# 5. $p$-adic Numbers

**5.1. Motivating examples.** We all know that $\sqrt{2}$ is irrational, so that $2$ is not a square in the rational field $\mathbb{Q}$, but that we can enlarge $\mathbb{Q}$ to the real field $\mathbb{R}$ where $2$ is a square. In $\mathbb{R}$, we may represent irrational numbers by (non-terminating, non-recurring) decimal expansions:

$$\sqrt{2} = 1.414213562373\cdots = 1 + 4\cdot 10^{-1} + 1\cdot 10^{-2} + 4\cdot 10^{-3} + 2\cdot 10^{-4} + \dots$$

In general, real numbers are expressible as

$$x = \pm \sum_{k=-\infty}^{n} a_k 10^k,$$

where the digits $a_k \in \{0,1,2,3,4,5,6,7,8,9\}$; there are only finitely many terms with $k > 0$, but may be infinitely many with $k < 0$; the series always converges in $\mathbb{R}$; and the sequence of digits $(a_k)$ is usually uniquely determined by $x$. (The exceptions are numbers $x$ with finite decimal expansions, where we can replace the tail $\dots a000\dots$ with $\dots(a-1)999\dots$.)

Another way of thinking about the decimal expansion of the irrational number $\sqrt{2}$ is to say that $\sqrt{2}$ is the limit of a sequence $(x_k)$ of rational numbers: $x_0 = 1$, $x_1 = 14/10$, $x_2 = 141/100$, .... This is a Cauchy sequence of rational numbers, and has no limit in $\mathbb{Q}$, but does have a limit $\sqrt{2} = \lim_{k\to\infty} x_k$ in the larger complete field $\mathbb{R}$. The rational numbers $x_k$ are rational approximations to $\sqrt{2}$, each being a better approximation than the previous one:

$$|\sqrt{2} - x_k| \leq 10^{-k}.$$

As a first example of a $p$-adic number for $p = 7$, we consider the quadratic congruences

$$x^2 \equiv 2 \pmod{7^k}$$

for $k = 1, 2, 3 \dots$. When $k = 1$ there are two solutions: $x = x_1 \equiv \pm 3 \pmod 7$. Any solution $x_2$ to the congruence modulo $7^2$ must also be a solution modulo $7$, hence of the form $x_2 = x_1 + 7y = \pm 3 + 7y$; choosing $x_1 = 3$ gives $x_2 = 3 + 7y$, which must satisfy

$$0 \equiv x_2^2 - 2 \equiv (3 + 7y)^2 - 2 \equiv 7(1 + 6y) \pmod{7^2};$$

equivalently, $1 + 6y \equiv 0 \pmod 7$ with unique solution $y \equiv 1 \pmod 7$; so $x_2 = 3 + 1 \cdot 7 = 10$.

Continuing in a similar way, setting $x_3 = x_2 + 7^2 y$ and substituting, we find that $x_3^2 \equiv 2 \pmod{7^3} \iff y \equiv 2 \pmod 7$, so $x_3 \equiv x_2 + 2 \cdot 7^2 \equiv 108 \pmod{7^3}$. The process may be continued indefinitely. At each stage there is a unique solution, so (after fixing the initial choice of $x_1 = 3$) we find, uniquely,

$$\begin{aligned} x_1 &= 3 = 3, \\ x_2 &= 10 = 3 + 1 \cdot 7, \\ x_3 &= 108 = 3 + 1 \cdot 7 + 2 \cdot 7^2, \\ x_4 &= 2166 = 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3, \dots \end{aligned}$$

The general formula is $x_{k+1} \equiv x_k^2 + x_k - 2 \pmod{7^{k+1}}$.

What happens "in the limit"? Does it even make sense to talk about the limit of the sequence $x_k$? Certainly there can be no *single* integer $x$ satisfying $x^2 \equiv 2 \pmod{7^n}$ simultaneously for all $n \geq 1$, for then $x^2 - 2$ would be divisible by arbitrarily large powers of $7$ which is only possible when $x^2 - 2 = 0$. Also, the infinite series $3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + \dots$ does not converge in the normal sense, since the successive terms do not tend to $0$.

We will define a new kind of number called a $p$-adic number, for each prime $p$. The $p$-adic integers will form a ring $\mathbb{Z}_p$, which contains $\mathbb{Z}$; there is one such ring for each prime $p$. In the ring $\mathbb{Z}_7$ of 7-adic integers, our sequence $3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + \dots$ will converge to a 7-adic limit, so that the equation $x^2 = 2$ has a solution in $\mathbb{Z}_7$. The solution can be expressed as an infinite 7-adic expansion:

$$\begin{aligned} x &= 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 7^4 + 2 \cdot 7^5 + 7^6 + 2 \cdot 7^7 + 4 \cdot 7^8 + 6 \cdot 7^9 + \dots \\ &= \sum_{k=0}^{\infty} a_k 7^k, \end{aligned}$$

where the “digits” $a_k$ are all in the set $\{0, 1, 2, 3, 4, 5, 6\}$ and are uniquely determined after fixing $x \equiv 3 \pmod 7$: $a_0 = 3$, $a_1 = 1$, $a_2 = 2$, $a_3 = 6$, $\dots$.

