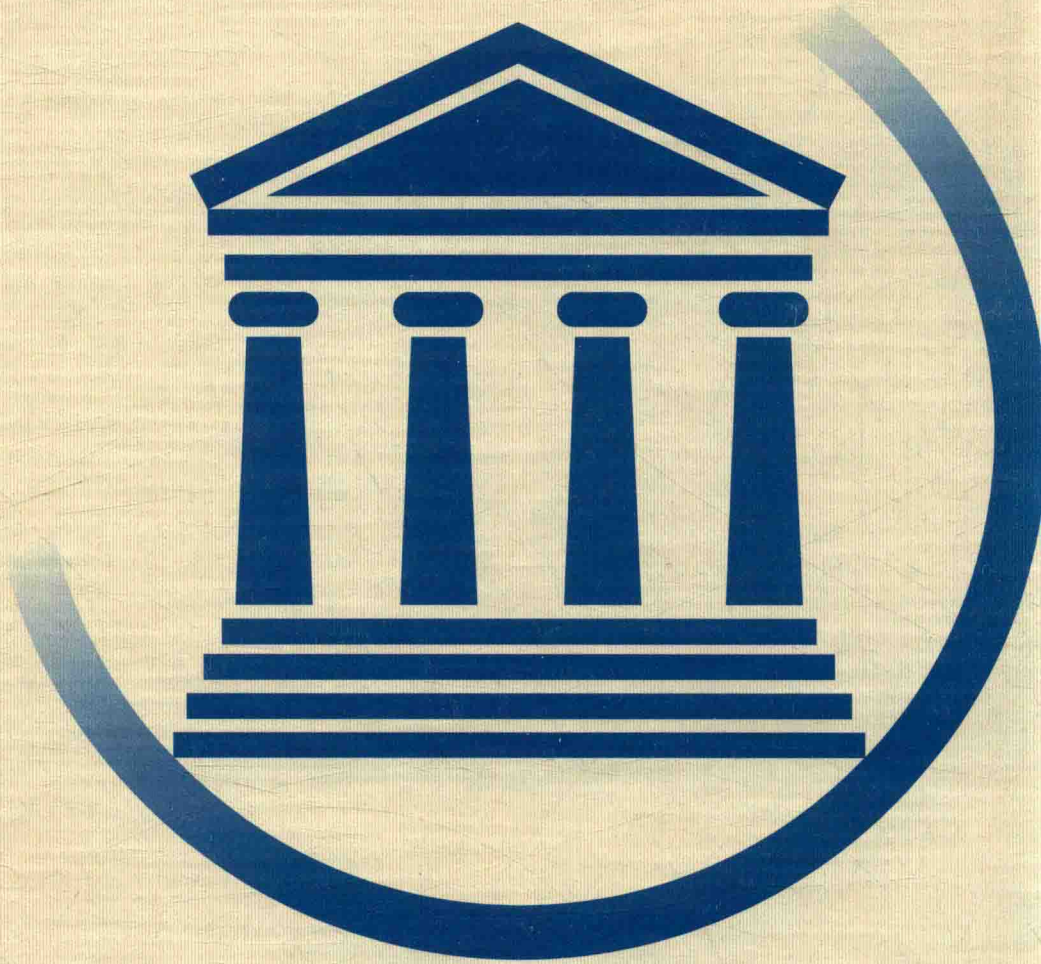
美国数学会经典影印系列

AMS
AMERICAN MATHEMATICAL SOCIETY

1001 Problems in Classical Number Theory

经典数论中的1001个问题

Jean-Marie De Koninck, Armel Mercier
Translated by Jean-Marie De Koninck



高等教育出版社

美国数学会经典影印系列

AMS
AMERICAN MATHEMATICAL SOCIETY

1001 Problems in Classical Number Theory

经典数论中的1001个问题

Jean-Marie De Koninck, Armel Mercier
Translated by Jean-Marie De Koninck

高等教育出版社·北京

图字：01-2016-2531 号

经典数论中的
1001 个问题

Jingdian Shulun zhong de
1001 ge Wenti

图书在版编目 (CIP) 数据

经典数论中的 1001 个问题 = 1001 Problems in Classical Number Theory : 英文 / (加) 让 - 玛利 · 德 · 科尼克，(加) 阿梅尔 · 莫西尔 (Armel Mercier) 著 . — 影印本 . — 北京 : 高等教育出版社 , 2017.4
ISBN 978-7-04-046999-8
Ⅰ. ①经… Ⅱ. ①让… ②阿… Ⅲ. ①数论—英文
Ⅳ. ①O156
中国版本图书馆 CIP 数据核字 (2016) 第 326761 号

策划编辑 李 鹏　　责任编辑 李 鹏
封面设计 张申申　　责任印制 赵义民

出版发行 高等教育出版社
社址 北京市西城区德外大街 4 号
邮政编码 100120
购书热线 010-58581118
咨询电话 400-810-0598
网址 http://www.hep.edu.cn
http://www.hep.com.cn
网上订购 http://www.hepmall.com.cn
http://www.hepmall.com
http://www.hepmall.cn
印刷 北京中科印刷有限公司

开本 787mm × 1092mm 1/16
印张 22.25
字数 550 千字
版次 2017 年 4 月第 1 版
印次 2017 年 4 月第 1 次印刷
定价 135.00 元

美国数学会经典影印系列

出版者的话

近年来，我国的科学技术取得了长足进步，特别是在数学等自然科学基础领域不断涌现出一流的研究成果。与此同时，国内的科研队伍与国外的交流合作也越来越密切，越来越多的科研工作者可以熟练地阅读英文文献，并在国际顶级期刊发表英文学术文章，在国外出版社出版英文学术著作。

