Graduate Texts in Mathematics

J.L. Doob

Measure Theory

测度论

Springer

世界图书出版公司
www.wpcbj.com.cn

Neal Koblitz

p-adic Numbers, p-adic Analysis, and Zeta-Functions

Second Edition

Springer

图书在版编目（CIP）数据

p进数，p进分析和ζ函数：第2版：英文／（美）科比利兹（Koblitz，N.）著．—北京：世界图书出版公司北京公司，2009.6

书名原文：p-adic Numbers，p-adic Analysis，and Zeta-Functions 2nd ed.

ISBN 978-7-5100-0453-7

Ⅰ.p… Ⅱ.科… Ⅲ.P阶数域—教材—英文 Ⅳ.0156.2

中国版本图书馆CIP数据核字（2009）第085034号

书　　名：*p*-adic Numbers，*p*-adic Analysis，and Zeta-Functions 2nd ed.
作　　者：Neal Koblitz

中 译 名：*p*进数，*p*进分析和ζ函数 第2版
责任编辑：高蓉　刘慧

出 版 者：世界图书出版公司北京公司
印 刷 者：三河国英印务有限公司
发　　行：世界图书出版公司北京公司（北京朝内大街137号　100010）
联系电话：010-64021602，010-64015659
电子信箱：kjb@wpcbj.com.cn

开　　本：24开
印　　张：7
版　　次：2009年06月
版权登记：图字：01-2009-1099

书　　号：978-7-5100-0453-7/O·668　　定　　价：25.00元

Neal Koblitz
Department of Mathematics GN-50
University of Washington
Seattle, WA 98195
USA

Mathematics Subject Classifications: 1991: 11-01, 11E95, 11Mxx

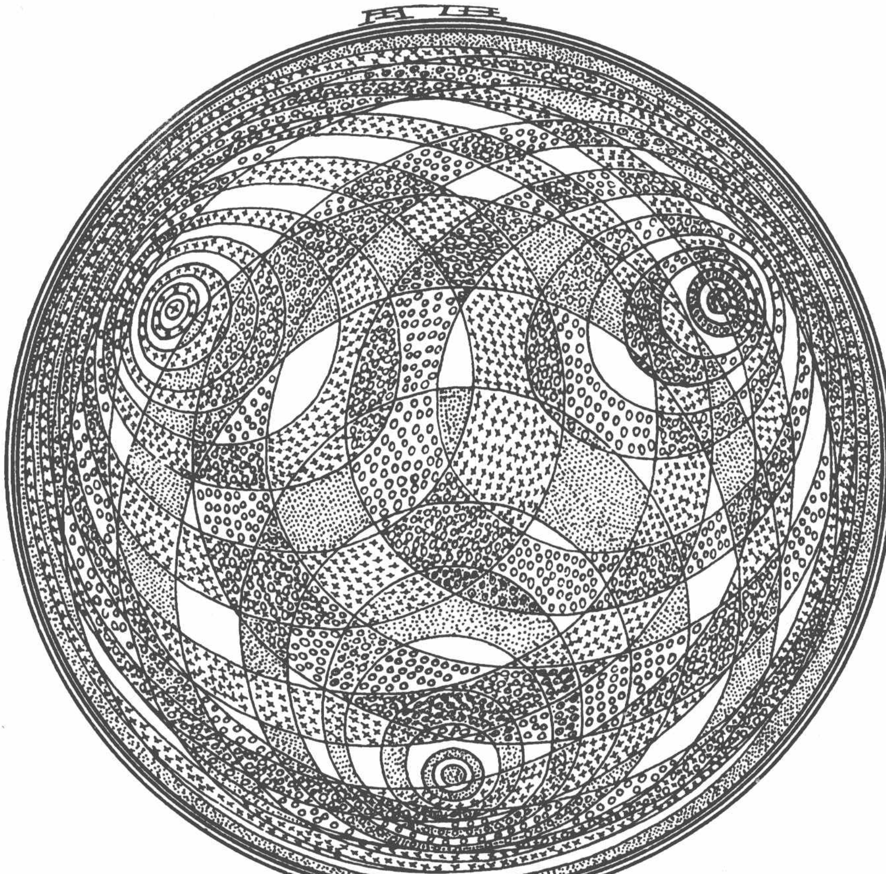
Library of Congress Cataloging in Publication Data
Koblitz, Neal, 1948–
P-adic numbers, p-adic analysis and zeta-functions.
(Graduate texts in mathematics; 58)
Bibliography: p.
Includes index.
1. p-adic numbers. 2. p-adic analysis. 3. Functions, Zeta I. Title. II. Series.
QA241.K674 1984 512'.74 84-5503

