

Chapter 1

p -adic Numbers

1.1 Congruences Modulo p^n and Hensel's Lemma

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial, let $m \geq 1$ be an integer, and suppose that we want to find solutions to the congruence

$$f(x) \equiv 0 \pmod{m}.$$

An initial simplification is to factor m as a product of primes, $m = \prod_{i=1}^r p_i^{e_i}$, and solve each of the congruences

$$f(x) \equiv 0 \pmod{p_i^{e_i}}. \quad (1.1)$$

If a_i is a solution to the congruence with modulus $p_i^{e_i}$, then the Chinese remainder theorem says that there is a unique number $a \pmod{m}$ satisfying

$$a \equiv a_i \pmod{p_i^{e_i}} \quad \text{for all } 1 \leq i \leq r.$$

This number a is a solution to the congruence (1.1) for all i , so a is a solution to $f(x) \equiv 0 \pmod{m}$.

This reduces the solution of congruences modulo m to the case that m is a prime power. Hensel's lemma, which we now state and prove, gives conditions under which a solution modulo a prime p leads to solutions modulo p^n for all powers of p . (In the statement of Hensel's lemma, we write $f'(x)$ for the derivative of the polynomial $f(x)$.)

Theorem 1.1 (Hensel's Lemma: Version I). *Let $f(x) \in \mathbb{Z}[x]$ be a nonzero polynomial, let p be a prime, and let $a \in \mathbb{Z}$ be an integer such that*

$$f(a) \equiv 0 \pmod{p} \quad \text{and} \quad f'(a) \not\equiv 0 \pmod{p}.$$

Then there exists a sequence of integers (a_0, a_1, a_2, \dots) starting with $a_0 = a$ and satisfying

$$f(a_n) \equiv 0 \pmod{p^{n+1}} \quad \text{and} \quad a_{n+1} \equiv a_n \pmod{p^{n+1}} \quad \text{for all } n \geq 0. \quad (1.2)$$

Further, the value of a_n is uniquely determined modulo p^{n+1} .

Proof. We construct the sequence inductively. We are given that $a_0 = a$ satisfies $f(a_0) \equiv 0 \pmod{p}$, so (1.2) is true for $n = 0$. Suppose now that we have constructed a_0, a_1, \dots, a_n satisfying (1.2). In order to form a_{n+1} , the second condition in (1.2) forces us to take

$$a_{n+1} = a_n + up^{n+1} \quad \text{for some } u \in \mathbb{Z}.$$

The question then is whether we can find some value of u so as to make the first condition in (1.2) true, i.e., we seek a value of u such that

$$f(a_{n+1}) = f(a_n + up^{n+1}) \equiv 0 \pmod{p^{n+2}}.$$

To do this, we use the Taylor expansion of $f(x)$ around $x = a_n$,

$$f(x) = f(a_n) + f'(a_n)(x - a_n) + \frac{1}{2}f''(a_n)(x - a_n)^2 + \dots + \frac{1}{d!}f^{(d)}(a_n)(x - a_n)^d.$$

We actually don't need such a precise formula. All that we will use is the fact that there is a polynomial $g(x) \in \mathbb{Z}[x]$ with integer coefficients satisfying

$$f(x) = f(a_n) + f'(a_n)(x - a_n) + g(x)(x - a_n)^2.$$

We substitute $x = a_n + up^{n+1}$ to obtain the formula

$$f(a_n + up^{n+1}) = f(a_n) + f'(a_n)up^{n+1} + g(a_n + up^{n+1})u^2p^{2n+2}.$$

Remember that we are trying to choose u so as to make this expression congruent to 0 modulo p^{n+2} , so want to solve the congruence

$$f(a_n) + f'(a_n)up^{n+1} \equiv 0 \pmod{p^{n+2}}.$$

Further, the induction hypothesis tells us that $f(a_n) \equiv 0 \pmod{p^{n+1}}$, so there is an integer c such that $f(a_n) = cp^{n+1}$. This leads to the congruence

$$cp^{n+1} + f'(a_n)up^{n+1} \equiv 0 \pmod{p^{n+2}},$$

and dividing by p^{n+1} , we need to solve

$$c + f'(a_n)u \equiv 0 \pmod{p}. \quad (1.3)$$

Finally, we observe that the assumption $f'(a) \not\equiv 0 \pmod{p}$ and the induction hypothesis imply that

$$f'(a_n) \equiv f'(a_0) = f'(a) \not\equiv 0 \pmod{p}.$$

Thus $f'(a_n)$ has an inverse modulo p , so (1.3) has a (unique) solution

$$u \equiv -f'(a_n)^{-1}c \pmod{p}.$$

We have not shown that there exists an integer $a_{n+1} = a_n + up^{n+1}$ satisfying

$$f(a_{n+1}) \equiv 0 \pmod{p^{n+2}} \quad \text{and} \quad a_{n+1} \equiv a_n \pmod{p^{n+1}},$$

and further that the value of a_{n+1} is unique modulo p^{n+2} . This completes the proof by induction of Hensel's lemma. \square

Example 1.2. We illustrate Hensel's lemma and its proof by solving the congruence

$$x^2 + 1 \equiv 0 \pmod{5^{n+1}}$$

for $n = 0, 1$, and 2 . For $n = 0$ there are two solutions, namely $x = 2$ and $x = 3$. Starting with $a_0 = 2$, we substitute $a_1 = 2 + 5u$ and solve

$$\begin{aligned} (2 + 5u)^2 + 1 &\equiv 0 \pmod{25} \\ 5 + 20u &\equiv 0 \pmod{25} \\ 1 + 4u &\equiv 0 \pmod{5} \\ u &\equiv 1 \pmod{5}. \end{aligned}$$

So $a_1 = 2 + 5 \cdot 1 = 7$ is a solution to $x^2 + 1 \equiv 0 \pmod{25}$.

