数学书，就是一件好事，也是值得继续做下去的事情。大体上分一下，这 23 本书中，包括基础数学书 5 本，应用数学书 6 本与计算数学书 12 本，其中有些书也具有交叉性质。 这些书都是很新的，2000 年以后出版的占绝大部分，共计 16 本，其余的也是 1990 年以后出版的。这些书可以使读者较快地了解数学某方面的前沿，例如基础数学中的数论、代数与拓扑三本，都是由该领域大数学家编著的“数学百科全书”的分册。对从事这方面研究的数学家了解该领域的前沿与全貌很有帮助。按照学科的特点，基础数学类的书以“经典”为主，应用和计算数学类的书以“前沿”为主。这些书的作者多数是国际知名的大数学家，例如《拓扑学》一书的作者诺维科夫是俄罗斯科学院的院士，曾获“菲尔兹奖”和“沃尔夫数学奖”。这些大数学家的著作无疑将会对我国的科研人员起到非常好的指导作用。

当然，23 本书只能涵盖数学的一部分，所以，这项工作还应该继续做下去。更进一步，有些读者面较广的好书还应该翻译成中文出版，使之有更大的读者群。

总之，我对科学出版社影印施普林格出版社的部分数学著作这一举措表示热烈的支持，并盼望这一工作取得更大的成绩。

王　元

2005 年 12 月 3 日

And he brought him forth abroad, and said, Look now toward heaven, and tell the stars, if thou be able to number them: and he said unto him, So shall thy seed be.

Genesis 15, verse 5

Contents

Introduction

This book is written from the perspective of several passionately held beliefs about mathematical education. The first is that mathematics is a good story. Theorems are not discovered in isolation, but happen as part of a culture, and they are generally motivated by paradigms. In this book we are going to show how one result from antiquity can be used to illuminate the study of much that forms the undergraduate curriculum in number theory at a typical U.K. university. The result is the Fundamental Theorem of Arithmetic. Our hope is that students will understand that number theory is not just a collection of tricks and isolated results but has a coherence fueled directly by a connected narrative that spans centuries.

The second belief is that mathematics students (and indeed professional mathematicians) come to the subject with different preferences and evolving strengths. Therefore, we have endeavored to present differing approaches to number theory. One way to achieve this is the obvious one of selecting material from both the algebraic and the analytic disciplines. Less obviously, in the early part of the book particularly, we sometimes present several different proofs of a single result. The aim is to try to capture the imagination of the reader and help her or him to discover his or her own taste in mathematics. The book is written under the assumption that students are being exposed to the power of analysis in courses such as complex variables, as well as the power of abstraction in courses such as algebra. Thus we use notions from finite group theory at several points to give alternative proofs. Often the resulting approaches simplify and promote generalization, as well as providing elegance. We also use this approach because we want to try to explain how different approaches to elementary results are worked out later in different approaches to the subject in general. Thus Euler's proof of the Fundamental Theorem of Arithmetic could be taken to prefigure the development of analytic number theory with its ingenious use of the Euler product Formula. When we move further into the analytic aspects of arithmetic, Euler's relatively simple observation may seem like a rather flimsy pretext. However, the view that many nineteenth-century mathematicians took of functions (complex func-

tions particularly) was profoundly influenced by the Fundamental Theorem of Arithmetic. In their view, many functions are factorizable objects, and we will try to illustrate this in describing some of the great achievements of that century.

Having spoken of different approaches, it will surprise few readers that number theory has many streams. A major surprise is the fact that some of these meet again: Chapter 11 shows that many of the themes in Chapters 1–10 become reconciled further on. The classical class number formula reconciles the analytic stream of ideas with the algebraic. We also discuss – necessarily in general terms – the L-function associated with an elliptic curve and the conjectures of Birch and Swinnerton-Dyer, which draw together the elliptic, algebraic and analytic streams. The underlying motif is the theory of L-functions. As we enter a new millennium, it has become clear that one of the ways into the deepest parts of number theory requires a better understanding of these fundamental objects.

The third belief is that number theory is a living subject, even when studied at an elementary level. The onset of electronic computing gave the subject an enormous boost, and it is a pleasure to be able to record some recent developments. The language of arithmetical complexity has helped to change the way we think about numbers. Modern computers can carry out calculations with numbers that are almost unimaginably large. We recommend that any reader unfamiliar with modern number theory packages tries a few experiments using some of the excellent free software available from the internet. To start to think of the issues raised by large integer calculation can be no bad thing. Intellectually too, this computational topic illustrates an interesting point about the enduring nature of the paradigm. Our story begins over two millennia ago, yet it is the same questions that continue to fascinate us. What are the primes like? Where can they be found? How can the prime factors of an integer be computed? Whether these questions will endure awhile longer nobody can tell. The history of these problems already presents a fascinating story worth telling, and one that says a lot about one of the most important and beautiful narratives of enquiry in human history – mathematics.