The ring $\mathbb{Z}_p$ has a field of fractions $\mathbb{Q}_p$, which contains the rational field $\mathbb{Q}$. In fact, $\mathbb{Q}_p$ may be constructed directly from $\mathbb{Q}$ by a process similar to the construction of the real numbers as the set of limits of Cauchy sequences of rationals. $\mathbb{R}$ is the completion of $\mathbb{Q}$, complete in the usual analytic sense that Cauchy sequences converge in $\mathbb{R}$. Just as one can define the real numbers as (equivalence classes of) Cauchy sequences of rational numbers, we will start by defining $p$-adic integers as equivalence classes of suitable sequences of ordinary integers.

### 5.2. **Definition of $\mathbb{Z}_p$.** Fix, once and for all, a prime number $p$.

**Definition 5.2.1.** *A $p$-adic integer $\alpha$ is defined by a sequence of integers $x_k$ for $k \geq 1$*

$$\alpha = \{x_k\}_{k=1}^{\infty} = \{x_1, x_2, x_3, \dots\},$$

*satisfying the conditions*

$$x_{k+1} \equiv x_k \pmod{p^k} \qquad \textit{for all } k \geq 1, \tag{5.2.1}$$

*with two sequences* $\{x_k\}$ *and* $\{y_k\}$ *determining the same* $p$*-adic integer* $\alpha$ *if and only if*

$$x_k \equiv y_k \pmod{p^k} \qquad \textit{for all } k \geq 1.$$

*The set of* $p$*-adic integers is denoted* $\mathbb{Z}_p$*.*

An integer sequence satisfying (5.2.1) will be called *coherent*. Thus, each $p$-adic integer is actually an equivalence class of coherent sequences of ordinary integers, any one of which may be used to represent it. The representation of a $p$-adic integer $x = \{x_k\}$ will be called *reduced* if $0 \leq x_k < p^k$ for all $k \geq 1$. Every $p$-adic integer has a unique reduced representation.

The ordinary integers $\mathbb{Z}$ embed into $\mathbb{Z}_p$ as constant sequences, via $x \mapsto \{x, x, x, \dots\}$; this map is injective since if $x, y \in \mathbb{Z}$ satisfy $x \equiv y \pmod{p^k}$ for all $k \geq 1$, then $x = y$. So we can view $\mathbb{Z}$ as a subset of $\mathbb{Z}_p$. We may call elements of $\mathbb{Z}$ *rational integers* to distinguish them from $p$-adic integers.

**Examples:** Take $p = 3$. Here are three elements of $\mathbb{Z}_3$:

$$\begin{aligned} \alpha &= 40 = \{40, 40, 40, 40, 40, \dots\} = \{1, 4, 13, 40, 40, \dots\}; \\ \beta &= -1 = \{-1, -1, -1, -1, -1, \dots\} = \{2, 8, 26, 80, 242, \dots\}; \\ \gamma &= ? = \{1, 7, 16, 70, 151, \dots\}. \end{aligned}$$

the last representation is reduced in each case. Later we will see that $\gamma$ is actually a representation of the rational number $-7/8$! In the reduced representation of $-1$, notice that

$$\begin{aligned}
2 &= 3 - 1 = 2, \\
8 &= 3^2 - 1 = 2 + 2 \cdot 3, \\
26 &= 3^3 - 1 = 2 + 2 \cdot 3 + 2 \cdot 3^2, \\
80 &= 3^4 - 1 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3, \\
242 &= 3^5 - 1 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4,
\end{aligned}$$

suggesting that the limiting value of the sequence $x_k$ is $2(1 + 3 + 3^2 + 3^3 + \dots)$. This geometric series does not converge in the usual sense; but if it did converge, the usual formula would give as its sum the correct value $2/(1 - 3) = -1$. We will see later that this is a perfectly valid computation within the field $\mathbb{Q}_3$ of $3$-adic numbers.

It follows from the coherence condition (5.2.1) that $\alpha = \{x_1, x_2, x_3, \dots\} = \{x_2, x_3, x_4, \dots\}$! In other words, we can shift the sequence any number of steps, or even delete any finite number of terms without affecting the value. At first sight this seems strange, but if you think of the value of $\alpha$ as being the *limit* of the sequence $(x_k)$ (which we will later see to be the case), then it is natural.

We will see this index-shifting in action in proving some facts about $p$-adic numbers soon.

As suggested by the second example above, we now consider an alternative representation of a $p$-adic integer $\alpha$ with reduced representation $\{x_k\}$. Writing $x_k$ to base $p$, we have

(5.2.2)
$$x_k = a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots + a_{k-1} \cdot p^{k-1}$$

with each "digit" $a_i \in \{0, 1, 2, \ldots, p-1\}$. The coherency condition (5.2.1) implies that $x_1 = a_0$, $x_2 = a_0 + a_1 p$, $x_3 = a_0 + a_1 p + a_2 p^2$, and so on, with the *same* digits $a_i$. So each $\alpha \in \mathbb{Z}_p$ determines a unique infinite sequence of *p-adic digits* $(a_i)_{i=0}^{\infty}$ with $0 \le a_i \le p-1$, and conversely every such digit sequence determines a unique $p$-adic integer $\alpha = \{x_k\}$ via (5.2.2). In the examples, the $3$-adic digits of $\alpha = 40 = 1 + 3 + 3^2 + 3^3$ are $1, 1, 1, 1, 0, 0, \ldots$ (effectively a finite sequence), those of $\beta = -1$ form the infinite recurring sequence $2, 2, 2, 2, 2, \ldots$ and those of $\gamma = 1 + 2 \cdot 3 + 3^2 + 2 \cdot 3^3 + 3^4 + \ldots$ are $1, 2, 1, 2, 1, \ldots$.

