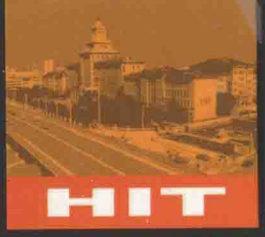

HIT

国外优秀数学著作
原 版 系 列

Number Theory

数论

[波] W. 纳尔凯维奇 (W. Narkiewicz) 著

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

国外优秀数学著作
原版系列

Number Theory
数论

●[波] W. 纳尔凯维奇 (W. Narkiewicz) 著

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

黑版贸审字 08-2017-097 号

图书在版编目(CIP)数据

数论:英文/(波)W. 纳尔凯维奇(W. Narkiewicz)著.
—哈尔滨:哈尔滨工业大学出版社,2018.1
书名原文:NUMBER THEORY
ISBN 978-7-5603-6941-9

Ⅰ.①数… Ⅱ.①W… Ⅲ.①数论-高等学校-教材-英文 Ⅳ.①O156

中国版本图书馆 CIP 数据核字(2017)第 224786 号

策划编辑 刘培杰
责任编辑 张永芹 聂兆慈
封面设计 孙茵艾
出版发行 哈尔滨工业大学出版社
社 址 哈尔滨市南岗区复华四道街 10 号 邮编 150006
传 真 0451-86414749
网 址 http://hitpress.hit.edu.cn
印 刷 哈尔滨市工大节能印刷厂
开 本 787mm×1092mm 1/16 印张 25.5 字数 384 千字
版 次 2018 年 1 月第 1 版 2018 年 1 月第 1 次印刷
书 号 ISBN 978-7-5603-6941-9
定 价 78.00 元

FOREWORD

This book aims to present the fundamentals of number theory, one of the oldest mathematical disciplines. An exhaustive treatment of this large independent field of mathematics is obviously impossible in a book of reasonable size. We have thus confined ourselves in this book to some selected results in number theory, and the various chapters are devoted to the most typical problems of various aspects of the theory. We discuss in Chapter I, after some introductory remarks, the theory of congruences. Particular attention is given to congruences of degree two, and the quadratic reciprocity law is proved. Chapter II discusses classical arithmetic functions (Euler's function, sigma function) and a proof of the theorem of Erdös on the characterization of the logarithm among additive functions is given. Birch's result characterizing the powers among multiplicative functions is also presented. These two chapters are concerned with the so-called elementary number theory, and are presented rather simply as there is a detailed treatment in Professor Wacław Sierpiński's book, *Theory of Numbers*.

In Chapter III, we give the fundamental results of the theory of prime numbers, namely the prime number theorem and Dirichlet's theorem on primes in progressions. These results are proved using the Tauberian theorem of Delange-Ikehara.

Chapter IV discusses the sieve methods developed in recent years. The Eratosthenes' sieve, Selberg's sieve and the large sieve are studied and some applications pointed out. Brun's result on twin primes and Gallagher's theorem on primitive roots are proved.

Chapter V is concerned with geometrical problems. We first give some elementary fact concerning convex sets and lattices, and then prove Minkowski's theorem on convex bodies. Vinogradov's elementary method of finding the number of lattice points in plane regions is also discussed.

In Chapter VI we consider additive number theory. The reader will find in it elements of Schnirelman's density, which we use to prove Schnirelman's theorem on the representation of natural numbers as the sum of prime numbers. We prove also Mann's theorem concerning this density and the theorem of Waring-Hilbert.

Chapter VII gives the elements of probabilistic number theory. We prove three fundamental results of this theory, namely the inequality of Turán-Kubilius, the Erdös-Kac theorem on the normal decomposition, and the theorem of Erdös on asymptotic distribution of additive functions.

In Chapter VIII we consider Diophantine approximation, i.e. the approximation of irrational numbers by rational numbers. We discuss continued fractions and prove the theorem of Hurwitz on the best approximation. Here we also introduce the concept of uniform distribution, prove Weyl's criterion, and the classical result of Weyl concerning the uniform distribution of the sequence of values of polynomials.

