The p-adic numbers

There are quite a few reasons to be interested in the p-adic numbers $\mathbb{Q}_p$. They are useful for solving diophantine equations, using tools like Hensel's lemma and the Hasse principle, which we won't say anything about. They are basic examples for things like valuations and profinite groups.

For us they are interesting because they form a topological group, a useful and common one that isn't just a variation of Euclidean space. There is also a p-adic topology on the rationals which we will see is nothing like the Euclidean topology, and we get to go through the process of completion.

The p-adic topology on $\mathbb{Q}$

Given a prime p, we define a valuation on the rationals by

$$\operatorname{val}_p \frac{a}{b} p^n = n,$$

where a and b are not divisible by p, and n is some integer. This is a valuation, and makes the rationals (and the integers) a discrete valuation ring. We then define the *p-adic norm* on $\mathbb{Q}$ by

$$|x|_p = p^{-\operatorname{val}_p x},$$

for any non-zero x, and setting $|0| = 0$.

This is a norm: Clearly $|x| = 0$ if and only if $x = 0$, and multiplicativity is also clear. The triangle inequality requires a bit of work. Let $x = \frac{a}{b}$ and $y = \frac{c}{d}$ be any two rational numbers, in lowest terms. If either is zero, or their sum is, then we are done. So assume not, then

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

and turning this upside down we get

$$|x+y| = p^{-\operatorname{val}(x+y)} \leq p^{-\max(\operatorname{val} x, \operatorname{val} y)} = \max(|x|, |y|),$$

which is stronger than the triangle inequality, so we have a norm. This inequality is called the ultrametric inequality, and norms that satisfy it are called non-Archimedean.

The ultrametric inequality is actually an equality if $|x| \neq |y|$. If we assume $|y| > |x|$, then

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

and

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

since $|x|$ is smaller than $|y|$. So $|x+y| = |y|$. This shouldn't come as a surprise: If x and y are divisible by different powers of p, their sum is divisible by the lowest of the two powers of p, and no higher powers of p. If x and y are divisible by the same power of p, then their sum might be divisible by a larger power:

$$2^2 + 2^2 = 2^3.$$

Non-Archimedean norms do not always behave quite like Archimedean norms. For instance, every point in an open ball is a centre of the ball. Let

$$D(a, r) = \{|x - a| < r\}$$

and choose some point b in $D(a, r)$. Then $D(b, r) = D(a, r)$, for if $x \in D(b, r)$ then

$$|x - a| = |x - b + b - a| \leq \max(|x - b|, |b - a|) \leq r,$$

so $x \in D(a, r)$, and the other inclusion is shown by switching a and b.

Now that we have a norm on the rationals, we get a topology in the usual way: We take all the open balls as a basis. The topology we get is called the *p-adic topology* on the rationals. This is not the same as the Euclidean topology. Small in the p-adic topology means divisible by a large power of p, which is quite likely to take us very far, in Euclidean terms, from 0. We can also look at the induced topology on the integers. The Euclidean topology on $\mathbb{Z}$ is just the discrete topology (balls of radius smaller than 1 are singletons), but one-point sets are not open in the p-adic topology on $\mathbb{Z}$: The open balls with centre 0 (and so the only balls containing 0) are $p^n\mathbb{Z}$ for some natural n, but any finite intersection is going to be just the smallest one.

Addition and taking negatives are continuous functions $K^2 \to K$ and $K \to K$ for any field K with topology arising from a norm, so $\mathbb{Q}$ is a topological group, with the p-adic norm.

The p-adic topologies for different primes are also all different. Clearly, $|p^n|_p$ is small for large n, but $|p^n|_q = 1$, if q is a prime not equal to p. We also have the following useful theorem.

Theorem. *Let $|\cdot|_1$ and $|\cdot|_2$ be two norms on some field k. Then the following are equivalent:*

1. *The two norms induce the same topology on k,*
2. *the unit discs are equal, $\{|x|_1 < 1\} = \{|x|_2 < 1\}$,*
3. *there exists a positive real α such that $|x|_1^\alpha = |x|_2$ for all x in k.*

If these conditions are satisfied, we say the norms are equivalent. For a proof, see [Vaaler]. Note that a norm being equivalent to a p-adic norm just means replacing $\frac{1}{p}$ by $\frac{1}{p}^\alpha$, that is we could have defined the same topology using any number in $(0, 1)$ as the base.

So we know several different norms on the rationals, and it can be shown that there are no more.

Theorem. *(Ostrowski) Every norm on $\mathbb{Q}$ is equivalent to the Euclidean norm, a p-adic norm, or the trivial norm ($|0| = 0$, $|x| = 1$ for all other x).*

For a proof, see [Koblitz, 1984].

The p-adics: Completion

One property the p-adic topology shares with the Euclidean is that neither is complete. (Recall that a topological space is complete if every Cauchy sequence converges, and $\{x_n\}$ is Cauchy if for any $\varepsilon > 0$ there exists N such that $n, m \geq N$ implies $|x_m - x_n| < \varepsilon$.) To fix this in the Euclidean case, analysis constructs the real numbers by inserting every missing limit. We will do the same, using the exact same method, for the p-adic topology.