We will write $\alpha = \{x_k\} = \sum_{i=0}^{\infty} a_i p^i$ when the $p$-adic digits of $\alpha$ are $a_i$, so that $x_k = \sum_{i=0}^{k-1} a_i p^i$ for $k \ge 1$. For now, this infinite series should be regarded as just a formal expression or shorthand.

5.3. **The ring $\mathbb{Z}_p$.** To add and multiply $p$-adic integers, just add and multiply the representative sequences termwise:

$$\{x_k\} + \{y_k\} = \{x_k + y_k\};$$
$$\{x_k\} \cdot \{y_k\} = \{x_k y_k\}.$$

One must check that the sequences on the right are coherent (in the sense of (5.2.1)), and that replacing $\{x_k\}$ or $\{y_k\}$ by an equivalent sequence does not change the equivalence classes of the sequences on the right: these are straightforward exercises, as are the verifications that all the ring axioms hold. For example, the negative of $\alpha = \{x_k\}$ is just $-\alpha = \{-x_k\}$. Expressing these operations in terms of the expansions $\alpha = \sum a_i p^i$ is not so easy: we will see examples later.

This gives $\mathbb{Z}_p$ the structure of a *commutative ring*, with $\mathbb{Z}$ as a subring. The factorization theory of $p$-adic integers turns out to be rather simple. There are no zero-divisors:

**Proposition 5.3.1.** *$\mathbb{Z}_p$ is an integral domain.*

Next we determine the units $U(\mathbb{Z}_p)$:

**Proposition 5.3.2.** *Let* $\alpha = \{x_k\} = \sum a_i p^i \in \mathbb{Z}_p$. *The following are equivalent:*

(i) $\alpha \in U(\mathbb{Z}_p)$;
(ii) $p \not| x_1$;
(iii) $p \not| x_k$ *for all* $k \geq 1$;
(iv) $a_0 \neq 0$;

**Examples:** If $a \in \mathbb{Z}$ with $p \not| a$, then $a$ is a $p$-adic unit. Its inverse is given by the coherent sequence $\{x_k\}$ where $x_k$ satisfies $ax_k \equiv 1 \pmod{p^k}$ for $k \geq 1$.

For example, $3$ is a $5$-adic unit, so $1/3 \in \mathbb{Z}_5$. To find the terms $x_k$ in its defining sequence for $k \leq 4$, solve $3x_4 \equiv 1 \pmod{5^4}$ to get $x_4 = 417$. Reducing this modulo lower powers of $5$ then gives the start of the sequence in reduced form: $1/3 = \{2, 17, 42, 417, \dots\}$. And since $417 = 2 + 3 \cdot 5 + 5^2 + 3 \cdot 5^3$, the $5$-adic digits of $1/3$ start $2, 3, 1, 3, \dots$. In fact the digit sequence recurs: $2, 3, 1, 3, 1, 3, 1, 3, 1, 3 \dots$. We can verify this by summing the series:

$$1 + (1 + 3 \cdot 5)(1 + 5^2 + 5^4 + \dots) = 1 + 16/(1 - 25) = (24 - 16)/24 = 1/3.$$

As another example, expanding $-7/8$ in $\mathbb{Z}_3$ gives the example denoted $\gamma$ above (exercise).

It is easy to tell whether a $p$-adic integer is divisible by $p$, or by a power of $p$:

**Proposition 5.3.3.** *For* $\alpha = \{x_k\} \in \mathbb{Z}_p$*:*

(i) $p|\alpha \iff \alpha \notin U(\mathbb{Z}_p) \iff x_1 \equiv 0 \pmod{p} \iff x_k \equiv 0 \pmod{p}\ (\forall k \geq 1)$;
(ii) *for* $n \geq 1$, $p^n|\alpha \iff x_n \equiv 0 \pmod{p^n} \iff x_k \equiv 0 \pmod{p^n}\ (\forall k \geq n)$.

Now we know that every $p$-adic integer is either a unit or a multiple of $p$, but never both. From this we can show that $\mathbb{Z}_p$ is a UFD, with $p$ the only prime:

**Theorem 5.3.4.** *$\mathbb{Z}_p$ is a UFD (unique factorization domain). The only irreducible (prime) element, up to associates, is $p$.*

That is, every nonzero element $\alpha \in \mathbb{Z}_p$ may be uniquely expressed as $\alpha = p^m \varepsilon$ where $m \in \mathbb{Z}$, $m \geq 0$ and $\varepsilon \in U(\mathbb{Z}_p)$.

Every rational number $r = b/a$ with $a, b \in \mathbb{Z}$ and $p \nmid a$ is also in $\mathbb{Z}_p$, since both $a$ and $b$ are, and $a$ is a $p$-adic unit. We have $b/a = \{x_k\}$ where $ax_k \equiv b \pmod{p^k}$ for $k \geq 1$. The rational numbers $r$ which have this form are those for which $\text{ord}_p(r) \geq 0$, since $\text{ord}_p(b/a) = \text{ord}_p(b) - \text{ord}_p(a)$. These are called *$p$-integral* rational numbers. Define

$$R_p = \left\{ \frac{n}{d} \in \mathbb{Q} : p \nmid d \right\} = \{ x \in \mathbb{Q} \mid \text{ord}_p(x) \geq 0 \}.$$

The set $R_p$ of $p$-integral rationals is a subring both of $\mathbb{Q}$ and of $\mathbb{Z}_p$. Within $\mathbb{Z}_p$ they may be recognized as the $p$-adic integers whose digit sequence is ultimately periodic (just as the rationals are the real numbers with ultimately periodic decimal expansions).