然而，在国内阅读海外原版英文图书仍不是非常便捷。一方面，这些原版图书主要集中在科技、教育比较发达的大中城市的大型综合图书馆以及科研院所的资料室中，普通读者借阅不甚容易；另一方面，原版书价格昂贵，动辄上百美元，购买也很不方便。这极大地限制了科技工作者对于国外先进科学技术知识的获取，间接阻碍了我国科技的发展。

高等教育出版社本着植根教育、弘扬学术的宗旨服务我国广大科技和教育工作者，同美国数学会（American Mathematical Society）合作，在征求海内外众多专家学者意见的基础上，精选该学会近年出版的数十种专业著作，组织出版了“美国数学会经典影印系列”丛书。美国数学会创建于1888年，是国际上极具影响力的专业学术组织，目前拥有近30000会员和580余个机构成员，出版图书3500多种，冯·诺依曼、莱夫谢茨、陶哲轩等世界级数学大家都是其作者。本影印系列涵盖了代数、几何、分析、方程、拓扑、概率、动力系统等所有主要数学分支以及新近发展的数学主题。

我们希望这套书的出版，能够对国内的科研工作者、教育工作者以及青年学生起到重要的学术引领作用，也希望今后能有更多的海外优秀英文著作被介绍到中国。

高等教育出版社

2016年12月

À ma mère qui m'a montré le chemin.

À Daphnée, un rayon de soleil dans ma vie.

Preface

Number theory is one of the few areas of mathematics for which most problems can be understood by just about anyone, or at least by all those who are familiar with very basic notions of algebra, combinatorics and analysis. Every teacher knows the importance of practicing problem solving: indeed it turns out to be a great way to learn how to reason, no matter the area of mathematics the problems come from. Number theory is quite appropriate for this kind of exercise. For these reasons, a collection of problems in elementary or classical number theory seems in our opinion to be a complementary pedagogical tool for any learning process in mathematics. Moreover, a clever choice of problems can greatly help to raise the curiosity of those who try to solve them.

