What is number theory? The study of numbers of course! But what is a number?

- $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ can be defined in several ways:
  - Finite ordinals ($0 := \{\}$, $n + 1 := n \cup \{n\}$).
  - Finite cardinals (isomorphism classes of finite sets).
  - Strings over a unary alphabet ("", "1", "11", "111", ...).

  $\mathbb{N}$ is a *commutative semiring*: addition and multiplication satisfy the usual commutative/associative/distributive properties with identities 0 and 1 (and 0 annihilates). Totally ordered (as ordinals/cardinals), making it a (positive) *ordered semiring*.
- $\mathbb{Z} = \{\pm n : n \in \mathbb{N}\}$. A *commutative ring* (commutative semiring, additive inverses). Contains $\mathbb{Z}_{>0} = \mathrm{N} - \{0\}$ closed under $+, \times$ with $\mathbb{Z} = -\mathbb{Z}_{>0} \sqcup \{0\} \sqcup \mathbb{Z}_{>0}$. This makes $\mathbb{Z}$ an *ordered ring* (in fact, an *ordered domain*).
- $\mathbb{Q} = \{a/b : a, \in \mathbb{Z}, b \neq 0\}/\sim$, where $a/b \sim c/d$ if $ad = bc$. A *field* (commutative ring, multiplicative inverses, $0 \neq 1$) containing $\mathbb{Z} = \{n/1\}$. Contains $\mathbb{Q}_{>0} = \{a/b : a, b \in \mathbb{Z}_{>0}\}$ closed under $+, \times$ with $\mathbb{Q} = -\mathbb{Q}_{>0} \sqcup \{0\} \sqcup \mathbb{Q}_{>0}$. This makes $\mathbb{Q}$ an *ordered field*.
- $\mathbb{R}$ is the *completion* of $\mathbb{Q}$, making it a *complete ordered field*.

Each of the algebraic structures $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ is canonical in the following sense: every non-trivial algebraic structure of the same type (ordered semiring, ordered ring, ordered field, complete ordered field) contains a copy of $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ inside it.

1.1 Constructing the real numbers

What do we mean by the *completion* of $\mathbb{Q}$? There are two possibilities:

1. Dedekind: every non-empty subset has a least upper bound (with respect to $\leq$).
2. Cauchy: every Cauchy sequence converges (with respect to $|\ |$).

We will use the second definition.

Definition 1.1. The (archimedean) absolute value of $\mathbb{Q}$ is the function $\mathbb{Q} \to \mathbb{Q}_{\geq 0}$

$$|x| := \begin{cases} x & \text{if } x \geq 0, \\ -x & \text{if } x < 0. \end{cases}$$

Definition 1.2. A *Cauchy sequence* (of rational numbers) is a sequence $(x_1, x_2, x_3, \ldots)$ such that for every $\epsilon \in \mathbb{Q}_{>0}$ there exists $N_\epsilon \in \mathbb{Z}_{>0}$ such that $|x_m - x_n| < \epsilon$ for all $m, n \geq N_\epsilon$.
Examples:

- $(x, x, x, \ldots)$ and $(a, b, c, \ldots, d, e, f, x, x, x, \ldots)$;
- $(1/2, 3/4, 7/8, \ldots)$ and $(1/2, 1/3, 1/4, \ldots)$, any sequence that converges in $\mathbb{Q}$;
- $(1/1, 1/2, 2/3, 3/5, 5/8, 8/13, \ldots)$;
- $(3, 3.1, 3.14, 3.141, 3.1415, \ldots)$;
- Any subsequence of a Cauchy sequence;

Non-example: $(H_1, H_2, H_3, \ldots)$, where $H_n = \sum_{k=1}^{n} \frac{1}{k}$, even though $|H_n - H_{n+1}| \to 0$.

Lemma 1.3. *Every Cauchy sequence (x_n) is bounded.*

Proof. Fix $\epsilon = 1$, say, and $N = N_\epsilon$, and let $B = \max\{x_n : n \le N\} + 1$. Then $|x_n| \le B$ for all $n \le N$, and for any $n > N_\epsilon$ we have

$$|x_n| = |x_n - x_N + x_N| \le |x_n - x_N| + |x_N| \le 1 + B - 1 = B,$$

where we have used the *triangle inequality* $|x + y| \le |x| + |y|$. □

Lemma 1.4. *If (x_n) and (y_n) are Cauchy sequences, so are $(x_n + y_n)$ and $(x_n y_n)$.*

