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

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

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."

It is not too hard to show that the set of *all* finite-tailed Laurent series in powers of p (i.e., of all p-adic expansions) is a field (Problem 5 again), just as $\mathbb{C}((X-\alpha))$ is a field. We will denote this field by $\mathbb{Q}_p$, and call it the *field of p-adic numbers*. As before, we can describe much of what we have done by saying that the function

$$x \mapsto p\text{-adic expansion of } x$$

gives an inclusion of fields

$$\mathbb{Q} \hookrightarrow \mathbb{Q}_p.$$

(We have not yet shown that $\mathbb{Q}_p$ is strictly bigger than $\mathbb{Q}$; the next section will show that this is true.)

The definition of a p-adic number as a formal object (a finite-tailed Laurent expansion in powers of p) is of course rather unsatisfactory according to the tastes of today. We will remedy this in Chapter 3, where we will show how to construct the field $\mathbb{Q}_p$ as an analogue of the field of real numbers. For now, note only that whatever the "real" definition is, it must allow our series to converge, so that powers p^n must get *smaller* as n grows. This is pretty strange, so let's give ourselves time to get used to the idea. The problems in this section are intended to help the reader feel a little more comfortable with p-adic expansions.

Problem 4 Consider a p-adic number

$$x = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots .$$

What is $-x$? (This means: what is its p-adic expansion?)

Problem 5 Show that $\mathbb{Q}_p$ is indeed a field. (You will have to begin by making explicit what the operations are, and this is a bit tricky because of "carrying." For example, the coefficient of a given power of p in the sum of two expansions depends on the coefficients of *all* the lower powers in the summands; however, this is still a finite rule.) Then show that the map $\mathbb{Q} \longrightarrow \mathbb{Q}_p$ given by sending each rational number to its expansion is a homomorphism.

Problem 6 By analogy with the real numbers, it's natural to guess that every rational number will have a periodic (or eventually periodic) p-adic expansion, and that conversely any such expansion represents a rational number. Show that this is in fact correct. (Just follow the proof for real numbers.)

Problem 7 When one deals with real numbers, one uses the notation $3.14159\ldots$ to refer to the infinite series

$$3 + \frac{1}{10} + \frac{4}{10^2} + \frac{1}{10^3} + \frac{5}{10^4} + \frac{9}{10^5} + \ldots$$

Devise a similar notation for p-adic numbers, and explain how to sum and multiply numbers expressed in your notation. Using your notation, re-do some of the examples we gave above.

Problem 8 (Some Abstract Algebra required!) Another point at which our analogy seems to break down is the fact that rational functions $f(X) \in \mathbb{C}(X)$ are really *functions*: one can really compute their value at a complex number α. This problem explains a highfalutin' way of interpreting rational numbers as functions too.

i) First of all, show that we can identify the set of complex numbers α with the set of maximal ideals in $\mathbb{C}[X]$ via the correspondence $\alpha \leftrightarrow (X - \alpha)$.

ii) Fix a complex number α. Show that the map $f \mapsto f(\alpha)$ defines a homomorphism from the ring $\mathbb{C}[X]$ to $\mathbb{C}$, whose kernel is exactly the ideal $(X - \alpha)$.

iii) Now let $f(X)$ be a rational function. Show that the map $f \mapsto f(\alpha)$ still makes sense provided the denominator of f is not divisible by $X - \alpha$. If the denominator is divisible by $(X - \alpha)^n$ but not by $(X - \alpha)^{n+1}$, explain why this means that f has a pole of order n at α.

iv) Now take $x = a/b \in \mathbb{Q}$, and choose a prime $p \in \mathbb{Z}$. If p does not divide b, define the *value of* x *at* p to be $a/b \pmod p$, which means $ab' \pmod p$, where b' is an integer satisfying $bb' \equiv 1 \pmod p$. We think of this value as an element of $\mathbb{F}_p$, the field with p elements. If p does divide b, we say that x has a pole at p. Explain how to define the order of the pole. This interprets the elements of $\mathbb{Q}$ as a sort of "function" on the primes $p \in \mathbb{Z}$. It is a bit weird, because this "function" doesn't have a "range:" the value at each p belongs to a different field $\mathbb{F}_p$.

v) Discuss whether this way of thinking of rational numbers as functions is reasonable. Does it make the analogy any tighter?