**Proposition 5.3.5.** *$R_p$ is a ring, with $\mathbb{Z} \subset R_p \subset \mathbb{Q}$, and $\mathbb{Z} \subset R_p \subset \mathbb{Z}_p$. Also, $R_p = \mathbb{Z}_p \cap \mathbb{Q}$.*

**Corollary 5.3.6.** (a) *Every rational number is in $\mathbb{Z}_p$ for all but a finite number of primes $p$.*
(b) *$\bigcap_{p \in \mathbb{P}} R_p = \mathbb{Z}$.*

We now extend the function $\text{ord}_p$, which we have already defined on $\mathbb{Z}$ and on $\mathbb{Q}$, to $\mathbb{Z}_p$. Since the prime $p$ is fixed we may sometimes write ord instead of $\text{ord}_p$.

**Definition 5.3.7.** *For nonzero $\alpha \in \mathbb{Z}_p$ we define $\mathrm{ord}_p(\alpha) = m$ where $m$ is the largest integer for which $p^m|\alpha$ (in $\mathbb{Z}_p$). We also set $\mathrm{ord}_p(0) = \infty$.*

So $\mathrm{ord}_p(\alpha) = m \geq 0$ is the power of $p$ appearing in its factorization $\alpha = p^m\varepsilon$. This definition agrees with the old definition of $\mathrm{ord}_p$ for rationals when $\alpha \in \mathbb{Z}_p \cap \mathbb{Q} = R_p$.

**Proposition 5.3.8.** *The function $\mathrm{ord}_p : \mathbb{Z}_p \to \mathbb{N}_0 \cup \{\infty\}$ has the following properties:*
(1) *for $n \in \mathbb{Z}$ (or $\mathbb{Q}$), this definition of $\mathrm{ord}_p(n)$ agrees with the one in Chapter 1;*
(2) *$\mathrm{ord}_p(\alpha\beta) = \mathrm{ord}_p(\alpha) + \mathrm{ord}_p(\beta)$;*
(3) *$\alpha|\beta \iff \mathrm{ord}_p(\alpha) \leq \mathrm{ord}_p(\beta)$;*
(4) *$\mathrm{ord}_p(\alpha + \beta) \geq \min\{\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta)\}$, with equality if $\mathrm{ord}_p(\alpha) \neq \mathrm{ord}_p(\beta)$.*

We can also consider congruences in $\mathbb{Z}_p$. The next proposition shows that these are effectively the same as congruences in $\mathbb{Z}$ modulo powers of $p$.

**Proposition 5.3.9.** *For each $m \geq 0$, every $\alpha \in \mathbb{Z}_p$ is congruent modulo $p^m$ to a unique integer $n$ with $0 \leq n < p^m$. Moreover there is a ring isomorphism*

$$\mathbb{Z}_p/p^m\mathbb{Z}_p \cong \mathbb{Z}/p^m\mathbb{Z}.$$

5.4. **The field $\mathbb{Q}_p$.** Since the ring $\mathbb{Z}_p$ is an integral domain we can form its *field of fractions*, the field of *$p$-adic numbers* $\mathbb{Q}_p$:

$$\mathbb{Q}_p = \{\alpha/\beta \mid \alpha, \beta \in \mathbb{Z}_p, \beta \neq 0\}.$$

This forms a field under the usual rules for arithmetic of fractions, with $\mathbb{Z}_p$ as a subring and $\mathbb{Q}$ as a subfield. Since every nonzero $p$-adic integer has the form $p^n\varepsilon$ with $\varepsilon$ a $p$-adic unit, we see that the nonzero elements of $\mathbb{Q}_p$ all have the form $x = p^m\varepsilon$ where now the exponent $m$ is an arbitrary integer. We extend the order function from $\mathbb{Z}_p$ to a function $\text{ord}_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ by setting $\text{ord}_p(x) = m$. So $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid \text{ord}_p(x) \geq 0\}$ (including $0$ since $\text{ord}_p(0) = \infty$.) Parts (2) and (4) of Proposition 5.3.8 still apply.

$$\{0\} \subset \cdots \subset p^3\mathbb{Z}_p \subset p^2\mathbb{Z}_p \subset p\mathbb{Z}_p \subset \mathbb{Z}_p \subset p^{-1}\mathbb{Z}_p \subset p^{-2}\mathbb{Z}_p \subset p^{-3}\mathbb{Z}_p \cdots \subset \mathbb{Q}_p.$$

Let $x \in \mathbb{Q}_p \setminus \mathbb{Z}_p$, so $\text{ord}_p(x) = -m < 0$ and $x = p^{-m}\varepsilon$ with $\varepsilon \in U(\mathbb{Z}_p)$. Write $\varepsilon = a + p^m\beta$ with $\beta \in \mathbb{Z}_p$ and $a \in \mathbb{Z}$; by Proposition 5.3.9 this is uniquely possible with $0 \leq a < p^m$, and since $\varepsilon$ is a unit, $p \nmid a$. Now

$$x = p^{-m}\varepsilon = p^{-m}(a + p^m\beta) = \frac{a}{p^m} + \beta;$$

so all $p$-adic numbers may be written (uniquely) as a $p$-adic integer plus a *fractional part* which is an ordinary rational number $r$ satisfying $0 \leq r < 1$, with denominator a power of $p$.