9 8 7 6 5 4 3

ISBN 0-387-96017-1 Springer-Verlag New York Berlin Heidelberg
ISBN 3-540-96017-1 Springer-Verlag Berlin Heidelberg New York SPIN 10670823

Graduate Texts in Mathematics 58

Springer
New York
Berlin
Heidelberg
Barcelona
Budapest
Hong Kong
London
Milan
Paris
Santa Clara
Singapore
Tokyo



Artist's conception of the 3-adic unit disk.

Drawing by A.T. Fomenko of Moscow State University, Moscow, U.S.S.R.

To Professor Mark Kac

Preface to the second edition

The most important revisions in this edition are: (1) enlargement of the treatment of p-adic functions in Chapter IV to include the Iwasawa logarithm and the p-adic gamma-function, (2) rearrangement and addition of some exercises, (3) inclusion of an extensive appendix of answers and hints to the exercises, the absence of which from the first edition was apparently a source of considerable frustration for many readers, and (4) numerous corrections and clarifications, most of which were proposed by readers who took the trouble to write me. Some clarifications in Chapters IV and V were also suggested by V. V. Shokurov, the translator of the Russian edition. I am grateful to all of these readers for their assistance. I would especially like to thank Richard Bauer and Keith Conrad, who provided me with systematic lists of misprints and unclarities.

I would also like to express my gratitude to the staff of Springer-Verlag for both the high quality of their production and the cooperative spirit with which they have worked with me on this book and on other projects over the past several years.

Seattle, Washington N. I. K.

Preface to the first edition

These lecture notes are intended as an introduction to p-adic analysis on the elementary level. For this reason they presuppose as little background as possible. Besides about three semesters of calculus, I presume some slight exposure to more abstract mathematics, to the extent that the student won't have an adverse reaction to matrices with entries in a field other than the real numbers, field extensions of the rational numbers, or the notion of a continuous map of topological spaces.

The purpose of this book is twofold: to develop some basic ideas of p-adic analysis, and to present two striking applications which, it is hoped, can be as effective pedagogically as they were historically in stimulating interest in the field. The first of these applications is presented in Chapter II, since it only requires the most elementary properties of $\mathbf{Q}_p$; this is Mazur's construction by means of p-adic integration of the Kubota–Leopoldt p-adic zeta-function, which "p-adically interpolates" the values of the Riemann zeta-function at the negative odd integers. My treatment is based on Mazur's Bourbaki notes (unpublished). The book then returns to the foundations of the subject, proving extension of the p-adic absolute value to algebraic extensions of $\mathbf{Q}_p$, constructing the p-adic analogue of the complex numbers, and developing the theory of p-adic power series. The treatment highlights analogies and contrasts with the familiar concepts and examples from calculus. The second main application, in Chapter V, is Dwork's proof of the rationality of the zeta-function of a system of equations over a finite field, one of the parts of the celebrated Weil Conjectures. Here the presentation follows Serre's exposition in *Séminaire Bourbaki*.

These notes have no pretension to being a thorough introduction to p-adic analysis. Such topics as the Hasse–Minkowski Theorem (which is in Chapter 1 of Borevich and Shafarevich's *Number Theory*) and Tate's thesis (which is also available in textbook form, see Lang's *Algebraic Number Theory*) are omitted.

