Problem Books in Mathematics

Edited by P. R. Halmos

D.P. Parent

Exercises in Number Theory

D.P. Parent

A Pseudonym for

D. Barsky F. Bertrandias G. Christol
A. Decomps H. Delange J.-M. Deshouillers
K. Gérardin J. Lagrange J.-L. Nicolas
M. Pathiaux G. Rauzy M. Waldschmidt

Exercises in Number Theory

Springer-Verlag
New York Berlin Heidelberg Tokyo

Series Editor
Paul R. Halmos
Department of Mathematics
Indiana University
Bloomington, IN 47405
U.S.A.

AMS Classification: 00A07, 12-01, 10-01

Library of Congress Cataloging in Publication Data
Parent, D. P.
Exercises in number theory.
(Problem books in mathematics)
Translation of: Exercises de théorie des nombres.
Bibliography: p.
Includes indexes.
1. Numbers, Theory of--Problems, exercises, etc.
I. Title. II. Series.
QA241.P2913 1984 512'.7 84-16056

Title of the original French edition: *Exercices de théorie des nombres*, © BORDAS, Paris, 1978.

Printed and bound by R.R. Donnelley & Sons, Harrisonburg, Virginia.
Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN 0-387-96063-5 Springer-Verlag New York Berlin Heidelberg Tokyo
ISBN 3-540-96063-5 Springer-Verlag Berlin Heidelberg New York Tokyo

Problem Books in Mathematics

Edited by P. R. Halmos

Problem Books in Mathematics

Series Editor: P.R. Halmos

Unsolved Problems in Intuitive Mathematics, Volume I: Unsolved Problems in Number Theory
by *Richard K. Guy*
1981. xviii, 161 pages. 17 illus.

Theorems and Problems in Functional Analysis
by *A.A. Kirillov* and *A.D. Gvishiani*
1982. ix, 347 pages. 6 illus.

Problems in Analysis
by *Bernard Gelbaum*
1982. vii, 228 pages. 9 illus.

A Problem Seminar
by *Donald J. Newman*
1982. viii, 113 pages.

Problem-Solving Through Problems
by *Loren C. Larson*
1983. xi, 344 pages. 104 illus.

Demography Through Problems
by *N. Keyfitz* and *J.A. Beekman*
1984. viii, 141 pages. 22 illus.

Problem Book for First Year Calculus
by *George W. Bluman*
1984. xvi. 384 pages. 384 illus.

Exercises in Integration
by *Claude George*
1984. x. 550 pages. 6 illus.

Exercises in Number Theory
by *D.P. Parent*
1984. x. 541 pages.

Preface

After an eclipse of some 50 years, Number Theory, that is to say the study of the properties of the integers, has regained in France a vitality worthy of its distinguished past. More and more researchers have been attracted by problems which, though it is possible to express in simple statements, whose solutions require all their ingenuity and talent. In so doing, their work enriches the whole of mathematics with new and fertile methods.

To be in a position to tackle these problems, it is necessary to be familiar with many specific aspects of number theory. These are very different from those encountered in analysis or geometry. The necessary know-how can only be acquired by studying and solving numerous problems. Now it is very easy to formulate problems whose solutions, while sometimes obvious, more often go beyond current methods. Moreover, there is no doubt that, even more than in other disciplines, in mathematics one must have exercises available whose solutions are accessible. This is the objective realised by this work. It is the collaborative work of several successful young number theorists. They have drawn these exercises from their own work, from the work of their associated research groups as well as from published work. Without running through all the areas in number theory, which

would have been excessive, the exercises given here deal with those directions that now appear most important. The solutions are rarely easy, but this book always gives a method to solve them. The appearance of this volume is gratefully welcomed. To all those who have made the effort to delve into the problems proposed here, it will solidify their attachment to the theory of numbers.

Ch. Pisot

Introduction

This book is the work of a group of mathematicians, including a large number of participants from the Seminaire Delange-Pisot-Poitou. It was written as follows: first many exercises were collected, mostly from university examinations. Then a choice was made, and they were grouped so as to constitute 10 chapters arranged in a random order. Certain important areas in number theory, notably the area of Diophantine Equations, have been left out.

Many books on number theory have appeared recently in France, among them those of Y. Amice, A. Blanchard, W.J. Ellison and M. Mendes-France, G. Rauzy, P. Samuel, J.P. Serre and M. Waldschmidt (see the bibliography). Readers of these books will find here supplementary and illustrative material. Conversely, a neophyte mathematician, who is curious about, say, p-adic anaylsis, or distributions modulo 1, after having been interested by certain attractive exercises, will have a strong motive for learning the theory. A part of our problems are accessible to a reader at the level of good second or third year students of a university. The introduction of each chapter is there to recall the definitions and principal theorems that one will need.