**Example:** Let $x = \frac{1}{10} \in \mathbb{Q}_5$, with $\text{ord}_5(x) = -1$. Then $5x = \frac{1}{2} = 3 + 2\cdot 5 + 2\cdot 5^2 + 2\cdot 5^3 + \ldots$ (using the method of earlier examples), so

$$x = 3\cdot 5^{-1} + 2 + 2\cdot 5 + 2\cdot 5^2 + \ldots,$$

with fractional part $\frac{3}{5}$ and $5$-integral part $x - \frac{3}{5} = -\frac{1}{2} = 2 + 2\cdot 5 + 2\cdot 5^2 + \ldots$.

Secondly, let $x = \frac{1}{100} \in \mathbb{Q}_5$, so $\text{ord}_5(x) = -2$ and $5^2x = \frac{1}{4} \in \mathbb{Z}_5$. To find the fractional part of $x$ we approximate $\frac{1}{4}$ modulo $5^2$ by solving $4y \equiv 1 \pmod{25}$ to get $y \equiv 19 \pmod{25}$. Then

$x - \frac{19}{25} = \frac{1-4\cdot 19}{100} = \frac{-75}{100} = -\frac{3}{4} \in \mathbb{Z}_5$, so the fractional part of $x$ is $\frac{19}{25}$ and the $5$-integral part is $-\frac{3}{4}$. (You can also get this by squaring $\frac{1}{10}$.)

We may use the $\operatorname{ord}_p$ function on $\mathbb{Q}_p$ to define a metric (distance function) and hence a topology on $\mathbb{Q}_p$. Then we may talk about convergence, continuity and such like; in particular, we will be able to justify the computations with infinite series we have seen in earlier examples. The key idea is that of a *norm* on a field.

**Definition 5.4.1.** *Let $F$ be a field. A* norm *on $F$ is a function $x \mapsto \|x\|$ from $F$ to the real numbers satisfying the following properties:*

(i) *Positivity: $\|x\| \geq 0$, and $\|x\| = 0 \iff x = 0$;*
(ii) *Multiplicativity: $\|xy\| = \|x\|\,\|y\|$;*
(iii) *Triangle inequality: $\|x+y\| \leq \|x\| + \|y\|$.*

For example, the usual absolute value $|x|$ is a norm on the fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. We sometimes write this as $|x|_\infty$ by analogy with the $p$-adic norms introduced below. The *trivial norm*, defined by $\|x\| = 1$ for all nonzero $x$, is a norm on any field. Note that the multiplicativity and positivity always imply that $\|1\| = \|-1\| = 1$, so that $\|-x\| = \|x\|$ for all $x \in F$.

Given a norm $\|\cdot\|$ on $F$, we may use it to define a *metric* or distance function on $F$, by setting $d(x,y) = \|x-y\|$ for $x, y \in F$. This has the following properties:

(i) Positivity: $d(x,y) \geq 0$, and $d(x,y) = 0 \iff x = y$;
(ii) Symmetry: $d(x,y) = d(y,x)$;
(iii) Triangle inequality: $d(x,z) \leq d(x,y) + d(y,z)$.

The field $F$, equipped with the metric from a norm on $F$, becomes a metric space, and hence also a topological space, so that we may consider such concepts as convergence of sequences and continuous functions on $F$. If $F$ has more than one norm, this will lead to different metrics and (in general) different topologies on $F$. However, if we just replace a norm $\|x\|$ by $\|x\|^\alpha$ for a positive real number $\alpha$, then the metrics will be equivalent (in the sense of metric spaces) and the topologies the same. We call a pair of norms which are related in this way *equivalent*.

We now introduce the *$p$-adic norms* on the field $\mathbb{Q}$. Fix a prime number $p$. Recall that the function $\text{ord}_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ has the following properties; these also hold in $\mathbb{Q}_p$.

**Lemma 5.4.2.** (1) *$\text{ord}_p(xy) = \text{ord}_p(x) + \text{ord}_p(y)$;*
(2) *$\text{ord}_p(x + y) \geq \min\{\text{ord}_p(x), \text{ord}_p(y)\}$, with equality if $\text{ord}_p(x) \neq \text{ord}_p(y)$.*

**Definition 5.4.3.** *Let $p$ be a prime. For nonzero $x \in \mathbb{Q}_p$ we define the $p$-adic norm of $x$ to be*

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

*and set $|0|_p = 0$.*

**Proposition 5.4.4.** *For each prime $p$ the $p$-adic norm is a norm on $\mathbb{Q}$ and on $\mathbb{Q}_p$. It satisfies the following stronger form of the triangle inequality:*

$$|x + y|_p \leq \max\{|x|_p, |y|_p\}.$$

*The associated $p$-adic metric $d(x, y) = |x - y|_p$ on $\mathbb{Q}_p$ satisfies*

$$d(x, z) \leq \max\{d(x, y), d(y, z)\},$$

*with equality if $d(x, y) \neq d(y, z)$.*

A norm or metric which satisfies this stronger form of the triangle inequality is called *non-Archimedean*, in contrast to more familiar *Archimedean* metrics. This inequality is sometimes known as the "isosceles triangle principle", since it implies that in a space with a non-Archimedean metric every triangle is isosceles!.