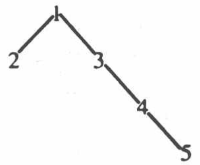
Moreover, there is no attempt to present results in their most general form. For example, p-adic L-functions corresponding to Dirichlet characters are only discussed parenthetically in Chapter II. The aim is to present a selection of material that can be digested by undergraduates or beginning graduate students in a one-term course.

The exercises are for the most part not hard, and are important in order to convert a passive understanding to a real grasp of the material. The abundance of exercises will enable many students to study the subject on their own, with minimal guidance, testing themselves and solidifying their understanding by working the problems.

p-adic analysis can be of interest to students for several reasons. First of all, in many areas of mathematical research—such as number theory and representation theory—p-adic techniques occupy an important place. More naively, for a student who has just learned calculus, the "brave new world" of non-Archimedean analysis provides an amusing perspective on the world of classical analysis. p-adic analysis, with a foot in classical analysis and a foot in algebra and number theory, provides a valuable point of view for a student interested in any of those areas.

I would like to thank Professors Mark Kac and Yu. I. Manin for their help and encouragement over the years, and for providing, through their teaching and writing, models of pedagogical insight which their students can try to emulate.

Logical dependence of chapters



Cambridge, Massachusetts N. I. K.

Contents

CHAPTER I

p-adic numbers

1. Basic concepts

If X is a nonempty set, a distance, or *metric*, on X is a function d from pairs of elements (x, y) of X to the nonnegative real numbers such that

(1) $d(x, y) = 0$ if and only if $x = y$.
(2) $d(x, y) = d(y, x)$.
(3) $d(x, y) \leq d(x, z) + d(z, y)$ for all $z \in X$.

A set X together with a metric d is called a *metric space*. The same set X can give rise to many different metric spaces (X, d), as we'll soon see.

The sets X we'll be dealing with will mostly be fields. Recall that a field F is a set together with two operations $+$ and $\cdot$ such that F is a commutative group under $+$, $F - \{0\}$ is a commutative group under $\cdot$, and the distributive law holds. The examples of a field to have in mind at this point are the field $\mathbb{Q}$ of rational numbers and the field $\mathbb{R}$ of real numbers.

The metrics d we'll be dealing with will come from *norms* on the field F, which means a map denoted $\|\ \|$ from F to the nonnegative real numbers such that

(1) $\|x\| = 0$ if and only if $x = 0$.
(2) $\|x \cdot y\| = \|x\| \cdot \|y\|$.
(3) $\|x + y\| \leq \|x\| + \|y\|$.

When we say that a metric d "comes from" (or "is induced by") a norm $\|\ \|$, we mean that d is defined by: $d(x, y) = \|x - y\|$. It is an easy exercise to check that such a d satisfies the definition of a metric whenever $\|\ \|$ is a norm.

A basic example of a norm on the rational number field $\mathbb{Q}$ is the absolute value $|x|$. The induced metric $d(x, y) = |x - y|$ is the usual concept of distance on the number line.

My reason for starting with the abstract definition of distance is that the point of departure for our whole subject of study will be a new type of distance, which will satisfy Properties (1)–(3) in the definition of a metric but will differ fundamentally from the familiar intuitive notions. My reason for recalling the abstract definition of a field is that we'll soon need to be working not only with **Q** but with various "extension fields" which contain **Q**.

2. Metrics on the rational numbers

We know one metric on **Q**, that induced by the ordinary absolute value. Are there any others? The following is basic to everything that follows.

Definition. Let $p \in \{2, 3, 5, 7, 11, 13, \ldots\}$ be any prime number. For any nonzero integer a, let the p-adic ordinal of a, denoted $\text{ord}_p\, a$, be the highest power of p which divides a, i.e., the greatest m such that $a \equiv 0 \pmod{p^m}$. (The notation $a \equiv b \pmod{c}$ means: c divides $a - b$.) For example,

$$\text{ord}_5\, 35 = 1, \qquad \text{ord}_5\, 250 = 3, \qquad \text{ord}_2\, 96 = 5, \qquad \text{ord}_2\, 97 = 0.$$

(If $a = 0$, we agree to write $\text{ord}_p\, 0 = \infty$.) Note that ord_p behaves a little like a logarithm would: $\text{ord}_p(a_1 a_2) = \text{ord}_p\, a_1 + \text{ord}_p\, a_2$.

