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 $\mathbf{Q}$ of rational numbers and the field $\mathbf{R}$ 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 $\mathbf{Q}$ 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 $\mathbf{Q}$ but with various "extension fields" which contain $\mathbf{Q}$.

2. Metrics on the rational numbers

We know one metric on $\mathbf{Q}$, 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 $\operatorname{ord}_p a$, 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,

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

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

Now for any rational number $x = a/b$, define $\operatorname{ord}_p x$ to be $\operatorname{ord}_p a - \operatorname{ord}_p b$. 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 $\operatorname{ord}_p x = \operatorname{ord}_p ac - \operatorname{ord}_p bc$.

Further define a map $|\ |_p$ on $\mathbf{Q}$ as follows:

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

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

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 $\operatorname{ord}_p(x + y) = \operatorname{ord}_p(ad + bc) - \operatorname{ord}_p b - \operatorname{ord}_p d$. 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

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

Therefore, $|x + y|_p = p^{-\operatorname{ord}_p(x+y)} \leq \max(p^{-\operatorname{ord}_p x}, p^{-\operatorname{ord}_p y}) = \max(|x|_p, |y|_p)$, 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 $\mathbf{Q}$.

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

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 $(1/p)^{\operatorname{ord}_p x}$ we could have written $\rho^{\operatorname{ord}_p x}$ 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* $\mathbf{Q}$ *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

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

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 $\|q\| = 1$.

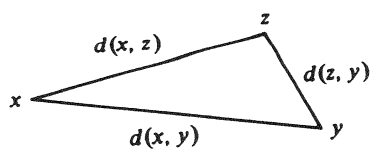
We're now virtually done, since any positive integer a can be factored into prime divisors: $a = {p_1}^{b_1}{p_2}^{b_2} \cdots {p_r}^{b_r}$. Then $\|a\| = \|p_1\|^{b_1} \cdot \|p_2\|^{b_2} \cdots \|p_r\|^{b_r}$. But the only $\|p_i\|$ which is not equal to 1 will be $\|p\|$ if one of the p_i's is p.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

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

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 $\|y\| = \|x - y\|$.

Thus, if our two sides x and y are not equal in length, the longer of the two must have the same length as the third side. Every "triangle" is isosceles!

This really shouldn't be too surprising if we think what this says in the case of $|\ |_p$ on $\mathbb{Q}$. It says that, if two rational numbers are divisible by different powers of p, then their difference is divisible precisely by the *lower* power of p (which is what it means to be the same "size" as the *bigger* of the two).

This basic property of a non-Archimedean field—that $\|x \pm y\| \leq \max(\|x\|, \|y\|)$, with equality holding if $\|x\| \neq \|y\|$—will be referred to as the "isosceles triangle principle" from now on.

As a second example, we define the (open) disc of radius r (r is a positive real number) with center a (a is an element in the field F) to be

$$D(a, r^-) = \{x \in F \mid \|x - a\| < r\}.$$

Suppose $\|\ \|$ is a non-Archimedean norm. Let b be *any* element in $D(a, r^-)$. Then

$$D(a, r^-) = D(b, r^-),$$

i.e., every point in the disc is a center! Why is this? Well

$$\begin{aligned} x \in D(a, r^-) &\Rightarrow \|x - a\| < r \\ &\Rightarrow \|x - b\| = \|(x - a) + (a - b)\| \\ &\qquad \leq \max(\|x - a\|, \|a - b\|) \\ &\qquad < r \\ &\Rightarrow x \in D(b, r^-), \end{aligned}$$

and the reverse implication is proved in the exact same way.

If we define the closed disc of radius r with center a to be

$$D(a, r) = \{x \in F \mid \|x - a\| \leq r\},$$

for non-Archimedean $\|\ \|$ we similarly find that every point in $D(a, r)$ is a center.

Exercises

1. For any norm $\|\ \|$ on a field F, prove that addition, multiplication, and finding the additive and multiplicative inverses are continuous. This means that: (1) for any $x, y \in F$ and any $\varepsilon > 0$, there exists $\delta > 0$ such that $\|x' - x\| < \delta$ and $\|y' - y\| < \delta$ imply $\|(x' + y') - (x + y)\| < \varepsilon$; (2) the same statement with $\|(x' + y') - (x + y)\|$ replaced by $\|x'y' - xy\|$; (3) for any nonzero $x \in F$ and any $\varepsilon > 0$, there exists $\delta > 0$ such that $\|x' - x\| < \delta$ implies $\|(1/x') - (1/x)\| < \varepsilon$; (4) for any $x \in F$ and any $\varepsilon > 0$, there exists $\delta > 0$ such that $\|x' - x\| < \delta$ implies $\|(-x') - (-x)\| < \varepsilon$.

2. Prove that if $\|\ \|$ is any norm on a field F, then $\|-1\| = \|1\| = 1$. Prove that if $\|\ \|$ is non-Archimedean, then for any integer n: $\|n\| \leq 1$. (Here "n" means the result of adding $1 + 1 + 1 + \cdots + 1$ together n times in the field F.)

3. Prove that, conversely, if $\|\ \|$ is a norm such that $\|n\| \leq 1$ for every integer n, then $\|\ \|$ is non-Archimedean.

4. Prove that a norm $\|\ \|$ on a field F is non-Archimedean if and only if

$$\{x \in F \mid \|x\| < 1\} \cap \{x \in F \mid \|x - 1\| < 1\} = \varnothing.$$

5. Let $\|\ \|_1$ and $\|\ \|_2$ be two norms on a field F. Prove that $\|\ \|_1 \sim \|\ \|_2$ if and only if there exists a positive real number α such that: $\|x\|_1 = \|x\|_2^\alpha$ for all $x \in F$.

6. Prove that, if $0 < \rho < 1$, then the function on $x \in \mathbb{Q}$ defined as $\rho^{\mathrm{ord}_p x}$ if $x \neq 0$ and 0 if $x = 0$, is a non-Archimedean norm. Note that by the previous problem it is equivalent to $|\ |_p$. What happens if $\rho = 1$? What about if $\rho > 1$?

7. Prove that $|\ |_{p_1}$ is not equivalent to $|\ |_{p_2}$ if p_1 and p_2 are different primes.

8. For $x \in \mathbb{Q}$ define $\|x\| = |x|^\alpha$ for a fixed positive number α, where $|\ |$ is the usual absolute value. Show that $\|\ \|$ is a norm if and only if $\alpha \leq 1$, and that in that case it is equivalent to the norm $|\ |$.