**Example:** Consider the $5$-adic norm on $\mathbb{Q}$. Take $x = \frac{3}{10}$ and $y = 40$. Since $\mathrm{ord}_5(x) = -1$ and $\mathrm{ord}_5(y) = 1$ we have $|x|_5 = 5$ and $|y|_5 = 5^{-1}$. The third side of the "triangle" with vertices $0$, $x$, $y$ has length $|x - y|_5$. Now $x - y = -\frac{397}{10}$ so $\mathrm{ord}_5(x - y) = -1$, and hence $|x - y|_5 = 5 = |x|_5$.

**Exercise:** Prove the *Product Formula*: for every nonzero $x \in \mathbb{Q}$ we have

$$|x|_\infty \prod_{p \in \mathbb{P}} |x|_p = 1.$$

The main theorem on norms on the rational field $\mathbb{Q}$ states that (up to equivalence) the only norms are the ones we have seen:

**Theorem 5.4.5.** *[Ostrowski's Theorem] Every nontrivial norm on $\mathbb{Q}$ is equivalent either to the standard absolute value $|x|$ or to the $p$-adic norm $|x|_p$ for some prime $p$. All these norms are inequivalent.*

We omit the proof. The idea is that if $\|n\| \geq 1$ for all nonzero $n \in \mathbb{Z}$, then one can show that $\|x\| = |x|_\infty^\alpha$ for some $\alpha > 0$, while if $\|n\| < 1$ for some $n > 1$ then the least such $n$ must be a prime $p$, and $\|x\| = \beta^{\mathrm{ord}_p(x)}$ where $\beta = \|p\|$.

One can prove that $\mathbb{Q}_p$, with the $p$-adic metric, is complete. In fact, an alternative construction of $\mathbb{Q}_p$ is to start with the $p$-adic metric on $\mathbb{Q}$ and form the *completion* of $\mathbb{Q}$ with respect to this metric; this is entirely analogous to the construction of the real numbers by completing $\mathbb{Q}$ with respect to the usual metric. Either way we end up with a complete field $\mathbb{Q}_p$ in which $\mathbb{Q}$ is *dense* (we prove this below).

The theory of $p$-adic analysis has many counter-intuitive features, such as the fact that every $p$-adic triangle is isosceles. Another one is: a series $\sum_{n=1}^{\infty} a_n$ with terms $a_n \in \mathbb{Q}_p$ converges *if and only if* the terms tend to zero, i.e. $\lim_{n\to\infty} a_n = 0$. We will prove a special case of this in the next proposition.

Rather than continuing with this analytic theory, however, we will content ourselves with some examples, which in particular show that the earlier computations we carried out with power series are valid in $\mathbb{Q}_p$, once we have equipped it with its ($p$-adic) metric.

**Proposition 5.4.6.** (1) *Let $\alpha \in \mathbb{Z}_p$ be given by a coherent sequence $\{x_k\}$ of integers. Then $\lim_{k\to\infty} x_k = \alpha$, the limit being in the $p$-adic topology on $\mathbb{Z}_p$.*

(2) *Let $(a_i)_{i=0}^{\infty}$ be a sequence of integers with $0 \le a_i \le p-1$ for all $i \ge 0$. Then the series $\sum_{i=0}^{\infty} a_i p^i$ converges in $\mathbb{Z}_p$ to the $p$-adic integer $\alpha = \{x_k\}$, where $x_k = \sum_{i=0}^{k-1} a_i p^i$.*

**Corollary 5.4.7.** *Every $p$-adic integer in $\mathbb{Z}_p$ is the limit of a convergent sequence of rational integers. Every $p$-adic number in $\mathbb{Q}_p$ is the limit of a sequence of rational numbers.*

In other words, $\mathbb{Z}$ is *dense* in $\mathbb{Z}_p$, and $\mathbb{Q}$ is *dense* in $\mathbb{Q}_p$.

**Examples**:

$$\begin{aligned}
\sqrt{2} &= 3 + 1\cdot 7 + 2\cdot 7^2 + 6\cdot 7^3 + 7^4 + 2\cdot 7^5 + 7^6 + 2\cdot 7^7 + 4\cdot 7^8 + 6\cdot 7^9 + \cdots \in \mathbb{Z}_7;\\
40 &= 1 + 3 + 9 + 27 \in \mathbb{Z}_3 \text{ (a finite sum)};\\
-1 &= 2(1 + 3 + 3^2 + 3^3 + \dots) \in \mathbb{Z}_3;\\
-\frac{7}{8} &= 1 + 2\cdot 3 + 3^2 + 2\cdot 3^3 + 3^4 + \cdots \in \mathbb{Z}_3;\\
\frac{1}{3} &= 2 + 3\cdot 5 + 5^2 + 3\cdot 5^3 + 5^4 + 3\cdot 5^5 + 5^6 + \cdots \in \mathbb{Z}_5;\\
\frac{1}{10} &= 3\cdot 5^{-1} + 2 + 2\cdot 5 + 2\cdot 5^2 + \cdots \in \mathbb{Q}_5;
\end{aligned}$$

5.5. **Squares in $\mathbb{Z}_p$.** The method we used in Section 5.1 to find the $7$-adic approximation to $\sqrt{2}$ is valid more generally. The case $p = 2$ is harder, so we start with odd primes.