Unfortunately, very few books are entirely dedicated to problems in number theory. These include the classical work of the great master W. Sierpinski entitled *250 Problems in Elementary Number Theory* and published in Varsovie in 1970, a book which is not well known and unfortunately out of print. Hence, our manuscript does fill an important gap in this area and moreover it has the advantage of having been written to reach a large audience. One can also see it as a practical complement of an earlier book of the authors, that is *Introduction à la théorie des nombres* published by MODULO (2nd edition, 1997), or to any other introductory book in number theory.

Nevertheless, we must admit that our main motivation for writing this book has been our passion for number theory, namely this branch of mathematics which distinguishes itself by its beauty and its numerous mysteries, by its simplicity and its complexity, that is from the proof that there are infinitely many primes to the recently established proof of Fermat's Last Theorem.

This book obviously contains many problems from elementary number theory. Some of these are well known and can be found here and there in introductory books in number theory, while others are not so common. This is namely the case of several problems which we picked from the lesser known manuscript of Sierpinski mentioned above. Our book also contains some problems submitted to the readers of three well known journals: *American Mathematical Monthly*, *Mathematics Magazine* and *The College Mathematics Journal*. Finally, our book contains some 300 new problems never published before.

The choice of problems is obviously subjective; hence, it is no coincidence that the section on arithmetical functions is the longest! In any event, an effort has been made to cover, or at least brush, each of the classical themes of elementary number theory. On the other hand, since more and more students now have to

use computers and software to do mathematics, our book can certainly help them in this task. Indeed, many of the problems encourage the reader to use computer software and at times, while searching for a solution, indicate how to write the program that will bring about the solution to the problem.

Although most problems presented here use basic results which can be found in just about any elementary book in number theory, we chose to include a section which provides the basic definitions and the main theorems one needs to handle the various subjects covered in the book. This "tool box" has the advantage that the reader does not have to search here and there for the basic notions needed to solve the problems. Finally, we found it convenient to include in this section a list of the main arithmetic functions with their definitions, as well as a list of the constants and symbols most frequently used in the text.

Our presentation is as follows: the first section provides the basic theory relevant for the understanding and the resolution of the stated problems; the second section gathers the statements of the problems; while the third section lists all the solutions. At the end of the book, the reader will find a bibliography, a terminology index and an index of authors.

We want to thank all those who, by their remarks and suggestions, contributed to the realization of this manuscript. In particular, our thanks go to Jean-Lou De Carufel (Québec), Nicolas Doyon (Québec), David Gill (Québec), Jacques Grah (Québec), Nicolas Guay (Québec), Aleksandar Ivić (Belgrade), Imre Kátai (Budapest), Claude Levesque (Québec), Marc-Hubert Nicole (Québec), Erik Pronovost (Québec) and Guy Robin (Limoges).

Part of this work was done in 2003 and 2004 while the first author was on sabbatical in Tucson, Arizona. This author is grateful to the Department of Mathematics of the University of Arizona, in particular to Professor William Yslas Velez, for making this possible.

Jean-Marie De Koninck

Armel Mercier

Contents

Distribution of the Problems according to Their Topics

Part 1

Key Elements from the Theory

Notations

Let $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ stand respectively for the set of positive integers (also called natural numbers), the set of integers, the set of rational numbers, the set of real numbers and the set of complex numbers.

Unless indicated otherwise,

- the letters $a, b, c, d, i, j, k, \ell, m, n, r$ and s stand for integers,
- the letters p and q stand for prime numbers,
- the letters $p_1, p_2, p_3, p_4, p_5, p_6, p_7, \ldots$ represent the sequence of prime numbers $2, 3, 5, 7, 11, 13, 17, \ldots$,
- by twin primes, we mean a pair of prime numbers $\{p, q\}$ such that $q = p+2$.

Given an integer $n \geq 2$, we often write

$$n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r}$$

for its *canonical representation* as a product of distinct prime powers: here the q_i's are the primes dividing n written in increasing order and the exponents α_i's are positive integers (see Theorem 11).

