Universitext

Universitext

Universitext is a series of textbooks that presents material from a wide variety of mathematical disciplines at master's level and beyond. The books, often well class-tested by their author, may have an informal, personal, even experimental approach to their subject matter. Some of the most successful and established books in the series have evolved through several editions, always following the evolution of teaching curricula, into very polished texts.

Thus as research topics trickle down into graduate-level teaching, first textbooks written for new, cutting-edge courses may make their way into *Universitext*.

For further volumes:
www.springer.com/series/223

Olivier Bordellès

Arithmetic Tales

Translated by Véronique Bordellès

Springer

Olivier Bordellès
allée de la Combe 2
Aiguilhe, France

Translator
Véronique Bordellès
allée de la Combe
Aiguilhe, France

Translation from the French language edition:
Thèmes d'Arithmétiques
by Olivier Bordellès

www.editions-ellipses.fr/

ISSN 0172-5939 ISSN 2191-6675 (electronic)
Universitext
ISBN 978-1-4471-4095-5 ISBN 978-1-4471-4096-2 (eBook)
DOI 10.1007/978-1-4471-4096-2
Springer London Heidelberg New York Dordrecht

Library of Congress Control Number: 2012940391

Mathematics Subject Classification: 11-01, 11A, 11L07, 11M06, 11N05, 11N13, 11N25, 11N37, 11R04, 11R09, 11R11, 11R16, 11R18, 11R21, 11R27, 11R29, 11R42

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

"Mathematical science is the queen of sciences, and arithmetic is the queen of mathematics", Gauss said. Indeed, number theory is the study of whole numbers, also called positive integers, the first ones we learn at school. Thus, the theory of numbers deals with problems that are often both easy to understand and very hard to solve. For instance, one of the most famous number theory problems is *Fermat's last theorem*, abbreviated as FLT, stating that the *Fermat equation* $x^n + y^n = z^n$, where x, y, z are positive integers and $n \geqslant 3$ is an integer, has no solution. This proof came from Andrew Wiles in 1995, after more than 350 years of efforts from many mathematicians, such as Ernst Kummer, Sophie Germain, André Weil, Jean-Pierre Serre, Gerd Faltings, Kenneth Ribet and Yves Hellegouarch.

The author's initial aim was simply to have his book entitled *Thèmes d'Arithmétique*, published in 2006 by Ellipses eds, translated into English. But things turned out differently as what you are holding here is an extended, more complete version of the French edition. Not only have the chapters doubled in size but many exercises, all of them with complete solutions, have been added and, more importantly, the sections called *Further Developments* included in each chapter have been significantly enlarged.

Each chapter is divided into three parts. The course itself is suitable for undergraduates. As for the exercises, they either illustrate the course or are designed as springboards for approaching other related topics. Finally, the section Further Developments introduces trickier notions and even occasionally topics that researchers are familiar with. Many results are proved and whenever the proof goes beyond the scope of the book, the reader is cross-referred to the standard sources and references in the subject area. The book includes among other things an almost exhaustive exposition of the recent *discrete Hardy–Littlewood method* developed by Enrico Bombieri, Martin Huxley, Henryk Iwaniec, Charles Mozzochi and Nigel Watt, applications of Vaughan's famous identity, a historico-mathematical introduction to the class field theory together with a detailed illustration of the contribution of analytic tools to the tricky problems of algebraic number theory, such as obtaining upper bounds for class numbers or lower bounds for discriminants and regulators of algebraic number fields.

The first two chapters are intended to supply the main basic tools an undergraduate student should have a good grasp of to acquire the necessary grounding for subsequent work. The emphasis is on summation formulae such as Abel and Euler–MacLaurin summations that are unavoidable in modern number theory.

Chapter 3 is devoted to the study of prime numbers, from the beginning with Euclid's work to modern analysis relating the distribution of primes to the non-trivial zeros of the Riemann zeta-function. A fairly complete account of Chebyshev's benchmarking method is given, along with totally explicit estimates for the usual prime number functions.

Chapter 4 extends the analysis of the previous chapter by dealing with multiplicative functions. A large number of these are given, their average order most of the time being studied in detail through the Möbius inversion formula and through some basic results in summation methods. A complete study of the Dirichlet series from an arithmetic viewpoint is supplied. Furthermore, some estimates for other types of summation are investigated, such as multiplicative functions over short segments or additive functions. Finally, a brief account of Selberg's sieve and the large sieve is also given.