Chapter IX, the last chapter, is concerned with the generalization of the concept of integers. We discuss algebraic integers and give an elementary theory of algebraic number fields and of Dedekind rings. We also introduce p-adic integers, define p-adic fields and prove their fundamental properties.

As one of the objectives of this book is to show the relationship of number theory with other fields of mathematics, we do not restrict oursleves to the conventional elementary methods. Methods and techniques in algebra, topology, analysis and probability theory are used quite liberally, but attempts have been made to keep the prerequisites to that of the undergraduate level. The reader is expected to have a knowledge of the fundamental concepts of algebra such as groups, rings and fields. In Chapter III, familiarity with fundamental facts of the theory of analytic function is needed, and in Chapter VII, elements of probability theory. Some notion of topology in metric spaces and elements of the theory of extension of fields will be necessary to read Chapter IX.

This book is based on lectures given at Wrocław University in memory of B. Bierut, and at Bordeaux University I. It was Assistant Professor Marceli Stark who persuaded me to write it. Without his encouragement, the plan to write this book would never be realized.

I wish to thank Professor Andrzej Schinzel for many valuable remarks and for pointing out a series of inaccuracies, and Professor Helmut Koch and Master Jan Śliwa for valuable simplifications of proofs. I thank Mrs. Teresa Bochynek for typing the manuscripts.

Wrocław, February 1975 *Władysław Narkiewicz*

NOTATION

We shall give here notation and symbols which will be used in the text without specific explanation. We shall denote by the letter $\mathcal{Z}$ the ring of rational integers, $\mathcal{N}$ will denote the set of natural numbers, where we make a convention that 0 is not an element of $\mathcal{N}$. We denote the set $\mathcal{N} \cup \{0\}$ by $\mathcal{N}_0$. The letter $\mathcal{Q}$ denotes the field of rational numbers, and the letter $\mathcal{R}$ the field of real numbers. We denote the field of complex numbers by $\mathcal{C}$.

By the symbol $[x]$ we denote the integral part of the number x and by the symbol $\{x\}$ its fractional part, i.e. if $x = n + r$, where $n \in \mathcal{Z}$ and $r \in [0, 1)$, then $[x] = n$, $\{x\} = r$.

If $F(x)$, $G(x)$ are real-valued functions defined on some set X, and moreover there exists a positive constant B such that for all $x \in X$ the inequality

$$|F(x)| \leqslant BG(x)$$

holds and $G(x) > 0$, then we write

$$F(x) = O(G(x)) \ .$$

If the set X is a subset of the real line or the complex plane and for some $x_0 \in X$ we have

$$\lim_{x \to x_0} \frac{F(x)}{G(x)} = 0 \ ,$$

then we write

$$F(x) = o(G(x)) \qquad \text{(as } x \text{ tends to } x_0) \ .$$

We use the same symbol in the case when

$$\lim_{x \to \infty} \frac{F(x)}{G(x)} = 0 \ .$$

If from the context it is clear what x_0 is, then we simply write

$$F(x) = o(G(x)) \quad .$$

These notations were introduced by E. Landau. Instead of $F(x) = o(G(x))$, we often write $F(x) \ll G(x)$; I. M. Vinogradov introduced this symbolism.

We note that in using the symbols o and O it is necessary to take care because e.g. on the set of natural numbers greater than 1 we have

$$x = O(x^2)$$

and

$$x^{\frac{1}{2}} = O(x^2) \ ,$$

but the equality $x = x^{\frac{1}{2}}$ is false. One should, however, not think that these notations are not precise and could lead to a contradiction. One should simply understand the designation $F = O(G)$ as one which means that the function F belongs to the family of those functions which are bounded when divided by G.