9. Prove that two equivalent norms on a field F are either both non-Archimedean or both Archimedean.

10. Prove that, if N and M are relatively prime integers, then there exist integers n and m such that $nN + mM = 1$.

11. Evaluate:

(i) $\mathrm{ord}_3 54$	(ii) $\mathrm{ord}_2 128$	(iii) $\mathrm{ord}_3 57$
(iv) $\mathrm{ord}_7(-700/197)$	(v) $\mathrm{ord}_2(128/7)$	(vi) $\mathrm{ord}_3(7/9)$
(vii) $\mathrm{ord}_5(-0.0625)$	(viii) $\mathrm{ord}_3(10^9)$	(ix) $\mathrm{ord}_3(-13.23)$
(x) $\mathrm{ord}_7(-13.23)$	(xi) $\mathrm{ord}_5(-13.23)$	(xii) $\mathrm{ord}_{11}(-13.23)$
(xiii) $\mathrm{ord}_{13}(-26/169)$	(xiv) $\mathrm{ord}_{103}(-1/309)$	(xv) $\mathrm{ord}_3(9!)$

12. Prove that $\mathrm{ord}_p((p^N)!) = 1 + p + p^2 + \cdots + p^{N-1}$.

13. If $0 \leq a \leq p - 1$, prove that: $\mathrm{ord}_p((ap^N)!) = a(1 + p + p^2 + \cdots + p^{N-1})$.

14. Prove that, if $n = a_0 + a_1 p + a_2 p^2 + \cdots + a_s p^s$ is written to the base p, so that $0 \leq a_i \leq p - 1$, and if we set $S_n = \sum a_i$ (the sum of the digits to the base p), then we have the formula:

$$\mathrm{ord}_p(n!) = \frac{n - S_n}{p - 1}.$$

15. Evaluate $|a - b|_p$, i.e., the p-adic distance between a and b, when:

(i) $a = 1, b = 26, p = 5$	(ii) $a = 1, b = 26, p = \infty$
(iii) $a = 1, b = 26, p = 3$	(iv) $a = 1/9, b = -1/16, p = 5$
(v) $a = 1, b = 244, p = 3$	(vi) $a = 1, b = 1/244, p = 3$
(vii) $a = 1, b = 1/243, p = 3$	(viii) $a = 1, b = 183, p = 13$
(ix) $a = 1, b = 183, p = 7$	(x) $a = 1, b = 183, p = 2$
(xi) $a = 1, b = 183, p = \infty$	(xii) $a = 9!, b = 0, p = 3$
(xiii) $a = (9!)^2/3^9, b = 0, p = 3$	(xiv) $a = 2^{2^N}/2^N, b = 0, p = 2$
(xv) $a = 2^{2^N}/(2^N)!, b = 0, p = 2.$	

16. Say in words what it means for a rational number x to satisfy $|x|_p \leq 1$.

17. For $x \in \mathbb{Q}$, prove that $\lim_{i \to \infty} |x^i/i!|_p = 0$ if and only if: $\text{ord}_p x \geq 1$ when $p \neq 2$, $\text{ord}_2 x \geq 2$ when $p = 2$.

18. Let x be a nonzero rational number. Prove that the product over *all* primes *including* ∞ of $|x|_p$ equals 1. (Notice that this "infinite product" actually only includes a finite number of terms that are not equal to 1.) Symbolically, $\prod_p |x|_p = 1$.

19. Prove that for any p ($\neq \infty$), any sequence of integers has a subsequence which is Cauchy with respect to $|\ |_p$.

20. Prove that if $x \in \mathbb{Q}$ and $|x|_p \leq 1$ for every prime p, then $x \in \mathbb{Z}$.

3. Review of building up the complex numbers

We now have a new concept of distance between two rational numbers: two rational numbers are considered to be close if their difference is divisible by a large power of a fixed prime p. In order to work with this so-called "p-adic metric" we must enlarge the rational number field $\mathbb{Q}$ in a way analogous to how the real numbers $\mathbb{R}$ and then the complex numbers $\mathbb{C}$ were constructed in the classical Archimedean metric $|\ |$. So let's review how this was done.

Let's go back even farther, logically and historically, than $\mathbb{Q}$. Let's go back to the natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$. Every step in going from $\mathbb{N}$ to $\mathbb{C}$ can be analyzed in terms of a desire to do two things:

(1) Solve polynomial equations.
(2) Find limits of Cauchy sequences, i.e., "complete" the number system to one "without holes," in which every Cauchy sequence has a limit in the new number system.

First of all, the integers $\mathbb{Z}$ (including $0, -1, -2, \ldots$) can be introduced as solutions of equations of the form

$$a + x = b, \qquad a, b \in \mathbb{N}.$$

Next, rational numbers can be introduced as solutions of equations of the form

$$ax = b, \qquad a, b \in \mathbb{Z}.$$

So far we haven't used any concept of distance.

One of the possible ways to give a careful definition of the real numbers is to consider the set S of Cauchy sequences of rational numbers. Call two Cauchy sequences $s_1 = \{a_j\} \in S$ and $s_2 = \{b_j\} \in S$ equivalent, and write $s_1 \sim s_2$, if $|a_j - b_j| \to 0$ as $j \to \infty$. This is obviously an equivalence relation, that is, we have: (1) any s is equivalent to itself; (2) if $s_1 \sim s_2$, then $s_2 \sim s_1$; and (3) if $s_1 \sim s_2$ and $s_2 \sim s_3$, then $s_1 \sim s_3$. We then define $\mathbb{R}$ to be the set of *equivalence classes* of Cauchy sequences of rational numbers. It is not hard

to define addition, multiplication, and finding additive and multiplicative inverses of equivalence classes of Cauchy sequences, and to show that $\mathbb{R}$ is a field. Even though this definition seems rather abstract and cumbersome at first glance, it turns out that it gives no more nor less than the old-fashioned real number line, which is so easy to visualize.

Something similar will happen when we work with $|\ |_p$ instead of $|\ |$: starting with an abstract definition of the p-adic completion of $\mathbb{Q}$, we'll get a very down-to-earth number system, which we'll call $\mathbb{Q}_p$.

Getting back to our historical survey, we've gotten as far as $\mathbb{R}$. Next, returning to the first method—solving equations—mathematicians decided that it would be a good idea to have numbers that could solve equations like $x^2 + 1 = 0$. (This is taking things in logical order; historically speaking, the definition of the complex numbers came before the rigorous definition of the real numbers in terms of Cauchy sequences.) Then an amazing thing happened! As soon as $i = \sqrt{-1}$ was introduced and the field of complex numbers of the form $a + bi$, $a, b \in \mathbb{R}$, was defined, it turned out that:

(1) *All* polynomial equations with coefficients in $\mathbb{C}$ have solutions in $\mathbb{C}$—this is the famous Fundamental Theorem of Algebra (the concise terminology is to say that $\mathbb{C}$ is *algebraically closed*); and
(2) $\mathbb{C}$ is already "complete" with respect to the (unique) norm which extends the norm $|\ |$ on $\mathbb{R}$ (this norm is given by $|a + bi| = \sqrt{a^2 + b^2}$), i.e., any Cauchy sequence $\{a_j + b_j i\}$ has a limit of the form $a + bi$ (since $\{a_j\}$ and $\{b_j\}$ will each be Cauchy sequences in $\mathbb{R}$, you just let a and b be their limits).

So the process stops with $\mathbb{C}$, which is only a "quadratic extension" of $\mathbb{R}$ (i.e., obtained by adjoining a solution of the quadratic equation $x^2 + 1 = 0$). *$\mathbb{C}$ is an algebraically closed field which is complete with respect to the Archimedean metric.*

But alas! Such is not to be the case with $|\ |_p$. After getting $\mathbb{Q}_p$, the completion of $\mathbb{Q}$ with respect to $|\ |_p$, we must then form an *infinite* sequence of field extensions obtained by adjoining solutions to higher degree (not just quadratic) equations. Even worse, the resulting algebraically closed field, which we denote $\overline{\mathbb{Q}}_p$, is *not complete*. So we take this already gigantic field and "fill in the holes" to get a still larger field Ω.