Next we set $a_2 = 7 + 25u$ and substitute to get

$$\begin{aligned} (7 + 25u)^2 + 1 &\equiv 0 \pmod{5^3} \\ 50 + 350u &\equiv 0 \pmod{5^3} \\ 2 + 14u &\equiv 0 \pmod{5} \\ u &\equiv 2 \pmod{5}. \end{aligned}$$

This gives $a_2 = 7 + 25 \cdot 2 = 57$ as a solution to $x^2 + 1 \equiv 0 \pmod{125}$.

Remark 1.3. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial and let p be a prime number. Hensel's lemma (more or less) says that if we can find the solutions to

$$f(x) \equiv 0 \pmod{p}, \tag{1.4}$$

then we can find the solutions to

$$f(x) \equiv 0 \pmod{p^n}$$

for all $n \geq 1$. But how do we get started with the solutions to (1.4)? If p is not too large, we can simply check each value $x = 0, 1, \dots, p - 1$. For large primes, there are reasonably efficient methods for finding the roots; see Exercise 1.1.

1.2 The Ring of p -adic Integers

If we view Hensel's lemma as an algorithm, then its input is a solution $x = a_0$ to the congruence $f(x) \equiv 0 \pmod{p}$ and its output is a coherent sequence of values (a_0, a_1, a_2, \dots) that solve $f(x) \equiv 0 \pmod{p^{n+1}}$ for all $n \geq 0$. The coherence of the sequence refers to the fact that each term is congruent to the previous one modulo an appropriate power of p . This suggests that we look at the set of all coherent sequences, where rather than a sequence of integers, we take a_n to be a number modulo p^{n+1} . This leads to the construction of the ring of p -adic integers.

Definition. A p -adic number is a sequence

$$(a_0, a_1, a_2, \dots)$$

such that for all $n \geq 0$ we have

$$a_n \in \mathbb{Z}/p^{n+1}\mathbb{Z} \quad \text{and} \quad a_{n+1} \equiv a_n \pmod{p^n}.$$

In other words, a p -adic number is a sequence of values modulo higher and higher powers of p , with the coherence property that the terms in the sequence are congruent to one another modulo appropriate powers of p .

We can add and multiply p -adic numbers in the obvious way by adding and multiplying their coordinates,

$$\begin{aligned} (a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) &= (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots), \\ (a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) &= (a_0 \cdot b_0, a_1 \cdot b_1, a_2 \cdot b_2, \dots). \end{aligned}$$

Definition. The set of p -adic numbers is denoted \mathbb{Z}_p and is called the *ring of p -adic integers*. The ring of ordinary integers \mathbb{Z} is a subring of \mathbb{Z}_p via the natural inclusion

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p, \quad a \longmapsto (a \bmod p, a \bmod p^2, a \bmod p^3, \dots).$$

Intuition. The fact that a p -adic number is an infinite sequence may seem confusing at first, but eventually you will want to view elements of \mathbb{Z}_p as simply numbers. If this seems unrealistic, consider your mental image of a real number such as $\sqrt{2}$ or π . Presumably you view π as a “number,” but matters are not that simple if you want to understand the real numbers in a rigorous way. There are many ways to construct the real numbers, but all require manipulation of infinite sets of rational numbers. For example, one way to construct the real numbers is as equivalence classes of Cauchy sequences, in which case the “number” π is represented by the sequence of rational numbers such as

$$\left(3, \frac{31}{10}, \frac{314}{100}, \frac{3141}{1000}, \frac{31415}{10000}, \frac{314159}{100000}, \dots \right).$$

Further, making matters even more confusing is the fact that each real number is represented by many different sequences. So you can be thankful that there is a unique sequence representing each p -adic number.

Our next result says that the ring of p -adic integers is a *local ring*, which by definition means that it is a ring with a unique maximal ideal.

Proposition 1.4. *Let*

$$\mathfrak{M} = \{\alpha = (a_0, a_1, a_2, \dots) \in \mathbb{Z}_p : a_0 = 0\}.$$

(a) \mathfrak{M} is the unique maximal ideal of \mathbb{Z}_p , and the map

$$\mathbb{Z}_p/\mathfrak{M} \longrightarrow \mathbb{Z}/p\mathbb{Z}, \quad \alpha = (a_0, a_1, \dots) \longmapsto a_0,$$

is an isomorphism.

(b) Every element of \mathbb{Z}_p is either in \mathfrak{M} or is a unit, i.e., has a multiplicative inverse. Thus \mathbb{Z}_p is the disjoint union of its maximal ideal \mathfrak{M} and its group of units \mathbb{Z}_p^* .

Proof. The map

$$\mathbb{Z}_p \longrightarrow \mathbb{Z}/p\mathbb{Z}, \quad \alpha = (a_0, a_1, \dots) \longmapsto a_0,$$

is a surjective homomorphism whose kernel is precisely \mathfrak{M} , so a standard theorem from ring theory says that \mathfrak{M} is an ideal and the induced map $\mathbb{Z}_p/\mathfrak{M} \rightarrow \mathbb{Z}/p\mathbb{Z}$ is an isomorphism. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, it follows that \mathfrak{M} is a maximal ideal of \mathbb{Z}_p .

We next prove that if $\alpha \in \mathbb{Z}_p$ is not in \mathfrak{M} , then α is a unit. The assumption that $\alpha = (a_0, a_1, \dots) \notin \mathfrak{M}$ means that $a_0 \neq 0$, i.e., a_0 is a nonzero element of the field $\mathbb{Z}/p\mathbb{Z}$, so a_0 is a unit. Let $b_0 \in \mathbb{Z}/p\mathbb{Z}$ be its inverse. We are going to construct b_0, b_1, b_2, \dots inductively to satisfy

$$a_i b_i \equiv 1 \pmod{p^{i+1}} \quad \text{and} \quad b_i \equiv b_{i-1} \pmod{p^i}. \quad (1.5)$$

For $i = 0$ the first congruence is true by the choice of b_0 and the second is vacuous. Now assume that (1.5) is true for all $i = n$. The coherence of the sequence defining α and the assumption that $a_0 \neq 0$ imply that

$$a_{n+1} \equiv a_0 \not\equiv 0 \pmod{p},$$

so a_{n+1} has an inverse modulo p^{n+2} . We denote this inverse by b_{n+1} , so

$$a_{n+1} b_{n+1} \equiv 1 \pmod{p^{n+2}}.$$

Reducing modulo p^{n+1} and using the coherence of the α -sequence and the induction hypothesis, we find that

$$b_{n+1} \equiv a_{n+1}^{-1} 1 \equiv a_n^{-2} \equiv b_n \pmod{p^{n+1}}.$$

This completes the construction of a sequence b_0, b_1, b_2, \dots satisfying (1.5) for all $i \geq 0$. The second part of (1.5) tells us that $\beta = (b_0, b_1, \dots) \in \mathbb{Z}_p$, and the first part implies that $\alpha\beta = 1$.