In using Landau's symbol it is worth remembering the following properties whose proof the reader should do it himself if he wishes:

(i) *If* $f_1 = O(f_2)$ *and* $f_2 = O(f_3)$, *then* $f_1 = O(f_3)$.

(ii) *If* $f_1, f_2 = O(f)$, *then* $f_1 \pm f_2 = O(f)$.

(iii) *If* $f = O(g)$, *then* $fh = O(g|h|)$.

(iv) *If* $f_1 = o(f_2)$ *and* $f_2 = O(f_3)$, *then* $f_1 = o(f_3)$.

(v) *If* $f_1, f_2 = o(f)$, *then* $f_1 \pm f_2 = o(f)$.

(vi) *If* $f_1 = o(f_2)$ *and* g *does not vanish, then* $f_1 g = o(f_2 g)$.

CONTENTS

CHAPTER I

DIVISIBILITY, CONGRUENCES

§1. Divisibility. Prime numbers

1. We say that an integer $m \neq 0$ *divides* an integer a if there exists an integer n such that $mn = a$, that is when the number a/m is an integer. We express this fact by $m|a$. If an integer m does not divide an integer a, then we write $m\nmid a$. Replacing the word "an integer" by "an element of a ring R" in this definition, we obtain the notion of divisibility in the ring R. In Chapter IX we shall have an occasion to apply this general notion.

From the definition follow the following properties of the notion of divisibility:

Theorem 1.1

(i) *If* $m|a$ *and* $m|b$, *then* $m|a+b$ *and* $m|a-b$.
(ii) *If* $m|a$ *and* $a|n$, *then* $m|n$.
(iii) *If* $m|a$ *and* $b \in \mathscr{Z}$, *then* $m|ab$.
(iv) *If* $a|b$ *and* $b \neq 0$, then $|a| \leqslant |b|$.
(v) *If* $a|b$ *and* $b|a$, *then* $b = a$ *or* $b = -a$.

Proof. If $m|a$ and $m|b$, then we can write $a = a_1 m$, $b = b_1 m$, where $a_1, b_1 \in \mathscr{Z}$, and this gives $a \pm b = (a_1 \pm b_1)m$, thereby proving (i). To prove (ii), let us write $a = a_1 m$, $n = an_1$ ($a_1, n_1 \in \mathscr{Z}$) and note that we then have $n = m(a_1 n_1)$. Now (iii) follows in view of $a|ab$ and (ii). Next for a proof of (iv), we note that from $a|b$ follows the integrality of the number b/a, and so by $b \neq 0$, we must have $|b/a| \geqslant 1$. Finally, (v) follows from (iv) on noting that if a and b are real numbers having the same absolute value, then $b = a$ or $b = -a$. ∎

Remark. From (i) and (iii), it follows that the set of all integers divisible by a given integer m forms an ideal in the ring $\mathscr{Z}$.

Theorem 1.2 (division algorithm). *If $a, b \in \mathscr{Z}$, and $b \neq 0$, then there exists exactly one pair of integers q, r satisfying the conditions:*

$$a = bq + r, \qquad 0 \leqslant r < |b| .$$

Furthermore, $b \mid a$ holds iff $r = 0$.

Proof. In the case $b > 0$, let us take $q = [a/b]$ and $r = a - bq$. Then, in view of $q \leqslant a/b < q+1$ we have $bq \leqslant a < bq + b$, so that $0 \leqslant r < b = |b|$. In the case of a negative b, we take $q = -[a/|b|]$.

If we have $a = bq_1 + r_1 = bq_2 + r_2$, $0 \leqslant r_1, r_2 < |b|$, then $r_2 - r_1 = b(q_1 - q_2)$, hence $b \mid (r_2 - r_1)$. If we have $r_1 \neq r_2$, then by Theorem 1.1 (iv) the inequality $|b| \leqslant |r_2 - r_1| < b$ would hold, which is impossible. Therefore $r_1 = r_2$, and so $q_1 = q_2$. The last part of the theorem now follows from Theorem 1.1 (i). ∎

We call the integer r the *residue* of a divided by b and call q the (*incomplete*) *quotient* of this division.