Proof. For the sum, given $\epsilon > 0$ then all $m, n > N_{\epsilon/2}$ we have

$$|x_m + y_m - (x_n + y_n)| \le |x_m + y_m| + |x_n + y_n| \le \epsilon/2 + \epsilon/2 = \epsilon,$$

by the triangle inequality. For the product, choose B so $|x_n|, |y_n| \le B/2$ for all n. Given $\epsilon > 0$, for all $m, n > N_{\epsilon/B}$ we have

$$\begin{aligned} |x_m y_m - x_n y_n| &= |x_m y_m - x_m y_n + x_m y_n - x_n y_n| \\ &= |x_m(y_m - y_n) + (x_m - x_n) y_n| \\ &= |x_m| \cdot |y_m - y_n| + |x_m - x_n| \cdot |y_n| \\ &\le B/2 \cdot \epsilon/B + \epsilon/B \cdot B/2 = \epsilon. \end{aligned}$$

Note that we have used $|xy| = |x| \cdot |y|$. □

Thus we can add and multiply Cauchy sequences. The constant sequences $0 = (0, 0, \ldots)$ and $1 = (1, 1, \ldots)$ are additive and multiplicative identities, and every Cauchy sequence (x_n) has an additive inverse $(-x_n)$. So Cauchy sequences form a commutative ring.

But many Cauchy sequences do not have multiplicative inverses. Worse, the product of two nonzero Cauchy sequences may be zero: consider $(1, 0, 0, \ldots) \cdot (0, 1, 0, 0, \ldots)$.

Definition 1.5. A Cauchy sequence (x_n) is *equivalent to zero* if $\lim_{n\to\infty} |x_n| = 0$. Two Cauchy seuqences (x_n) and (y_n) are *equivalent* if their difference $(x_n - y_n)$ is equivalent to zero. We can add/multiply equivalence classes of Cauchy sequences by adding/multiplying representatives (because $(x_n) \sim 0$ implies $(x_n) + (y_n) \sim (y_n)$ and $(x_n)(y_n) \sim 0$).

Lemma 1.6. *Every nonzero equivalence class of Cauchy sequences has a multiplicative inverse.*

Proof. Let $[(x_n)] \neq 0$. Then $\lim_{n\to\infty} |x_n| > 0$, so for some $N \in \mathbb{Z}_{>0}$ we have $x_n \neq 0$ for all $n \ge N$. So let $y_n = 0$ for $n < N$ and $y_n = x_n^{-1}$ otherwise. Then $(x_n)(y_n) \sim 1$. □

Corollary 1.7. *The set of equivalence classes of Cauchy sequences forms a field.*

Proof. We also need $1 \neq 0$, i.e., $(1, 1, \ldots) \not\sim (0, 0, \ldots)$, but this holds: $\lim_{n\to\infty} |1 - 0| = 1$. □

Definition 1.8. $\mathbb{R}$ is the field of equivalence classes of Cauchy sequences. We embed $\mathbb{Q}$ in $\mathbb{R}$ via the map $x \mapsto [(x, x, x, \ldots)]$, which is injective because $\lim_{n\to\infty} |x - y| = |x - y| \neq 0$ unless $x = y$ (here we use $|x| = 0 \Leftrightarrow x = 0$). We extend the absolute value of $\mathbb{Q}$ to $\mathbb{R}$ via

$$|[(x_n)]| := [(|x_n|)].$$

We then have $\mathbb{R}_{>0} = \{x \in \mathbb{R} - \{0\} : |x| = x\}$ containing $\mathbb{Q}_{>0}$ and $\mathbb{R} = -\mathbb{R}_{>0} \sqcup \{0\} \sqcup \mathbb{R}_{>0}$. Thus $\mathbb{R}$ is an ordered field whose order extends that of $\mathbb{Q}$.

Lemma 1.9. *$\mathbb{Q}$ is dense in $\mathbb{R}$: for all $x \in \mathbb{R}$ and $\epsilon \in \mathbb{Q}_{>0}$ there exists $r \in \mathbb{Q}$ with $|x-r| < \epsilon$.*

Proof. Given $x = [(x_n)]$ and $\epsilon \in \mathbb{Q}_{>0}$, let $r = x_{N_\epsilon}$. Then $|x - r| < \epsilon$ (formally, this means the equivalence class of the Cauchy sequence $(\epsilon - |x_n - r|)_n$ lies in $\mathbb{R}_{>0}$, which is true). □

Remark 1.10. This implies we could replace $\epsilon \in \mathbb{Q}_{>0}$ with $\epsilon \in \mathbb{R}_{>0}$ throughout. We only used $\epsilon \in \mathbb{Q}_{>0}$ at the start because we had not defined the real numbers yet.

Definition 1.11. A sequence (x_n) *converges* to the *limit* z if for every $\epsilon \in \mathbb{Q}_{>0}$ there is an $N_\epsilon \in \mathbb{Z}_{>0}$ for which $|x_n - z| < \epsilon$ for all $n \geq N_\epsilon$. The limit of a convergent sequence is unique (if z_1 and z_2 were two distinct limits taking $\epsilon = |z_1 - z_2|/2$ would yield a contradiction).