On behalf of the authors, I would like to thank those who have aided us, either by suggesting problems or in making up the solutions: J.P. Borel, P. Cassou-Nogues, H. Cohen, P. Damey, F. Dress, A. Durand, J. Fresnel, E. Helsmoortel, J. Martinet, B. de Mathan, M. Mendes-France, M. Mignotte, J.J. Payan, J. Queyrut, G. Revuz, G. Rhin, M.F. Vigneras. We would equally like to thank the Mathematical Society of France which helped in the publication of the original version of this book.

J.L. Nicolas

While reading the proofs of this introduction, I learned of the death of Professor Charles Pisot. All the contributors of this book dedicate this English translation to his memory.

Contents

CHAPTER 1

Prime Numbers: Arithmetic Functions: Selberg's Sieve

INTRODUCTION

1.1 PRIME NUMBERS

With x a real number and $x \geqslant 0$, we *denote* by $\pi(x)$ the *NUMBER OF PRIME NUMBERS NOT EXCEEDING* x and we set

$$\vartheta(x) = \sum_{p \leqslant x} \log p.$$

The essential result in the theory of prime numbers is the following:

THEOREM: (Prime Number Theorem): *When* $x \to +\infty$

$$\pi(x) \sim \frac{x}{\log x}.$$

This relation is equivalent to:

$$\vartheta(x) \sim x$$

(as will be seen in Exercise 1·3*).*

In fact, results quite a bit more precise than this are known (cf., for example, [E11]).

We will also give estimates for certain quantities related to

the primes, notably the sum $\sum_{p\leq x} \frac{1}{p}$ and the product $\prod_{p\leq x} \left(1 - \frac{1}{p}\right)$, for which we have the celebrated *MERTENS' FORMULA*:

$$\prod_{p\leq x} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log x} \qquad (x \to +\infty),$$

where γ is Euler's constant (cf., Exercises 1·5 and 1·6).

1.2 A FREQUENTLY USEFUL LEMMA

The following Lemma is often useful, in particular for the evaluation of the sum $\sum_{p\leq x} \frac{1}{p}$ mentioned above.

LEMMA: *Let E be a set of real numbers such that for every real t, $E \cap (-\infty, t]$ is empty or finite.*

Let g be a real or complex function defined on E, and let

$$G(t) = \sum_{\substack{u\in E \\ u\leq t}}{}' g(u)$$

If F is a C^1 function on the closed interval $[a,b]$, then

$$\sum_{\substack{u\in E \\ a<u\leq b}} F(u)g(u) = F(b)G(b) - F(a)G(a) - \int_a^b G(t)F'(t)dt.$$

This formula is obtained immediately after noticing that for all $u \in E$ such that $a < u \leq b$ we have:

$$F(b)g(u) - F(u)g(u) = \int_a^b g(u)Y(t-u)F'(t)dt,$$

where

$$Y(x) = \begin{cases} 0 & \text{for } x < 0, \\ 1 & \text{for } x \geq 0, \end{cases}$$

and adding.

In fact, this is the formula for integrating by parts the Stieltjes integral $\int_a^b F(t)\mathrm{d}G(t)$, which is equal to the sum $\sum_{\substack{u\in E\\ a<u\leqslant b}} F(u)g(u)$ (cf., [Wid]). It is the best way to remember it.

We have

$$\int_a^b F(t)\mathrm{d}G(t) = F(b)G(b) - F(a)G(a) - \int_a^b G(t)F'(t)\mathrm{d}t.$$

EXAMPLE: Let $E=\mathbb{N}^*$, $g(u)=1$, $[a,b]=[1,x]$, $F(t)=\frac{1}{t}$. We have:

$$\sum_{1<n\leqslant x}\frac{1}{n} = \int_1^x \frac{1}{t}\,\mathrm{d}[t] = \frac{[x]}{x} - 1 + \int_1^x \frac{[t]}{t^2}\,\mathrm{d}t$$

$$= \log x - \frac{x-[x]}{x} - \int_1^x \frac{t-[t]}{t^2}\,\mathrm{d}t,$$

whence

$$\sum_{n\leqslant x}\frac{1}{n} = \log x + 1 - \int_1^{+\infty}\frac{t-[t]}{t^2}\,\mathrm{d}t - \frac{x-[x]}{x} + \int_x^{+\infty}\frac{t-[t]}{t^2}\,\mathrm{d}t$$

$$= \log x + \gamma + \eta(x),$$

where

$$\gamma = 1 - \int_1^{+\infty}\frac{t-[t]}{t^2}\,\mathrm{d}t \quad\text{and}\quad |\eta(x)| \leqslant \frac{1}{x}.$$

1.3 IDEA OF AN ARITHMETIC FUNCTION: THE USUAL ARITHMETIC FUNCTIONS

Any real or complex function defined on $\mathbb{N}^*$ is called an *ARITHMETIC FUNCTION*.

Usually, we consider functions for which $f(n)$ is determined

from arithmetic properties of the integer n.