2. Every natural number $n > 1$ has at least two natural divisors —— 1 and n. If there are no other divisiors, then we say that n is a *prime number*. We denote the set of all prime numbers by $\mathscr{P}$. Integers $n > 1$ which are not prime numbers are called *composite numbers*. Hence the integers 2, 3, 5, 7, 11, 257, 65537 are prime numbers, and the integers 4, 6, 8, 21, 35, 99999 are composite numbers.

The greatest known prime number is $2^{19937}-1$ with 6002 digits. It was found by B. Tuckerman [1] in 1971*. We shall soon note that the set $\mathscr{P}$ is an infinite set, so the discovery of larger and larger prime numbers may verify the development of computational technique but does not contribute significantly to the theory itself.

Theorem 1.3. *Every natural number $n > 1$ can be expressed in the form $n = p_1 \ldots p_k$, $p_i \in \mathscr{P}$.*

Proof. We use induction. For $n = 2$ we take $k = 1, p_1 = 2$. Now suppose the validity of the assertion for all $n < N$. If N is a prime number, then we take $k = 1$, $p_1 = N$; and if $N = ab$, $1 < a, b < N$, then by the induction hypothesis we have $a = p_1 \ldots p_r, b = p_{r+1} \ldots p_s$ with $p_i \in \mathscr{P}$, and we obtain $N = p_1 \ldots p_s$. ∎

Corollary 1. *Every natural number $n > 1$ has at least one prime factor.* ∎

Corollary 2. *Every natural number $n > 1$ can be expressed in the form $n = p_1^{\alpha_1} \ldots p_t^{\alpha_t}$, where $\alpha_i \in \mathscr{N}$, and $p_1, \ldots, p_t$ are prime numbers.* ∎

* Translator's note: This is actually the 24th Mersenne prime M_{19937} (cf. Exercise 6 at the end of this section). Recently, three further Mersenne primes have been found: M_{21701}, M_{23209}, M_{44497}, see e.g. D. Slovinski [1] and L.-K. Hua [3], p. 21.

Added in proof: Meanwhile D. Slovinski has found a much larger prime $2^{86243}-1$ with 25,962 digits. But it is not known whether it is the 28th Mersenne prime (see Math. Intelligencer 5, No. 1 (1983), p. 60).

We denote the number of distinct prime divisors of an integer n by $\omega(n)$. Additionally we define the value of the function $\omega(n)$ for $n = 1$ by putting $\omega(1) = 0$. We shall be concerned with the investigation of various properties of this function in later chapters.

Denote the number of primes not exceeding x by $\pi(x)$. We have then, $\pi(2) = 1, \pi(3) = 2, \ldots, \pi(10) = 4$, and it can be checked that $\pi(100) = 25$, $\pi(1000) = 168$. As early as in Euclid's *Elements*, we can find a proof of the fact that there are infinitely many primes, that is $\pi(x) \to \infty$.

Let us give three proofs of this result:

Theorem 1.4. *The set $\mathscr{P}$ of all primes is infinite.*

Proof I (Euclid). Assume that the set $\mathscr{P}$ is finite, $\mathscr{P} = \{p_1, \ldots, p_n\}$. Then the integer $N = 1 + p_1 \ldots p_n$ is greater than 1 and moreover it gives the residue 1 when divided by $p_1, \ldots, p_n$, which contradicts Corollary 1 to Theorem 1.3. ∎

Proof II (Euler). As in the preceding proof, let us assume that $\{p_1, \ldots, p_n\}$ is the set of all prime numbers. For $x > 1$ we have

$$\prod_{k=1}^{n} \left(1 - \frac{1}{p_k^x}\right)^{-1} = \prod_{k=1}^{n} \sum_{j=0}^{\infty} \frac{1}{p_k^{jx}} \tag{1.1}$$

$$= \sum_{j_1=0}^{\infty} \ldots \sum_{j_n=0}^{\infty} \frac{1}{(p_1^{j_1} \ldots p_n^{j_n})^x} \geqslant \sum_{m=1}^{\infty} \frac{1}{m^x},$$

because by Corollary 2 to Theorem 1.3 each natural number can be expressed in the form $m = p_1^{j_1} \ldots p_n^{j_n}$.