We have proven everything except that fact that the ideal \mathfrak{M} is the unique maximal ideal of \mathbb{Z}_p . Suppose that I is an ideal of \mathbb{Z}_p with $I \not\subset \mathfrak{M}$. This means that there is some $\alpha \in I$ with $\alpha \notin \mathfrak{M}$. But we just proved that such an α is a unit, so I contains a unit, so $I = \mathbb{Z}_p$. Thus \mathfrak{M} contains every ideal of \mathbb{Z}_p other than \mathbb{Z}_p itself, so \mathbb{Z}_p can have no other maximal ideals. \square

We now describe a way to measure the “size” of a p -adic number. The idea is that a p -adic number is deemed to be small if its defining sequence (a_0, a_1, a_2, \dots) starts with a lot of zeros.¹

Definition. Let $\alpha = (a_0, a_1, a_2, \dots) \in \mathbb{Z}_p$ be a p -adic number. The p -adic valuation of α , denoted $\text{ord}_p(\alpha)$, is the quantity

$$\text{ord}_p(\alpha) = \min\{n \geq 0 : a_n \neq 0\}.$$

(We formally set $\text{ord}_p(\alpha) = \infty$ if $\alpha = 0$.) Thus $\text{ord}_p(a)$ is the index of the first term in the sequence that does not vanish. The associated p -adic absolute value is

$$|\alpha|_p = p^{-\text{ord}_p(\alpha)},$$

with the convention that $|0|_p = 0$.

The p -adic absolute value is so named because it has properties similar to those enjoyed by the usual absolute value on \mathbb{R} .

Proposition 1.5. *The p -adic absolute value $|\alpha|_p$ has the following properties:*

- (a) $|\alpha|_p \geq 0$ for all α , and $|\alpha|_p = 0$ if and only if $\alpha = 0$.
- (b) $|\alpha\beta|_p = |\alpha|_p |\beta|_p$.
- (c) $|\alpha + \beta|_p \leq \max\{|\alpha|_p, |\beta|_p\}$. Further, if $|\alpha|_p \neq |\beta|_p$, then this inequality is an equality.

Proof. (a) This is clear from the definition of $|\cdot|_p$, since $\alpha = 0$ if and only if every coordinate in the sequence defining α is 0.

(b) Let $\alpha = (a_0, a_1, \dots)$ and $\beta = (b_0, b_1, \dots)$, and denote their valuations by

$$i = \text{ord}_p(\alpha) \quad \text{and} \quad j = \text{ord}_p(\beta).$$

This means that

$$a_i \not\equiv 0 \pmod{p^{i+1}} \quad \text{and} \quad a_i \equiv a_{i-1} \equiv 0 \pmod{p^i},$$

so for all $n \geq 0$ we can write

$$\alpha_n \equiv p^i u_n \pmod{p^{n+1}} \quad \text{with } p \nmid u_n.$$

Similarly,

$$\beta_n \equiv p^j v_n \pmod{p^{n+1}} \quad \text{with } p \nmid v_n.$$

Hence

$$\alpha_n \beta_n \equiv p^{i+j} u_n v_n \pmod{p^{n+1}} \quad \text{with } p \nmid u_n v_n,$$

so $\text{ord}_p(\alpha_n \beta_n) = i + j$. In terms of the p -adic absolute value, this is equivalent to the desired result, since it implies that

¹This is analogous to the fact that a real number $0 \leq \alpha < 1$ is small if, when we write out its decimal expansion $\alpha = \frac{a_1}{10} + \frac{a_2}{100} + \frac{a_3}{1000} + \dots$, the sequence of digits (a_1, a_2, \dots) starts with a lot of zeros.

$$|\alpha\beta|_p = p^{-\text{ord}_p(\alpha\beta)} = p^{-(i+j)} = p^{-i}p^{-j} = p^{-\text{ord}_p(\alpha)}p^{-\text{ord}_p(\beta)} = |\alpha|_p|\beta|_p.$$

(c) Continuing with the notation from the proof of (b), we have

$$\alpha_n + \beta_n \equiv p^i u_n + p^j v_n \pmod{p^{n+1}} \quad \text{with } p \nmid u_n v_n.$$

The expression $p^i u_n + p^j v_n$ is clearly divisible by $p^{\min(i,j)}$, and if $i \neq j$, then $p^{\min(i,j)}$ is the exact power of p that divides $p^i u_n + p^j v_n$. Hence

$$\text{ord}_p(\alpha_n + \beta_n) \geq \min\{\text{ord}_p(\alpha), \text{ord}_p(\beta)\}, \quad (1.6)$$

and if $\text{ord}_p(\alpha) \neq \text{ord}_p(\beta)$, then the inequality (1.6) is an equality. Rewriting this statement in terms of the p -adic absolute value gives the desired result,

$$|\alpha + \beta|_p = p^{-\text{ord}_p(\alpha+\beta)} \leq p^{-\min\{\text{ord}_p(\alpha), \text{ord}_p(\beta)\}} = \max\{|\alpha|_p, |\beta|_p\},$$

with equality if $|\alpha|_p \neq |\beta|_p$. \square

Corollary 1.6. *The ring of p -adic integers \mathbb{Z}_p is an integral domain.*

Proof. Suppose that $\alpha\beta = 0$. Then $0 = |\alpha\beta|_p = |\alpha|_p|\beta|_p$, so either $|\alpha|_p = 0$ or $|\beta|_p = 0$. Hence either $\alpha = 0$ or $\beta = 0$. \square

We have stated Proposition 1.5 in terms of the p -adic absolute value $|\cdot|_p$, but it is sometimes more convenient to work with the p -adic valuation ord_p .