One of the most striking and pleasurable aspects of number theory is the extent of time and range of cultures over which it has been studied. We do not go into a detailed history of the developments described here, but the names and places given in the list of "Dramatis Personae" should give some idea of how widely number theory has been studied. The names in this list are rather crudely Anglicized and the locations somewhat arbitrarily modernized. The many living mathematicians who have made significant contributions to the topics covered here have been omitted but may be found on the Web site in [113]. A densely written, comprehensive review of number theory up to about 1920 may be found in Dickson's history [42], [43], [44]; a discursive and masterly account of the four millennia ending in 1798 is provided by Weil [157].

Finally, we say something about the way this book could be used. It is based on three courses taught at the University of East Anglia on various aspects of number theory (analytic, algebraic/geometric, and computational), mostly at the final-year undergraduate level. We were motivated in part by G. A. and J. M. Jones' attractive book [84]. Their book sets out to deal with the subject as it is actually taught. Typically, third-year students will not have done a course in number theory and their experience will necessarily be fragmentary. Like [84], our book begins in quite an elementary way. We have found that the different years at a university do not equate neatly with different abilities: Students in their early years can often be stretched well beyond what seems possible, and upper-level students do not complain about beginning in simple ways. We will try to show how different chapters can be put together to make a course; the book can be used as a basis for two upper-level courses and one at an intermediate level.

We thank many people for contributing to this text. Notable among them are Christian Röttger, for writing up notes from an analytic number theory course at UEA; Sanju Velani, for making available notes from his analytic number theory course; several cohorts of UEA undergraduates for feedback on lecture courses; Neal Koblitz and Joe Silverman for their inspiring books; and Elena Nardi for help with the ancient Greek in Section 1.7.1. We thank Karim Belabas, Robin Chapman, Sue Everest, Gareth and Mary Jones, Graham Norton, David Pierce, Peter Pleasants, Christian Röttger, Alice Silverberg, Shaun Stevens, Alan and Honor Ward, and others for pointing out errors and suggesting improvements. Errors and solecisms that remain are entirely the authors' responsibility.

February 14, 2005 Graham Everest
Norwich, UK Thomas Ward

Notation and terminology

"Arithmetic" is used both as a noun and an adjective. The particular notation used is collected at the start of the index. The symbols $\mathbb{N}$, $\mathbb{P}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ denote the natural numbers $\{1, 2, 3, \dots\}$, prime numbers $\{2, 3, 5, 7, \dots\}$, integers, rational numbers, real numbers, and complex numbers, respectively. Any field with $q = p^r$ elements, $p \in \mathbb{P}$ and $r \in \mathbb{N}$, is denoted $\mathbb{F}_q$, and $\mathbb{F}_q^*$ denotes its multiplicative group; the field $\mathbb{F}_p$, $p \in \mathbb{P}$, is identified with the set $\{0, 1, \dots, p-1\}$ under addition and multiplication modulo p. For a complex number $s = \sigma + it$, $\Re(s) = \sigma$ and $\Im(s) = t$ denote the real and imaginary parts of s respectively. The symbol $|$ means "divides", so for $a, b \in \mathbb{Z}$, $a|b$ if there is an integer k with $ak = b$. For any set X, $|X|$ denotes the cardinality of X. The greatest common divisor of a and b is written $\gcd(a, b)$. Products are written using $\cdot$ as in $12 = 3 \cdot 4$ or $n! = 1 \cdot 2 \cdots (n-1) \cdot n$. The order of growth of functions f, g (usually these are functions $\mathbb{N} \to \mathbb{R}$) is compared using the following notation:

$f \sim g$ if $\dfrac{f(x)}{g(x)} \longrightarrow 1$ as $x \to \infty$;

$f = \mathrm{O}(g)$ if there is a constant $A > 0$ with $f(x) \leqslant Ag(x)$ for all x;

$f = \mathrm{o}(g)$ if $\dfrac{f(x)}{g(x)} \longrightarrow 0$ as $x \to \infty$.

In particular, $f = \mathrm{O}(1)$ means that f is bounded. The relation $f = \mathrm{O}(g)$ will also be written $f \ll g$, particularly when it is being used to express the fact that two functions are commensurate, $f \ll g \ll f$. A sequence $a_1, a_2, \ldots$ will be denoted (a_n).