Now for any rational number $x = a/b$, define $\text{ord}_p\, x$ to be $\text{ord}_p\, a - \text{ord}_p\, b$. Note that this expression depends only on x, and not on a and b, i.e., if we write $x = ac/bc$, we get the same value for $\text{ord}_p\, x = \text{ord}_p\, ac - \text{ord}_p\, bc$.

Further define a map $|\ |_p$ on **Q** as follows:

$$|x|_p = \begin{cases} \dfrac{1}{p^{\text{ord}_p x}}, & \text{if } x \neq 0; \\ 0, & \text{if } x = 0. \end{cases}$$

Proposition. $|\ |_p$ *is a norm on* **Q**.

Proof. Properties (1) and (2) are easy to check as an exercise. We now verify (3).

If $x = 0$ or $y = 0$, or if $x + y = 0$, Property (3) is trivial, so assume x, y, and $x + y$ are all nonzero. Let $x = a/b$ and $y = c/d$ be written in lowest terms. Then we have: $x + y = (ad + bc)/bd$, and $\text{ord}_p(x + y) = \text{ord}_p(ad + bc) - \text{ord}_p\, b - \text{ord}_p\, d$. Now the highest power of p dividing the sum of two numbers is *at least* the minimum of the highest power dividing the first and the highest power dividing the second. Hence

$$\begin{aligned} \text{ord}_p(x + y) &\geq \min(\text{ord}_p\, ad, \text{ord}_p\, bc) - \text{ord}_p\, b - \text{ord}_p\, d \\ &= \min(\text{ord}_p\, a + \text{ord}_p\, d, \text{ord}_p\, b + \text{ord}_p\, c) - \text{ord}_p\, b - \text{ord}_p\, d \\ &= \min(\text{ord}_p\, a - \text{ord}_p\, b, \text{ord}_p\, c - \text{ord}_p\, d) \\ &= \min(\text{ord}_p\, x, \text{ord}_p\, y). \end{aligned}$$

Therefore, $|x + y|_p = p^{-\text{ord}_p(x+y)} \leq \max(p^{-\text{ord}_p x}, p^{-\text{ord}_p y}) = \max(|x|_p, |y|_p)$, and this is $\leq |x|_p + |y|_p$. □

We actually proved a stronger inequality than Property (3), and it is this stronger inequality which leads to *the* basic definition of p-adic analysis.

Definition. A norm is called *non-Archimedean* if $\|x + y\| \leq \max(\|x\|, \|y\|)$ always holds. A metric is called *non-Archimedean* if $d(x, y) \leq \max(d(x, z), d(z, y))$; in particular, a metric is non-Archimedean if it is induced by a non-Archimedean norm, since in that case $d(x, y) = \|x - y\| = \|(x - z) + (z - y)\| \leq \max(\|x - z\|, \|z - y\|) = \max(d(x, z), d(z, y))$.

Thus, $| \ |_p$ is a non-Archimedean norm on $\mathbb{Q}$.

A norm (or metric) which is not non-Archimedean is called *Archimedean*. The ordinary absolute value is an Archimedean norm on $\mathbb{Q}$.

In any metric space X we have the notion of a *Cauchy sequence* $\{a_1, a_2, a_3, \ldots\}$ of elements of X. This means that for any $\varepsilon > 0$ there exists an N such that $d(a_m, a_n) < \varepsilon$ whenever both $m > N$ and $n > N$.

We say two metrics d_1 and d_2 on a set X are *equivalent* if a sequence is Cauchy with respect to d_1 if and only if it is Cauchy with respect to d_2. We say two norms are *equivalent* if they induce equivalent metrics.

In the definition of $| \ |_p$, instead of $(1/p)^{\mathrm{ord}_p x}$ we could have written $\rho^{\mathrm{ord}_p x}$ with any $\rho \in (0, 1)$ in place of $1/p$. We would have obtained an equivalent non-Archimedean norm (see Exercises 5 and 6). The reason why $\rho = 1/p$ is usually the most convenient choice is related to the formula in Exercise 18 below.

