Fernando Q. Gouvêa

p-adic Numbers

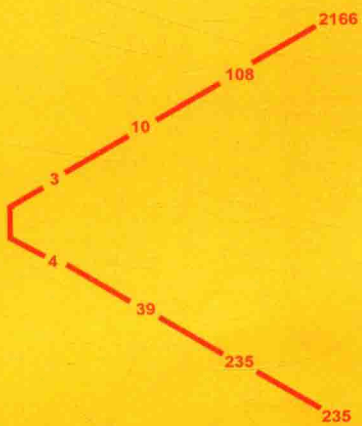
An Introduction

Second Edition

Universitext

*p*进数导论

第2版



Springer

世界图书出版公司
www.wpcbj.com.cn

Fernando Q. Gouvêa

p-adic Numbers

An Introduction

Second Edition 1997
With 15 Figures



Springer

Fernando Q. Gouvêa
Colby College
Department of Mathematics
Waterville, ME 04901
USA
e-mail: fqgouvea@colby.edu
URL: http://www.colby.edu/personal/f/fqgouvea/

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme
Gouvêa, Fernando Q.:
P-adic numbers : an introduction / Fernando Gouvêa. - 2. ed. - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1997
(Universitext)
ISBN 3-540-62911-4

Corrected 3rd printing 2003
ISBN 3-540-62911-4 Springer-Verlag Berlin Heidelberg New York

Mathematics Subject Classification (2000): 11-01, 11S-XX

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilm or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Reprint from English language edition:
p-adic Numbers: An Introduction Second Edition
by Fernando Q. Gouvêa
Copyright © Springer Berlin Heidelberg 1993, 1997
Springer Berlin Heidelberg is a part of Springer Science+Business Media
All Rights Reserved

This reprint has been authorized by Springer Science & Business Media for distribution in China Mainland only and not for export therefrom.

Contents

Introduction 1

1 Apéritif 7
1.1 Hensel's Analogy 7
1.2 Solving Congruences Modulo p^n 14
1.3 Other Examples 19

2 Foundations 23
2.1 Absolute Values on a Field 23
2.2 Basic Properties 29
2.3 Topology 32
2.4 Algebra 39

3 p-adic Numbers 43
3.1 Absolute Values on $\mathbb{Q}$ 43
3.2 Completions 49
3.3 Exploring $\mathbb{Q}_p$ 59
3.4 Hensel's Lemma 69
3.5 Local and Global 77

4 Elementary Analysis in $\mathbb{Q}_p$ 87
4.1 Sequences and Series 88
4.2 Functions, Continuity, Derivatives 92
4.3 Power Series 95
4.4 Functions Defined by Power Series 102
4.5 Some Elementary Functions 111
4.6 Interpolation 126

5 Vector Spaces and Field Extensions 133
5.1 Normed Vector Spaces over Complete Valued Fields 134
5.2 Finite-dimensional Normed Vector Spaces 139
5.3 Finite Field Extensions 143
5.4 Properties of Finite Extensions 158
5.5 Analysis 169
5.6 Example: Adjoining a p-th Root of Unity 171
5.7 On to $\mathbb{C}_p$ 176

6 Analysis in $\mathbb{C}_p$ 187
6.1 Almost Everything Extends 187
6.2 Deeper Results on Polynomials and Power Series 191
6.3 Entire Functions 208
6.4 Newton Polygons 212
6.5 Problems 231

A Hints and Comments on the Problems 235

B A Brief Glance at the Literature 291
B.1 Texts 291
B.2 Software 292
B.3 Other Books 293

Bibliography 295

Index 299

Introduction

In the course of their undergraduate careers, most mathematics majors see little beyond "standard mathematics:" basic real and complex analysis, abstract algebra, some differential geometry, etc. There are few adventures in other territories, and few opportunities to visit some of the more exotic corners of mathematics. The goal of this book is to offer such an opportunity, by way of a visit to the p-adic universe. Such a visit offers a glimpse of a part of mathematics which is both important and fun, and which also is something of a meeting point between algebra and analysis.

Over the last century, p-adic numbers and p-adic analysis have come to play a central role in modern number theory. This importance comes from the fact that they afford a natural and powerful language for talking about congruences between integers, and allow the use of methods borrowed from calculus and analysis for studying such problems. More recently, p-adic numbers have shown up in other areas of mathematics, and even in physics.