References

The references are not comprehensive, and material that is not explicitly cited is nonetheless well-known. It is inevitable that we have borrowed ideas and used them inadvertently without citation; we apologize for any egregious instances of this. The general references that are likely to be most accessible without much background are as follows. For Chapter 2, [147]; for Chapters 3 and 4, [77], [96], [147], and [154]; for Chapters 5–7, [27] and [143]; for Chapters 8–10, [4], [75], and [81]; for Chapter 9, [6]; and for Chapter 12, [21], [22], [36], [90], and [66].

Possible Courses

A course on analytic number theory could follow Chapters 1, 8, 9, and 10; one on Diophantine problems or elliptic curves could follow Chapters 1, 2, 5, 6, and 7. A lower-level course on algebraic number theory could be based on Chapters 1, 2, 3 and 4; one on complexity could be based on Chapters 1 and 12. (These could also be used for the complexity part of a course on cryptography.) The exercises are generally routine applications of the methods in the text, but exercises marked * are to be viewed as projects, some of them requiring further reading and research.

Dramatis Personae

Person	Date	Country
Pythagoras of Samos	569 B.C.–475 B.C.	Greece, Egypt
Euclid of Alexandria	325 B.C.–265 B.C.	Greece, Egypt
Eratosthenes of Cyrene	276 B.C.–194 B.C.	Libya, Greece, Egypt
Diophantus of Alexandria	200–284	Greece, Egypt
Hypatia of Alexandria	370–415	Egypt
Sun Zi	400–460	China
Brahmagupta	598–670	India
Abu Ali al-Hasan ibn al-Haytham	965–1040	Iraq, Egypt
Bhaskaracharya	1114–1185	India
Leonardo Pisano Fibonacci	1170–1250	Italy
Qin Jiushao	1202–1261	China
Pietro Antonio Cataldi	1548–1626	Italy
Claude Gaspar Bachet de Méziriac	1581–1638	France
Marin Mersenne	1588–1648	France
Pierre de Fermat	1601–1665	France
James Stirling	1692–1770	Scotland
Leonhard Euler	1707–1783	Switzerland, Russia
Joseph–Louis Lagrange	1736–1813	Italy, France
Lorenzo Mascheroni	1750–1800	Italy, France
Adrien-Marie Legendre	1752–1833	France
Jean Baptiste Joseph Fourier	1768–1830	France
Johann Carl Friedrich Gauss	1777–1855	Germany
Siméon Denis Poisson	1781–1840	France
August Ferdinand Möbius	1790–1868	Germany
Niels Henrik Abel	1802–1829	Norway
Carl Gustav Jacob Jacobi	1804–1851	Germany
Johann Peter Gustav Lejeune Dirichlet	1805–1859	France, Germany
Joseph Liouville	1809–1882	France
Ernst Eduard Kummer	1810–1893	Germany
Evariste Galois	1811–1832	France
Karl Theodor Wilhelm Weierstrass	1815–1897	Germany
Pafnuty Lvovich Tchebychef	1821–1894	Russia
Georg Friedrich Bernhard Riemann	1826–1866	Germany, Italy
François Edouard Anatole Lucas	1842–1891	France
Jules Henri Poincaré	1854–1912	France
David Hilbert	1862–1943	Germany
Srinivasa Aiyangar Ramanujan	1887–1920	India, England
Louis Joel Mordell	1888–1972	USA, England
Carl Ludwig Siegel	1896–1981	Germany
Emil Artin	1898–1962	Austria, Germany
Kurt Mahler	1903–1988	Germany, UK, Australia
Derrick Henry Lehmer	1905–1991	USA
André Weil	1906–1998	France, USA

1

A Brief History of Prime

Most of the results in this book grow out of one theorem that has probably been known in some form since antiquity.

Theorem 1.1. [FUNDAMENTAL THEOREM OF ARITHMETIC] *Every integer greater than* 1 *can be expressed as a product of prime numbers in a way that is unique up to order.*

For the moment, we are using the term *prime* in its most primitive form – to mean an irreducible integer greater than one. Thus a positive integer p is prime if $p > 1$ and the factorization $p = ab$ into positive integers implies that either $a = 1$ or $b = 1$. The expression "up to order" means simply that we regard, for example, the two factorizations $6 = 2 \cdot 3 = 3 \cdot 2$ as the same.