Begin by forming the ring of Cauchy sequences, call it C, with termwise addition and multiplication. The set of sequences converging to 0, let's call it M, is an ideal. The sum of two sequences converging to 0 will clearly converge to 0, and the product of a sequence converging to 0 with some other Cauchy sequence will also, since Cauchy sequences are bounded. It is also easy to see that M is maximal. For, take some ideal I between M and C, then I contains a sequence a not converging to 0, which must have a last zero term a_n. Add a sequence which is non-zero where a is zero and zero elsewhere, this will have all zeros after n, so is in M, so in I. So we can assume a has no

zero terms, so it can be inverted (and the inverse is Cauchy, as a_n does not go to 0), so I is all of C, hence M is maximal. So the quotient will be a field, and we define this to be the field of p-adic numbers,

$$\mathbb{Q}_p = C/M.$$

Another way of saying the same thing is that a_n, b_n are equivalent if $|a_n - b_n| \to 0$, and that $\mathbb{Q}_p$ is the set of equivalence classes, and then checking that the ring operations on representatives give well-defined operations on equivalence classes. For multiplication, we check that if a_n and a'_n are equivalent, and b_n and b'_n are, then

$$\begin{aligned} |a'_n b'_n - a_n b_n| &= |a'_n(b'_n - b_n) + b_n(a'_n - a_n)| \\ &\leq |a'_n||b'_n - b_n| + |b_n||a'_n - a_n| \to 0, \end{aligned}$$

as both sequences are Cauchy and bounded, so the two pairs of representatives give the same class when multiplied. We can do the same thing for addition. Zero is the equivalence class of the all-zero sequence, and the definition of negatives is obvious. The multiplicative identity is the sequence of all ones. Inverses are a bit more tricky: we'd like to just invert every term, but we need to guarantee that they are non-zero. We do the same thing as we did when checking that M is maximal: if a sequence does not converge to zero, it has a last zero term, and we can add on a sequence converging to zero that makes those terms non-zero, this gives a different representative of the same class, and it is easily inverted. So again we have a field.

The rationals are a subfield of the p-adic numbers, via the inclusion of $x \in \mathbb{Q}$ as the constant sequence $x_n = x$.

Now the whole point of this exercise was to make the rationals complete with respect to $|\cdot|_p$. We can't even think about completeness without a topology, so our next step is to define a norm on $\mathbb{Q}_p$. Define

$$|\{x_n\}|_p = \lim_{n\to\infty} |x_n|_p,$$

where the second norm is the norm on $\mathbb{Q}$. This limit exists: If $a_n \to 0$, it is just 0. If a_n does not converge to zero, then for some $\varepsilon > 0$, and any index N there is some $i \geq N$ such that $|a_i| > \varepsilon$. Since a_n is Cauchy we can also choose N large enough to get $|a_m - a_n| < \varepsilon$ for all $m, n \geq N$. Then for any $n \geq N$, $|a_n - a_i| < \varepsilon$ and $|a_n - a_i| \leq \max(|a_n|, |a_i|) > \varepsilon$. (Remember that the norm on $\mathbb{Q}$ is non-Archimedean. If we were completing with respect to an Archimedean norm, as in the construction of the reals, we would need to choose a slightly different approach here.) Now if $|a_n| \neq |a_i|$, then the $\leq$ is

an equality, which is impossible. So for all $n \geq N$, $|a_n|$ is stationary at $|a_i|$, so $|a_n| \to |a_i|$.

Note that the possible values the norm can take are still p^n, for integer n, the same values we had on $\mathbb{Q}$. This contrasts with the reals, whose norm takes all real values, while the (Euclidean) norm on the rationals takes only rational values.

As for $\mathbb{Q}$, $\mathbb{Q}_p$ is a topological group simply because the topology comes from a norm.

Note that this norm agrees with the p-adic norm on $\mathbb{Q}$ for rationals embedded in $\mathbb{Q}_p$ as constant sequences. We also see that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, as any sequence x_n of rationals is the limit of the constant sequences x_n, so a limit of rationals. Multiplicativity and the ultrametric inequality follow from the $\mathbb{Q}$-norm, since limits commute with sums, products and taking maximums. So we really have made a non-Archimedean norm on the p-adic numbers.

Now we can show that $\mathbb{Q}_p$ is complete. Take a Cauchy sequence $\{a_j\}$ of p-adic numbers, i.e. of equivalence classes of Cauchy sequences of rationals, and choose a representative $\{a_{ji}\}_i$ of each class. For each j, let N_j be a number such that $|a_{jm} - a_{jn}| < p^{-j}$ for any $m, n \geq N_j$. Then $\{a_{jN_j}\}_j$ is the limit of the sequence $\{a_j\}$. For more detail, see [Baker, 2009].