Proposition 1.7. *The p -adic valuation ord_p has the following properties:*

- (a) $\text{ord}_p(\alpha) \geq 0$, and $\text{ord}_p(\alpha) = \infty$ if and only if $\alpha = 0$.
- (b) $\text{ord}_p(\alpha\beta) = \text{ord}_p(\alpha) + \text{ord}_p(\beta)$.
- (c) $\text{ord}_p(\alpha + \beta) \geq \min\{\text{ord}_p(\alpha), \text{ord}_p(\beta)\}$. If $\text{ord}_p(\alpha) \neq \text{ord}_p(\beta)$, this inequality is an equality.

Definition. The fact that \mathbb{Z}_p is an integral domain means that it has a field of fractions, which is denoted \mathbb{Q}_p and is called the *field of p -adic rational numbers*. Informally,

$$\mathbb{Q}_p = \left\{ \frac{\alpha}{\beta} : \alpha, \beta \in \mathbb{Z}_p, \beta \neq 0 \right\},$$

where of course we identify two fractions α/β and α'/β' if $\alpha\beta' = \alpha'\beta$. We extend the p -adic valuation and absolute value to \mathbb{Q}_p in the natural way,

$$\text{ord}_p\left(\frac{\alpha}{\beta}\right) = \text{ord}_p(\alpha) - \text{ord}_p(\beta), \quad \left|\frac{\alpha}{\beta}\right|_p = \frac{|\alpha|_p}{|\beta|_p}.$$

Proposition 1.5 ensures that equivalent p -adic fractions have the same absolute value.

The p -adic integers \mathbb{Z}_p , the group of units \mathbb{Z}_p^* and the maximal ideal \mathfrak{M} of \mathbb{Z}_p may be characterized as follows in terms of the p -adic absolute value:

$$\begin{aligned}\mathbb{Z}_p &= \{\alpha \in \mathbb{Q}_p : |\alpha|_p \leq 1\}, \\ \mathbb{Z}_p^* &= \{\alpha \in \mathbb{Q}_p : |\alpha|_p = 1\}, \\ \mathfrak{M} &= \{\alpha \in \mathbb{Q}_p : |\alpha|_p < 1\}.\end{aligned}$$

For this reason, people sometimes refer to \mathbb{Z}_p as the (closed) unit p -adic disk and \mathfrak{M} as the (open) unit p -adic disc, while \mathbb{Z}_p^* is the p -adic circle.

We can also use the definition of \mathbb{Z}_p and the p -adic absolute value to reformulate and strengthen Hensel's lemma.

Theorem 1.8 (Hensel's Lemma: Version II). *Let $f(x) \in \mathbb{Z}_p[x]$ be a nonzero polynomial and let $\alpha \in \mathbb{Z}_p$ be a p -adic number such that*

$$|f(\alpha)|_p < 1 \quad \text{and} \quad |f'(\alpha)|_p = 1.$$

Then there exists a unique $\beta \in \mathbb{Z}_p$ satisfying

$$f(\beta) = 0 \quad \text{and} \quad |\beta - \alpha|_p < 1.$$

Proof. We leave the proof, which is essentially the same as the proof of Theorem 1.1, to the reader; see Exercise 1.5. \square

Example 1.9. The polynomial $f(x) = x^2 + 1$ satisfies

$$|f(2)|_5 = |5|_5 = \frac{1}{5} < 1 \quad \text{and} \quad |f'(2)|_5 = |4|_5 = 1,$$

so Hensel's lemma says that there is a 5-adic number $\alpha \in \mathbb{Z}_5$ satisfying $f(\alpha) = 0$. Notice that $\alpha^2 = -1$, so \mathbb{Z}_5 contains a square root of -1 . The first few entries in a sequence for $\sqrt{-1} \in \mathbb{Z}_5$ are

$$\sqrt{-1} = (2, 7, 57, \dots).$$

(We computed these values earlier in Example 1.2. See also Exercise 1.8.)

1.3 The Ring of p -adic Integers is Complete

We recall from real analysis that a sequence of real numbers $\alpha_1, \alpha_2, \dots$ is said to be a *Cauchy sequence* if

$$\lim_{i,j \rightarrow \infty} |\alpha_i - \alpha_j| = 0.$$

The field \mathbb{R} of real numbers is a *complete field*, which by definition means that every Cauchy sequence of real numbers converges to a real number. By way of contrast, the rational numbers do not have this property, since for example, any sequence of rational numbers that converges (in \mathbb{R}) to $\sqrt{2}$ will be Cauchy, but does not converge to a rational number. The fact that the real numbers are complete is, in some sense, their defining quality. Indeed, the field of real numbers \mathbb{R} may be characterized as

the smallest field that contains the rational numbers \mathbb{Q} and is complete with respect to the usual absolute value on \mathbb{Q} .²

Convergence of a sequence of elements in the field \mathbb{Q}_p is defined in exactly the same way as convergence of a sequence of real numbers, except that we use the p -absolute value in place of the real absolute value.

Definition. A sequence $\alpha_1, \alpha_2, \dots$ of p -adic rational numbers converges to $\beta \in \mathbb{Q}_p$ if for every $\epsilon > 0$ there exists an index $I(\epsilon)$ such that

$$|\alpha_i - \beta|_p < \epsilon \quad \text{for all } i \geq I(\epsilon).$$

Cauchy sequences are defined similarly.

Definition. A sequence $\alpha_1, \alpha_2, \dots$ of p -adic rational numbers is *Cauchy* (with respect to the p -adic absolute value) if

$$\lim_{i,j \rightarrow \infty} |\alpha_i - \alpha_j|_p = 0.$$

A fundamental property of the field of p -adic numbers \mathbb{Q}_p is that it is a complete field with respect to the p -adic absolute value.

Theorem 1.10. Every Cauchy sequence in \mathbb{Q}_p converges to an element of \mathbb{Q}_p .