What happens then? Do we now have to enlarge Ω to be able to solve polynomial equations with coefficients in Ω? Does this process continue on and on, in a frightening spiral of ever more far-fetched abstractions? Well, fortunately, with Ω the guardian angel of p-adic analysis intervenes, and it turns out that Ω is already algebraically closed, as well as complete, and our search for the non-Archimedean analogue of $\mathbb{C}$ is ended.

But this Ω, which will be the convenient number system in which to study the p-adic analogy of calculus and analysis, is much less thoroughly understood than $\mathbb{C}$. As I. M. Gel'fand has remarked, some of the simplest

questions, e.g., characterizing $\mathbb{Q}_p$-linear field automorphisms of Ω, remain unanswered.

So let's begin our journey to Ω.

4. The field of p-adic numbers

For the rest of this chapter, we fix a prime number $p \neq \infty$.

Let S be the set of sequences $\{a_i\}$ of rational numbers such that, given $\varepsilon > 0$, there exists an N such that $|a_i - a_{i'}|_p < \varepsilon$ if both $i, i' > N$. We call two such Cauchy sequences $\{a_i\}$ and $\{b_i\}$ equivalent if $|a_i - b_i|_p \to 0$ as $i \to \infty$. We define the set $\mathbb{Q}_p$ to be the set of equivalence classes of Cauchy sequences.

For any $x \in \mathbb{Q}$, let $\{x\}$ denote the "constant" Cauchy sequence all of whose terms equal x. It is obvious that $\{x\} \sim \{x'\}$ if and only if $x = x'$. The equivalence class of $\{0\}$ is denoted simply by 0.

We define the norm $|\ |_p$ of an equivalence class a to be $\lim_{i\to\infty} |a_i|_p$, where $\{a_i\}$ is any representative of a. The limit exists because

(1) If $a = 0$, then by definition $\lim_{i\to\infty} |a_i|_p = 0$.
(2) If $a \neq 0$, then for some ε and for every N there exists an $i_N > N$ with $|a_{i_N}|_p > \varepsilon$.

If we choose N large enough so that $|a_i - a_{i'}|_p < \varepsilon$ when $i, i' > N$, we have:

$$|a_i - a_{i_N}|_p < \varepsilon \quad \text{for all } i > N.$$

Since $|a_{i_N}|_p > \varepsilon$, it follows by the "isosceles triangle principle" that $|a_i|_p = |a_{i_N}|_p$. Thus, for all $i > N$, $|a_i|_p$ has the constant value $|a_{i_N}|_p$. This constant value is then $\lim_{i\to\infty} |a_i|_p$.

One important difference with the process of completing $\mathbb{Q}$ to get $\mathbb{R}$ should be noted. In going from $\mathbb{Q}$ to $\mathbb{R}$ the possible values of $|\ | = |\ |_\infty$ were enlarged to include all nonnegative real numbers. But in going from $\mathbb{Q}$ to $\mathbb{Q}_p$ the possible values of $|\ |_p$ remain the same, namely $\{p^n\}_{n\in\mathbb{Z}} \cup \{0\}$.

Given two equivalence classes a and b of Cauchy sequences, we choose any representatives $\{a_i\} \in a$ and $\{b_i\} \in b$, and define $a \cdot b$ to be the equivalence class represented by the Cauchy sequence $\{a_i b_i\}$. If we had chosen another $\{a_i'\} \in a$ and $\{b_i'\} \in b$, we would have

$$\begin{aligned} |a_i' b_i' - a_i b_i|_p &= |a_i'(b_i' - b_i) + b_i(a_i' - a_i)|_p \\ &\leq \max(|a_i'(b_i' - b_i)|_p, |b_i(a_i' - a_i)|_p); \end{aligned}$$

as $i \to \infty$, the first expression approaches $|a|_p \cdot \lim |b_i' - b_i|_p = 0$, and the second expression approaches $|b|_p \cdot \lim |a_i' - a_i|_p = 0$. Hence $\{a_i' b_i'\} \sim \{a_i b_i\}$.

We similarly define the sum of two equivalence classes of Cauchy sequences by choosing a Cauchy sequence in each class, defining addition term-by-term, and showing that the equivalence class of the sum only depends on the equivalence classes of the two summands. Additive inverses are also defined in the obvious way.

For multiplicative inverses we have to be a little careful because of the possibility of zero terms in a Cauchy sequence. However, it is easy to see that every Cauchy sequence is equivalent to one with no zero terms (for example, if $a_i = 0$, replace a_i by $a_i' = p^i$). Then take the sequence $\{1/a_i\}$. This sequence will be Cauchy *unless* $|a_i|_p \to 0$, i.e., unless $\{a_i\} \sim \{0\}$. Moreover, if $\{a_i\} \sim \{a_i'\}$ and no a_i or a_i' is zero, then $\{1/a_i\} \sim \{1/a_i'\}$ is easily proved.

It is now easy to prove that the set $\mathbb{Q}_p$ of equivalence classes of Cauchy sequences is a field with addition, multiplication, and inverses defined as above. For example, distributivity: Let $\{a_i\}$, $\{b_i\}$, $\{c_i\}$ be representatives of $a, b, c \in \mathbb{Q}_p$; then $a(b + c)$ is the equivalence class of

$$\{a_i(b_i + c_i)\} = \{a_i b_i + a_i c_i\},$$

and $ab + ac$ is also the equivalence class of this sequence.

$\mathbb{Q}$ can be identified with the *subfield* of $\mathbb{Q}_p$ consisting of equivalence classes containing a constant Cauchy sequence. Under this identification, note that $|\ |_p$ on $\mathbb{Q}_p$ restricts to the usual $|\ |_p$ on $\mathbb{Q}$.

Finally, it is easy to prove that $\mathbb{Q}_p$ is complete: if $\{a_j\}_{j=1,2,\ldots}$ is a sequence of equivalence classes which is Cauchy in $\mathbb{Q}_p$, and if we take representative Cauchy sequences of rational numbers $\{a_{ji}\}_{i=1,2,\ldots}$ for each a_j, where for each j we have $|a_{ji} - a_{ji'}|_p < p^{-j}$ whenever $i, i' \geq N_j$, then it is easily shown that the equivalence class of $\{a_{jN_j}\}_{j=1,2,\ldots}$ is the limit of the a_j. We leave the details to the reader.

It's probably a good idea to go through one such tedious construction in any course or seminar, so as not to totally forget the axiomatic foundations on which everything rests. In this particular case, the abstract approach also gives us the chance to compare the p-adic construction with the construction of the reals, and see that the procedure is logically the same. However, after the following theorem, it would be wise to forget as rapidly as possible about "equivalence classes of Cauchy sequences," and to start thinking in more concrete terms.

Theorem 2. *Every equivalence class a in $\mathbb{Q}_p$ for which $|a|_p \leq 1$ has exactly one representative Cauchy sequence of the form $\{a_i\}$ for which:*

(1) $0 \leq a_i < p^i$ *for* $i = 1, 2, 3, \ldots$.
(2) $a_i \equiv a_{i+1} \pmod{p^i}$ *for* $i = 1, 2, 3, \ldots$.