Let $\alpha = \prod_{k=1}^{n} \left(1 - \frac{1}{p_k}\right)^{-1}$ and let T be a natural number chosen in such a way that the inequality

$$\sum_{m=1}^{T} \frac{1}{m} > \alpha.$$

holds. Then, using (1.1), we have

$$\alpha = \lim_{x \to 1} \prod_{k=1}^{n} \left(1 - \frac{1}{p_k^x}\right)^{-1} \geqslant \limsup_{x \to 1} \sum_{m=1}^{\infty} \frac{1}{m^x}$$

$$\geqslant \limsup_{x \to 1} \sum_{m=1}^{T} \frac{1}{m^x} = \sum_{m=1}^{T} \frac{1}{m} > \alpha.$$

The obtained contradiction proves our contention. ∎

Proof III (G. Pólya and G. Szegö). The numbers $2^{2^n} + 1$ are greater than 1 for $n = 1, 2, \ldots$, hence they have prime divisors. Denote by q_n any one of prime divisors of

numbers $2^{2^n}+1$, e.g. the least one. Let us show that the prime numbers $q_1, q_2, \ldots$ are all distinct. In fact, if for some $m < n$ we have $q_m = q_n$, then for some $a \in \mathcal{N}$

$$2^{2^m} = aq_m - 1,$$

therefore

$$2^{2^n}+1 = (2^{2^m})^{2^{n-m}}+1 = (aq_m-1)^{2^{n-m}}+1.$$

Applying Newton's binomial expansion, we see that all the terms except the last one are divisible by q_m, and the last term is equal to $(-1)^{2^{n-m}} = 1$. This gives in turn (for a suitable natural number b) the equality $2^{2^n}+1 = bq_m+2$. Since from the supposition q_m must divide $2^{2^n}+1$, hence q_m divides 2, that is $q_m = 2$, which is impossible because the number $2^{2^m}+1$ is not divisible by 2. ∎

The numbers appearing in the third proof of Theorem 1.4 are called the *Fermat numbers* and denoted by F_n. It is not difficult to check that $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65{,}537$ are prime numbers, and Fermat in 1640 raised a conjecture that for each n the number F_n is a prime number. However, it is not true, as Euler noted, $F_5 = 641 \cdot 6700417$ and next it was shown that all Fermat numbers F_n for $n = 5, 6, \ldots, 16$ are composite. (See for example W. Sierpiński [4], pp. 344-345.) We do not know any Fermat prime greater than F_4.

The method used in the second proof of the preceding theorem can also be adopted to prove the following more powerful result:

Theorem 1.5. *If $p_1 < p_2 < \ldots$ is a sequence consisting of all the primes, then the series*

$$\sum_{n=1}^{\infty} \frac{1}{p_n}$$

is divergent.

Proof. For a natural number N we have

$$\prod_{n=1}^{N} \left(1-\frac{1}{p_n}\right)^{-1} = \prod_{n=1}^{N} \left(1+\frac{1}{p_n}+\frac{1}{p_n^2}+\ldots\right) \geqslant \sum_{m \leqslant p_N} \frac{1}{m},$$

because each integer $m \leqslant p_N$ is the product of powers of primes not exceeding p_N. But the right-hand side of this inequality for a suitable choice of N can be made arbitrarily large, which, however, proves the divergence of the product

$$\prod_{n=1}^{\infty} \left(1-\frac{1}{p_n}\right)^{-1}.$$

It remains to note that the convergence of $\sum_{n=1}^{\infty} \frac{1}{p_n}$ would imply the convergence of this product. ∎

Other simple proofs of this theorem can be found in the following papers: R. Bellman [1], P. Erdös [2], L. Moser [1].