Proof. We first do the case that $\alpha_1, \alpha_2, \dots$ is a Cauchy sequence of p -adic integers, i.e., we assume that the α_i are all in \mathbb{Z}_p . We write each α_i as

$$\alpha_i = (a_{i0}, a_{i1}, a_{i2}, \dots) \quad \text{with } a_{in} \in \mathbb{Z}/p^{n+1}\mathbb{Z}.$$

Claim. For any fixed $n \geq 0$, the sequence of values

$$a_{1n}, a_{2n}, a_{3n}, \dots \in \mathbb{Z}/p^{n+1}\mathbb{Z}$$

eventually stabilizes, i.e., each column in Figure 1.1 eventually becomes constant.

$$\begin{array}{ccccccc} \alpha_1 & = & (& a_{10} & a_{11} & \dots & a_{1n} & \dots) \\ \alpha_2 & = & (& a_{20} & a_{21} & \dots & a_{2n} & \dots) \\ \alpha_3 & = & (& a_{30} & a_{31} & \dots & a_{3n} & \dots) \\ & & \vdots & & \vdots & \ddots & \vdots & \\ \alpha_i & = & (& a_{i0} & a_{i1} & \dots & a_{in} & \dots) \\ & & \vdots & & \vdots & & \vdots & \end{array}$$

Figure 1.1: A sequence of p -adic numbers

More formally, we are asserting that for every $n \geq 0$ there exists an $I(n)$ such that

$$a_{in} = a_{jn} \quad \text{for all } i, j \geq I(n).$$

²Intuitively, this means that if K is any extension field of \mathbb{Q} that is complete with respect to the usual absolute value, then there is a unique embedding of \mathbb{R} in K .

We now verify the claim. The assumption that the sequence $(\alpha_i)_{i \geq 1}$ is Cauchy means that for the given value of n , we can find an index $I(n)$ such that

$$|\alpha_i - \alpha_j|_p < p^{-n-1} \quad \text{for all } i, j \geq I(n).$$

Then the definition of the p -adic absolute value immediately implies that $a_{in} = a_{jn}$.

Using the claim, we define $\beta \in \mathbb{Z}_p$ to be the sequence

$$\beta = (b_0, b_1, b_2, \dots)$$

such that

$$b_n = a_{I(n)n} = a_{in} \quad \text{for any } i \geq I(n).$$

We must check that β is in \mathbb{Z}_p and that $\lim \alpha_i = \beta$.

The coherence property of the sequence defining β is easy, since if we take $i \geq \max\{I(n+1), I(n)\}$, then

$$b_{n+1} = a_{i,n+1} \equiv a_{in} = b_n \pmod{p^{n+1}}.$$

The convergence is similarly easy from the definitions. Let $\epsilon > 0$ be given and choose n such that $p^{-n} < \epsilon$. Then for any $i \geq I(n)$ we have $b_n = a_{in}$, so

$$|\beta - \alpha_i|_p \leq p^{-n} < \epsilon \quad \text{for all } i \geq I(n).$$

This completes the proof that $\lim \alpha_i = \beta$ for Cauchy sequences in \mathbb{Z}_p .

In general, let $\alpha_1, \alpha_2, \dots$ be a Cauchy sequence in \mathbb{Q}_p . We claim that $|\alpha_i|_p$ is bounded as $i \rightarrow \infty$. Suppose not. Then for any j we can find an i with $|\alpha_i|_p \geq 1$ and $|\alpha_i|_p > |\alpha_j|_p$. But then the ultrametric triangle inequality implies that

$$|\alpha_i - \alpha_j|_p = |\alpha_i|_p \geq 1,$$

contradicting the assumption that the sequence is Cauchy. Hence $|\alpha_i|_p$ is bounded, say

$$\sup_{i \geq 0} |\alpha_i|_p = p^k.$$

Then $|p^k \alpha_i|_p = p^{-k} |\alpha_i|_p \leq 1$ for all i , so $p^k \alpha_i \in \mathbb{Z}_p$. Further,

$$\lim_{i,j \rightarrow \infty} |p^k \alpha_i - p^k \alpha_j|_p = p^{-k} \lim_{i,j \rightarrow \infty} |\alpha_i - \alpha_j|_p = 0,$$

so the sequence $p^k \alpha_1, p^k \alpha_2, \dots$ is a Cauchy sequence in \mathbb{Z}_p . Our earlier proof shows that it converges to an element $\beta \in \mathbb{Z}_p$, and then the original sequence converges to $p^{-k} \beta \in \mathbb{Q}_p$. \square

When studying calculus, one learns that if a series of real numbers $\sum \alpha_i$ converges, then $\alpha_i \rightarrow 0$, but that the converse need not be true as shown by the harmonic series $\sum 1/i$. In the world of p -adic numbers, we now show that the converse is true, which makes proving convergence of p -adic series much easier than it is for real series.

Proposition 1.11. *Let $(\alpha_i)_{i \geq 1}$ be a sequence of p -adic rational numbers. Then*

$$\sum_{i=1}^{\infty} \alpha_i \text{ converges} \iff \lim_{i \rightarrow \infty} \alpha_i = 0.$$

Proof. The proof of the \Rightarrow implication is the same as in calculus, so we leave it for you to do (Exercise 1.11). For the other direction, we assume that $\alpha_i \rightarrow 0$ and need to prove that the series $\sum \alpha_i$ converges. Letting

$$S_k = \sum_{i=1}^k \alpha_i$$

be the k^{th} partial sum, we must show that the sequence of values $(S_k)_{k \geq 1}$ converges in \mathbb{Q}_p . We do this by showing that it is a Cauchy sequence. Thus for any $k \geq j \geq 1$ we have

$$|S_k - S_j|_p = \left| \sum_{i=j+1}^k \alpha_i \right|_p \leq \max_{j < i \leq k} |\alpha_i|_p.$$

The assumption that $\lim \alpha_i \rightarrow 0$ with respect to the p -adic metric means that $|\alpha_i|_p \rightarrow 0$, so we have

$$\lim_{j, k \rightarrow \infty} |S_k - S_j|_p = 0.$$

Thus the sequence $(S_k)_{k \geq 1}$ is Cauchy with respect to the p -adic metric, so by the completeness of \mathbb{Q}_p (Theorem 1.10) it converges to an element of \mathbb{Q}_p . \square

1.4 Absolute Values

In this section we develop the theory of p -adic number from an alternative perspective and show that the real numbers \mathbb{R} and the p -adic rational numbers \mathbb{Q}_p are the only completions of \mathbb{Q} .