Lemma 1.12. *A Cauchy sequence of rational numbers converges (x_n) converges to $[(x_n)]$.*

Proof. Let $z = [(x_n)]$. Given $\epsilon > 0$, pick N_ϵ so that $|x_m - x_n| < \epsilon$ for all $m, n \geq N_\epsilon$. Then $|x_n - z| < \epsilon$ for all $n \geq N_\epsilon$. □

Since $\mathbb{R}$ is a field with an absolute value, we can define a Cauchy sequence (x_n) of real numbers just as we did for rational numbers (now each x_n is itself an equivalence class of Cauchy sequences of rational numbers).

Corollary 1.13. *Every Cauchy sequence of real numbers converges to a real number. Equivalently, $\mathbb{R}$ is **complete**.*

Proof. Given a Cauchy sequence of real numbers (x_n), let (r_n) be a sequence of rational numbers with $|x_n - r_n| < 1/n$ for all n (such a sequence exists because $\mathbb{Q}$ is dense in $\mathbb{R}$). Then (r_n) is Cauchy and $\lim_{n\to\infty} |x_n - r_n| = 0$. It follows that (x_n) converges to a real number if and only if (r_n) does, and (r_n) converges to the real number $[(r_n)]$, by Lemma 1.12. □

1.2 Absolute values

The construction of the real numbers as equivalence classes of Cauchy sequences ultimately rests on properties of the absolute value function $|\ |\colon \mathbb{Q} \to \mathbb{Q}_{\geq 0}$; this is what determines which sequences of rational numbers are Cauchy sequences and which Cauchy sequences are equivalent. In our construction of $\mathbb{R}$ we relied on just three properties of absolute values, which we now formalize.

Definition 1.14. An *absolute value* on a field k is a function $\|\ \|\colon k \to \mathbb{R}_{\geq 0}$ such that

(1) $\|x\| = 0$ if and only if $x = 0$;
(2) $\|xy\| = \|x\| \cdot \|y\|$ for all $x, y \in k$;
(3) $\|x + y\| \leq \|x\| + \|y\|$ for all $x, y \in k$.

Example 1.15. The following are examples of absolute values on $\mathbb{Q}$:

- The *trivial* absolute value: $\|x\| = 1$ for all nonzero $x \in \mathbb{Q}$;
- The *archimedean* absolute value $|\ |$;
- The *p-adic* absolute value $|\ |_p$ for a prime p:

$$|x|_p := p^{-v_p(x)},$$

where $v_p(x)$ is the *p-adic valuation* of x.

By the fundamental theorem of arithmetic, every nonzero rational number x can be written uniquely as a product of prime powers

$$x = \pm \prod_p p^{e_p},$$

where p ranges over all primes and all but finitely many $e_p \in \mathbb{Z}$ are zero.

Definition 1.16. The exponent e_p in the unique prime factorization of a nonzero rational number x is the *p-adic valuation* of x, denoted $v_p(x)$. By convention we also put $v_p(0) := \infty$ and define $p^{-\infty} := 0$ so that $|0|_p = p^{-v_p(0)} = p^{-\infty} = 0$.

To check that $|\ |_p$ satisfies the triangle inequality, note that for integers a and b we have

$$v_p(a+b) \geq \min(v_p(a), v_p(b)) \quad \Longrightarrow \quad |a+b|_p \leq \max(|a|_p, |b|_p) \leq |a|_p + |b|_p.$$

The same holds for $x, y \in \mathbb{Q}$, since we can assume $x = a/c$ and $y = b/c$ with $a, b, c \in \mathbb{Z}$, and

$$|x+y|_p = |a+b|_p/|c|_p = \max(|a|_p, |b|_p)/|c|_p = \max(|x|_p, |y|_p) \leq |x|_p + |y|_p.$$

Remark 1.17. Note that the sign in $|x|_p = p^{-v_p(x)}$ is crucial. For example

$$|1+2|_3 = 3^{-1} \leq 2 = |1|_3 + |2|_3,$$

but this would not hold if we used $|x|_p = p^{v_p(x)}$.

Definition 1.18. An absolute value $\|\ \|$ that satisfies the stronger triangle inequality

$$\|x+y\| \leq \max(\|x\|, \|y\|)$$

is called *nonarchimedean* (otherwise it is *archimedean*). The trivial absolute value is nonarchimedean, as are all p-adic absolute values on $\mathbb{Q}$. In fact, the absolute value $|\ |$ is essentially the only archimedean absolute value on $\mathbb{Q}$ (as we shall see).