To determine whether a given integer N is prime or not is not in general a simple problem. In an obtrusive method relying upon the test whether N is divisible by prime numbers $< N$, one can restrict oneself to primes $\leqslant N^{1/2}$ because each composite number N has a prime divisor $\leqslant N^{1/2}$, but the number of these primes exceed $\frac{N^{\frac{1}{2}}}{\log N}$ for large N, (which follows from the so-called prime number theorem to be proved in Chapter III), therefore one should execute at least $\frac{N^{\frac{1}{2}}}{\log N}$ operations. The fastest known method is due to J. M. Pollard [1] which requires at most $BN^{1/4}$ operations, where B is some constant. Of course, for integers having a special form the number of operations can be made smaller.

3. One of the fundamental results in elementary number theory is the theorem on unique factorization of natural numbers into prime factors, which we shall now prove.

Theorem 1.6. *Every natural number n greater than 1 can be uniquely expressed in the form*

$$n = p_1 \dots p_k, \tag{1.2}$$

where $p_i \in \mathscr{P}$ $(i = 1, \dots, k)$ and $p_1 \leqslant p_2 \leqslant \dots \leqslant p_k$. Each prime divisor of the integer n must appear among the primes $p_1, \dots, p_k$.

Proof. Let us first show that the second part of the assertion of the theorem is a consequence of the first part. In fact, if n has a unique decomposition into prime factors, $n = p_1 \dots p_k$ and $p \mid n$, then decomposing $n/p = q_1 \dots q_l$ into prime factors, we obtain $n = pq_1 \dots q_l = p_1 \dots p_k$, hence the prime p must appear among the primes p_i.

We prove the first part of the theorem by two different methods.

Proof I. By Theorem 1.2 the ring $\mathscr{Z}$ of rational integers is a Euclidean domain, hence it must be a unique factorization domain, and this coincides with our assertion. ∎

Proof II (without the use of algebraic concepts). It is obvious that each prime number has only one representation of the form (1.2), therefore our theorem is true for $n = 2$. Suppose that our theorem is false and denote by N the smallest number having at least two different decompositions (1.2), say

$$N = p_1 \dots p_r = q_1 \dots q_s,$$

where $p_1 \leqslant p_2 \leqslant \dots \leqslant p_r$, $q_1 \leqslant q_2 \leqslant \dots \leqslant q_s$ are prime numbers. Without loss of generality we can suppose that $p_1 \leqslant q_1$. If $p_1 = q_1$, then the number

$$N/p_1 = p_2 \dots p_r = q_2 \dots q_s$$

is an integer less than N having two different decompositions which is against the choice of N. Hence $p_1 < q_1$. Therefore we can write

$$q_1 = ap_1 + b \qquad (a \geqslant 0,\ 0 < b < p_1,\ a, b \in \mathscr{Z}),$$

whence

$$N = (ap_1+b)q_2 \dots q_s = ap_1 q_2 \dots q_s + bq_2 \dots q_s.$$

The integer b is either equal to 1 or has a unique factorization into prime factors. Let $b = Q_1 \dots Q_t$ be this factorization (if $b = 1$, then we take $t = 0$). As the integer $m = bq_2 \dots q_s$ is less than N, it has also a unique factorization and we see that the prime numbers $Q_1, \dots, Q_t, q_2, \dots, q_s$ arranged in increasing order appear as factors in this factorization. But $m = N - ap_1 q_2 \dots q_s$ is an integer divisible by p_1, so from the remark made in the beginning of the proof it follows that p_1 is one of $Q_1, \dots, Q_t, q_2, \dots, q_s$, hence $p_1 = Q_i$ for some i. Therefore $p_1 | b$, which is contradictory to $0 < b < p_1$. The obtained contradiction proves that no integer exists with two different decompositions. ■

Corollary 1. *Every natural number $n > 1$ can be uniquely expressed in the form*

$$n = \prod_{i=1}^{r} p_i^{\alpha_i},$$

where $p_1 < p_2 < \dots < p_r$ are prime numbers, $r = \omega(n)$ and $\alpha_i \in \mathcal{N}$.