**Proposition 5.5.1.** *Let $p$ be an odd prime and $\alpha = \{x_k\} \in U(\mathbb{Z}_p)$. Then there exists $\beta \in \mathbb{Z}_p$ with $\alpha = \beta^2$ if and only if $\left(\frac{x_1}{p}\right) = +1$ ($x_1$ is a quadratic residue modulo $p$). In particular, every rational integer which is a quadratic residue modulo $p$ is a $p$-adic square.*

An equivalent condition to $\left(\frac{x_1}{p}\right) = +1$ is $\left(\frac{a_0}{p}\right) = +1$ where $a_0$ is the first $p$-adic digit of $\alpha$, since $\alpha \equiv x_1 \equiv a_0 \pmod{p}$. For $\alpha \in \mathbb{Z}_p$ we define $\left(\frac{\alpha}{p}\right) = \left(\frac{a_0}{p}\right) = \left(\frac{x_1}{p}\right)$.

**Remark:** A square unit in $\mathbb{Z}_p$ must have exactly two square roots, since $\mathbb{Z}_p$ is an integral domain, so the polynomial $x^2-\alpha$ cannot have more than $2$ roots. In the proof of the proposition one can see that after making an initial choice of $y_1$ as one of two possible choices for the square root modulo $p$, at all subsequent steps there is a unique choice.

An alternative approach to finding $p$-adic square roots is to start with a value $y=y_1$ which is a "first-order approximation", meaning a solution to $y^2\equiv\alpha \pmod{p}$, and then iterate the map $y\mapsto y'=y+u(y^2-\alpha)$ where $u$ satisfies $1+2uy_1\equiv 0 \pmod{p}$. At each step we obtain a better approximation, and in the limit we obtain an exact solution. To see why this works, the computation

$$(y')^2-\alpha=(y+u(y^2-\alpha))^2-\alpha=(y^2-\alpha)(1+2uy)+u^2(y^2-\alpha)^2$$

shows that the valuation of $y^2-\alpha$ strictly increases at each step, so $\beta=\lim y$ satisfies $\beta^2-\alpha=\lim(y^2-\alpha)=0$.

**Examples: 1.** Taking $p=7$ and $\alpha=2$ we see that $2$ is a $7$-adic square since $\left(\frac{2}{7}\right)=1$. One square root is $\beta=3+1\cdot 7+2\cdot 7^2+6\cdot 7^3+\dots$ (see the calculation done in Section 5.1) and the other is $-\beta=4+5\cdot 7+4\cdot 7^2+0\cdot 7^3\dots$.

**2.** Take $p=3$ and $\alpha=-2$. Using the second approach, take $y=1$ which satisfies $y^2\equiv -2 \pmod{3}$ as a first approximation. Let $u=1$ so that $1+2uy\equiv 0 \pmod{3}$, and iterate $y\mapsto y+u(y^2-\alpha)=y^2+y+2$. The first few values of $y$ are (reducing the $k$'th one modulo $3^k$):

$$1,4,22,22,22,508,508,2695,\dots.$$

Expanding 2695 to base $3$ gives the expansion

$$\sqrt{-2} = 1 + 3 + 2 \cdot 3^2 + 2 \cdot 3^5 + 3^7 + \cdots \in \mathbb{Z}_3$$

where the next nonzero term is $a_{11}3^{11}$ since $2695^2 + 2 = 3^{11} \cdot 41$, so $|\sqrt{-2} - 2695|_3 = 3^{-11}$. (The last statement should be checked carefully.)

Now we have identified the $p$-adic units which are squares, it is a simple matter to determine all the squares in $\mathbb{Z}_p$.

**Proposition 5.5.2.** *Let $p$ be an odd prime. Let $\alpha = p^m\varepsilon$ be a nonzero $p$-adic integer with $m = \text{ord}(\alpha)$ and $\varepsilon \in U(\mathbb{Z}_p)$. Then $\alpha$ is a square in $\mathbb{Z}_p$ if and only if $m$ is even and $\left(\frac{\varepsilon}{p}\right) = 1$.*

The case of $2$-adic squares is a little different: for a $2$-adic unit to be a square, it is not sufficient to be a square modulo $2$ (which is true for all $2$-adic units since they are all congruent to $1 \pmod 2$); they must be congruent to $1$ modulo $8$. This is due to the fact that odd integer squares are all congruent to $1$ modulo $8$. The next result is that being congruent to $1 \pmod 8$ is sufficient for a $2$-adic unit to be a square in $\mathbb{Z}_2$.

**Proposition 5.5.3.** *A $2$-adic unit $\alpha$ is a square in $\mathbb{Z}_2$ if and only if $\alpha \equiv 1 \pmod 8$.*

The proof shows how to find a $2$-adic square root in practice: start with $y = 1$ and repeatedly replace $y$ by $y' = y + 2^{k-1}$ where $k = \text{ord}_2(y^2 - \alpha)$.

**Example:** We compute $\sqrt{17}$ in $\mathbb{Z}_2$, which exists since $17 \equiv 1 \pmod 8$.

Start with $y = 1$. Then $y^2 - 17 = -16 = -2^4$, so replace $y$ by $y + 2^3 = 9$.

Now $y^2 - 17 = 9^2 - 17 = 64 = 2^6$, so replace $y$ by $y + 2^5 = 41$.

Now $y^2-17=41^2-17=2^7\cdot 13$, so replace $y$ by $y+2^6=105$.