The p-adic absolute values on $\mathbb{Q}$ are very different from the archimedean absolute value. For example, $|x|_p = 1$ for infinitely many rational numbers x (all those whose numerator and denominator are prime to p), whereas $|x| = 1$ only for the two values ± 1. The most important thing to keep in mind is that numbers with *small* p-adic absolute values are divisible by *large* powers of p. The p-adic absolute value of an integer is never greater than 1; indeed, for primes p and q,

$$\lim_{n\to\infty} |q^n|_p = \begin{cases} 0 & \text{if } q = p \\ 1 & \text{if } q \neq p \end{cases}$$

whereas this limit always tends to infinity if we use the archimedean absolute value.

Remark 1.19. For those familiar with topology, defining $d(x,y) := \|x-y\|$ gives us a metric on $\mathbb{Q}$ that defines a topology. This topology is clearly different for each p-adic absolute value, and for the archimedean absolute value. On the other hand, given any absolute value $\|\ \|$ and any real number $\alpha \in (0,1)$, one can check that $\|\ \|^\alpha$ is also an absolute value. But this "new" absolute value gives exactly the same topology.

1.3 Completions

We now generalize our construction of the real numbers to the completion of any field with respect to any absolute value.

Definition 1.20. Let k be a field with absolute value $\|\ \|$. The *completion* of k with respect to $\|\ \|$ is the field $\hat{k}$ of equivalence classes of Cauchy sequences of elements of k (where the Cauchy criterion uses $\|\ \|$). We view k as a subfield of $\hat{k}$ via the injective map $x \mapsto [(x, x, x, \ldots)]$ and extend the absolute value on k to $\hat{k}$ by defining

$$\|[(x_n)]\| = [(\|x_n\|)] = \lim_{n\to\infty} \|x_n\| \in \mathbb{R}_{\geq 0}$$

for any Cauchy sequence (x_n). The sequence of real numbers $\|x_n\|$ converges because $(\|x_n\|)$ is a Cauchy sequence of real numbers (since (x_n) is a Cauchy sequence). One can check that the extended absolute value $\|\ \|$ is nonarchimedean if and only if $\|\ \|$ is nonarchimedean.

Lemma 1.21. *Let k be a field with absolute value $\|\ \|$ and completion $\hat{k}$. For any $x \in \hat{k}$ and $\epsilon \in \mathbb{R}_{>0}$ there exists $y \in k$ such that $\|x - y\| < \epsilon$. Equivalently, k is **dense** in its completion.*

Proof. Identical to the proof that $\mathbb{Q}$ is dense in $\mathbb{R}$. □

Definition 1.22. Let k be a field with absolute value $\|\ \|$. A sequence (x_n) of elements of k *converges* to the limit $z \in k$ if for every $\epsilon \in \mathbb{R}_{>0}$ there exists an $N_\epsilon \in \mathbb{Z}_{>0}$ for which $\|x_n - z\| < \epsilon$ for all $n \geq N_\epsilon$.

Definition 1.23. A field with an absolute value is *complete* if every Cauchy sequence converges.

Lemma 1.24. *Let $\hat{k}$ be the completion of a field k with absolute value $\|\ \|$. Any Cauchy sequence (x_n) of $\hat{k}$ whose elements lie in $k \subseteq \hat{k}$ converges to the element $[(x_n)]$ of $\hat{k}$.*

Proof. Identical to the proof of Lemma 1.12. □

Proposition 1.25. *The completion $\hat{k}$ of a field k with absolute value $\|\ \|$ is complete.*

Proof. Identical to the proof that $\mathbb{R}$ is complete. □

1.4 p-adic fields

Definition 1.26. Let p be a prime. The completion of $\mathbb{Q}$ with respect to the p-adic absolute value $|\ |_p$ is the field of *p-adic* numbers, denoted $\mathbb{Q}_p$. The *p-adic integers*

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\},$$

form a subring of $\mathbb{Q}_p$ containing $\mathbb{Z}$ (it is closed under $+$ because $|\ |_p$ is nonarchimedean).

In addition to be being nonarchimedean, p-adic absolute values are *discrete*. This means that if $r = |x|_p$ is a nonzero p-adic absolute value then for some sufficiently small $\epsilon > 0$ the real interval $(r - \epsilon, r + \epsilon)$ contains no p-adic absolute values other than r. This is clear for the p-adic absolute value on $\mathbb{Q}$, since these are all integer powers of p, and this property carries over to $\mathbb{Q}_p$ because $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. This allows us to extend the p-adic valuation

$$v_p(x) := -\log_p |x|_p$$

for any nonzero $x \in \mathbb{Q}_p$. We can then write any nonzero $x \in \mathbb{Q}_p$ as

$$x = p^{v_p(x)}u,$$

where u is a *p-adic unit*, an element with p-adic absolute value 1. If $[(x_n)]$ is a nonzero element of $\mathbb{Q}_p$, then the p-adic valuations $v_p(x_n)$ are eventually constant. Thus to represent element of $\mathbb{Q}_p$ we just need to know how to represent p-adic units. For this we need just one basic number-theoretic fact.

