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, they 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 UK 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 fuelled 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 endeavoured 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 her or his 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 do this 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 might seem like a rather flimsy pretext. However, the view that many 19th Century mathematicians took of functions (complex functions 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 current of ideas with the algebraic. We also discuss – necessarily in general terms – the L-function associated to 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. 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 a while 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 on p. XV 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 [110]. 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 millenia ending in 1798 is provided by Weil [154].

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. & J.M. Jones' attractive book [81]. 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 their book, ours begins in quite an elementary way. We have found that the different years at 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 these 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 & Mary Jones, Graham Norton, Peter Pleasants, Christian Röttger, Alice Silverberg, Shaun Stevens, Alan & Honor Ward and others for pointing out errors and suggesting improvements. Errors and solecisms that remain are entirely the authors' responsibility.

Graham Everest & Thomas Ward
School of Mathematics
University of East Anglia
Norwich
g.everest@uea.ac.uk, t.ward@uea.ac.uk

Notation and terminology

'Arithmetic' is used both as noun and adjective. Particular notation used is collected at the start of the index. The symbols $\mathbb{N} = \{1, 2, 3, \ldots\}$, $\mathbb{P}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ denote the natural numbers, prime numbers, 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 $\{0, 1, \ldots, p-1\}$ under addition and multiplication modulo p. For a complex number $s = a+\mathrm{i}b$, $\Re(s) = a$ and $\Im(s) = b$ denote the real and imaginary parts of s respectively. The symbol $\Big|$ means 'divides', so for $a, b \in \mathbb{Z}$, $a\Big|b$ 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:

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

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

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

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, [140]. For Chapters 3 and 4, [74], [93], [140] and [147]. For Chapters 5–7, [27] and [136]. For Chapters 8–10, [4], [72] and [78]. For Chapter 9, [6]. For Chapter 12, [21], [22], [36], [87] and [152].

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 (this 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 personæ

Pythagoras of Samos	569 BC–475 BC	Greece, Egypt
Euclid of Alexandria	325 BC–265 BC	Greece, Egypt
Eratosthenes of Cyrene	276 BC–194 BC	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
Godfrey Harold Hardy	1877–1947	England
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