For all their importance, p-adic numbers are not an extremely difficult concept; in fact, they are quite accessible to an undergraduate audience. The goal of these notes is to realize this possibility, taking its readers for a short promenade along the p-adic path. Our aim is sightseeing, rather than a scientific expedition, so we will not worry too much if we fail to emphasize a subtle point here and there, nor if our theorems are less general than they could be, nor, in fact, if we do not learn all there is to know. Rather, our goal is to introduce the reader to the rather strange world of the p-adic numbers, and to begin to make it feel familiar. What we will cover will not be sufficient for those students which will need to use p-adic numbers as a research tool. For them, a lot more reading will be necessary (and in an appendix we discuss some of the texts that are available for further reading). Instead, we try to touch a lot of bases, and set the stage for further study.

There are many ways to begin our task. Of the available options, I chose to go with the theory of absolute values on fields, and to view the p-adic numbers as directly analogous to the real numbers. In this approach, the main ingredient is a change of attitude about absolute values. It starts with the observation that from an *algebraic* point of view there is no reason to view the usual absolute value on the field $\mathbb{Q}$ of rational numbers as a given. Rather, any function satisfying the same basic properties should be just as

good. If we start with the usual absolute value and look for a completion[1] of $\mathbb{Q}$ as a metric space, we get the real numbers; starting with a different absolute value, we get something else. What that something else is, and why it is interesting, is the subject of this book.

Besides its importance, the study of p-adic numbers is attractive because it blends together so many parts of mathematics. While it is certainly a part of number theory, its language is often the language of analysis, and its theorems are often analogous to, but slightly different from, those found in calculus textbooks. Both the analogy and the differences are fascinating, so that at times one gets the feeling that things are slightly out of whack, and p-adic analysis seems like classical analysis in a distorting mirror. I have tried to include many examples of this sort of thing, and I hope they are convincing.

I have done much less to convince the reader that p-adic numbers are actually useful. For the most part, I have limited myself to stating that certain things are true or that certain methods are fruitful. In every case, developing the details of the application would make this book much harder than it is supposed to be. Once again, a lot can be learned from other texts, and the student who wants to know should go to the references mentioned in the text and in the appendix.

One final pointer to Appendix B is in order. While they are working through the book, some readers may enjoy being able to work with a computer software package that can handle p-adic numbers. There aren't many of these, but a note about those that do exist has been added to the discussion of other sources of information.

Some business: the pre-requisites for reading this book are a basic knowledge of algebra and number theory, and a few courses in calculus or analysis. To be a bit more precise, the reader should be familiar with the language of congruences, with the basic theory of fields and rings, and with basic concepts about point-set topology, continuity, and infinite series. I have tried to provide as many definitions (and also informal descriptions) as I could, consistent with the requirement that the result not be too ungainly. I hope that this approach may be useful both to refresh students' memories of other subjects and to display the unity and interconnectedness of mathematics in a dramatic way.

The use of the topics mentioned above as pre-requisites is not uniform. Most students will know enough to read the first few chapters without needing to run back to their textbooks from other courses. The analysis requirements become more serious beginning in Chapter 4, and the algebraic requirements come in more strongly in Chapter 5. Even so, the whole book remains[2] well within the reach of undergraduate mathematics majors.

[1] If you're wondering what a "completion" is, the definition will be met later, in full gory detail. Don't worry about it yet.

[2] I hope!

There are many kinds of books about mathematics, from encyclopedic treatises to brief surveys, from dry as dust to boringly chatty. This book is closer to being a survey than to being encyclopedic, and is intended to be easy to read, but not as bed-time reading: the reader is expected to do some work. (Maybe even a lot of work.) To this end, I have included a great many problems throughout. The problems are meant to be solved, or at least attempted, at about the time when they are met in the text.[3] Most of them offer an opportunity to work with concepts that have just been introduced, and it is the author's fond hope that such problems will help create familiarity with the material. The majority of these problems ask the reader to work out the details of arguments which have been only sketched in the text, or to supply the proofs for statements given in the text (for the most part, this is only done when the proof is straightforward, and even then hints are often given). Other problems stretch out to mention matters not touched upon in the text, to indicate to the reader that there are many themes we have not had time to discuss. Finally, many are intended to prepare the reader for the discussion to follow. Such problems will often become trivial in the light of what comes later (they may be special cases or simple corollaries of theorems we will prove); leaving them for later will only render them boring.