PROOF. We first prove uniqueness. If $\{a_i'\}$ is a different sequence satisfying (1) and (2), and if $a_{i_0} \neq a_{i_0}'$, then $a_{i_0} \not\equiv a_{i_0}' \pmod{p^{i_0}}$, because both are between 0 and p^{i_0}. But then, for all $i \geq i_0$, we have $a_i \equiv a_{i_0} \not\equiv a_{i_0}' \equiv a_i' \pmod{p^{i_0}}$, i.e., $a_i \not\equiv a_i' \pmod{p^{i_0}}$. Thus

$$|a_i - a_i'|_p > 1/p^{i_0}$$

for all $i \geq i_0$, and $\{a_i\} \not\sim \{a_i'\}$.

So suppose we have a Cauchy sequence $\{b_i\}$. We want to find an equivalent sequence $\{a_i\}$ satisfying (1) and (2). To do this we use a simple lemma.

Lemma. *If $x \in \mathbb{Q}$ and $|x|_p \leq 1$, then for any i there exists an integer $\alpha \in \mathbb{Z}$ such that $|\alpha - x|_p \leq p^{-i}$. The integer α can be chosen in the set $\{0, 1, 2, 3, \ldots, p^i - 1\}$.*

PROOF OF LEMMA. Let $x = a/b$ be written in lowest terms. Since $|x|_p \leq 1$, it follows that p does not divide b, and hence b and p^i are relatively prime. So we can find integers m and n such that: $mb + np^i = 1$. Let $\alpha = am$. The idea is that mb differs from 1 by a p-adically small amount, so that m is a good approximation to $1/b$, and so am is a good approximation to $x = a/b$. More precisely, we have:

$$\begin{aligned} |\alpha - x|_p &= |am - (a/b)|_p = |a/b|_p \, |mb - 1|_p \\ &\leq |mb - 1|_p = |np^i|_p = |n|_p/p^i \leq 1/p^i. \end{aligned}$$

Finally, we can add a multiple of p^i to the integer α to get an integer between 0 and p^i for which $|\alpha - x|_p \leq p^{-i}$ still holds. The lemma is proved. □

Returning to the proof of the theorem, we look at our sequence $\{b_i\}$, and, for every $j = 1, 2, 3, \ldots$, let $N(j)$ be a natural number such that $|b_i - b_{i'}|_p \leq p^{-j}$ whenever $i, i' \geq N(j)$. (We may take the sequence $N(j)$ to be strictly increasing with j; in particular, $N(j) \geq j$.) Notice that $|b_i|_p \leq 1$ if $i \geq N(1)$, because for all $i' \geq N(1)$

$$\begin{aligned} |b_i|_p &\leq \max(|b_{i'}|_p, |b_i - b_{i'}|_p) \\ &\leq \max(|b_{i'}|_p, 1/p), \end{aligned}$$

and $|b_{i'}|_p \to |a|_p \leq 1$ as $i' \to \infty$.

We now use the lemma to find a sequence of integers a_j, where $0 \leq a_j < p_j$, such that

$$|a_j - b_{N(j)}|_p \leq 1/p^j.$$

I claim that $\{a_j\}$ is the required sequence. It remains to show that $a_{j+1} \equiv a_j \pmod{p^j}$ and that $\{b_i\} \sim \{a_j\}$.

The first assertion follows because

$$\begin{aligned} |a_{j+1} - a_j|_p &= |a_{j+1} - b_{N(j+1)} + b_{N(j+1)} - b_{N(j)} - (a_j - b_{N(j)})|_p \\ &\leq \max(|a_{j+1} - b_{N(j+1)}|_p, |b_{N(j+1)} - b_{N(j)}|_p, |a_j - b_{N(j)}|_p) \\ &\leq \max(1/p^{j+1}, 1/p^j, 1/p^j) \\ &= 1/p^j. \end{aligned}$$

The second assertion follows because, given any j, for $i \geq N(j)$ we have

$$\begin{aligned} |a_i - b_i|_p &= |a_i - a_j + a_j - b_{N(j)} - (b_i - b_{N(j)})|_p \\ &\leq \max(|a_i - a_j|_p, |a_j - b_{N(j)}|_p, |b_i - b_{N(j)}|_p) \\ &\leq \max(1/p^j, 1/p^j, 1/p^j) \\ &= 1/p^j. \end{aligned}$$

Hence $|a_i - b_i|_p \to 0$ as $i \to \infty$. The theorem is proved. □

What if our p-adic number a does not satisfy $|a|_p \leq 1$? Then we can multiply a by a power p^m of p (namely, by the power of p which equals $|a|_p$), to get a p-adic number $a' = ap^m$ which does satisfy $|a'|_p \leq 1$. Then a' is represented by a sequence $\{a_i'\}$ as in the theorem, and $a = a'p^{-m}$ is represented by the sequence $\{a_i\}$ in which $a_i = a_i'p^{-m}$.

It is now convenient to write all the a_i' in the sequence for a' to the base p, i.e.,

$$a_i' = b_0 + b_1 p + b_2 p^2 + \cdots + b_{i-1}p^{i-1},$$

where the b's are all "digits," i.e., integers in $\{0, 1, \ldots, p-1\}$. Our condition $a_i' \equiv a_{i+1}' \pmod{p^i}$ precisely means that

$$a_{i+1}' = b_0 + b_1 p + b_2 p^2 + \cdots + b_{i-1}p^{i-1} + b_i p^i,$$

where the digits b_0 through b_{i-1} are all the *same* as for a_i'. Thus, a' can be thought of intuitively as a number, written to the base p, which extends infinitely far to the right, i.e., we add a new digit each time we pass from a_i' to a_{i+1}'.

Our original a can then be thought of as a base p decimal number which has only finitely many digits "to the right of the decimal point" (i.e., corresponding to negative powers of p, but actually written starting from the left) but has infinitely many digits for positive powers of p:

$$a = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \cdots + \frac{b_{m-1}}{p} + b_m + b_{m+1}p + b_{m+2}p^2 + \cdots.$$

Here for the time being the expression on the right is only shorthand for the sequence $\{a_i\}$, where $a_i = b_0p^{-m} + \cdots + b_{i-1}p^{i-1-m}$, that is, a convenient way of thinking of the sequence $\{a_i\}$ all at once. We'll soon see that this equality is in a precise sense "real" equality. This equality is called the "p-adic expansion" of a.

We let $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a|_p \leq 1\}$. This is the set of all numbers in $\mathbb{Q}_p$ whose p-adic expansion involves no negative powers of p. An element of $\mathbb{Z}_p$ is called a "p-adic integer." (From now on, to avoid confusion, when we mean an old-fashioned integer in $\mathbb{Z}$, we'll say "rational integer.") The sum, difference, and product of two elements of $\mathbb{Z}_p$ is in $\mathbb{Z}_p$, so $\mathbb{Z}_p$ is what's called a "subring" of the field $\mathbb{Q}_p$.

If $a, b \in \mathbb{Q}_p$, we write $a \equiv b \pmod{p^n}$ if $|a - b|_p \leq p^{-n}$, or equivalently, $(a - b)/p^n \in \mathbb{Z}_p$, i.e., if the first nonzero digit in the p-adic expansion of $a - b$ occurs no sooner than the p^n-place. If a and b are not only in $\mathbb{Q}_p$ but are actually in $\mathbb{Z}$ (i.e., are rational integers), then this definition agrees with the earlier definition of $a \equiv b \pmod{p^n}$.