Lemma 1.27. *Let p be a prime and let b be an integer that is not divisible by p. For any $n \in \mathbb{Z}_{>0}$ there exists an integer $c \in [0, p^n - 1]$ such that $bc \equiv 1 \bmod p^n$.*

Proof. The set $\{c : c \in [0, p^n - 1]\}$ is a complete set of distinct residue class representatives modulo p^n. We claim that the set $\{bc : c \in [0, p^n - 1]\}$ is also, which implies the lemma. If not, then $bc_1 - bc_2 = b(c_1 - c_2)$ is divisible by p^n for some distinct $c_1, c_2 \in [0, p^n - 1]$. But p does not divide p^n so it must divide $c_1 - c_2$, but then $c_1 \equiv c_2 \bmod p^n$, a contradiction. □

Remark 1.28. The value of c in the preceding lemma can be efficiently computed with the Euclidean algorithm (which also gives an alternative proof).

Proposition 1.29. *Every p-adic unit u can be represented by a Cauchy sequence of integers.*

Proof. We can assume without loss of generality that u is represented by a Cauchy sequence (a_n/b_n) of rational numbers with $a_n, b_n \in \mathbb{Z}$ and $v_p(a_n/b_n) = 0$; this must be true eventually and removing a finite prefix does not change the equivalence class of a Cauchy sequence. We now choose c_n so that $b_n c_n \equiv 1 \bmod p^n$ (by the lemma) and let $u_n = a_n c_n \in \mathbb{Z}$. Then

$$v_p(u_n - a_n/b_n) = v_p((a_n b_n c_n - a_n)/b_n) = v_p(b_n c_n - 1) + v_p(a_n/b_n) = v_p(b_n c_n - 1) \geq n.$$

It follows that $\lim_{n\to\infty} |u_n - a_n/b_n|_p = 0$ and therefore (u_n) is equivalent to (a_n/b_n). □

Corollary 1.30. *Every p-adic unit can be uniquely represented by an integer sequence*

$$(d_0,\ d_0 + d_1 p,\ d_0 + d_1 p + d_2 p^2,\ d_0 + d_1 p + d_2 p^2 + d_3 p^3,\ \ldots)$$

with $d_n \in [0, p-1]$ and $d_0 \neq 0$. Conversely, every such sequence defines a p-adic unit.

Proof. Let $u = [(x_n)]$ be a p-adic unit with $x_n \in \mathbb{Z}$. We may assume $x_{n+1} \equiv x_n \bmod p^n$, since any Cauchy sequence of integers necessarily contains an equivalent subsequence with this property. Now define $d_n = (x_{n+1} - x_n)/p^n \in \mathbb{Z}$ and $u_1 = d_0$ and $u_{n+1} = u_n + d_n p^n$ and note that $u_n \equiv x_n \bmod p^n$ and therefore $(u_n) \sim (x_n)$, so $u = [(u_n)]$.

The integers d_n are unique because if $u = [(u'_n)]$ with u'_n defined by p-adic digits d'_n that differ from d_n, say $d'_m \neq d_m$, then $v_p(u_n - u'_n) \leq m$ for all $n \geq m$ and $[(u_n)] \neq [(u'_n)]$.

Given a sequence $d_0, d_1, d_2, \ldots$ with $d_n \in [0, p-1]$ and $d_0 \neq 0$, the sequence

$$(d_0,\ d_0 + d_1 p,\ d_0 + d_1 p + d_2 p^2,\ d_0 + d_1 p + d_2 p^2 + d_3 p^3,\ \ldots)$$

is clearly Cauchy (the difference of any two terms after the Nth term is divisible by p^N), and every term has p-adic absolute value 1, hence the sequence defines a p-adic unit. □

This corollary gives us a concrete way to represent p-adic numbers without having to think about equivalence classes of Cauchy sequences. We can compactly represent p-adic units in the form

$$0.d_0d_1d_2d_3\cdots,$$

where the p-adic "decimal point" marks the separation between places corresponding to negative powers of p, which appear to the left of the decimal because they are more significant, and places corresponding to positive powers of p which are less significant. For general p-adic numbers in the form p^nu, we simply shift the representation of u to the right by n digits (or to the left by $-n$ digits if $n<0$). This notation is not really standard but it helps to emphasize the key feature of p-adic numbers: *large* powers of p correspond to *small* numbers. For example, in $\mathbb{Q}_5$ we have

$$1=0.1_5,\quad 17=0.23_5,\quad 100=0.004_5,\quad -1=0.44\overline{4}_5,\quad 1/2=0.32\overline{2}_5,\quad 7/25=21.0_5.$$

Notice that in $\mathbb{Q}_5$ the rational number $7/25=21.0_5$ is much bigger than $100=0.004_5$,

$$|7/25|_5=5^2>5^{-2}=|100|_5,$$

and this is reflected by our choice of notation. Unlike the decimal representations of a real number, the p-adic representation of a p-adic number has the feature of being unique.