Besides offering practice and a chance of active interaction with the material, the many problems are intended to stimulate the reader to read in a certain way. In many mathematics textbooks, one finds proofs that are "left to the reader" or dismissed as "clear" and throwaway lines mentioning interesting sidelines to the material being discussed. The experienced mathematical reader knows that these are signals to dig out pencil and paper and verify what has been said. In this book, I have tried to make sure that most such signals are followed by explicit problems. My hope is that this will help my less experienced readers gain experience of how to interact with mathematical texts.

A note to the specialists: this book is intended as a pedagogical tool. It is *not* intended as a replacement for the standard references (it is much too sketchy for that), nor as a model of elegant or detailed treatment of this (or any other) subject. Rather, I have tried to make it fun to work with, demanding, and ample. I have often spent time discussing interesting mathematics (the point-set topology, for example, or the various definitions of the field norm) just because it was interesting. I welcome any comments, and ask students in particular to tell me their reactions.

Every writer creates in his or her mind an imaginary audience for his or her text. In the case of this book, what I imagined was an upper-level undergraduate course for mathematics majors. It would include honest-to-goodness

[3] I realize this is very different from what most of my readers are used to. Try to think of this text as a workbook rather than a textbook: each thing should be done in turn, before going on to the next step.

undergraduates and not only graduate-level students who just happen not to have finished their undergraduate degrees yet. (In other words, this is not only for hot-shots, though hot-shots should be welcome too.) The course would very likely use an approach where students are asked to read the text, attempt the problems, and discuss the results with each other and with their instructor. The many problems asking the reader to "make a conjecture," or to attempt something ("Can you...") presuppose such a situation. For emergencies, I have provided some hints and comments on the problems. These are usually not complete solutions, but rather attempts to jump-start the solution process; they should be used only after some meditation on the problem, or they may spoil the fun.

This book grew from a set of notes for a mini-course given at the "17° Colóquio Brasileiro de Matemática," the 1989 edition of the bi-annual congress of Brazilian mathematicians. It has since been used in a course (much like the one described above) at Colby College. I would like to thank the organizers of the "Colóquio" for their invitation, and also to thank the students who sat through preliminary versions of this material for their interest and for their patience with its shortcomings. Many shortcomings will undoubtedly remain, and I would like to hear about them (who knows, there may even be a second edition someday). Please drop me a note if you have any comments.

During the final stages of the writing of this book, the author's research was partially supported by NSF grant number DMS–9203469. The writing was done in three phases, at the Universidade de São Paulo, at Queen's University at Kingston, Ontario, and at Colby College. I would like to thank NSF and all three universities for their support; Colby College, where most of the work was done, and whose computer equipment is responsible for the physical existence of this book, deserves special thanks for providing pleasant and fruitful working conditions.

This book was typeset in LaTeX using several different kinds of computers and a large number of standard macro packages. It depends, thus, on the work of many people who have given of their talents to the community of TeX users. I thank you all.

Finally, I would also like to thank César Polcino, of the Universidade de São Paulo, who first put a book on p-adic numbers in my hands, and Noriko Yui, of Queen's University, who insisted that I develop the original notes into this book; the project would not have been undertaken without them.

Note on the second edition: I am grateful to Springer-Verlag for giving me the opportunity to revise the book for this new printing. The largest changes happened in chapter four. I'd like to thank the various people who made comments and suggestions, including Silvio Levy, Alain Robert, and especially Keith Conrad.

Note on the second printing of the second edition: The need for a new printing has given me the opportunity to correct several typos, update references, and make a few small changes in the text.

Note on the third printing of the second edition: The main change for this new printing was to correct the numbering of the solutions to the problems, which was incorrect in the previous printing. I apologize to those who were inconvenienced by that mistake. Other than that, I have only made a few minor changes.

I'd like to thank the many people who found typos, made suggestions and comments, and generally gave me useful feedback. You are all encouraged to keep at it!

τι ποιεῖτε, πάντα εἰς δόξαν θεοῦ ποιεῖτε

1 Apéritif

The idea of considering new ways to measure the "distance" between two rational numbers, and then of considering the corresponding completions, did not arise merely from some desire to generalize, but rather from several concrete situations involving problems from algebra and number theory. The new "metrics" on $\mathbb{Q}$ will be each connected to a certain prime, and they will "codify" a great deal of arithmetic information related to that prime. The goal of this first chapter is to offer an *informal* introduction to these ideas. Thus, we proceed without worrying too much about mathematical rigor[1] or precision, but rather emphasizing the ideas that are behind what we are trying to accomplish. Then, in the next chapter, we will begin to develop the theory in a more formal way.