Proof. This follows from the theorem by grouping together the identical prime factors. ■

Corollary 2. *Every $n \in \mathcal{Z}$ different from 0 and ± 1 can be uniquely expressed in the form*

$$n = \operatorname{sgn} n \prod_{i=1}^{r} p_i^{\alpha_i},$$

where $p_1 < \dots < p_r$ are prime numbers,

$$\operatorname{sgn} n = \begin{cases} 1, & \text{if} \quad n > 0, \\ -1, & \text{if} \quad n < 0 \end{cases}$$

and $\alpha_i \in \mathcal{N}$.

Proof. Let us write $n = |n| \operatorname{sgn} n$ and apply the preceding corollary to $|n|$. ■

Corollary 3. *Every non-zero integer n can be uniquely written in the form*

$$n = \operatorname{sgn} n \prod_{p \in \mathcal{P}} p^{\alpha_p(n)},$$

where $\alpha_p(n) \in \mathcal{N}_0$. The product appearing here contains finitely many factors different from 1, i.e. for a given n, the exponent $\alpha_p(n)$ is different from zero for finitely many primes p.

Proof. For $n = \pm 1$ we take $\alpha_p(n) = 0$ for all p. If, on the contrary, n is of the form as in the preceding corollary, then for $p = p_i$ $(i = 1, 2, \dots, r)$ we take $\alpha_p(n) = \alpha_i$,

and for the remaining primes we put $\alpha_p(n) = 0$. Uniqueness of the representation follows immediately from the preceding corollary. ∎

Corollary 4. *Every rational number w different from zero can be uniquely expressed in the form*

$$w = \operatorname{sgn} w \prod_{p \in \mathcal{P}} p^{\alpha_p(w)},$$

where $\alpha_p(w) \in \mathcal{Z}$. The product appearing here contains only finitely many factors different from 1.

Proof. We can write $w = \operatorname{sgn} w \left(\frac{a}{b}\right)$, where $a, b \in \mathcal{N}$. Applying the preceding corollary to a and b, we obtain

$$w = \operatorname{sgn} w \prod_{p \in \mathcal{P}} p^{\alpha_p(a) - \alpha_p(b)}.$$

Note that the difference $\alpha_p(a) - \alpha_p(b)$ depends exclusively on w, but not on the choice of a and b. In fact, if $w = \operatorname{sgn} w \frac{a_1}{b_1}$ $(a_1, b_1 \in \mathcal{N})$, then $ab_1 = a_1 b$. Hence we have

$$\prod_{p \in \mathcal{P}} p^{\alpha_p(a)} \prod_{p \in \mathcal{P}} p^{\alpha_p(b_1)} = \prod_{p \in \mathcal{P}} p^{\alpha_p(a_1)} \prod_{p \in \mathcal{P}} p^{\alpha_p(b)},$$

i.e.

$$\prod_{p \in \mathcal{P}} p^{\alpha_p(a) + \alpha_p(b_1)} = \prod_{p \in \mathcal{P}} p^{\alpha_p(a_1) + \alpha_p(b)}.$$

By Corollary 3 we have the equality $\alpha_p(a) + \alpha_p(b_1) = \alpha_p(a_1) + \alpha_p(b)$, for every p, that is $\alpha_p(a) - \alpha_p(b) = \alpha_p(a_1) - \alpha_p(b_1)$, as asserted.

Hence if we define the function $\alpha_p(w)$ for $w \neq 0$ $(w \in \mathcal{Q})$ by the formula

$$\alpha_p(w) = \alpha_p(a) - \alpha_p(b) \qquad \left(|w| = \frac{a}{b},\ a, b \in \mathcal{N}\right),$$

then we get the representation required.