Some classical examples are the following:

$d(n)$ = *NUMBER OF DIVISORS* of n;

$\sigma(n)$ = *SUM OF THE DIVISORS* of n;

$\varphi(n)$ = *number of integers* m *such that* $1 \leqslant m \leqslant n$ *and* $(m,n) = 1$ (*EULER'S* TOTIENT *FUNCTION*);

$\nu(n)$ = *NUMBER OF* PRIME *DIVISORS* of n;

$\Omega(n)$ = *TOTAL NUMBER OF FACTORS* in the decomposition of n into *prime* factors;

($\Omega(1) = 0$ and, if $n = q_1^{\alpha_1}q_2^{\alpha_2}\cdots q^{\alpha_k}$, where $q_1,q_2,\ldots,q_k$ are prime numbers and $\alpha_1,\alpha_2,\ldots,\alpha_k$ are some integers greater than zero, $\Omega(n) = \alpha_1 + \alpha_2 + \cdots + \alpha_k$).

$$\lambda(n) = (-1)^{\Omega(n)} \qquad (\textit{LIOUVILLE'S FUNCTION})$$

Other examples are:

$$\mu(n) = \begin{cases} (-1)^{\nu(n)} & \text{if } n \text{ is divisible by the square of no prime number,} \\ 0 & \text{in the opposite case;} \end{cases}$$

the *MÖBIUS FUNCTION*, and *VON MANGOLDT'S FUNCTION* Λ defined by:

$$\Lambda(n) = \begin{cases} \log p \text{ if } n = p^k \text{ with } p \text{ a prime number and } k \geqslant 1, \\ 0 \quad \text{if } n \text{ is not of that form.} \end{cases}$$

We shall *denote* by z the *function which is identically one on the integers*, and *denote* by i the *identity mapping of* $\mathbb{N}^*$ *onto* $\mathbb{N}^*$.

1.4 ADDITIVE FUNCTIONS AND MULTIPLICATIVE FUNCTIONS

An arithmetic function is called an *ADDITIVE FUNCTION* if:

$$f(mn) = f(m) + f(n) \quad \textit{whenever } (m,n) = 1. \tag{1}$$

This clearly implies that $f(1) = 0$.

Furthermore, if $n_1, n_2, \ldots, n_k$ *are pairwise relatively prime*, then:

$$f(n_1 n_2 \cdots n_k) = f(n_1) + f(n_2) + \cdots + f(n_k).$$

The functions ν *and* Ω *are additive.* The function log clearly *is as well.*

A function f is called a *MULTIPLICATIVE FUNCTION* if

$$f(1) = 1$$

and

$$f(mn) = f(m)f(n) \quad \textit{whenever } (m,n) = 1. \tag{2}$$

(The condition $f(1) = 1$, ignored by certain authors, serves only to avoid considering as multiplicative the function that is identically zero).

If f is multiplicative and if $n_1, n_2, \ldots, n_k$ are pairwise relatively prime, then:

$$f(n_1 n_2 \cdots n_k) = f(n_1)f(n_2)\cdots f(n_k).$$

The functions $d, \sigma, \varphi, \lambda, \mu$ *are multiplicative.* It is obvious that z *and* i *are as well.*

PROPOSITION: *An additive or multiplicative function is completely determined by its values on the powers of the primes.*

In fact, if $n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$, where $q_1, q_2, \ldots, q_k$ are distinct

prime numbers and $\alpha_1,\alpha_2,\ldots,\alpha_k$ are integers greater than zero, then:

$$f(n) = f(q_1^{\alpha_1}) + f(q_2^{\alpha_2}) + \cdots + f(q_k^{\alpha_k}) \quad \text{if } f \text{ is additive,}$$

$$f(n) = f(q_1^{\alpha_1})f(q_2^{\alpha_2})\cdots f(q_k^{\alpha_k}) \quad \text{if } f \text{ is multiplicative,}$$

which can be written more concisely as:

$$f(n) = \sum_{p^r \| n} f(p^r) \quad \text{or} \quad f(n) = \prod_{p^r \| n} f(p^r).$$

We see, moreover, that *there exists exactly one additive function and one multiplicative function taking given values on the powers of the prime numbers.*

A function f is a *COMPLETELY ADDITIVE FUNCTION* if:

$$f(mn) = f(m) + f(n),$$

for arbitrary m and n, and not only when $(m,n) = 1$

Thus the function Ω is *completely additive.*

A function f is a *COMPLETELY MULTIPLICATIVE FUNCTION* if:

$$f(1) = 1 \quad \text{and} \quad f(mn) = f(m)f(n),$$

for all m and n.

A completely additive or completely multiplicative function is determined by its values on the prime numbers, for,

$$f(p^r) = rf(p) \quad \text{or} \quad f(p^r) = (f(p))^r,$$

respectively.