Corollary 1.31. *The field $\mathbb{Q}_p$ is uncountable.*

Proof. By diagonalization, there are uncountably many sequences of p-adic digits. □

We can perform the usual arithmetic operations using p-adic representations just as we do with decimal representations, the only difference is that we work left-to-right rather than right-to-left (borrowing/carrying from the digit to the right) because the digits the less significant digits to the right actually correspond to larger powers of p, the opposite of what happens in decimal arithmetic. Here are some examples in $\mathbb{Q}_5$:

$$\begin{aligned} 15&=0.03_5\\ \underline{+23}&=\underline{0.34_5}\\ 38&=0.321_5 \end{aligned}$$

$$\begin{aligned} 1/5&=1.000_5\\ \underline{-1/2}&=\underline{0.32\overline{2}_5}\\ -3/10&=1.22\overline{2}_5 \end{aligned}$$

$$\begin{aligned} 2/3&=0.4\overline{13}_5\\ \underline{\times 3/2}&=\underline{0.42\overline{2}_5}\\ &\quad 0.123\overline{13}_5\\ &\quad 0.033\overline{13}_5\\ &\quad 0.003\overline{31}_5\\ &\quad\cdots\\ 1&=0.1\overline{0}_5 \end{aligned}$$

Let's try a harder example and see if we can compute

$$\sqrt{-1} = \sqrt{0.44\overline{4}_5} = \pm 0.d_0d_1d_2d_3\cdots .$$

Clearly we must have $d_0 = \pm 2$. Let's pick $d_0 = 2$. We then have

$$(2 + d_1 5 + \cdots)^2 = 4 + 4d_1 5 + \cdots ,$$

so we are forced to put $d_1 = 1$. To compute d_2 we calculate

$$(2 + 1\cdot 5 + d_2 5^2 + \cdots)^2 = 4 + 4\cdot 5 + (4d_2 + 1)5^2 + \cdots$$

which forces $d_2 = 2$. Continuing in this fashion, we obtain

$$0.2121342303220413240434041241411314142011332240424031240330300031 3\cdots_5 .$$

Assuming we can continue this indefinitely, the limit of the Cauchy sequence

$$(d_0, d_0 + d_1 p, d_0 + d_1 p + d_2 p^2, \ldots)$$

is a square-root of -1 in $\mathbb{Q}_5$ (its negation is the other square-root). Note that $\mathbb{Q}_5$ is complete, so this limit exists (indeed, it is represented by the sequence itself!).

Remark 1.32. The fact that we have a square-root of -1 in $\mathbb{Q}_5$ makes it crystal clear that $\mathbb{Q}_5$ is not simply $\mathbb{R}$ in disguise; even if we ignore the absolute value (hence the topology), it's algebraic properties are different. This is remarkable, and is what makes p-adic numbers so useful: by changing the topology, we have gained algebraic insight (if you remember nothing else from this lecture, remember this!).

How do we know for sure that we can actually continue this process indefinitely? To generalize the situation slightly, let us suppose we are trying to compute the rth root of an integer z with p-adic representation $0.z_0z_1z_2\ldots$, and that we have already computed the p-adic representation $0.d_0d_1\ldots d_n$ of an integer whose rth power has a p-adic representation that begins $0.z_0z_1\ldots z_n$. We now want to choose d_{n+1} so that

$$\left(d_0 + d_1 p + \cdots + d_n p^n + d_{n+1}p^{n+1}\right)^r \equiv z_0 + z_1 p + \cdots + z_n p^n + z_{n+1}p^{n+1} \pmod{p^{n+2}}$$

This looks complicated, but the only unknown is d_{n+1} and the only term in which it appears that is not obviously zero modulo p^{n+2} is $rd_0^{r-1}d_{n+1}$. Thus we just we need to solve

$$rd_0^{r-1}d_{n+1} \equiv b \bmod p,$$

where the value of b depends only on things we already know. So long as rd_0 is not divisible by p we can always solve for d_{n+1}: multiply both sides by an integer c for which $crd_0^{-1} \equiv 1 \bmod p$. In our calculation of $\sqrt{-1}$ in $\mathbb{Q}_5$, we had $2d_0 = 4$ not divisible by 5, which works. In general we are fine whenever p does not divide r and $d_0 \neq 0$.