We define $\mathbb{Z}_p^\times$ as $\{x \in \mathbb{Z}_p \mid 1/x \in \mathbb{Z}_p\}$, or equivalently as $\{x \in \mathbb{Z}_p \mid x \not\equiv 0 \pmod{p}\}$, or equivalently as $\{x \in \mathbb{Z}_p \mid |x|_p = 1\}$. A p-adic integer in $\mathbb{Z}_p^\times$—i.e., whose first digit is nonzero—is sometimes called a "p-adic unit."

Now let $\{b_i\}_{i=-m}^{\infty}$ be any sequence of p-adic integers. Consider the sum

$$S_N = \frac{b_{-m}}{p^m} + \frac{b_{-m+1}}{p^{m-1}} + \cdots + b_0 + b_1 p + b_2 p^2 + \cdots + b_N p^N.$$

This sequence of partial sums is clearly Cauchy: if $M > N$, then $|S_N - S_M|_p < 1/p^N$. It therefore converges to an element in $\mathbb{Q}_p$. As in the case of infinite series of real numbers, we define $\sum_{i=-m}^{\infty} b_i p^i$ to be this limit in $\mathbb{Q}_p$.

More generally, if $\{c_i\}$ is *any* sequence of p-adic numbers such that $|c_i|_p \to 0$ as $i \to \infty$, the sequence of partial sums $S_N = c_1 + c_2 + \cdots + c_N$ converges to a limit, which we denote $\sum_{i=1}^{\infty} c_i$. This is because: $|S_M - S_N|_p = |c_{N+1} + c_{N+2} + \cdots + c_M|_p \leq \max(|c_{N+1}|_p, |c_{N+2}|_p, \cdots, |c_M|_p)$ which $\to 0$ as $N \to \infty$. Thus, p-adic infinite series are easier to check for convergence than infinite series of real numbers. *A series converges in $\mathbb{Q}_p$ if and only if its terms approach zero.* There is nothing like the harmonic series $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$ of real numbers, which diverges even though its terms approach 0. Recall that the reason for this is that $|\ |_p$ of a sum is bounded by the *maximum* (rather than just the sum) of the $|\ |_p$ of the summands when $p \neq \infty$, i.e., when $|\ |_p$ is non-Archimedean.

Returning now to p-adic expansions, we see that the infinite series on the right in the definition of the p-adic expansion

$$\frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \cdots + \frac{b_{m-1}}{p} + b_m + b_{m+1} p + b_{m+2} p^2 + \cdots$$

(here $b_i \in \{0, 1, 2, \ldots, p-1\}$) converges to a, and so the equality can be taken in the sense of the sum of an infinite series.

Note that the uniqueness assertion in Theorem 2 is something we don't have in the Archimedean case. Namely, terminating decimals can also be represented by decimals with repeating 9s: $1 = 0.9999\cdots$. But if two p-adic expansions converge to the same number in $\mathbb{Q}_p$, then they are the same, i.e., all of their digits are the same.

One final remark. Instead of $\{0, 1, 2, \ldots, p-1\}$ we could have chosen any other set $S = \{\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{p-1}\}$ of p-adic integers having the property that $\alpha_i \equiv i \pmod{p}$ for $i = 0, 1, 2, \ldots, p-1$, and could then have defined our p-adic expansion to be of the form $\sum_{i=-m}^{\infty} b_i p^i$, where now the "digits" b_i are in the set S rather than in the set $\{0, 1, \ldots, p-1\}$. For most purposes, the set $\{0, 1, \ldots, p-1\}$ is the most convenient. But there is another set S, the so-called "Teichmüller representatives" (see Exercise 13 below), which is in some ways an even more natural choice.

5. Arithmetic in $\mathbb{Q}_p$

The mechanics of adding, subtracting, multiplying, and dividing p-adic numbers is very much like the corresponding operations on decimals which we learn to do in about the third grade. The only difference is that the

"carrying," "borrowing," "long multiplication," etc. go from left to right rather than right to left. Here are a few examples in $\mathbb{Q}_7$:

$$\begin{array}{r} 3 + 6\times 7 + 2\times 7^2 + \cdots \\ \times\ 4 + 5\times 7 + 1\times 7^2 + \cdots \\ \hline 5 + 4\times 7 + 4\times 7^2 + \cdots \\ 1\times 7 + 4\times 7^2 + \cdots \\ 3\times 7^2 + \cdots \\ \hline 5 + 5\times 7 + 4\times 7^2 + \cdots \end{array} \qquad \begin{array}{r} 2\times 7^{-1} + 0\times 7^0 + 3\times 7^1 + \cdots \\ -\ 4\times 7^{-1} + 6\times 7^0 + 5\times 7^1 + \cdots \\ \hline 5\times 7^{-1} + 0\times 7^0 + 4\times 7^1 + \cdots \end{array}$$

$$3 + 5\times 7 + 1\times 7^2 + \cdots \overline{)\ 1 + 2\times 7 + 4\times 7^2 + \cdots}\ \ 5 + 1\times 7 + 6\times 7^2 + \cdots$$

$$\begin{array}{r} 1 + 6\times 7 + 1\times 7^2 + \cdots \\ \hline 3\times 7 + 2\times 7^2 + \cdots \\ 3\times 7 + 5\times 7^2 + \cdots \\ \hline 4\times 7^2 + \cdots \\ 4\times 7^2 + \cdots \\ \hline \end{array}$$

As another example, let's try to extract $\sqrt{6}$ in $\mathbb{Q}_5$, i.e., we want to find $a_0, a_1, a_2, \ldots, 0 \leq a_i \leq 4$, such that

$$(a_0 + a_1 \times 5 + a_2 \times 5^2 + \cdots)^2 = 1 + 1 \times 5.$$

Comparing coefficients of $1 = 5^0$ on both sides gives $a_0^2 \equiv 1 \pmod 5$, and hence $a_0 = 1$ or 4. Let's take $a_0 = 1$. Then comparing coefficients of 5 on both sides gives $2a_1 \times 5 \equiv 1 \times 5 \pmod{5^2}$, so that $2a_1 \equiv 1 \pmod 5$, and hence $a_1 = 3$. At the next step we have:

$$1 + 1 \times 5 \equiv (1 + 3 \quad 5 + a_2 \times 5^2)^2 \equiv 1 + 1 \times 5 + 2a_2 \times 5^2 \pmod{5^3}.$$

Hence $2a_2 \equiv 0 \pmod 5$, and $a_2 = 0$. Proceeding in this way, we get a series

$$a = 1 + 3 \times 5 + 0 \times 5^2 + 4 \times 5^3 + a_4 \times 5^4 + a_5 \times 5^5 + \cdots$$

where each a_i after a_0 is uniquely determined.

But remember that we had two choices for a_0, namely 1 and 4. What if we had chosen 4 instead of 1? We would have gotten

$$\begin{aligned} -a = {} & 4 + 1 \times 5 + 4 \times 5^2 + 0 \times 5^3 \\ & + (4 - a_4) \times 5^4 + (4 - a_5) \times 5^5 + \cdots. \end{aligned}$$

The fact that we had two choices for a_0, and then, once we chose a_0, only a single possibility for $a_1, a_2, a_3, \ldots$, merely reflects the fact that a nonzero element in a field like $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{Q}_p$ always has exactly two square roots in the field if it has any.