1.2 Solving Congruences Modulo p^n

The "p-adic numbers" we have just constructed are closely related to the problem of solving congruences modulo powers of p. We will look at some examples of this.

Let's start with the easiest possible case, an equation which has solutions in $\mathbb{Q}$, such as

$$X^2 = 25.$$

We want to consider it modulo p^n for every n, i.e., to solve the congruences

$$X^2 \equiv 25 \pmod{p^n}.$$

Now, of course, our equation has solutions already in the integers: $X = \pm 5$. This automatically gives a solution of the congruence for every n; just put $X \equiv \pm 5 \pmod{p^n}$ for every n.

Problem 9 Check that these are the only solutions, up to congruence, of $X^2 \equiv 25 \pmod{p^n}$, at least when $p \neq 2, 5$. What happens in these special cases?

Let's try to understand these solutions a little better from the p-adic point of view. To make our life easier, we take $p = 3$ once again. We begin by rewriting our solutions using residue class representatives between 0 and $3^n - 1$ for the solutions modulo 3^n. The first solution, $X = 5$, gives:

$$\begin{aligned} &X \equiv 2 \pmod 3 \\ &X \equiv 5 = 2 + 3 \pmod 9 \\ &X \equiv 5 = 2 + 3 \pmod{27} \\ &\text{etc.} \end{aligned}$$

which never changes any more, and therefore just gives the 3-adic expansion of this solution:

$$X = 5 = 2 + 1 \times 3.$$

For $X = -5$, the results are a little more interesting; the representatives are

$$\begin{aligned} &X \equiv -5 \equiv 1 \pmod 3 \\ &X \equiv -5 \equiv 4 = 1 + 3 \pmod 9 \\ &X \equiv -5 \equiv 22 = 1 + 3 + 2 \times 9 \pmod{27} \\ &X \equiv -5 \equiv 76 = 1 + 3 + 2 \times 9 + 2 \times 27 \pmod{81} \\ &\text{etc.} \end{aligned}$$

Again, continuing this gives the 3-adic expansion of the solution, which is a bit more interesting because it is infinite:

$$X = -5 = 1 + 1 \times 3 + 2 \times 3^2 + 2 \times 3^3 + 2 \times 3^4 + \cdots$$

(Check this against your answer in Problem 4.)

Notice that the two systems of solutions are "coherent," in the sense that when we look at, say, $X = 76$ (which is the solution modulo 3^4) and reduce it modulo 3^3, we get $X = 22$ (which is the solution modulo 3^3). Let's give this a formal definition:

Definition 1.2.1 *Let p be a prime. We say a sequence of integers α_n such that $0 \le \alpha_n \le p^n - 1$ is* coherent *if, for every $n \ge 1$, we have*

$$\alpha_{n+1} \equiv \alpha_n \pmod{p^n}.$$

If we need to emphasize the choice of prime p, we will say the sequence is p-adically coherent.

We can picture our two coherent sequences of solutions as branches in a tree (see figure 1.1). Of course this is all rather painfully obvious in the case we are considering, since the sequences of solutions are coherent simply because they "are" solutions in $\mathbb{Z}$ (76 is congruent to 22 just because both are congruent to -5). The only real bit of information we have obtained is the connection between expressing the roots as a coherent sequence and obtaining their p-adic expansions.

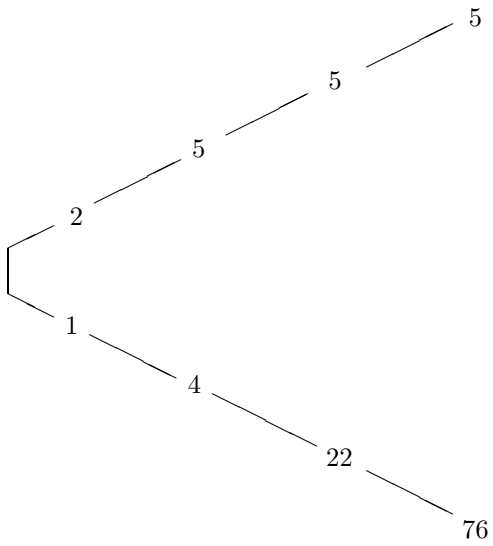

Figure 1.1: Solutions of $X^2 \equiv 25 \pmod{3^n}$

Problem 10 Before we go on to something more interesting, do a couple of similar examples on your own, say with $X^2 = 49$ and $p = 5$, and $X^3 = 27$ and $p = 2$.