The study of the local law of a certain class of multiplicative functions requires counting the number of points with integer coordinates very near smooth plane curves. The aim of Chap. 5 is to provide some nice results of the theory in a very intricate, but elementary[1] way. The methods of Martin Huxley and Patrick Sargos and Michael Filaseta and Ognian Trifonov are completely investigated to show how some clever combinatorial ideas, introduced in the 1950s essentially by Heini Halberstam, Klaus Roth and Hans-Egon Richert, and in the 1970s by Sir Henry Peter Francis Swinnerton-Dyer, may lead to very good results which appear to be well beyond the scope of any current exponential-sums method.

As can be seen with the famous Dirichlet divisor problem, many questions in analytic number theory reduce to estimate certain exponential sums. Chapter 6 is devoted to the theory of such sums, following the lines of van der Corput's method, eventually leading to its A- and B-processes and, after some rearrangements by Eric Phillips, to the exponent-pairs method, systematically used nowadays. Historically, three methods were developed independently in the 1920s: among other things, Hermann Weyl treated exponential sums with polynomials, Johannes Gualtherus van der Corput extended Weyl's ideas to quasi-monomial functions combining the Poisson summation formula and the stationary phase method, and Ivan Matveevich Vinogradov's work dealt with counting the number of solutions of certain tricky Diophantine systems. This chapter could be viewed as an analytic equivalent to Chap. 5.

Finally, Chap. 7 is an introduction to algebraic number theory, which arose from both a generalization of the arithmetic in $\mathbb{Z}$ and the necessity to solve certain Diophantine equations. Although the idea of using a larger field than $\mathbb{Q}$ was already known at that time, the theory really took off in the 19th century, and among the

[1] Note that the word "elementary" means only that the complex analysis is not used.

founding fathers the names of Ernst Kummer, Richard Dedekind, David Hilbert, Leopold Kronecker and Hermann Minkowski may be mentioned. The chapter is aimed at showing that the *ideal numbers* were the right tool to restore unique factorization. Furthermore, the reader is invited to compare the major results, such as the fundamental theorem of ideal theory or the zero-free region of the Dedekind zeta-function, with the corresponding ones from Chap. 3.

Aiguilhe, France Olivier Bordellès

Acknowledgements

When writing this book, I was helped in many crucial ways.

Thanks must first go to my long-suffering wife, who among other things provided invaluable help in translating the French edition into English.

It is also my delight to acknowledge the help of the following colleagues whose careful reading of the manuscript was expertly done and who suggested numerous improvements on preliminary drafts of this book: Guy Bénat, Jean-Jacques Galzin, Roger Mansuy, Bruno Martin, Landry Salle and Patrick Sargos.

Last but not least, I am gratefully indebted to the Springer staff for trustfully accepting this project. Among them I would like to thank especially Lauren Stoney for her very efficient support.

Olivier Bordellès

Notation

General Notation

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are respectively the sets of integers, rational numbers, real numbers and complex numbers. If $a \in \mathbb{Z}$, we may also adopt the notation $\mathbb{Z}_{\geqslant a}$ of all integers $n \geqslant a$. When $a = 1$, the corresponding set is usually denoted[1] by $\mathbb{N}$. Finally, if p is a prime number, $\mathbb{F}_p$ is the finite field with p elements.

Letters n, m and a, b, c, d, k, l, r, ... refer to integers, whereas p indicates a prime number.

$a \mid b$ means a divides b, i.e. there exists $k \in \mathbb{Z}$ such that $b = ka$. Similarly, $a \nmid b$ means a does not divide b.

$a \mid b^\infty$ means $p \mid a \Longrightarrow p \mid b$.

$p^k \parallel n$ means $p^k \mid n$ and $p^{k+1} \nmid n$.

$P^+(n)$ is the greatest prime factor of $n \in \mathbb{Z}_{\geqslant 2}$, with the convention $P^+(1) = 1$. This symbol is sometimes abbreviated as $P(n)$.

(a, b) and $[a, b]$ are respectively the greatest common divisor and the least common multiple of a and b. We set the gcd and lcm of three positive integers in the same way, as for instance

$$(a, b, c) = \big((a, b), c\big)$$

and extend this definition by induction to a finite number of positive integers.

For any positive integer n, the number $n! = 1 \times 2 \times \cdots \times n$ is the factorial of n, with the convention that $0! = 1$.