Do all numbers in $\mathbb{Q}_5$ have square roots? We saw that 6 does, what about 7? If we had

$$(a_0 + a_1 \times 5 + \cdots)^2 = 2 + 1 \times 5,$$

it would follow that $a_0^2 \equiv 2 \pmod 5$. But this is impossible, as we see by checking the possible values $a_0 = 0, 1, 2, 3, 4$. For a more systematic look at square roots in $\mathbb{Q}_p$, see Exercises 6–12.

This method of solving the equation $x^2 - 6 = 0$ in $\mathbb{Q}_5$—by solving the congruence $a_0^2 - 6 \equiv 0 \pmod 5$ and then solving for the remaining a_i in a step-by-step fashion—is actually quite general, as shown by the following important "lemma." This form of the lemma was apparently first given in Serge Lang's Ph.D. thesis in 1952 (*Annals of Mathematics*, Vol. 55, p. 380).

Theorem 3 (Hensel's lemma). *Let $F(x) = c_0 + c_1x + \cdots + c_nx^n$ be a polynomial whose coefficients are p-adic integers. Let $F'(x) = c_1 + 2c_2x + 3c_3x^2 + \cdots + nc_nx^{n-1}$ be the derivative of $F(x)$. Let a_0 be a p-adic integer such that $F(a_0) \equiv 0 \pmod p$ and $F'(a_0) \not\equiv 0 \pmod p$. Then there exists a unique p-adic integer a such that*

$$F(a) = 0 \quad \text{and} \quad a \equiv a_0 \pmod p.$$

(*Note*: In the special case treated above, we had $F(x) = x^2 - 6$, $F'(x) = 2x$, $a_0 = 1$.)

PROOF OF HENSEL'S LEMMA. I claim that there exists a unique sequence of rational integers $a_1, a_2, a_3, \ldots$ such that for all $n \geq 1$:

(1) $F(a_n) \equiv 0 \pmod{p^{n+1}}$.
(2) $a_n \equiv a_{n-1} \pmod{p^n}$.
(3) $0 \leq a_n < p^{n+1}$.

We prove that such a_n exist and are unique by induction on n.

If $n = 1$, first let $\tilde{a}_0$ be the unique integer in $\{0, 1, \ldots, p-1\}$ which is congruent to $a_0 \bmod p$. Any a_1 satisfying (2) and (3) must be of the form $\tilde{a}_0 + b_1p$, where $0 \leq b_1 \leq p - 1$. Now, looking at $F(\tilde{a}_0 + b_1p)$, we expand the polynomial, remembering that we only need congruence to $0 \bmod p^2$, so that any terms divisible by p^2 may be ignored:

$$\begin{aligned} F(a_1) = F(\tilde{a}_0 + b_1p) &= \sum c_i(\tilde{a}_0 + b_1p)^i \\ &= \sum (c_i\tilde{a}_0^i + ic_i\tilde{a}_0^{i-1}b_1p + \text{terms divisible by } p^2) \\ &\equiv \sum c_i\tilde{a}_0^i + \Big(\sum ic_i\tilde{a}_0^{i-1}\Big)b_1p \pmod{p^2} \\ &= F(\tilde{a}_0) + F'(\tilde{a}_0)b_1p. \end{aligned}$$

(Note the similarity to the first order Taylor series approximation in calculus: $F(x + h) = F(x) + F'(x)h +$ higher order terms.) Since $F(a_0) \equiv 0 \pmod p$ by assumption, we can write $F(\tilde{a}_0) \equiv \alpha p \pmod{p^2}$ for some $\alpha \in \{0, 1, \ldots, p-1\}$. So in order to get $F(a_1) \equiv 0 \pmod{p^2}$ we must get $\alpha p + F'(\tilde{a}_0)b_1p \equiv 0 \pmod{p^2}$, i.e., $\alpha + F'(\tilde{a}_0)b_1 \equiv 0 \pmod p$. But, since $F'(a_0) \not\equiv 0 \pmod p$ by assumption, this equation can always be solved for the unknown b_1. Namely, using the lemma in the proof of Theorem 2, we choose $b_1 \in \{0, 1, \ldots, p-1\}$ so that $b_1 \equiv -\alpha/F'(\tilde{a}_0) \pmod p$. Clearly this $b_1 \in \{0, 1, \ldots, p-1\}$ is uniquely determined by this condition.

Now, to proceed with the induction, suppose we already have $a_1, a_2, \ldots, a_{n-1}$. We want to find a_n. By (2) and (3), we need $a_n = a_{n-1} + b_np^n$ with $b_n \in \{0, 1, \ldots, p-1\}$. We expand $F(a_{n-1} + b_np^n)$ as we did before in the case $n = 1$, only this time we ignore terms divisible by p^{n+1}. This gives us:

$$F(a_n) = F(a_{n-1} + b_np^n) \equiv F(a_{n-1}) + F'(a_{n-1})b_np^n \pmod{p^{n+1}}.$$

Since $F(a_{n-1}) \equiv 0 \pmod{p^n}$ by the induction assumption, we can write $F(a_{n-1}) \equiv \alpha' p^n \pmod{p^{n+1}}$, and our desired condition $F(a_n) \equiv 0 \pmod{p^{n+1}}$ now becomes

$$\alpha' p^n + F'(a_{n-1})b_np^n \equiv 0 \pmod{p^{n+1}}, \quad \text{i.e., } \alpha' + F'(a_{n-1})b_n \equiv 0 \pmod p.$$

Now, since $a_{n-1} \equiv a_0 \pmod p$, it easily follows that $F'(a_{n-1}) \equiv F'(a_0) \not\equiv 0 \pmod p$, and we can find the required $b_n \in \{0, 1, \ldots, p-1\}$ proceeding exactly as in the case of b_1, i.e., solving $b_n \equiv -\alpha'/F'(a_{n-1}) \pmod p$. This completes the induction step, and hence the proof of the claim.

The theorem follows immediately from the claim. We merely let $a = \tilde{a}_0 + b_1p + b_2p^2 + \cdots$. Since for all n we have $F(a) \equiv F(a_n) \equiv 0 \pmod{p^{n+1}}$, it follows that the p-adic number $F(a)$ must be 0. Conversely, any $a = \tilde{a}_0 + b_1p + b_2p^2 + \cdots$ gives a sequence of a_n as in the claim, and the uniqueness of that sequence implies the uniqueness of the a. Hensel's lemma is proved. □

Hensel's lemma is often called the p-adic Newton's lemma because the approximation technique used to prove it is essentially the same as Newton's