Problem 11 Things already get slightly more interesting if we take $p = 2$ and the equation $X^2 = 81$. In this case, the "tree" of solutions modulo 2^n is much more complex: there are two infinite branches that correspond to the solutions $X = \pm 9$, but there are also lots of finite branches (solutions modulo 2^n that do not "lift" to solutions modulo 2^{n+1}). We will later consider what is special about this situation.

Things become much more interesting if we follow the same process with an equation that does *not* have rational roots. For example, take the system of congruences

$$X^2 \equiv 2 \pmod{7^n}, \qquad n = 1, 2, 3, \ldots$$

For $n = 1$, the solutions are $X \equiv 3 \pmod 7$ and $X \equiv 4 \equiv -3 \pmod 7$. To find the solutions for $n = 2$, note that their reductions modulo 7 must be solutions for $n = 1$. Hence we set $X = 3 + 7k$ or $X = 4 + 7k$ and solve for k:

$$\begin{aligned} (3 + 7k)^2 &\equiv 2 \pmod{49} \\ 9 + 42k &\equiv 2 \pmod{49} \end{aligned}$$

(notice that the term involving $(7k)^2$ is congruent to zero)

$$\begin{aligned} 7 + 42k &\equiv 0 \pmod{49} \\ 1 + 6k &\equiv 0 \pmod 7 \\ k &\equiv 1 \pmod 7 \end{aligned}$$

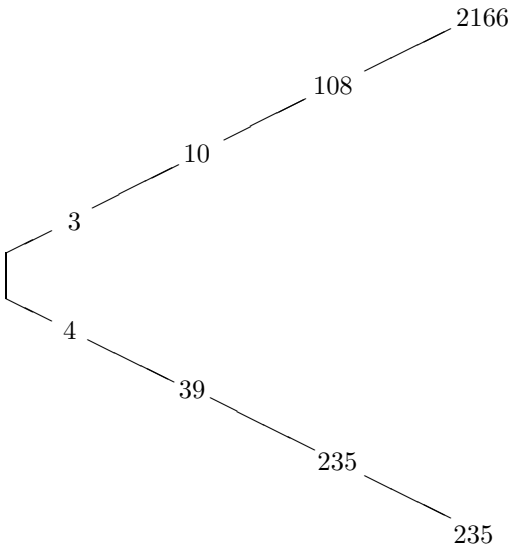

Figure 1.2: Solutions of $X^2 = 2 \pmod{7^n}$

which, since $X = 3 + 7k$, gives the solution $X \equiv 10 \pmod{49}$. Using $X = 4 + 7k$ gives the other solution $X \equiv 39 \equiv -10 \pmod{49}$.

Problem 12 Prove that for each n there can be at most two solutions. (All you need is $p \neq 2$.)

Problem 13 Show that the process above can be continued indefinitely, that is, that given a solution α_n of the congruence $X^2 \equiv 2 \pmod{7^n}$, there always exists a unique solution α_{n+1} of $x^2 \equiv 2 \pmod{7^{n+1}}$ satisfying $\alpha_{n+1} \equiv \alpha_n \pmod{7^n}$. Find a few more terms in each of the sequences of solutions above.

Again, the solutions can be represented as branches in a tree (see figure 1.2). This time, however, we can't predict *a priori* what the numbers that appear will be; instead, all we can do is convince ourselves that the process will continue as long as we want it to. The fact that one can continue finding roots indefinitely shows that there are two coherent sequences of solutions:

$$x_1 = (3,\, 10,\, 108,\, 2166,\, \ldots)$$

and

$$x_2 = (4,\, 39,\, 235,\, 235\, \ldots) = (-3,\, -10,\, -108,\, -2166\, \ldots) = -x_1.$$

Just as before, we can expand each number in each sequence 7-adically. The fact that the sequence is coherent means that the expansion of each root is

the truncation of the expansion of the following root, so that, for example,

$$\begin{aligned} 3 &= 3 \\ 10 &= 3 + 1 \times 7 \\ 108 &= 3 + 1 \times 7 + 2 \times 49 \end{aligned}$$

This gives us two 7-adic numbers:

$$x_1 = 3 + 1 \times 7 + 2 \times 49 + 6 \times 343 + \cdots$$

and

$$x_2 = 4 + 5 \times 7 + 4 \times 49 + 0 \times 343 + \cdots = -x_1.$$

It probably bears repeating: we are not claiming that we can predict the pattern here. All we know is that we can *continue* the pattern for as long as necessary, if we have enough time and patience. It's just like finding the decimal expansion of the square root of two: we can get as close as we like, and we can *prove* that, though we can't predict what the expansion will actually be like.