For any $x \in \mathbb{R}$, $[x]$ is the integer part[2] of x, the unique integer verifying

$$x - 1 < [x] \leqslant x$$

[1] This is a difference between Anglo-Saxon countries and France where the symbol $\mathbb{N}$ denotes the set of *non-negative* integers, sometimes denoted by $\mathbb{N}_0$ in the UK and the US. The aim of the notation $\mathbb{Z}_{\geqslant a}$ is then to avoid any risk of confusion, so that in this book $\mathbb{N} = \mathbb{Z}_{\geqslant 1}$ and $\mathbb{Z}_{\geqslant 0}$ is the set of non-negative integers.

[2] Some authors also use the *floor* and the *ceiling* functions, denoted respectively by $\lfloor x \rfloor$ and $\lceil x \rceil$, but there will be no need to make such a distinction in this book.

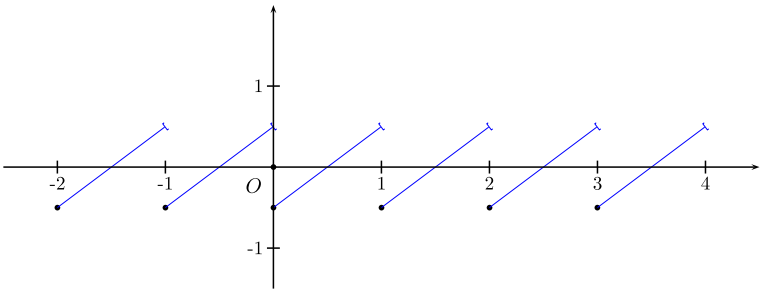

Fig. 1 Function ψ

and $\lfloor x \rceil$ is the nearest integer to x. The notation $\{x\}$ means the fractional part of x defined by $\{x\} = x - [x]$. Hence, for any $x \in \mathbb{R}$, we have

$$0 \leqslant \{x\} < 1.$$

We will also make use of the functions

$$\psi(x) = \{x\} - \frac{1}{2} \quad \text{and} \quad \psi_2(x) = \int_0^x \psi(t)\,\mathrm{d}t = \frac{\psi(x)^2}{2} - \frac{1}{8}.$$

The function ψ, see Fig. 1, called the *first Bernoulli function*, is an odd, 1-periodic function and then admits a Fourier series development. Since $\psi_2(0) = \psi_2(1) = 0$, the function ψ_2 is also 1-periodic and then bounded. Furthermore, it is not difficult to check that

$$\big|\psi(x)\big| \leqslant \frac{1}{2} \quad \text{and} \quad -\frac{1}{8} \leqslant \psi_2(x) \leqslant 0.$$

The distance of a real number x to its nearest integer is written $\|x\|$. Hence we have

$$\|x\| = \min\left(\frac{1}{2} + \psi(x), \frac{1}{2} - \psi(x)\right).$$

$\log x$ is the natural logarithm and e^x or $\exp x$ is the exponential function. It is also convenient to define the functions $e(x) = e^{2\pi i x}$ and $e_a(x) = e(x/a) = e^{2\pi i x/a}$.

If $\mathcal{E}$ is a finite set of integers, $|\mathcal{E}|$ is the number of elements belonging to $\mathcal{E}$.

Sums and Products

If $N \geqslant 1$ is any integer, we set

$$\sum_{n=1}^{N} f(n) = f(1) + f(2) + \cdots + f(N)$$

whilst

$$\sum_{p\leqslant N} f(p) = f(2) + f(3) + f(5) + \cdots$$

where the latest summation runs through prime numbers $p \leqslant N$. The two sums are related thanks to the following characteristic function of primes

$$\mathbf{1}_{\mathbb{P}}(n) = 1 + \left[\frac{2-\tau(n)}{n}\right] = \begin{cases} 1, & \text{if } n \text{ is prime} \\ 0, & \text{otherwise} \end{cases}$$

where $\tau(n)$ counts the number of positive divisors of n (see Chap. 4), so that

$$\sum_{p\leqslant N} f(p) = \sum_{n=2}^{N} \mathbf{1}_{\mathbb{P}}(n) f(n).$$

If $x \geqslant 1$ is a real number, then by convention

$$\sum_{n\leqslant x} f(n) = \sum_{n=1}^{[x]} f(n) \quad \text{and} \quad \sum_{p\leqslant x} f(p) = \sum_{p\leqslant [x]} f(p).$$

Certain sums run through some special subsets of $\mathbb{Z}$. For instance

$$\sum_{d|N} f(d)$$

means that the sum is taken over the positive divisors of N, e.g.

$$\sum_{d|15} f(d) = f(1) + f(3) + f(5) + f(15) \quad \text{and} \quad \sum_{p|15} f(p) = f(3) + f(5).$$

These examples are also valid for the products. For instance

$$\prod_{p\leqslant x} f(p) = f(2) \times f(3) \times f(5) \times \cdots$$

where the product runs through all prime numbers $p \leqslant [x]$.