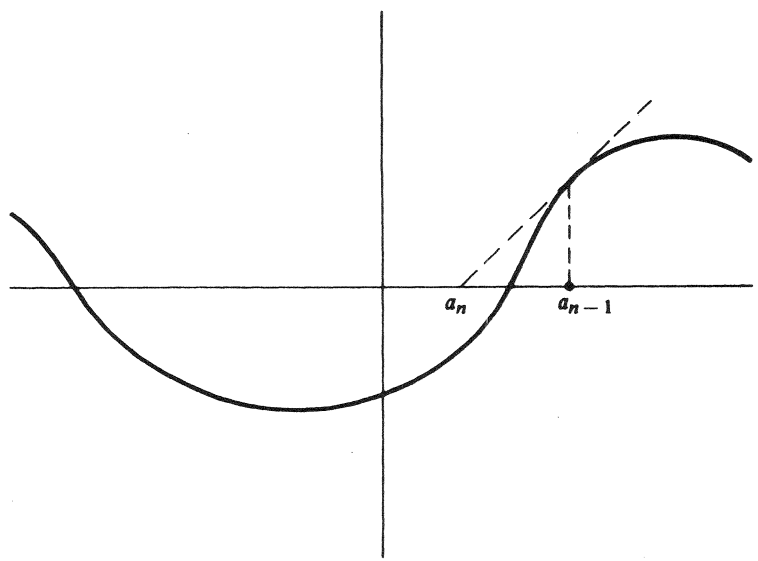


Figure I.1. Newton's method in the real case

method for finding a *real* root of a polynomial equation with real coefficients. In Newton's method in the real case, (see Figure I.1), if $f'(a_{n-1}) \neq 0$, we take

$$a_n = a_{n-1} - \frac{f(a_{n-1})}{f'(a_{n-1})}.$$

The correction term $-f(a_{n-1})/f'(a_{n-1})$ is a lot like the formula for the "correction term" in the proof of Hensel's lemma:

$$b_n p^n \equiv -\frac{\alpha' p^n}{F'(a_{n-1})} \equiv -\frac{F(a_{n-1})}{F'(a_{n-1})} \pmod{p^{n+1}}.$$

In one respect the p-adic Newton's method (Hensel's lemma) is much better than Newton's method in the real case. In the p-adic case, it's *guaranteed* to converge to a root of the polynomial. In the real case, Newton's method *usually* converges, but not always. For example, if you take $f(x) = x^3 - x$ and make the unfortunate choice $a_0 = 1/\sqrt{5}$, you get:

$$\begin{aligned} a_1 &= 1/\sqrt{5} - [1/5\sqrt{5} - 1/\sqrt{5}]/(3/5 - 1) \\ &= 1/\sqrt{5}[1 - (1/5 - 1)(3/5 - 1)] = -1/\sqrt{5}; \\ a_2 &= 1/\sqrt{5}; \quad a_3 = -1/\sqrt{5}, \quad \text{etc.} \end{aligned}$$

(See Figure I.2.) Such perverse silliness is impossible in $\mathbb{Q}_p$.

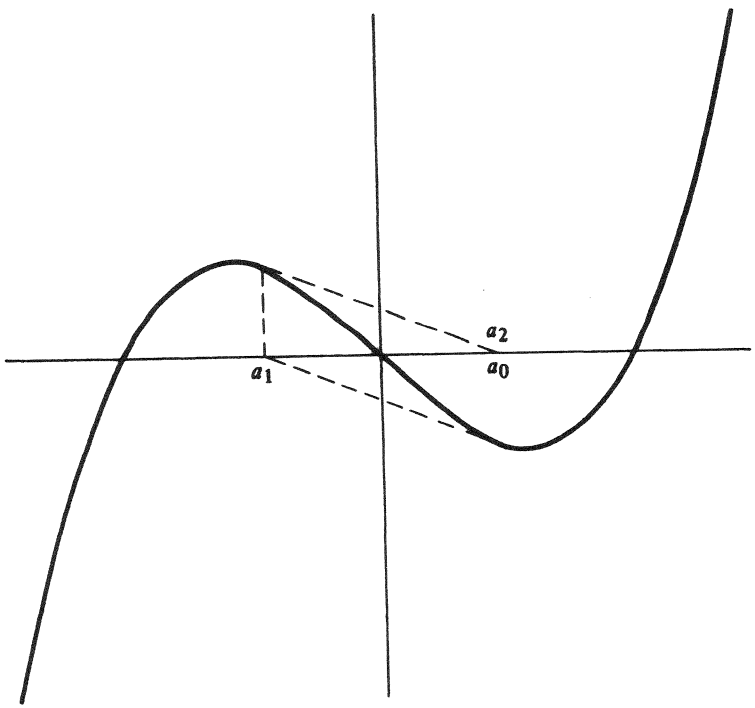


Figure I.2. Failure of Newton's method in the real case

Exercises

1. If $a \in \mathbb{Q}_p$ has p-adic expansion $a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \cdots + a_0 + a_1 p + \cdots$, what is the p-adic expansion of $-a$?

2. Find the p-adic expansion of:
   (i) $(6 + 4 \times 7 + 2 \times 7^2 + 1 \times 7^3 + \cdots)(3 + 0 \times 7 + 0 \times 7^2 + 6 \times 7^3 + \cdots)$ in $\mathbb{Q}_7$ to 4 digits
   (ii) $1/(3 + 2 \times 5 + 3 \times 5^2 + 1 \times 5^3 + \cdots)$ in $\mathbb{Q}_5$ to 4 digits
   (iii) $9 \times 11^2 - (3 \times 11^{-1} + 2 + 1 \times 11^1 + 3 \times 11^2 + \cdots)$ in $\mathbb{Q}_{11}$ to 4 digits
   (iv) $2/3$ in $\mathbb{Q}_2$ (v) $-1/6$ in $\mathbb{Q}_7$ (vi) $1/10$ in $\mathbb{Q}_{11}$
   (vii) $-9/16$ in $\mathbb{Q}_{13}$ (viii) $1/1000$ in $\mathbb{Q}_5$ (ix) $6!$ in $\mathbb{Q}_3$
   (x) $1/3!$ in $\mathbb{Q}_3$ (xi) $1/4!$ in $\mathbb{Q}_2$ (xii) $1/5!$ in $\mathbb{Q}_5$

3. Prove that the p-adic expansion of a nonzero $a \in \mathbb{Q}_p$ terminates (i.e., $a_i = 0$ for all i greater than some N) if and only if a is a *positive* rational number whose denominator is a power of p.

4. Prove that the p-adic expansion of $a \in \mathbb{Q}_p$ has repeating digits from some point on (i.e., $a_{i+r} = a_i$ for some r and for all i greater than some N) if and only if $a \in \mathbb{Q}$.

5. What is the cardinality of $\mathbb{Z}_p$? Prove your answer.

6. Prove the following generalization of Hensel's lemma: Let $F(x)$ be a polynomial with coefficients in $\mathbb{Z}_p$. If $a_0 \in \mathbb{Z}_p$ satisfies $F'(a_0) \equiv 0 \pmod{p^M}$ but $F'(a_0) \not\equiv 0 \pmod{p^{M+1}}$, and if $F(a_0) \equiv 0 \pmod{p^{2M+1}}$, then there is a unique $a \in \mathbb{Z}_p$ such that $F(a) = 0$ and $a \equiv a_0 \pmod{p^{M+1}}$.

7. Use your proof in Exercise 6 to find a square root of -7 in $\mathbb{Q}_2$ to 5 digits.

8. Which of the following 11-adic numbers have square roots in $\mathbb{Q}_{11}$?
   (i) 5 (ii) 7 (iii) -7
   (iv) $5 + 3 \times 11 + 9 \times 11^2 + 1 \times 11^3$
   (v) $3 \times 11^{-2} + 6 \times 11^{-1} + 3 + 0 \times 11 + 7 \times 11^2$
   (vi) $3 \times 11^{-1} + 6 + 3 \times 11 + 0 \times 11^2 + 7 \times 11^3$
   (vii) 1×11^7 (viii) $7 - 6 \times 11^2$
   (ix) $5 \times 11^{-2} + \sum_{n=0}^{\infty} n \times 11^n$.