Theorem 1.1, the Fundamental Theorem of Arithmetic, will reverberate throughout the text. The fact that the primes are the building blocks for all integers already suggests they are worth particular study, rather in the way that scientists study matter at an atomic level. In this case, we need a way of looking for primes and methods to construct them, identify them, and even quantify their appearance if possible. Some of these quests took thousands of years to fulfill, and some are still works in progress. At the end of this chapter, we will give a proof of Theorem 1.1, but for now we want to get on with our main theme.

1.1 Euclid and Primes

The first consequence of the Fundamental Theorem of Arithmetic for the primes is that there must be infinitely many of them.

Theorem 1.2. [EUCLID] *There are infinitely many primes.*

To emphasize the diversity of approaches to number theory, we will give several proofs of this famous result.

EUCLID'S PROOF IN MODERN FORM. If there are only finitely many primes, we can list them as $p_1, \ldots, p_r$. Let

$$N = p_1 \cdots p_r + 1 > 1.$$

By the Fundamental Theorem of Arithmetic, N can be factorized, so it must be divisible by some prime p_k of our list. Since p_k also divides $p_1 \cdots p_r$, it must divide the difference

$$N - p_1 \cdots p_r = 1,$$

which is impossible, as $p_k > 1$. □

EULER'S ANALYTIC PROOF. Assume that there are only finitely many primes, so they may be listed as $p_1, \ldots, p_r$. Consider the product

$$X = \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right)^{-1}.$$

The product is finite since 1 is not a prime and by hypothesis there are only finitely many primes. Now expand each factor into a convergent geometric series,

$$\frac{1}{1 - \frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots.$$

For any fixed K, we deduce that

$$\frac{1}{1 - \frac{1}{p}} \geqslant 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^K}.$$

Putting this into the equation for X gives

$$\begin{aligned} X &\geqslant \left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^K}\right) \cdot \left(1 + \frac{1}{3} + \frac{1}{3^2} + \cdots + \frac{1}{3^K}\right) \\ &\quad \cdot \left(1 + \frac{1}{5} + \frac{1}{5^2} + \cdots + \frac{1}{5^K}\right) \cdots \left(1 + \frac{1}{p_r} + \frac{1}{p_r^2} + \cdots + \frac{1}{p_r^K}\right) \\ &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots \\ &= \sum_{n \in \mathcal{N}(K)} \frac{1}{n}, \end{aligned} \tag{1.1}$$

where

$$\mathcal{N}(K) = \{n \in \mathbb{N} \mid n = p_1^{e_1} \cdots p_r^{e_r}, e_i \leqslant K \text{ for all } i\}$$

denotes the set of all natural numbers with the property that each prime factor appears no more than K times. Notice that the identity (1.1) requires

the Fundamental Theorem of Arithmetic. Given any number $n \in \mathbb{N}$, if K is large enough, then $n \in \mathcal{N}(K)$, so we deduce that

$$X \geqslant \sum_{n=1}^{\infty} \frac{1}{n}.$$

The series on the right-hand side (known as the *harmonic series*) diverges to infinity, but X is finite. Again we have reached a contradiction from the assumption that there are finitely many primes. □

Let us recall why the harmonic series diverges to infinity. As with Theorem 1.2, there are many ways to prove this; the first is elementary, while the second compares the series with an integral.

ELEMENTARY PROOF. Notice that

$$\begin{aligned} 1 + \frac{1}{2} &\geqslant \frac{1}{2}, \\ \frac{1}{3} + \frac{1}{4} &\geqslant \frac{1}{2}, \\ \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} &\geqslant \frac{1}{2}, \end{aligned}$$

and so on. For any $k \geqslant 1$,

$$\frac{1}{2^k + 1} + \frac{1}{2^k + 2} + \cdots + \frac{1}{2^{k+1}} \geqslant 2^k \cdot \frac{1}{2^{k+1}} = \frac{1}{2}.$$

This means that

$$\sum_{n=1}^{2^{k+1}} \frac{1}{n} \geqslant \frac{k}{2} \text{ for all } k \geqslant 1,$$

and it follows that $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n}$ diverges. □

Hidden in the last argument is some indication of the *rate* at which the harmonic series diverges. Since the sum of the first 2^{k+1} terms exceeds $k/2$, the sum of the first N terms must be approximately $C \log N$ for some positive constant C. The second proof improves on this: Equation (1.2) gives a sharper lower bound as well as an upper bound.

Exercise 1.1. Try to prove that $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^2}$ diverges using the same technique of grouping terms together. Of course, this will not work since this series converges, but you will see something mildly interesting. In particular, can you use this to estimate the sum?