Theorem 1.33. *Let p be a prime, and let z and r be integers not divisible by p with $r > 1$. Then z has an rth root in $\mathbb{Q}_p$ if and only if z is an rth power modulo p.*

Proof. We first note that $z_0 \equiv z \bmod p$ is nonzero. The "if" direction follows from the argument above: if z is an rth power we can choose $d_0 \in [0, p-1]$ so that $(d_0)^r \equiv z \bmod p$, and we must have $d_0 \neq 0$ since $z_0 \neq 0$. And since p does not divide r we can then proceed to compute $d_1, d_2, \ldots$ as above.

For the "only if" direction, suppose $z = d^r$ for some $d \in \mathbb{Q}_p$. Then $v_p(d^r) = v_p(z) = 0$ so d is a p-adic unit that we can write as $d = 0.d_0d_1d_2\ldots$, and we must have $z \equiv (d_0)^r \bmod p$. □

Remark 1.34. This theorem is a special case of *Hensel's lemma*, which allows one to "lift" a solution d_0 to a polynomial congruence $f(x) \equiv 0 \bmod p$ to a solution of $f(x) = 0$ in $\mathbb{Q}_p$ whenever $f'(d_0)$ is not divisible by p.

Theorem 1.35. *The fields $\mathbb{Q}_p$ are all non-isomorphic and none is isomorphic to $\mathbb{R}$.*

Proof. The field $\mathbb{Q}_p$ does not contain $\sqrt{p}$ (it would have a non-integral p-adic valuation, which is impossible), but $\mathbb{R}$ does. So no p-adic field is isomorphic to $\mathbb{R}$.

Now let $p < q$ be primes. Then q is not zero modulo p and we can choose $c \in [1, p-1]$ so that $cq \equiv 1 \equiv 1^r \bmod p$ is an rth power modulo p for any integer r. We have $v_q(cq) = 1$, so cq does not have an rth root in $\mathbb{Q}_q$ for any $r > 1$. But by Theorem 1.33, cq does have an rth root in $\mathbb{Q}_p$ for every $r > 1$ not divisible by p. So $\mathbb{Q}_p \not\cong \mathbb{Q}_q$. □

Theorem 1.36 (Ostrowski)**.** *The non-trivial completions of $\mathbb{Q}$ are $\mathbb{R}$ and the p-adic fields $\mathbb{Q}_p$.*

Proof. Consider the completion of $\mathbb{Q}$ with respect to an arbitrary absolute value $\| \ \|$. We first note that $\| \pm 1\| = 1$ always holds (by multiplicativity), and for any positive integer a

$$\|a\| = \|1 + \cdots + 1\| \le \|1\| + \cdots + \|1\| = a,$$

by the triangle inequality. Now let p and q be primes. For any positive integer n we can write p^n in base q with digits $d_i \in [0, q-1]$ satisfying $\|d_i\| \le d_i < q$ to obtain

$$\|p\|^n = \|p^n\| = \left\| \sum_{i=0}^{m} d_i q^i \right\| \le \sum_{i=0}^{m} \|d_i q^i\| \le \sum_{i=0}^{m} q \|q\|^i \le (m+1) q \max(\|q\|, \|q\|^m),$$

where $m = \lceil \log_q p^n \rceil \le n \log_q p + 1$ and we have used $\|q\|^i \le \max(\|q\|, \|q\|^m)$. If $\|p\| > 1$ then for sufficiently large n this inequality cannot hold unless $\|q\| > 1$: the LHS increases exponentially with n while the RHS is bounded by a constant factor of m, and hence of n, unless $\|q\| > 1$ (in which case $\max(\|q\|, \|q\|^m) = \|q\|^m$ increases exponentially with n).

It follows that if $\|p\| > 1$ for any prime p then $\|q\| > 1$ for every prime q. Let us suppose that this is the case. For any positive integer n we have

$$\|p\| = \sqrt[n]{\|p\|^n} \le \sqrt[n]{(m+1) q \|q\|^m} = \|q\|^{m/n} \sqrt[n]{(m+1)q}.$$

As $n \to \infty$ we have $m/n \le \log_q p + \epsilon$ for all $\epsilon > 0$ (hence we can drop the ϵ) and $\sqrt[n]{(m+1)q} \to 1$. Taking logarithms of both sides, applying $\log_q p = \log p / \log q$ and dividing by $\log p$ yeilds

$$\frac{\log \|p\|}{\log p} \le \frac{\log \|q\|}{\log q}.$$

The same inequality holds if we swap p and q, hence it is an equality. Now let $\alpha = \log \|p\| / \log p > 0$ so that $\|p\| = p^\alpha$. Then $\|q\| = q^\alpha$ for every prime q and it follows that

$$\|x\| = |x|^\alpha$$

for all nonzero $x \in \mathbb{Q}$. We now observe that a sequence of rational numbers is Cauchy with respect to the absolute value $\| \ \| = | \ |^\alpha$ if and only if it is also Cauchy with respect to $| \ |$ (just replace $\epsilon > 0$ with $\epsilon^\alpha > 0$), and the equivalence relation on Cauchy sequences given by the two absolute values are the same. It follows that the completion of $\mathbb{Q}$ with respect to $\| \ \|$ is equal to $\mathbb{R}$ whenever $\|p\| > 1$ for any (hence all) primes p.[1]