Some Classical Forms of Argument

THEOREM 1 (Induction Principle). *Let S be a set of natural numbers having the following two properties:*

(i) $1 \in S$,

(ii) *if $k \in S$, then $k + 1 \in S$.*

Then $S = \mathbb{N}$.

THEOREM 2 (Pigeonhole Principle). *If more than n objects are distributed amongst n boxes, then one of the boxes must contain at least two objects.*

THEOREM 3 (Inclusion-Exclusion Principle). *Let A be a set containing N elements and let $P_1, P_2, \ldots, P_r$ be distinct properties that each element of A must satisfy. If $n(P_{i_1}, P_{i_2}, \ldots, P_{i_k})$ stands for the number of elements of A having all the properties $P_{i_1}, P_{i_2}, \ldots, P_{i_k}$, then the number of elements of A having none of the r properties is equal to*

$$N - \Big(n(P_1) + n(P_2) + \cdots + n(P_r)\Big) + \Big(n(P_1, P_2) + n(P_1, P_3) + \cdots + n(P_{r-1}, P_r)\Big)$$
$$- \Big(n(P_1, P_2, P_3) + n(P_1, P_2, P_4) + \cdots + n(P_{r-2}, P_{r-1}, P_r)\Big) + \cdots$$
$$+ (-1)^r n(P_1, P_2, \ldots, P_r).$$

Inequalities

THEOREM 4 (Cauchy-Schwarz Inequality). *Let $a_1, a_2, \ldots, a_n$, $b_1, b_2, \ldots, b_n$ be real numbers. Then*

$$\left(\sum_{i=1}^{n} a_i b_i\right)^2 \leq \sum_{i=1}^{n} a_i^2 \sum_{i=1}^{n} b_i^2.$$

THEOREM 5 (Arithmetic-Geometric Means Inequality). *Let $a_1, a_2, \ldots, a_n$ be positive real numbers. Then*

$$(a_1 a_2 \ldots a_n)^{1/n} \leq \frac{a_1 + a_2 + \cdots + a_n}{n},$$

with equality if and only if $a_1 = a_2 = \ldots = a_n$.

Divisibility

DEFINITION 1 (Binomial Coefficients). *Let n be a positive integer and k an integer satisfying $0 \leq k \leq n$. We define the binomial coefficient $\binom{n}{k}$ by*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!},$$

where $0! = 1$ and $n! = n(n-1)\cdots 3 \cdot 2 \cdot 1$.

THEOREM 6 (Binomial Theorem). *Let $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$. Then*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

In particular, it follows from Theorem 6 that

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = (1-1)^n = 0 \quad \text{and} \quad \sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n.$$

DEFINITION 2. *Let $a, b \in \mathbb{Z}$ with $a \neq 0$. We say that a divides b if there exists an integer c such that $b = ac$, in which case we write $a|b$ and say that a is a divisor of b. If a does not divide b, we write $a \nmid b$. In the case where $a|b$ and $1 \leq a < b$, we shall say that a is a proper divisor of b. We write $p^\alpha \| n$ to mean that $p^\alpha | n$ while $p^{\alpha+1}$ does not divide n.*

THEOREM 7 (Euclidean Division). *Let $a, b \in \mathbb{Z}$, $a > 0$. Then, there exist integers q and r such that $b = aq + r$, where $0 \leq r < a$. Moreover, if a does not divide b, then $0 < r < a$.*

DEFINITION 3 (Greatest Common Divisor). *Let $a, b \in \mathbb{Z} \setminus \{0\}$. The greatest common divisor (or GCD) of a and b, denoted by (a, b), is the unique positive integer d satisfying the following two conditions:*

$$(i)\ d|a \text{ and } d|b, \qquad (ii)\ \text{if } c|a \text{ and } c|b, \text{ then } c \leq d.$$