We also have a family of Archimedean norms which are equivalent to the usual absolute value $| \ |$, namely $| \ |^\alpha$ when $0 < \alpha \leq 1$ (see Exercise 8).

We sometimes let $| \ |_\infty$ denote the usual absolute value. This is only a notational convention, and is not meant to imply any direct relationship between $| \ |_\infty$ and $| \ |_p$.

By the "trivial" norm we mean the norm $\| \ \|$ such that $\|0\| = 0$ and $\|x\| = 1$ for $x \neq 0$.

Theorem 1 (Ostrowski). *Every nontrivial norm $\| \ \|$ on $\mathbb{Q}$ is equivalent to $| \ |_p$ for some prime p or for $p = \infty$.*

PROOF. *Case* (i). Suppose there exists a positive integer n such that $\|n\| > 1$. Let n_0 be the least such n. Since $\|n_0\| > 1$, there exists a positive real number α such that $\|n_0\| = n_0^\alpha$. Now write any positive integer n to the base n_0, i.e., in the form

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_s n_0^s, \quad \text{where } 0 \leq a_i < n_0 \text{ and } a_s \neq 0.$$

Then

$$\begin{aligned} \|n\| &\leq \|a_0\| + \|a_1 n_0\| + \|a_2 n_0^2\| + \cdots + \|a_s n_0^s\| \\ &= \|a_0\| + \|a_1\| \cdot n_0^\alpha + \|a_2\| \cdot n_0^{2\alpha} + \cdots + \|a_s\| \cdot n_0^{s\alpha}. \end{aligned}$$

Since all of the a_i are $<n_0$, by our choice of n_0 we have $\|a_i\| \leq 1$, and hence

$$\begin{aligned}\|n\| &\leq 1 + n_0{}^{\alpha} + n_0{}^{2\alpha} + \cdots + n_0{}^{s\alpha}\\ &\leq n_0{}^{s\alpha}(1 + n_0{}^{-\alpha} + n_0^{-2\alpha} + \cdots + n_0^{-s\alpha})\\ &\leq n^{\alpha}\left[\sum_{i=0}^{\infty} (1/n_0{}^{\alpha})^i\right],\end{aligned}$$

because $n \geq n_0{}^s$. The expression in brackets is a finite constant, which we call C. Thus,

$$\|n\| \leq Cn^{\alpha} \quad \text{for all } n = 1, 2, 3, \ldots .$$

Now take any n and any large N, and put n^N in place of n in the above inequality; then take Nth roots. You get

$$\|n\| \leq \sqrt[N]{C}n^{\alpha}.$$

Letting $N \to \infty$ for n fixed gives $\|n\| \leq n^{\alpha}$.

We can get the inequality the other way as follows. If n is written to the base n_0 as before, we have $n_0^{s+1} > n \geq n_0{}^s$. Since $\|n_0^{s+1}\| = \|n + n_0^{s+1} - n\| \leq \|n\| + \|n_0^{s+1} - n\|$, we have

$$\begin{aligned}\|n\| &\geq \|n_0^{s+1}\| - \|n_0^{s+1} - n\|\\ &\geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n)^{\alpha},\end{aligned}$$

since $\|n_0^{s+1}\| = \|n_0\|^{s+1}$, and we can use the first inequality (i.e., $\|n\| \leq n^{\alpha}$) on the term that is being subtracted. Thus,

$$\begin{aligned}\|n\| &\geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n_0{}^s)^{\alpha} \quad (\text{since } n \geq n_0{}^s)\\ &= n_0^{(s+1)\alpha}\left[1 - \left(1 - \frac{1}{n_0}\right)^{\alpha}\right]\\ &\geq C'n^{\alpha}\end{aligned}$$

for some constant C' which may depend on n_0 and α but not on n. As before, we now use this inequality for n^N, take Nth roots, and let $N \to \infty$, finally getting: $\|n\| \geq n^{\alpha}$.