9. Compute $\pm\sqrt{-1}$ in $\mathbb{Q}_5$ and $\pm\sqrt{-3}$ in $\mathbb{Q}_7$ to 4 digits.

10. For which $p = 2, 3, 5, 7, 11, 13, 17, 19$ does -1 have a square root in $\mathbb{Q}_p$?

11. Let p be any prime besides 2. Suppose $\alpha \in \mathbb{Q}_p$ and $|\alpha|_p = 1$. Describe a test for whether α has a square root in $\mathbb{Q}_p$. What about if $|\alpha|_p \neq 1$? Prove that there exist four numbers $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \in \mathbb{Q}_p$ such that for all nonzero $\alpha \in \mathbb{Q}_p$ exactly one of the numbers $\alpha_1\alpha, \alpha_2\alpha, \alpha_3\alpha, \alpha_4\alpha$ has a square root. (In the case when p is replaced by ∞ and $\mathbb{Q}_p$ by $\mathbb{R}$, there are *two* numbers, for example ± 1 will do, such that for every nonzero $\alpha \in \mathbb{R}$ exactly one of the numbers $1 \cdot \alpha$ and $-1 \cdot \alpha$ has a square root in $\mathbb{R}$.)

12. The same as Exercise 11 when $p = 2$, except that now there will be *eight* numbers $\alpha_1, \ldots, \alpha_8 \in \mathbb{Q}_2$ such that for all nonzero $\alpha \in \mathbb{Q}_2$ exactly one of the

numbers $\alpha_1\alpha, \ldots, \alpha_8\alpha$ has a square root in $\mathbb{Q}_2$. Find such $\alpha_1, \ldots, \alpha_8$ (the choice of them is *not* unique, of course).

13. Find all 4 fourth roots of 1 in $\mathbb{Q}_5$ to four digits. Prove that $\mathbb{Q}_p$ always contains p solutions $a_0, a_1, \ldots, a_{p-1}$ to the equation $x^p - x = 0$, where $a_i \equiv i \pmod{p}$. These p numbers are called the "Teichmüller representatives" of $\{0, 1, 2, \ldots, p-1\}$ and are sometimes used as a set of p-adic digits instead of $\{0, 1, 2, \ldots, p-1\}$. If $p > 2$, which Teichmüller representatives are rational?

14. Prove the following "Eisenstein irreducibility criterion" for a polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$ with coefficients $a_i \in \mathbb{Z}_p$: If $a_i \equiv 0 \pmod{p}$ for $i = 0, 1, 2, \ldots, n-1$, if $a_n \not\equiv 0 \pmod{p}$, and if $a_0 \not\equiv 0 \pmod{p^2}$, then $f(x)$ is irreducible over $\mathbb{Q}_p$, i.e., it cannot be written as a product of two lower degree polynomials with coefficients in $\mathbb{Q}_p$.

15. If $p > 2$, use Exercise 14 to show that 1 has no pth root other than 1 in $\mathbb{Q}_p$. Prove that if $p > 2$, then the only roots of 1 in $\mathbb{Q}_p$ are the nonzero Teichmüller representatives; and in $\mathbb{Q}_2$ the only roots of 1 are ± 1.

16. Prove that the infinite sum $1 + p + p^2 + p^3 + \cdots$ converges to $1/(1-p)$ in $\mathbb{Q}_p$. What about $1 - p + p^2 - p^3 + p^4 - p^5 + \cdots$? What about $1 + (p-1)p + p^2 + (p-1)p^3 + p^4 + (p-1)p^5 + \cdots$?

17. Show that (a) every element $x \in \mathbb{Z}_p$ has a unique expansion of the form $x = a_0 + a_1(-p) + a_2(-p)^2 + \cdots + a_n(-p)^n + \cdots$, with $a_i \in \{0, 1, \ldots, p-1\}$, and (b) this expansion terminates if and only if $x \in \mathbb{Z}$.

18. Suppose that n is a (positive or negative) integer not divisible by p, and let $\alpha \equiv 1 \pmod{p}$. Show that α has an nth root in $\mathbb{Q}_p$. Give a counter-example if $n = p$. Show that α has a pth root if $\alpha \equiv 1 \pmod{p^2}$ and $p \neq 2$.

19. Let $\alpha \in \mathbb{Z}_p$. Prove that $\alpha^{p^M} \equiv \alpha^{p^{M-1}} \pmod{p^M}$ for $M = 1, 2, 3, 4, \ldots$. Prove that the sequence $\{\alpha^{p^M}\}$ approaches a limit in $\mathbb{Q}_p$, and that this limit is the Teichmüller representative congruent to $\alpha \bmod p$.

20. Prove that $\mathbb{Z}_p$ is sequentially compact, i.e., every sequence of p-adic integers has a convergent subsequence.

21. Define matrices with entries in $\mathbb{Q}_p$, their sums, products, and determinants exactly as in the case of the reals. Let $M = \{r \times r \text{ matrices with entries in } \mathbb{Z}_p\}$, let $M^\times = \{A \in M \mid A \text{ has an inverse in } M\}$ (it's not hard to see that this is equivalent to: $\det A \in \mathbb{Z}_p^\times$), and let $pM = \{A \in M \mid A = pB \text{ with } B \in M\}$. If $A \in M^\times$ and $B \in pM$, prove that there exists a unique $X \in M^\times$ such that: $X^2 - AX + B = 0$.

CHAPTER II

p-adic interpolation of the Riemann zeta-function

This chapter is logically independent of the following chapters, and is presented at this point in the middle of our ascent to Ω as a plateau in the level of abstraction—namely, everything in this chapter still takes place in the fields $\mathbb{Q}$, $\mathbb{Q}_p$, and $\mathbb{R}$.

The Riemann ζ-function is defined as a function of real numbers greater than 1 by

$$\zeta(s) \underset{\text{def}}{=} \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

It is easy to see (by comparison with the integral $\int_1^\infty (dx/x^s) = 1/(s-1)$ for fixed $s > 1$) that this sum converges when $s > 1$.

Let p be any prime number. The purpose of this chapter is to show that the numbers $\zeta(2k)$ for $k = 1, 2, 3, \ldots$ have a "p-adic continuity property." More precisely, consider the set of numbers

$$f(2k) = (1 - p^{2k-1})\frac{c_k}{\pi^{2k}}\zeta(2k), \quad \text{where } c_k = (-1)^k \frac{(2k-1)!}{2^{2k-1}},$$

as $2k$ runs through all positive even integers in the same congruence class $\bmod(p-1)$. It turns out that $f(2k)$ is always a rational number. Moreover, if two such values of $2k$ are close p-adically (i.e., their difference is divisible by a high power of p), then we shall see that the corresponding $f(2k)$ are also p-adically close. (We must also assume that $2k$ is not divisible by $p-1$.) This means that the function f can be extended in a unique way from integers to p-adic integers so that the resulting function is a *continuous function of a p-adic variable with values in* $\mathbb{Q}_p$. ("Continuous function" means, as in the real case, that whenever a sequence of p-adic integers $\{x_n\}$ approaches x p-adically, $\{f(x_n)\}$ approaches $f(x)$ p-adically.)