[1]The triangle equality forces $\alpha \le 1$ in this case, since $2^\alpha = \|2\| = \|1+1\| \le \|1\| + \|1\| = 2$, but we don't actually need to prove this, we already know that $\| \ \|$ is an absolute value.

We now suppose $\|p\| \le 1$ for all primes (and hence all integers). If $\|p\| = 1$ for every p then $\|\ \|$ is the trivial absolute value (in which case every Cauchy sequence is eventually constant and we get the trivial completion $\mathbb{Q}$). So let us now suppose otherwise and pick a prime p with $\|p\| < 1$. We claim that every prime $q \neq p$ must have absolute value equal to 1. If not, choose n so that $\|p\|^n, \|q\|^n < \frac{1}{2}$ and then choose an integer c so that $cp^n \equiv 1 \bmod q^n$. Then $cp^n + dq^n = 1$ for some integer d. We then have $\|c\|, \|d\| \le 1$ (since $c, d \in \mathbb{Z}$) and

$$1 = \|1\| = \|cp^n + dq^n\| \le \|cp^n\| + \|dq^n\| = \|c\| \cdot \|p\|^n + \|d\| \cdot \|q\|^n < \frac{1}{2} + \frac{1}{2} = 1,$$

which is a contradiction. So $\|q\| = 1$ for all primes $q \neq 1$ and we can write

$$\|x\| = \|p\|^{v_p(x)}$$

for any nonzero $x \in \mathbb{Q}$. Writing $\|p\|$ in the form $p^{-\alpha}$ for some $\alpha > 0$, we then have $\|x\| = |x|_p^\alpha$ for all $x \in \mathbb{Q}$, and as argued above, we get exactly the same set of equivalence classes of Cauchy sequences using $\|\ \| = |\ |_p^\alpha$ as we do with $|\ |_p$. Thus if $\|p\| < 1$ for any (hence exactly one) prime p, then the completion of $\mathbb{Q}$ with respect to $\|\ \|$ is $\mathbb{Q}_p$. □

Remark 1.37. Note that it is not true that every non-trivial absolute value on $\mathbb{Q}$ is either $|\ |$ or $|\ |_p$, it could be a power of one of these, but as we have defined things every non-trivial completion is exactly equal (not just isomorphic) to either $\mathbb{R}$ or some $\mathbb{Q}_p$.

Let us conclude with one final observation. While the fields $\mathbb{R}$ and the $\mathbb{Q}_p$ are "complete" in the topological sense we have defined here, they are still incomplete in an algebraic sense: they lack solutions to some polynomial equations (e.g., x^2+1 and x^2-p). We can go a step further and take the *algebraic closure* of any of these fields. We won't say exactly how this is done in general, but in the case of $\mathbb{R}$ it is enough to add the element $i = \sqrt{-1}$; together with $\mathbb{R}$ this generates the field of complex numbers $\mathbb{C}$. In addition to being algebraically closed , the field $\mathbb{C}$ is also complete (with respect to the archimedean absolute value).

But a funny thing happens when you take the algebraic closure of $\mathbb{Q}_p$. The resulting field $\overline{\mathbb{Q}}_p$ is no longer complete! So we then need to take the completion of $\overline{\mathbb{Q}}_p$ (with respect to the p-adic absolute value extended to $\overline{\mathbb{Q}}_p$). This yields a field denoted $\mathbb{C}_p$ which, thankfully, is still algebraically closed. Like $\mathbb{C}$, the field $\mathbb{C}_p$ is the smallest extension of $\mathbb{Q}$ that is both algebraically closed and complete with respect to (the extension of) an absolute value on $\mathbb{Q}$.

For those interested in learning more about p-adic numbers, you can check out the references below (these can all be accessed online from MIT via the provided links). You can also find material on p-adic numbers in the course notes for 18.782 Introduction to Arithmetic Geometry which are available on OCW.

References

[1] Fernando Q. Gouvêa, *p-adic Numbers: An Introduction*, second edition, Springer, 1997.

[2] Neal Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, second edition, Springer, 1984.

[3] Alain Robert, *A course in p-adic analysis*, Springer, 2000.