1.1 Hensel's Analogy

The p-adic numbers were first introduced by the German mathematician K. Hensel (though they are foreshadowed in the work of his predecessor E. Kummer). It seems that Hensel's main motivation was the analogy between the ring of integers $\mathbb{Z}$, together with its field of fractions $\mathbb{Q}$, and the ring $\mathbb{C}[X]$ of polynomials with complex coefficients, together with its field of fractions $\mathbb{C}(X)$. To be specific, an element of $f(X) \in \mathbb{C}(X)$ is a "rational function," i.e., a quotient of two polynomials:

$$f(X) = \frac{P(X)}{Q(X)},$$

with $P(X), Q(X) \in \mathbb{C}[X]$, $Q(X) \neq 0$; similarly, any rational number $x \in \mathbb{Q}$ is a quotient of two integers:

$$x = \frac{a}{b},$$

with $a, b \in \mathbb{Z}$, $b \neq 0$. Furthermore, the properties of the two rings are quite similar: both $\mathbb{Z}$ and $\mathbb{C}[X]$ are rings where there is *unique factorization*: any integer can be expressed uniquely as ± 1 times a product of primes, and any polynomial can be expressed uniquely as

$$P(X) = a(X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_n),$$

[1] which always runs the risk of becoming mathematical *rigor mortis*...

where a and $\alpha_1, \alpha_2, \ldots \alpha_n$ are complex numbers. This gives us the main point of the analogy Hensel explored: *The primes $p \in \mathbb{Z}$ are analogous to the linear polynomials $X - \alpha \in \mathbb{C}[X]$*

So far, we have nothing that is really notable, but Hensel noticed that the analogy, as it stands, goes a little deeper. Suppose we are given a polynomial $P(X)$ and a particular $\alpha \in \mathbb{C}$. Then it is possible (for example, using a Taylor expansion) to write the polynomial in the form

$$\begin{aligned} P(X) &= a_0 + a_1(X-\alpha) + a_2(X-\alpha)^2 + \cdots + a_n(X-\alpha)^n \\ &= \sum_{i=0}^{n} a_i(X-\alpha)^i \end{aligned}$$

with $a_i \in \mathbb{C}$. Now this also works naturally for integers (let's stick to positive integers for now): given a positive integer m and a prime[2] p, we can write it "in base p," that is, in the form

$$m = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n = \sum_{i=0}^{n} a_i p^i$$

with $a_i \in \mathbb{Z}$ and $0 \leq a_i \leq p-1$.

The reason such expansions are interesting is that they give "local" information: the expansion in powers of $(X-\alpha)$ will show, for example, if $P(X)$ vanishes at α, and to what order. Similarly, the expansion "in base p" will show if m is divisible by p, and to what order. For example, expanding 72 in base 3 gives

$$72 = 0 + 0 \times 3 + 2 \times 3^2 + 2 \times 3^3,$$

which shows at once that 72 is divisible by 3^2.

Now, for polynomials and their quotients, one can in fact push this much further. Taking $f(X) \in \mathbb{C}(X)$ and $\alpha \in \mathbb{C}$, there is always an expansion

$$\begin{aligned} f(X) = \frac{P(X)}{Q(X)} &= a_{n_0}(X-\alpha)^{n_0} + a_{n_0+1}(X-\alpha)^{n_0+1} + \ldots \\ &= \sum_{i \geq n_0} a_i(X-\alpha)^i \end{aligned}$$

This is just the Laurent expansion from complex analysis, but in our case it can be very easily obtained by simply doing long division with the expansions of $P(X)$ and of $Q(X)$. Notice that it is a much more complicated object than the preceding expansion:

- We can have $n_0 < 0$, that is, the expansion can begin with a negative exponent; this would signal that α is a root of $Q(X)$ and not of $P(X)$ (more precisely, that its multiplicity as a root of $Q(X)$ is bigger). In the language of analysis, we would say that $f(X)$ has a *pole* at α, of order $-n_0$.

[2] Remember that in the analogy choosing $(X-\alpha)$ corresponds to choosing a prime.

- The expansion will usually not be finite. In fact, it will only be finite if when we write $f(X) = P(X)/Q(X)$ in lowest terms then $Q(X)$ happens to be a power of $(X - \alpha)$ (can you prove that?). In other words, this is usually an infinite series, and it can be shown that the series for $f(\lambda)$ will converge whenever λ is close enough (but not equal to) α. However, since we want to focus on the algebraic structure here, we will treat the series as a *formal* object: it is just there, and we do not care about convergence.