Similarly, if $a_1, a_2, \ldots, a_r \in \mathbb{Z} \setminus \{0\}$, the GCD of $a_1, a_2, \ldots, a_r$, denoted by $(a_1, a_2, \ldots, a_r)$, is the unique positive integer d satisfying the following two conditions:

$$(i)\ d|a_1,\ d|a_2,\ \ldots,\ d|a_r, \qquad (ii)\ \text{if } c|a_1,\ c|a_2,\ \ldots,\ c|a_r, \text{ then } c \leq d.$$

THEOREM 8. *Let $a_1, a_2, \ldots, a_r \in \mathbb{Z}\setminus\{0\}$. Then there exist integers $x_1, x_2, \ldots, x_r$ such that $(a_1, a_2, \ldots, a_r) = a_1 x_1 + a_2 x_2 + \cdots + a_r x_r$.*

THEOREM 9. *Let $a, b \in \mathbb{Z}$ be such that $ab \neq 0$. Let d be a positive integer. Then*

$$d = (a, b) \iff \begin{cases} d|a \text{ and } d|b, \\ c|a \text{ and } c|b \Rightarrow c|d. \end{cases}$$

THEOREM 10 (Euclid's Algorithm). *Let $a, b \in \mathbb{Z}$, $a > 0$. Applying successively the euclidean division (Theorem 7), we obtain the sequence of equalities*

$$\begin{aligned} b &= aq_1 + r_1, & 0 < r_1 < a, \\ a &= r_1 q_2 + r_2, & 0 < r_2 < r_1, \\ r_1 &= r_2 q_3 + r_3, & 0 < r_3 < r_2, \\ &\vdots \\ r_{j-2} &= r_{j-1} q_j + r_j, & 0 < r_j < r_{j-1}, \\ r_{j-1} &= r_j q_{j+1}, \end{aligned}$$

where $r_j = (a, b)$.

DEFINITION 4. *The integers $a_1, a_2, \ldots, a_r$ are said to be relatively prime if $(a_1, a_2, \ldots, a_r) = 1$, while they are said to be pairwise coprime if $(a_i, a_j) = 1$ when $i \neq j$.*

DEFINITION 5 (Lowest Common Multiple). *Let $a_1, a_2, \ldots, a_r \in \mathbb{Z} \setminus \{0\}$. The lowest common multiple (or LCM) of $a_1, a_2, \ldots, a_r$, denoted by $[a_1, a_2, \ldots, a_r]$, is the smallest positive integer amongst all the common multiples of $a_1, a_2, \ldots, a_r$.*

Prime Numbers

THEOREM 11 (Fundamental Theorem of Arithmetic). *Each integer $n \geq 2$ can be written as a product of prime numbers, and this representation is unique, apart from the order in which the prime factors appear. In particular, n can be written in the form*

$$n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r},$$

where the q_i's are distinct prime numbers and where the α_i's are positive integers.

THEOREM 12. *If $q_1, q_2, \ldots, q_r$ are prime numbers and if $a = \prod_{i=1}^{r} q_i^{\alpha_i}$ and $b = \prod_{i=1}^{r} q_i^{\beta_i}$, with $\alpha_i \geq 0$ and $\beta_i \geq 0$ for $i = 1, 2, \ldots, r$, then*

$$(a, b) = \prod_{i=1}^{r} q_i^{\min(\alpha_i, \beta_i)} \qquad \text{and} \qquad [a, b] = \prod_{i=1}^{r} q_i^{\max(\alpha_i, \beta_i)}.$$

Similarly, if $a = \prod_{i=1}^{r} q_i^{\alpha_i}$, $b = \prod_{i=1}^{r} q_i^{\beta_i}$, $c = \prod_{i=1}^{r} q_i^{\gamma_i}$ with $\alpha_i \geq 0$, $\beta_i \geq 0$ and $\gamma_i \geq 0$ for $i = 1, 2, \ldots, r$, then

$$(a, b, c) = \prod_{i=1}^{r} q_i^{\min\{\alpha_i, \beta_i, \gamma_i\}} \quad \text{and} \quad [a, b, c] = \prod_{i=1}^{r} q_i^{\max\{\alpha_i, \beta_i, \gamma_i\}}.$$