The field of rational numbers come equipped with the familiar absolute value,

$$|r| = \max\{r, -r\} = \begin{cases} r & \text{if } r \geq 0, \\ -r & \text{if } r < 0, \end{cases}$$

and this familiar absolute value has several familiar properties. We abstract these properties to make a general definition.

Definition. An *absolute value* on a field K is a real-valued function

$$\|\cdot\| : K \longrightarrow \mathbb{R}$$

with the following properties:

- $|r| \geq 0$, and $|r| = 0$ if and only if $r = 0$ (positivity).
- $|rs| = |r| |s|$ (multiplicativity).
- $|r + s| \leq |r| + |s|$ (triangle inequality).

The *trivial absolute value* is defined by $\|r\| = 1$ for all nonzero r . Two absolute values $\|\cdot\|_1$ and $\|\cdot\|_2$ are *equivalent*³ if there is a real number $\rho > 0$ such that $\|\cdot\|_1 = \|\cdot\|_2^\rho$.

It is natural to ask if there are any nontrivial absolute values on the field \mathbb{Q} of rational numbers other than the usual one. The answer is that there is one such absolute value for each prime number.

Definition. Let p be a prime. Given any nonzero rational number r , write r as a fraction in the form

$$r = p^k \cdot \frac{a}{b} \quad \text{with } k \in \mathbb{Z} \text{ and } p \nmid ab.$$

Then the *p -adic absolute value* of r is defined by

$$|r|_p = p^{-k}.$$

We further set $|0|_p = 0$. It is also convenient to define the *p -adic valuation* of r to be the quantity

$$\text{ord}_p(r) = k,$$

so $|r|_p = p^{-\text{ord}_p(r)}$. If we let $\text{ord}_p(0) = \infty$, then this formula is still true with the convention that $p^{-\infty} = 0$.

The intuition behind the p -adic absolute value is that a number is small if it is divisible by p , and it is very small if it is divisible by a very large power of p . In the other direction, rational numbers with powers of p in their denominator are p -adically large numbers. We observe that $|\cdot|_p$ is the same as the absolute value obtained by embedding \mathbb{Q} in \mathbb{Q}_p and using the absolute value on \mathbb{Q}_p that we defined in Section 1.2.

Example 1.12. Here are some examples of p -adic absolute values on \mathbb{Q} ,

$$|9|_3 = \frac{1}{9}, \quad |24|_2 = \frac{1}{8}, \quad \left| \frac{15}{28} \right|_7 = 7,$$

and some examples of p -adic valuations,

$$\text{ord}_3(18) = 2, \quad \text{ord}_2(1728) = 6, \quad \text{ord}_5\left(\frac{49}{50}\right) = -2.$$

Proposition 1.13. *The p -adic absolute value is an absolute value on \mathbb{Q} , i.e., it is positive definite, multiplicative, and satisfies the triangle inequality. In fact, it satisfies the stronger inequality*

$$|r + s|_p \leq \max\{|r|_p, |s|_p\} \quad (\text{ultrametric triangle inequality}).$$

Further

$$|r|_p \neq |s|_p \implies |r + s|_p = \max\{|r|_p, |s|_p\}.$$

³An absolute value defines a topology on the field K in the usual way, a basis of open neighborhoods of $\alpha \in K$ are the balls $\{\beta \in K : \|\beta - \alpha\| < \epsilon\}$. It is easy to see that equivalent absolute values define the same topology; and conversely if two absolute values define the same topology, then they are equivalent.

Proof. We proved this for \mathbb{Q}_p in Proposition 1.5. In Exercise 1.14 we ask you to give a direct proof. \square

If you are wondering why we single out the p -adic absolute values from among all of the possible absolute values on \mathbb{Q} , the next result provides a satisfactory explanation.

Theorem 1.14. (Ostrowski) *Up to equivalence, the only nontrivial absolute values on \mathbb{Q} are the usual absolute value and the p -adic absolute values.*

Proof. Let $\|\cdot\|$ be an absolute value on \mathbb{Q} . We observe that

$$\|-r\|^2 = \|(-r)^2\| = \|r^2\| = \|r\|^2,$$

so $\|-r\| = \|r\|$ for all r . In particular, $\|\cdot\|$ is completely determined by its values on \mathbb{N} .

We consider two cases, depending on the size of $\|\cdot\|$.

Case I: $\|n\| \leq 1$ for all $n \in \mathbb{N}$.

The nontriviality of $\|\cdot\|$ implies that $\|m\| \neq 1$ for some $m \in \mathbb{N}$. Let m be the smallest such positive integer. Our assumption for Case I implies that $\|m\| < 1$. We claim that m is prime. Suppose that $m = m_1 m_2$. Then

$$1 > \|m\| = \|m_1\| \|m_2\|,$$

so one of $\|m_1\|$ and $\|m_2\|$ is smaller than 1. Then the minimality of m tells us that $m_1 = m$ or $m_2 = m$. This proves that m is prime. For ease of exposition we relabel m as p . Thus p is a prime satisfying $\|p\| < 1$, and $\|n\| = 1$ for all $1 \leq n < p$.

Now let n be any integer with $p \nmid n$. We claim that $\|n\| = 1$. To prove this, we choose some large integer k and, noting that $\gcd(p, n^k) = 1$, we can write

$$up + vn^k = 1 \quad \text{with } u, v \in \mathbb{Z} \text{ and } 1 \leq v < p.$$

Then $\|v\| = 1$, and the triangle inequality yields

$$\|n\|^k = \|vn^k\| = \|1 - up\| \geq \|1\| - \|up\| \geq 1 - \|p\|.$$

(We have also used the fact that $\|u\| \leq 1$.) Thus

$$\|n\| \geq (1 - \|p\|)^{1/k} \quad \text{for all } k \geq 1.$$

Using the fact that $\|p\| < 1$ and letting $k \rightarrow \infty$ yields $\|n\| \geq 1$, which completes the proof that $\|n\| = 1$ for all n that are not divisible by p .