Suppose that

$$w = \operatorname{sgn} w \prod_{p \in \mathcal{P}} p^{\alpha_p(w)} = \operatorname{sgn} w \prod_{p \in \mathcal{P}} p^{c_p}.$$

Let us show that $c_p = \alpha_p(w)$ must hold for every $p \in \mathcal{P}$.

If $A = \{p \in \mathcal{P} : \alpha_p(w) > c_p\}$ and $B = \{p \in \mathcal{P} : \alpha_p(w) < c_p\}$, then the number

$$m = \prod_{p \in A} p^{\alpha_p(w) - c_p} = \prod_{p \in B} p^{c_p - \alpha_p(w)}$$

is a natural number. If the sum of the sets A and B were non-empty, then m would have two representations in the form of the product of prime powers, which contradicts Corollary 2. Therefore $A = B = \emptyset$, that is for every p we have the equality $\alpha_p(w) = c_p$. ■

Remark. The decomposition appearing in the above corollaries is called the *canonical decomposition* of the corresponding numbers.

We shall now give fundamental properties of the function $\alpha_p(w)$ appearing in Corollary 4:

Theorem 1.7.

(i) $\alpha_p(ab) = \alpha_p(a) + \alpha_p(b)$, $\alpha_p(a/b) = \alpha_p(a) - \alpha_p(b)$, $\alpha_p(-a) = \alpha_p(a)$.

(ii) *Let $w \neq 0$ be a rational number. Then $w \in \mathcal{Z}$ iff we have $\alpha_p(w) \geqslant 0$ for every p.*

(iii) *If $m, n \in \mathcal{Z}$, then $m|n$ iff we have $\alpha_p(m) \leqslant \alpha_p(n)$ for every p.*

(iv) *For $n \in \mathcal{Z}$ the largest power of p dividing n is $p^{\alpha_p(n)}$.*

(v) $\alpha_p(a \pm b) \geqslant \min(\alpha_p(a), \alpha_p(b))$, *and if $\alpha_p(a) \neq \alpha_p(b)$, then* $\alpha_p(a \pm b) = \min(\alpha_p(a), \alpha_p(b))$.

Proof.

(i) The equalities (i) follow at once from the definition of $\alpha_p(n)$.

(ii) If we have $\alpha_p(w) \geqslant 0$, for every p, then $w \in \mathcal{Z}$, as it is the product of integers. Conversely, if $w \in \mathcal{Z}$, then from Corollaries 3 and 4 follows $\alpha_p(w) \geqslant 0$.

(iii) m divides n iff $n|m \in \mathcal{Z}$. Hence it is enough to apply (i) and (ii).

(iv) It is apparent that $p^{\alpha_p(n)}|n$, and if we have

$$p^{\alpha_p(n)+1}|n = p^{\alpha_p(n)} \prod_{\substack{q \neq p \\ q \in \mathcal{P}}} q^{\alpha_q(n)},$$

then

$$p| \prod_{\substack{q \neq p \\ q \in \mathcal{P}}} q^{\alpha_q(n)},$$

and so p would divide some product of primes different from p, which is impossible because of Corollary 1.

(v) First consider the case $a, b \in \mathcal{Z}$. Then for $\alpha = \alpha_p(a)$, $\beta = \alpha_p(b)$ we have $p^\alpha|a$, $p^\beta|b$, hence $p^{\min(\alpha,\beta)}|a \pm b$, which gives, by (iv), the inequality $\min(\alpha, \beta) \leqslant \alpha_p(a \pm b)$.

In the general case we write $a = x/y$, $b = x'/y'$ $(x, y, x', y' \in \mathcal{Z}$ and $\neq 0)$. Then $a \pm b = (xy' \pm x'y)/yy'$, hence, using (i) and that part of (v) already proved, we obtain