So we have a complete field $\mathbb{Q}_p$, which has $\mathbb{Q}$ as a dense subfield, which is what we were looking for. This is the unique, up to isometric isomorphism, such field. (See [Vaaler])

Some properties of $\mathbb{Q}_p$

We'd like to not have to think about p-adic numbers as (classes of) Cauchy sequences, and by analogy with the reals we might hope for something similar to a decimal expansion. If we are lucky, we'll then get fairly straightforward arithmetic as well. We are lucky:

Define the *p-adic integers* to be the closed unit ball

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

Then we have

Theorem. *Every p-adic integer x has exactly one representative $\{x_n\}$ such that*

1. $0 \leq x_n < p^n$ *for each* $n \geq 1$,
2. $x_n \equiv x_{n+1} \mod p^n$ *for every* $n \geq 1$.

For a proof, see [Koblitz, 1984].

We can write out the x_n in terms of powers of p:

$$x_n = b_0 + b_1 p + \ldots + b_{n-1} p^{n-1},$$

with all the b_i integers in $[0, p-1]$, and the congruence condition means that x_{n+1} has the same $b_0, \ldots, b_{n-1}$, so we get a sequence $\{b_n\}$ that we can think of as a p-adic expansion of x with integer coefficients. In fact, the series

$$\sum b_i p^i$$

really does converge to x.

(Convergence testing, by the way, is really easy with a non-Archimedean norm: A series $\sum a_n$ converges if and only if $a_n \to 0$.)

If we have an $x \in \mathbb{Q}_p$ with norm greater than 1, then we can multiply by a positive power p^n of p to get an integer. If this then expands as $\sum_{i=0} b_i p^i$ then x is

$$x = \frac{b_0}{p^n} + \ldots + \frac{b_{n-1}}{p} + b_n + b_{n+1} p + \ldots.$$

Note that the theorem said exactly one; there is no chance of getting an equivalent of $1 = 0.999\ldots$.

With these 'decimal expansions' of p-adics we can do arithmetic just as we would with decimal representations of real numbers, with the one change that we start from the left and work our way right.

Now for some topological properties of $\mathbb{Q}_p$. We have already shown it is complete, and that $\mathbb{Q}$ is a dense subset. As a metric space, it is Hausdorff.

Like the rationals, but unlike the reals, the p-adics are totally disconnected. If x and y are any two p-adic numbers, let d be the distance between them, then the closed ball of radius $\frac{d}{\sqrt{2}}$ centred at x does not contain y, and the complement of the ball is open. Any boundary points z would have distance $|x - z| = \frac{d}{\sqrt{2}}$ from x, which is not a possible value of the norm, so the closed ball is equal to the open ball of the same radius, so is open. Thus the ball and its complement are a pair of disjoint open sets covering all of $\mathbb{Q}_p$. Since we can do this to any two numbers, the connected components are singletons.

The p-adic numbers are locally compact, and the ring of integers $\mathbb{Z}_p$ is compact. Compactness of the integers implies that $\mathbb{Q}_p$ is locally compact, as it gives an open ball around 0 with compact closure, and we can then translate this ball to any other point in $\mathbb{Q}_p$. To see that $\mathbb{Z}_p$ is compact, recall that a metric space is compact if it is complete and totally bounded. The p-adic integers are a closed subset of the p-adic numbers, so they inherit the completeness. To show that $\mathbb{Z}_p$ is totally bounded, we need to show it can be covered by finitely many ε-balls, for any $\varepsilon > 0$. We only need to consider

p^{-n}-balls, as the norm takes no other values. Now the p^{-n}-ball around 0 is $p^n\mathbb{Z}$, so other balls are cosets of this, and since $\mathbb{Z}_p/p^n\mathbb{Z}_p = \mathbb{Z}/p^n\mathbb{Z}$ (this is easily seen from the p-adic expansion), we only need finitely many to cover all of $\mathbb{Z}_p$.

So the p-adic integers are compact, totally disconnected and Hausdorff, which is what is required to be a profinite group. Equivalently, a profinite group is the inverse limit of an inverse system of discrete finite groups. In our case, $\mathbb{Z}_p$ is the limit of $\mathbb{Z}/p^n\mathbb{Z}$ as $n \to \infty$.

The p-adic numbers are the field of fractions of $\mathbb{Z}_p$.

The cardinality of $\mathbb{Q}_p$ and $\mathbb{Z}_p$ is that of $\mathbb{R}$, by the usual diagonal argument.

References

AJ Baker. An Introduction to p-adic Numbers and p-adic Analysis (Lecture Notes). 2009. URL `http://www.maths.gla.ac.uk/~ajb/dvi-ps/padicnotes.pdf`.

Neal Koblitz. *P-adic Numbers, p-adic Analysis, and Zeta-Functions*, volume 58 of *Graduate Texts in Mathematics*. Springer New York, New York, NY, 1984.

Jeff Vaaler. Notes on Local fields. (Ask Alan).