Hence if we write a rational number r as a fraction $r = p^k \cdot \frac{a}{b}$ with $p \nmid ab$, then

$$\|r\| = \|p\|^k \|a\| \|b\|^{-1} = \|p\|^k,$$

so if we set

$$\rho = -\frac{\log \|p\|}{\log p},$$

then $\|r\| = |r|_p^\rho$. Therefore $\|\cdot\|$ is equivalent to the p -adic absolute value $|\cdot|_p$. The complete the case that $\|\cdot\|$ is bounded on \mathbb{N} .

Case II: There exists an $m \in \mathbb{N}$ such that $\|m\| > 1$.

We observe that for any $n \in \mathbb{N}$, the triangle inequality implies that

$$\|n\| = \|1 + 1 + \cdots + 1\| \leq \|1\| + \|1\| + \cdots + \|1\| = n.$$

We are now going to prove a claim that actually is true in both Cases I and II, although in the former it simply states that $1 = 1$, so is not very useful.

Claim. For all $a, b \in \mathbb{N}$ we have

$$\{\|b\|, 1\}^{\log a} = \max\{1, \|a\|\}^{\log b}.$$

If $a = 1$, then $\log a = 0$ and $\|a\| = 1$, so the stated equality is true, and similarly if $b = 1$. So we may assume $a \geq 2$ and $b \geq 2$. We fix a (large) integer k and write b^k in base a ,

$$b^k = c_0 + c_1 a + c_2 a^2 + \cdots + c_t a^t \quad \text{with } 0 \leq c_i < a \text{ and } c_t \neq 0.$$

Then the triangle inequality yields

$$\begin{aligned} \|b\|^k &= \|c_0 + c_1 a + c_2 a^2 + \cdots + c_t a^t\| \\ &\leq \|c_0\| + \|c_1\| \|a\| + \|c_2\| \|a\|^2 + \cdots + \|c_t\| \max\{1, \|a\|\}^t \\ &\leq (t+1)(a-1) \max\{1, \|a\|\}^t \quad \text{since } \|c_i\| \leq c_i < a. \end{aligned}$$

We can relate k and t since $b^k \geq c_t a^t \geq a^t$, so

$$t \leq k \frac{\log b}{\log a}.$$

Substituting above yields

$$\|b\|^k \leq \left(k \frac{\log b}{\log a}\right) (a-1) \max\{1, \|a\|\}^{(k \log b)/(\log a)}.$$

Taking the k^{th} root of both sides and letting $k \rightarrow \infty$ gives

$$\|b\| \leq \max\{1, \|a\|\}^{(\log b)/(\log a)},$$

which proves one inequality. Reversing the roles of a and b gives the opposite inequality, which completes the proof of the claim.

We now resume the proof of Ostrowski's theorem. We are assuming that there is a integer $m \geq 1$ satisfying $\|m\| > 1$. Let $a \geq 2$ be an integer. Then applying the claim to a and m , we find that

$$\max\{1, \|a\|\}^{\log m} = \max\{1, \|m\|\}^{\log a} = \|m\|^{\log a} > 1,$$

so $\|a\| > 1$. This proves that $\max\{1, \|a\|\} = \|a\|$ for all $a \in \mathbb{N}$, so the claim implies that

$$\|a\|^{\log m} = \|m\|^{\log a} \quad \text{for all } a \in \mathbb{N}.$$

Equivalently, if we let

$$\rho = \frac{\log \|m\|}{\log m},$$

then

$$\|a\| = a^\rho \quad \text{for all } a \in \mathbb{N}.$$

It follows by multiplicativity that $\|r\| = r^\rho$ for all positive $r \in \mathbb{Q}$, hence $\|\cdot\|$ is equivalent to the usual absolute value on \mathbb{Q} . \square

Exercises

Section 1.1. Congruences Modulo p^n and Hensel's Lemma

1.1. (a)

Learn about Berlekamp's algorithm (1967) for factoring polynomials in $\mathbb{F}_q[x]$. Write a brief description of the algorithm, including an explanation of why it works.

Learn about the Cantor–Zassenhaus algorithm (1981) for factoring polynomials in $\mathbb{F}_q[x]$. Write a brief description of the algorithm, including an explanation of why it works.

1.2. Use Hensel's lemma to solve the following congruences, cf. Example 1.2.

- (a) Find a solution to $x^2 - 2 \equiv 0 \pmod{7^4}$ satisfying $x \equiv 3 \pmod{7}$.
 (b) Find a solution to $x^3 + x + 1 \equiv 0 \pmod{3^4}$ satisfying $x \equiv 1 \pmod{3}$.

Section 1.2. The Ring of p -adic Integers

1.3. Prove that the maximal ideal \mathfrak{M} of \mathbb{Z}_p as described in Proposition 1.4 is a principal ideal generated by p . More generally, show that every nonzero ideal of \mathbb{Z}_p is a principal ideal generated by p^k for some $k \geq 0$.

1.4. A *local ring* is a ring that has a unique maximal ideal. Prove that R is a local ring if and only if there is an ideal I of R such that

$$R = I \cup R^* \quad \text{and} \quad I \cap R^* = \emptyset.$$

1.5. Prove the following strengthened version of Hensel's lemma.

Theorem 1.15 (Hensel's Lemma: Version III). Let $f(x) \in \mathbb{Z}_p[x]$ be a nonzero polynomial and let $\alpha \in \mathbb{Z}_p$ be a p -adic number such that

$$|f(\alpha)|_p < |f'(\alpha)|_p^2.$$

Then there exists a unique $\beta \in \mathbb{Z}_p$ satisfying

$$f(\beta) = 0 \quad \text{and} \quad |\beta - \alpha|_p < 1.$$

(The special case $|f(\alpha)|_p < 1$ and $|f'(\alpha)|_p = 1$ is Theorem 1.8.)