THEOREM 13 (Euclid's Theorem). *There exist infinitely many prime numbers.*

THEOREM 14 (Dirichlet's Theorem). *Given two positive integers a and b with $(a, b) = 1$, the sequence of numbers $an + b$, $n = 1, 2, \ldots$, contains infinitely many prime numbers.*

THEOREM 15 (Bertrand's Postulate). *For each positive integer n, there exists a prime number p satisfying $n < p \leq 2n$.*

THEOREM 16. *The series $\sum_p 1/p$ and the product $\prod_p \left(1 + \frac{1}{p}\right)$, where in each case p runs through the set of all prime numbers, both diverge.*

THEOREM 17 (Prime Number Theorem). *Let $\pi(x)$ be the number of prime numbers $\leq x$. Then*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

THEOREM 18 (Mertens' Theorem). *As $x \to \infty$,*

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

where γ is Euler's constant defined by $\gamma = \lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k} - \log n\right)$.

Congruences

DEFINITION 6. *Let $a, b, m \in \mathbb{Z}$, $m \neq 0$. We say that a is congruent to b modulo m, and we write $a \equiv b \pmod{m}$, if $m|a-b$; if a is not congruent to b modulo m, we write $a \not\equiv b \pmod{m}$.*

THEOREM 19. *Let $a, b, c, d, m \in \mathbb{Z}$, $m > 0$. Then*

(1) $a \equiv a \pmod{m}$;
(2) $a \equiv b \pmod{m}$ *if and only if* $b \equiv a \pmod{m}$;
(3) *if* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$, *then* $a \equiv c \pmod{m}$;
(4) *if* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $ac \equiv bd \pmod{m}$ *and* $ax + cy \equiv bx + dy \pmod{m}$ *for all* $x, y \in \mathbb{Z}$;
(5) *if* $a \equiv b \pmod{m}$ *and* $d|m$, $d > 0$, *then* $a \equiv b \pmod{d}$.

THEOREM 20. *Let $a, m, m_1, m_2, \ldots, m_r \in \mathbb{N}$ and $x, y \in \mathbb{Z}$. Then*

(i) $ax \equiv ay \pmod{m}$ *if and only if* $x \equiv y \pmod{m/(a,m)}$;
(ii) *if* $ax \equiv ay \pmod{m}$ *and* $(a, m) = 1$, *then* $x \equiv y \pmod{m}$;
(iii) $x \equiv y \pmod{m_i}$ *for* $i = 1, 2, \ldots, r$ *if and only if*

$$x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}.$$

DEFINITION 7 (Residue modulo m). *If $x \equiv y \pmod{m}$, then y is called a residue of x modulo m. A set of integers $\{y_1, y_2, \ldots, y_m\}$ is called a complete residue system modulo m if for each integer x there exists one and only one y_i such that $x \equiv y_i \pmod{m}$.*

DEFINITION 8 (Reduced residue system). *A reduced residue system modulo m is a set of integers r_i such that $(r_i, m) = 1$, $r_i \not\equiv r_j \pmod{m}$ when $i \neq j$, and such that each integer x relatively prime to m is congruent to a certain r_i modulo m.*

DEFINITION 9 (Euler's function). *The Euler ϕ function is defined by*

$$\phi(n) = \#\{0 < m \leq n \mid (n, m) = 1\}.$$

THEOREM 21 (Fermat's Little Theorem). *Let p be a prime number and a a positive integer such that p does not divide a. Then $a^{p-1} \equiv 1 \pmod{p}$. Moreover, given any integer a, $a^p \equiv a \pmod{p}$.*

THEOREM 22 (Euler's Theorem). *Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}$ be such that $(a, m) = 1$. Then*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$