In any case, we do get two 7-adic numbers, and they are indeed roots of the equation $X^2 = 2$ in $\mathbb{Q}_7$, in the usual sense:

Problem 14 Show that the 7-adic number x_1 obtained as above satisfies $x_1^2 = 2$ in $\mathbb{Q}_7$. Conclude that the field $\mathbb{Q}_7$ is strictly bigger than $\mathbb{Q}$.

The tie between solving sequences of congruences modulo higher and higher powers of p and solving the corresponding equation in $\mathbb{Q}_p$ is quite close, as the problems below try to emphasize. It is also one of the more important reasons for using p-adic methods in number theory.

Problem 15 Check that $X^2 = 2$ has no solutions in the field $\mathbb{Q}_5$. (Begin by expressing the putative solution as a 5-adic expansion. Show that it must be of the form $a_0 + a_1 5 + a_2 5^2 + \ldots$, and conclude that a_0 must satisfy a congruence modulo 5. Finally, check that the congruence you obtained has no solutions modulo 5.) Notice that this shows (in a very roundabout way) that 2 has no square root in $\mathbb{Q}$, since any square root in $\mathbb{Q}$ would be a square root in any of the $\mathbb{Q}_p$ (remember that there is an inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$), hence in particular in $\mathbb{Q}_5$.

Problem 16 Check that $X^2 + 1 = 0$ has a solution in $\mathbb{Q}_5$, but not in $\mathbb{Q}_7$.

Problem 17 Show that a p-adic number

$$x = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots$$

is a solution in $\mathbb{Q}_p$ of an equation $X^2 = m$ if and only if the sequence

$$(a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \ldots)$$

is a coherent sequence of solutions of the congruences $X^2 \equiv m \pmod{p^n}$. (Hint: compute x^2 up to a certain power of p, and compare it with m to read off a congruence modulo that power of p.)

We have already mentioned that there is some analogy between p-adic numbers and real numbers. The next problem gives an example of this. Over $\mathbb{R}$, there is a simple condition that determines whether the equation $X^2 = m$ has a solution (just check the sign of m). In $\mathbb{Q}_p$, the condition is also simple:

Problem 18 Let m be any integer, and suppose that the congruence $X^2 \equiv m \pmod{p}$ has a solution; show that if $p \neq 2$ and $p \nmid m$ it is always possible to "extend" this solution to a full coherent sequence of solutions of $X^2 \equiv m \pmod{p^n}$. Use this to find a necessary and sufficient condition for the equation $X^2 = m$ to have a root in $\mathbb{Q}_p$ for $p \neq 2$. What is special about $p = 2$?

Problem 19 Show that for every p, the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ is strict, that is, some p-adic numbers are not (expansions of) rational numbers. (Hint: find an equation that has a root in $\mathbb{Q}_p$ but not in $\mathbb{Q}$; the root will be a p-adic number that is not rational. The basic work has all been done; just be careful with $p = 2$.)

Problem 20 In the same spirit as the previous problem, show that $\mathbb{Q}_p$ is never algebraically closed; more precisely, for each p one can find an algebraic equation with rational coefficients that has no roots in $\mathbb{Q}_p$.

1.3 Other Examples

Working with p-adic numbers is useful in all sorts of contexts. We round off this chapter by giving two rather whimsical examples.

Consider the equation $X = 1 + 3X$. This is of course easy to solve, but let's try something strange and look at it as a fixed-point problem, i.e, as the problem of finding a solution for $f(x) = x$ for some function $f(x)$. Such problems are often solved by iteration, plugging in an arbitrary initial value, then computing $f(x)$ over and over in the hope that we will get closer and closer to a fixed point. To try that in our case, we take $x_0 = 1$ and iterate, so that $x_{n+1} = 1 + 3x_n$. Here's what we get:

$$\begin{aligned} x_0 &= 1 \\ x_1 &= 1 + 3x_0 = 1 + 3 \\ x_2 &= 1 + 3x_1 = 1 + 3 + 3^2 \\ &\cdots \\ x_n &= 1 + 3 + 3^2 + \cdots + 3^n. \end{aligned}$$

In $\mathbb{R}$, this is a divergent sequence, and we were all taught in calculus classes never to have any dealings with them. On the other hand, it is the sequence of partial sums of a geometric series, and we all know that

$$1 + a + a^2 + a^3 + \cdots = \frac{1}{1 - a}$$

(Well, we know it for $|a| < 1$, but what the heck...) Plugging in blindly gives $x = 1/(1 - 3) = -1/2$, which is (surprise!) the correct answer.