1.6. Prove the following strengthened version of Hensel's lemma.

Theorem 1.16 (Hensel's Lemma: Version IV). Let $f(X) \in \mathbb{Z}_p[x]$, and suppose that when $f(X)$ is reduced modulo p , it factors as

$$f(X) \equiv G(X)H(X) \pmod{p}$$

for some $G(X), H(X) \in \mathbb{F}_p[X]$. Prove that there are polynomials $g(X), h(X) \in \mathbb{Z}_p[X]$ satisfying

$$f(X) = g(X)h(X), \quad g(X) \equiv G(X) \pmod{p}, \quad \text{and} \quad h(X) \equiv H(X) \pmod{p}.$$

*** Not quite correct, need the condition like $|f'(\alpha)|_p = 1$.

1.7. Let $f(x) \in \mathbb{Z}_p[x]$ be a nonzero polynomial and let $\alpha \in \mathbb{Z}_p$ be a p -adic number such that

$$|f(\alpha)|_p < 1 \quad \text{and} \quad |f'(\alpha)|_p = 1.$$

Define a sequence of p -adic numbers by setting

$$\beta_0 = \alpha \quad \text{and} \quad \beta_{n+1} = \beta_n - \frac{f(\beta_n)}{f'(\beta_n)}.$$

Prove that

$$|f(\beta_{n+1})|_p \leq |f(\beta_n)|_p^2 \quad \text{for all } n \geq 0.$$

(Hint. Prove by induction that

$$|\beta_n - \alpha|_p < 1, \quad |f(\beta_n)|_p < 1, \quad |f'(\beta_n)|_p = 1 \quad \text{for all } n \geq 0.)$$

Deduce that the sequence β_n converges in \mathbb{Z}_p to a root β of $f(x)$ and that the convergence is extremely rapid. More precisely, prove that

$$|\beta - \beta_n|_p \leq |f(\alpha)|_p^{2^n} \quad \text{and} \quad |f(\beta_n)|_p \leq |f(\alpha)|_p^{2^n}.$$

(This exercise is a p -adic version of the Newton–Raphson algorithm for finding real roots of polynomials.)

1.8. (a) Let r be a rational number whose denominator is not divisible by p . Prove that the binomial formula

$$(1+t)^r = \sum_{i=0}^{\infty} \binom{r}{i} t^i$$

is valid for all $t \in \mathbb{Z}_p$ with $|t|_p < 1$.

(b) Let $p \geq 3$ and let $\alpha \in \mathbb{Z}_p$ be congruent to 1 modulo p , so $\alpha = 1 + p\beta$ for some $\beta \in \mathbb{Z}_p$. Define $\gamma \in \mathbb{Z}_p$ by the series

$$\gamma = 1 + 2 \sum_{i=1}^{\infty} \frac{(-1)^{i-1}}{i} \binom{2i-2}{i-1} \left(\frac{p\beta}{4}\right)^i.$$

Prove that the series defining γ converges in \mathbb{Z}_p and satisfies $\gamma^2 = \alpha$. (Hint. Use (a) with $r = \frac{1}{2}$.)

- (c) Write down a convergent 5-adic series that is a solution in \mathbb{Z}_5 to the equation $x^2 = -1$. Use this series to solve $x^2 \equiv -1 \pmod{5^5}$. (*Hint.* To find a square root of -1 , write $-1 = 4 - 5 = 4(1 - 5/4)$ and compute $\sqrt{-1} = 2\sqrt{1 - 5/4}$.)

Section 1.3. The Ring of p -adic Integers is Complete

1.9. Let K be a field with an absolute value $\|\cdot\|$ having the following properties:

- (i) $\mathbb{Q} \subset K$.
- (ii) For every $r \in \mathbb{Q}$ we have $\|r\| = |r|_p$.
- (iii) The field K is complete with respect to the absolute value $\|\cdot\|$.

Prove that there is a unique inclusion of fields $\mathbb{Q}_p \hookrightarrow K$. (Informally, this says that \mathbb{Q}_p is the smallest extension of \mathbb{Q} that is complete with respect to the p -adic absolute value.)

1.10. For which $\alpha \in \mathbb{Q}_p$ do each of the following series converge in \mathbb{Q}_p ?

$$(a) \sum_{i=0}^{\infty} \alpha^i \quad (b) \sum_{i=0}^{\infty} \frac{\alpha^i}{i!} \quad (c) \sum_{i=1}^{\infty} \frac{\alpha^i}{i}$$

1.11. Let K be a field with an absolute value $|\cdot|$ and let $(\alpha_i)_{i \geq 1}$ be a sequence of elements in K . Prove that

$$\sum_{i=1}^{\infty} \alpha_i \text{ converges in } K \implies \lim_{i \rightarrow \infty} \alpha_i = 0.$$

Section 1.4. Absolute Values

1.12. Let $|\cdot|$ be an absolute value on a field K .

- (a) Suppose that instead of the axiom of positivity, we assume only that there exists some element $\alpha \in K$ with the property that $|\alpha| \neq 0$. Prove that this, together with the other axioms, is enough to prove that $|1| = 1$ and that $|\beta| \neq 0$ for all $\beta \neq 0$.
- (b) Let $R = \{\alpha \in K : |\alpha| \leq 1\}$ and $M = \{\alpha \in K : |\alpha| < 1\}$. Prove that R is a subring of K and that M is an ideal of R . Prove that $R = M \cup R^*$, i.e., prove that every element not in M is a unit in R . Deduce that M is the unique maximal ideal of R .

1.13. Let $\|\cdot\|$ be an absolute value on a field K of characteristic zero, so $\mathbb{Z} \subset K$. Suppose that $\|n\|$ is bounded for $n \in \mathbb{Z}$. Prove that $\|n\| \leq 1$ for all $n \in \mathbb{N}$.

1.14. Prove Proposition 1.13 directly using the definition of the absolute value on \mathbb{Q}_p .