It is important to note that, in all cases, the index p means a sum or a product running through prime numbers exclusively.

Functions

Let $a < b$ be real numbers and k be a non-negative integer. The notation $f \in C^k[a,b]$ means that f is a real-valued function k-times differentiable on $[a,b]$ and

$f^{(k)}$ is also continuous on $[a, b]$. By convention, $f^{(0)} = f$, $f^{(1)} = f'$, $f^{(2)} = f''$ and $f^{(3)} = f'''$.

Let $x \longmapsto f(x)$ and $x \longmapsto g(x)$ be functions defined for all sufficiently large x and $a, b > 0$.

- ▹ *Landau.* $f(x) = O(g(x))$, also sometimes written as $g = O(f)$, means that $g > 0$ and that there exist a real number x_0 and a constant $c_0 > 0$ such that, for all $x \geqslant x_0$, we have
$$\big|f(x)\big| \leqslant c_0 g(x).$$
For instance, $f(x) = O(1)$ means that f is bounded for all $x \in [x_0, +\infty[$.
- ▹ *Vinogradov.* $f(x) \ll g(x)$ is equivalent to $f(x) = O(g(x))$.
- ▹ *Titchmarsh.* $a \asymp b$ means that there exist $c_2 \geqslant c_1 > 0$ such that $c_1 b \leqslant a \leqslant c_2 b$. If a, b represent two functions f and g, then $f \asymp g$ is equivalent to $f \ll g$ and $g \ll f$.
- ▹ *Landau.* $f(x) = o(g(x))$ for $x \longrightarrow x_0$ means that $g \neq 0$ and
$$\lim_{x \to x_0} \frac{f(x)}{g(x)} = 0.$$
- ▹ *Landau.* $f(x) \sim g(x)$ for $x \longrightarrow x_0$ means that $g \neq 0$ and
$$\lim_{x \to x_0} \frac{f(x)}{g(x)} = 1.$$

An *asymptotic estimate* for the function f is a relation of the shape $f(x) \sim g(x)$. An *asymptotic formula* for f means a relation of the form $f(x) = g(x) + O(r(x))$, or equivalently $f(x) - g(x) = O(r(x))$, where $g(x)$ is called the *main term* and $O(r(x))$ is an *error term*. Obviously, such a relation is only meaningful if the error term $r(x)$ is of smaller order than $g(x)$. Otherwise, this relation is equivalent to $f(x) = O(r(x))$, so that the estimate is only an *upper bound*.

It is important to understand the difference between $f \asymp g$ and $f \sim g$. The first relation is less precise than the second one but can be used in a larger range. For instance, the Chebyshev estimates from Corollary 3.45 assert that
$$\pi(x) \asymp \frac{x}{\log x}$$
for all $x \geqslant 5$ while the Prime Number Theorem (Theorem 3.85), which was proved some forty years later, implies that
$$\pi(x) \sim \frac{x}{\log x}$$
as soon as $x \longrightarrow \infty$.

Finally, it should be mentioned that the constants implied in some error terms of the form $f(x) \ll g(x)$ depend sometimes on extra parameters. For instance, it is proven in Exercise 2 in Chap. 3 that
$$\tau(n) \ll n^{\varepsilon}$$

where the implied constant depends on $\varepsilon > 0$. This means that, for all $\varepsilon > 0$, there exists a constant $c(\varepsilon) > 0$ depending on $\varepsilon > 0$ such that, for all $n \geqslant 1$, we have $\tau(n) \leqslant c(\varepsilon) n^{\varepsilon}$. Such a situation[3] is sometimes denoted by

$$\tau(n) \ll_{\varepsilon} n^{\varepsilon}.$$

[3] It can be shown that $c(\varepsilon) = \exp(2^{1/\varepsilon}/\log 2^{\varepsilon})$ is admissible.

Contents