Thus, $\|n\| = n^{\alpha}$. It easily follows from Property (2) of norms that $\|x\| = |x|^{\alpha}$ for all $x \in \mathbb{Q}$. In view of Exercise 8 below, which says that such a norm is equivalent to the absolute value $|\ |$, this concludes the proof of the theorem in Case (i).

Case (ii). Suppose that $\|n\| \leq 1$ for all positive integers n. Let n_0 be the least n such that $\|n\| < 1$; n_0 exists because we have assumed that $\|\ \|$ is nontrivial.

n_0 must be a prime, because if $n_0 = n_1 \cdot n_2$ with n_1 and n_2 both $<n_0$, then $\|n_1\| = \|n_2\| = 1$, and so $\|n_0\| = \|n_1\| \cdot \|n_2\| = 1$. So let p denote the prime n_0.

We claim that $\|q\| = 1$ if q is a prime not equal to p. Suppose not; then $\|q\| < 1$, and for some large N we have $\|q^N\| = \|q\|^N < \frac{1}{2}$. Also, for some large M we have $\|p^M\| < \frac{1}{2}$. Since p^M and q^N are relatively prime—have no common divisor other than 1—we can find (see Exercise 10) integers n and m such that: $mp^M + nq^N = 1$. But then

$$1 = \|1\| = \|mp^M + nq^N\| \leq \|mp^M\| + \|nq^N\| = \|m\|\,\|p^M\| + \|n\|\,\|q^N\|,$$

by Properties (2) and (3) in the definition of a norm. But $\|m\|, \|n\| \leq 1$, so that

$$1 \leq \|p^M\| + \|q^N\| < \tfrac{1}{2} + \tfrac{1}{2} = 1,$$

a contradiction. Hence $\|q\| = 1$.

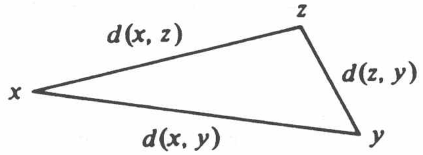
We're now virtually done, since any positive integer a can be factored into prime divisors: $a = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$. Then $\|a\| = \|p_1\|^{b_1} \cdot \|p_2\|^{b_2} \cdots \|p_r\|^{b_r}$. But the only $\|p_i\|$ which is not equal to 1 will be $\|p\|$ if one of the p_i's is p. Its corresponding b_i will be $\mathrm{ord}_p\, a$. Hence, if we let $\rho = \|p\| < 1$, we have

$$\|a\| = \rho^{\mathrm{ord}_p a}.$$

It is easy to see using Property (2) of a norm that the same formula holds with any nonzero rational number x in place of a. In view of Exercise 5 below, which says that such a norm is equivalent to $|\ |_p$, this concludes the proof of Ostrowski's theorem. □

Our intuition about distance is based, of course, on the Archimedean metric $|\ |_\infty$. Some properties of the non-Archimedean metrics $|\ |_p$ seem very strange at first, and take a while to get used to. Here are two examples.

For any metric, Property (3): $d(x, y) \leq d(x, z) + d(z, y)$ is known as the "triangle inequality," because in the case of the field $\mathbb{C}$ of complex numbers (with metric $d(a + bi, c + di) = \sqrt{(a - c)^2 + (b - d)^2}$) it says that in the complex plane the sum of two sides of a triangle is greater than the third side. (See the diagram.)



Let's see what happens with a non-Archimedean norm on a field F. For simplicity suppose $z = 0$. Then the non-Archimedean triangle inequality says: $\|x - y\| \leq \max(\|x\|, \|y\|)$. Suppose first that the "sides" x and y have different "length," say $\|x\| < \|y\|$. The third side $x - y$ has length

$$\|x - y\| \leq \|y\|.$$

But

$$\|y\| = \|x - (x - y)\| \leq \max(\|x\|, \|x - y\|).$$

Since $\|y\|$ is not $\leq \|x\|$, we must have $\|y\| \leq \|x - y\|$, and so $\|y\| = \|x - y\|$.