This dubious playing around with divergent sequences is clearly illegal in calculus class, but it works. Here's one way to understand why. While the sequence is certainly divergent in $\mathbb{R}$, there is nothing to keep us from looking at the sequence in $\mathbb{Q}_3$ (the elements in the sequence are in $\mathbb{Q}$, which is contained in both $\mathbb{R}$ and $\mathbb{Q}_3$). Now, in $\mathbb{Q}_3$, the sequence is obviously convergent, to the 3-adic number

$$1 + 3 + 3^2 + \cdots + 3^n + \cdots .$$

One then easily checks (by the same argument used over $\mathbb{R}$!) that this is equal to $-1/2$.

Of course it is silly to solve a linear equation in such a roundabout way, but the remarkable fact here is that an argument that was either dubious or outright illegal at first sight turns out to work perfectly well in the p-adic context. The series we used is divergent only if we insist of thinking of it as a series of real numbers. Once we put it in the "right" context, it becomes quite nice. In fact, we will see in the next chapter that there is an absolute value in $\mathbb{Q}_3$, and that with respect to the notion of size determined by that absolute value our series is convergent.

The point, then, is that introducing the p-adic fields broadens our world in such a way as to allow arguments that were previously impossible. This toy example points the way to many analogous situations where considering the p-adic numbers simplifies matters tremendously.

Problem 21 Show that, for any prime p, the formula

$$1 + p + p^2 + p^3 + \cdots = \frac{1}{1-p}$$

is true in $\mathbb{Q}_p$.

The next example is perhaps even more interesting. It shows that sometimes introducing p-adic ideas allows a more conceptual proof of a fact that seems obscure (and hard to prove) otherwise. This example is a bit more advanced, and we will take for granted things that we will prove only later, but the reader should be able to follow it. We will work with $p = 2$, that is, in the field $\mathbb{Q}_2$ of 2-adic numbers.

Consider the usual MacLaurin series for the logarithm of $1 + X$:

$$\log(1 + X) = X - \frac{X^2}{2} + \frac{X^3}{3} - \frac{X^4}{4} + \ldots .$$

Since powers of 2 are "small" in $\mathbb{Q}_2$, it turns out that we can plug in $X = -2$ to compute the logarithm of -1:

$$\log(-1) = \log(1 - 2) = -\left(2 + \frac{2^2}{2} + \frac{2^3}{3} + \frac{2^4}{4} + \cdots\right)$$

(This is of course wildly divergent in $\mathbb{R}$, but it turns out to be convergent in $\mathbb{Q}_2$; this is not completely obvious because of the denominators, but it does work—see ahead.) Now, if the series converges, it must converge to zero, by the usual properties of the logarithm:

$$2\log(-1) = \log(1) = 0.$$

This means that the partial sums

$$2 + \frac{2^2}{2} + \frac{2^3}{3} + \frac{2^4}{4} + \cdots + \frac{2^n}{n}$$

must get closer and closer to zero as n grows. Remember that what this means is that the terms in the 2-adic expansion "disappear to the right," that is, that the partial sums, written in base 2, begin with longer and longer stretches of zeros. Here's the upshot:

Fact 1.3.1 *For each integer $M > 0$ there exists an n such that the partial sum*

$$2 + \frac{2^2}{2} + \frac{2^3}{3} + \frac{2^4}{4} + \cdots + \frac{2^n}{n}$$

is divisible by 2^M.

Problem 22 Can you give a direct proof of that fact?

What this example points out is that using p-adic methods, and in particular the methods of the calculus in the p-adic context, we can often prove facts about divisibility by powers of p which are otherwise quite hard to understand. The proofs are often, as in this case, "cleaner" than any direct proof would be, and therefore easier to understand. We will look at many more examples of this before we are done.