Now $y^2-17=105^2-17=2^8\cdot 43$, so replace $y$ by $y+2^7=233$; and so on.

Thus we obtain a sequence $1, 9, 41, 105, 233, \dots$ converging to $\sqrt{17}\in\mathbb{Z}_2$, and $\sqrt{17}=1+2^3+2^5+2^6+2^7+\dots$.

Similarly we may compute (approximations to) $\sqrt{-7}$ in $\mathbb{Z}_2$, to get

$$\sqrt{-7}=\lim\{1,5,21,53,181,\dots\}=1+2^2+2^4+2^5+2^7+2^{14}+\dots$$

with digit sequence $1,0,1,0,1,1,0,1,0,0,0,0,0,0,1,\dots$. The long block of zero digits comes from the fact that $181^2+7=32768=2^{15}$, so $181$ is a rather good approximation to $\sqrt{-7}$ in $\mathbb{Z}_2$. We have $\operatorname{ord}(\sqrt{-7}-181)=14$, so $|\sqrt{-7}-181|_2=2^{-14}$.

5.6. **Hensel lifting.** The process we used in the previous section to find $p$-adic square roots for odd $p$ involves going from a solution of a congruence modulo $p^k$ to a solution modulo $p^{k+1}$. This process is called "Hensel lifting" after Kurt Hensel (1861–1941), the inventor of $p$-adic numbers. It is the $p$-adic equivalent of refining an approximate real solution to an equation to a more precise solution, correct to more decimal places.

We will prove a quite general result which generalises the $p$-adic square root procedure for odd primes $p$, and also shows why $p=2$ was different. Formally, this Hensel lifting is very similar to the Newton-Raphson method for finding roots of equations over $\mathbb{R}$.

**Theorem 5.6.1.** *[Hensel Lifting Theorem] Let $f(X)\in\mathbb{Z}_p[X]$ be a polynomial, and let $x_1\in\mathbb{Z}_p$ satisfy $f(x_1)\equiv 0 \pmod{p}$ and $f'(x_1)\not\equiv 0 \pmod{p}$. Then there exists a unique $x\in\mathbb{Z}_p$ such that $f(x)=0$ and $x\equiv x_1 \pmod{p}$.*

**Example:** Let $p$ be odd and $a \in \mathbb{Z}$ a quadratic residue modulo $p$. Then $a$ is a $p$-adic square: just take $f(X) = X^2 - a$ in the theorem with $x_1$ a solution to $x^2 \equiv a \pmod{p}$. The derivative condition is that $f'(x_1) = 2x_1 \not\equiv 0 \pmod{p}$, which holds since $p \neq 2$.

**Example:** Let $p$ be prime and take $f(X) = X^p - X$. We know from Fermat's Little Theorem that $f$ has $p$ roots modulo $p$, one in each residue class. Hensel's Theorem says that $f$ has $p$ roots in $\mathbb{Z}_p$ also. One of these is $0$; the others are $(p-1)$'st roots of unity in $\mathbb{Z}_p$. One way of constructing these will be in the exercises.

**Remark:** In this proof we have $y \equiv -a/f'(x_1) \equiv -(f(x_n)/p^n)/f'(x_1) \pmod{p}$, so

$$x_{n+1} = x_n + p^n y \equiv x_n - f(x_n)/f'(x_n) \pmod{p^{n+1}}.$$

Thus, Hensel lifting consists of starting with a "seed" $x = x_1$ which must be a simple root of $f$ $\pmod{p}$, and iterating the map

$$x \mapsto x - f(x)/f'(x),$$

just as in the classical Newton method. Every iteration gives one more $p$-adic "digit", and the sequence always converges! To use the iteration formula to go from a root modulo $p^n$ to a root modulo $p^{n+1}$, you can compute the inverse $u$ of $f'(x_1) \pmod{p}$ once and for all at the start, and simply iterate $x \mapsto x - uf(x)$, as in the next example.

**Example:** We'll compute an approximation to $\sqrt[3]{2} \in \mathbb{Q}_5$. An initial approximation is $x_1 = 3$, and since $3^3 \equiv 2 \pmod{25}$ we can also take $x_2 = 3$. Here $f(X) = X^3 - 2$, so $f'(X) = 3X^2$

and $f'(x_1) = 27 \equiv 2 \pmod 5$ with inverse $u = -2$, so the recurrence is $x \mapsto x + 2(x^3 - 2)$:

$$x_3 \equiv 3 + 2(27-2) \equiv 53 \pmod{5^3}; \qquad \text{now } 53^3 \equiv 127 \pmod{5^4} \implies$$
$$x_4 \equiv 53 + 2(127-2) \equiv 303 \pmod{5^4}; \qquad \text{now } 303^3 \equiv 2502 \pmod{5^5} \implies$$
$$x_5 \equiv 303 + 2(2502-2) \equiv 5305 \equiv 2178 \pmod{5^5}; \qquad \text{and so on.}$$

We have an approximation to $\sqrt[3]{2}$, good to five $5$-adic "digits":

$$\sqrt[3]{2} = 3 + 2 \cdot 5^2 + 2 \cdot 5^3 + 3 \cdot 5^4 + \cdots \in \mathbb{Q}_5.$$

This statement is analogous to saying that

$$\sqrt[3]{2} = 1.259921 \cdots = 1 + 2 \cdot 10^{-1} + 5 \cdot 10^{-2} + 9 \cdot 10^{-3} + \cdots \in \mathbb{R}.$$