Here's an example. Take the rational function

$$f(X) = \frac{X}{X-1},$$

and let's look at the expansions for different α. (This is a calculus exercise.) If $\alpha = 0$, we get

$$\frac{X}{X-1} = -X - X^2 - X^3 - X^4 - \dots$$

which shows that $f(0) = 0$ with multiplicity one. For $\alpha = 1$, we get

$$\frac{X}{X-1} = \frac{1 + X - 1}{X-1} = (X-1)^{-1} + 1$$

which highlights the pole of order one at $\alpha = 1$ (and also gives an example of an expansion that is finite). Finally, if we take, say, $\alpha = 2$, where there is neither pole nor zero, we get

$$\frac{X}{X-1} = 2 - (X-2) + (X-2)^2 - (X-2)^3 + \dots$$

Problem 1 Refresh your calculus skills by checking these three equalities. Can you find the region of convergence? (Hint: all you need to remember is the geometric series.)

Problem 2 Suppose $f(X) = P(X)/Q(X)$ is in lowest terms, so that $P(X)$ and $Q(X)$ have no common zeros. Show that the expansion of $f(X)$ in powers of $(X - \alpha)$ is finite if and only if $Q(X) = (X - \alpha)^m$ for some $m \geq 0$.

The punchline is that any rational function can be expanded into a series of this kind in terms of each of the "primes" $(X-\alpha)$. (The quotes aren't really necessary, since the ideals generated by the elements of the form $(X - \alpha)$ are exactly the prime ideals of the ring $\mathbb{C}[X]$, so that $(X - \alpha)$ is a rightful bearer of the title of "prime." But all that comes later.) On the other hand, not all such series come from rational functions. In fact, we have already met examples in our calculus courses: the series for $\sin(X)$, say, or the series for e^X, which cannot be expansions of any rational function (calculus exercise: why not?).

Now, from an algebraic point of view, here's how to read the situation. We have two fields: the field $\mathbb{C}(X)$ of all rational functions, and another field which consists of all Laurent series in $(X-\alpha)$. (The next exercise asks you to check that it is indeed a field.) Let's denote the second by $\mathbb{C}((X-\alpha))$. Then the function

$$f(X) \mapsto \text{expansion around } (X-\alpha)$$

defines an *inclusion* of fields

$$\mathbb{C}(X) \hookrightarrow \mathbb{C}((X-\alpha)).$$

There are, of course, infinitely many of these (one for each α), and each one contains "local" information about how rational functions behave near α.

Problem 3 Let $\mathbb{C}((X-\alpha))$ be the set of all finite-tailed Laurent series (with complex coefficients) in $(X-\alpha)$

$$f(X) = \sum_{i \geq n_0} a_i (X-\alpha)^i.$$

Define the sum and product of two elements of $\mathbb{C}((X-\alpha))$ in the "obvious" way, and show that the resulting object is a field. Show that one may in fact take the coefficients to be in any field, with the same result.

Hensel's idea was to extend the analogy between $\mathbb{Z}$ and $\mathbb{C}[X]$ to include the construction of such expansions. Recall that the analogue of choosing α is choosing a prime number p. As we have already seen, we already know the expansion for a positive integer m: it is just the "base p" representation of m:

$$m = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n,$$

with $a_i \in \mathbb{Z}$, $0 \leq a_i \leq p-1$. As in the case of polynomials, this is a finite expression[3].

To pass from positive integers to positive rationals, we simply do exactly as in the other case, that is, we expand both numerator and denominator in powers of p, and then *divide formally*. The only thing one has to be careful with is that one may have to "carry." The sum of two of our a_i, for example, may be larger than p, and one has to do the obvious thing. It's probably easier to go straight to an example.

Let's take $p = 3$, and consider the rational number $24/17$. Then we have

$$a = 24 = 0 + 2 \times 3 + 2 \times 3^2 = 2p + 2p^2$$

and

$$b = 17 = 2 + 2 \times 3 + 1 \times 3^2 = 2 + 2p + p^2.$$

[3]The condition $0 \leq a_i \leq p-1$ may seem to break the analogy with the complex case. But not so! The point is that the quotient of $\mathbb{C}[X]$ by the ideal generated by $(X-\alpha)$ is isomorphic to $\mathbb{C}$, and the constants in $\mathbb{C}[X]$ give a "canonical" choice of coset representatives. Similarly, the numbers between 0 and $p-1$ are a choice of coset representatives for the quotient of $\mathbb{Z}$ by the ideal generated by p.

(Though of course $p = 3$, it's probably less confusing to write p, because one is less tempted to "add it all up." The point is to operate *formally* with our expansions.)

Then the expansion of $a/b = 24/17$ is

$$\frac{a}{b} = \frac{24}{17} = \frac{2p + 2p^2}{2 + 2p + p^2} = p + p^3 + 2p^5 + p^7 + p^8 + 2p^9 + \dots$$

To check that this is correct, all we need to do is to multiply it by (the expansion of) 17, remembering that $p = 3$:

$$(2 + 2p + p^2)(p + p^3 + 2p^5 + p^7 + p^8 + 2p^9 + \dots) =$$

$$= 2p + 2p^2 + \underbrace{p^3 + 2p^3} + 2p^4 + p^5 + 4p^5 + 4p^6 +$$
$$+ 2p^7 + 2p^7 + 2p^8 + 2p^8 + p^9 + 2p^9 + 4p^9 \dots$$

since $p = 3$, we get $p^3 + 2p^3 = 3p^3 = p^4$, so

$$= 2p + 2p^2 + \underbrace{p^4 + 2p^4} + p^5 + 4p^5 + 4p^6 + 2p^7 + 2p^7 +$$
$$+ 2p^8 + 2p^8 + p^9 + 2p^9 + 4p^9 + \dots$$

$$= 2p + 2p^2 + \underbrace{p^5 + p^5 + 4p^5} + 4p^6 + 2p^7 + 2p^7$$
$$+ 2p^8 + 2p^8 + p^9 + 2p^9 + 4p^9 + \dots$$

$$= 2p + 2p^2 + \underbrace{2p^6 + 4p^6} + 2p^7 + 2p^7 + 2p^8 + p^9 + 2p^8 + 2p^9 + 4p^9 + \dots$$

$$= 2p + 2p^2 + \underbrace{2p^7 + 2p^7 + 2p^7} + 2p^8 + 2p^8 + p^9 + 2p^9 + 4p^9 + \dots$$

$$= 2p + 2p^2 + \underbrace{2p^8 + 2p^8 + 2p^8} + p^9 + 2p^9 + 4p^9 + \dots$$

$$= \dots$$

$$= 2p + 2p^2$$

so that the higher powers of p disappear "to the right," leaving us with $2p + 2p^2 = 24$! (The reader will probably feel something has been shoved under the rug, and in fact there is something to prove here. But the point is that, at least formally, it works.)

Provided that one can treat the whole process formally, it is easy to check that this always works, and that the resulting series reflects the properties of the rational number $x = a/b$ as regards the prime number p (we will get into the habit of saying "locally at p" or even "near p," to emphasize the analogy). Thus, for each prime p, we can write any (positive, for now) rational number a/b in the form

$$x = \frac{a}{b} = \sum_{n \geq n_0} a_n p^n,$$

and, for example, we have $n_0 \geq 0$ if and only if $p \nmid b$, and $n_0 > 0$ if and only if $p \nmid b$ and $p|a$ (assuming a/b is in lowest terms). In fact, the number n_0 (which is something like the order of a zero or pole) reflects the "multiplicity" of p in a/b; it is characterized by the equation

$$x = p^{n_0} \frac{a_1}{b_1} \qquad \text{with} \quad p \nmid a_1 b_1.$$

It remains to see how to get the negative rational numbers, but since our power series in p can clearly (see Problem 5) be multiplied, it is enough to get an expansion for -1. Keeping in mind that we are working formally, and with a little imagination, that is not too hard to do. We find, for any p, that

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + (p-1)p^3 + \cdots,$$

since, if we add 1, we get

$$\begin{aligned} &\underbrace{1 + (p-1)} + (p-1)p + (p-1)p^2 + (p-1)p^3 + \cdots = \\ &= \underbrace{p + (p-1)p} + (p-1)p^2 + (p-1)p^3 + \cdots \\ &= \underbrace{p^2 + (p-1)p^2} + (p-1)p^3 + \cdots \\ &= \cdots \\ &= 0. \end{aligned}$$

The conclusion is that, at least in a formal sense, every rational number x can be written as a "finite-tailed Laurent series in powers of p"

$$x = a_{n_0} p^{n_0} + a_{n_0+1} p^{n_0+1} + \ldots$$

("finite-tailed" refers, of course, to the fact that the expansion is finite *to the left*; it is usually infinite to the right). We will call this the *p-adic expansion* of x; remember that if x is a positive integer, it is just its expansion "in base p."