10. p-ADIC NUMBERS: II

So far we have just looked at the p-adic integers from the algebraic point of view. But one reason the reals are so interesting is that there is a notion of two reals being close together. We think of the sequence of approximations 1, $3/2 = 1.5$, $17/12 = 1.4166\dots$ as getting close to the true answer of $\sqrt{2}$. If we consider the p-adic integers 3, $3 + 1 \cdot 7$, $3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3$, we have to consider $98 = 2 \cdot 7^2$ as being smaller than $7 = 1 \cdot 7$ and $2058 = 6 \cdot 7^3$ as being smaller than $98 = 2 \cdot 7^2$.

Definition 10.1. *If p is a prime and $n \in \mathbb{Z}$ is an integer then $\nu_p(n) = e$ is called the **p-adic valuation**, where $n = p^e m$ and $(p, m) = 1$.*

We have $\nu_7(3) = 0$, $\nu_7(7) = 1$, $\nu_7(98) = 2$, $\nu_7(2058) = 3$. In fact $n \in \mathbb{Z}$ is small p-adically, if $\nu_p(n)$ is large. This suggests

Definition 10.2. *If p is a prime and $n \in \mathbb{Z}$ is a non-zero integer then the **p-adic absolute value** is*

$$|n|_p = \frac{1}{p^{\nu_p(n)}}.$$

By convention $|0|_p = 0$. Note that the p-adic absolute value shares many of the properties of the ordinary absolute value.

(i) It is a function

$$\mathbb{Z} \longrightarrow \mathbb{Q}.$$

(ii) $|n|_p \geq 0$ with equality if and only if $n = 0$.

(iii)

$$|ab|_p = |a|_p \cdot |b|_p.$$

(iv)

$$|a + b|_p \leq |a|_p + |b|_p.$$

In fact the p-adic absolute value satisfies a much stronger property than (iv), namely:

(v)

$$|a + b|_p \leq \max(|a|_p, |b|_p),$$

with equality unless $|a|_p = |b|_p$.

In fact one just needs to check that

$$\nu_p(a + b) \geq \min(\nu_p(a), \nu_p(b))$$

with equality unless $\nu_p(a) = \nu_p(b)$. But this follows from basic property of divisibility.

We can extend all of this from the integers to the rationals. It suffices to define the valuation, and this is easy:

$$\nu_p(a/b) = \nu_p(a) - \nu_p(b).$$

We may use the p-adic absolute value to give an alternative construction of the p-adic numbers.

Definition 10.3. *Fix a prime p. Let $a_1, a_2, \dots$ be a sequence of rational numbers. We say that the sequence is a **Cauchy sequence** if given any $\epsilon > 0$ there is an n_0 such that for all m and $n > n_0$ we have*

$$|a_n - a_m|_p < \epsilon.$$

*We say that a Cauchy sequence is a **null sequence** if given any $\epsilon > 0$ there is an n_0 such that for all $n > n_0$ we have*

$$|a_n|_p < \epsilon.$$

Note that the set of all sequences is a ring, with pointwise addition and multiplication.

Lemma 10.4. *The set of all Cauchy sequences is a subring R of the ring of all sequences.*

Proof. We just have to check that the sum and product of two Cauchy sequences is a Cauchy sequence. □

Lemma 10.5. *The set I of all null sequences is an ideal in R.*

Proof. Let $a_1, a_2, \dots$ and $b_1, b_2, \dots$ be two Cauchy sequences. We have to check

(1) If $a_1, a_2, \dots$ and $b_1, b_2, \dots$ are null sequences then so is their sum.
(2) If $a_1, a_2, \dots$ is a null sequence then the product of $a_1, a_2, \dots$ and $b_1, b_2, \dots$ is a null sequence. □

Definition-Lemma 10.6. *We say that two Cauchy sequences $a_1, a_2, \dots$ and $b_1, b_2, \dots$ are equivalent, denoted $a_1, a_2, \dots \sim b_1, b_2, \dots$, if the difference $c_1, c_2, \dots$ is a null sequence.*

$\sim$ is an equivalence relation. The set of all equivalence classes is denoted Q_p.

Proof. This can be checked directly. In fact two Cauchy sequences are equivalent if and only if they define the same left coset of I. □

Theorem 10.7. *Q_p is a field which contains $\mathbb{Q}$.*

Moreover Q_p is isomorphic to the ring $\mathbb{Q}_p$ we constructed in lecture 9.

Proof. Q_p is the quotient ring R/I. It is not hard to check that every non-zero element is invertible. The characteristic is zero and every field of characteristic zero contains $\mathbb{Q}$.

There is a natural map

$$\mathbb{Q}_p \longrightarrow Q_p$$

which sends the p-adic integer

$$\beta = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \dots,$$

where $0 \leq a_i < p$ are integers, to the equivalence class generated by the sequence

$$a_0, \quad a_0 + a_1 p, \quad a_0 + a_1 p + a_2 p^2, \quad \dots, \quad a_0 + a_1 p + a_2 p^2 + \dots + a_k p^k, \dots.$$

It is not hard to see that the sequence we have written down is a Cauchy sequence and that the map is a ring homomorphism. The key point is to check the map is surjective. Given an arbitrary Cauchy sequence $\alpha_1, \alpha_2, \dots$ we have to construct $\beta \in \mathbb{Q}_p$ with the property that its image is equivalent to $\alpha_1, \alpha_2, \dots$.

If $\alpha_1, \alpha_2, \dots$ is a null sequence, we may take $\beta = 0$. Therefore we may assume that $\alpha_1, \alpha_2, \dots$ is not a null sequence. In particular we may assume that only finitely many $\alpha_m = 0$. Possibly passing to a tail of the sequence, we may assume that $\alpha_m \neq 0$ for all m.

As α_n is a rational number, we may write

$$\alpha_n = p^{e_n} \frac{b_n}{c_n},$$

where b_n and c_n are coprime integers, coprime to p. Our goal is to first reduce to the case when $c_n = 1$.

To say that we have a Cauchy sequence implies that given k we may find n_0 such that if m and $n > n_0$ then

$$|\alpha_m - \alpha_n|_p < \frac{1}{p^k}.$$

In particular if we take $k = 0$ it follows that e_n is bounded from below, so that the minimum exists. e_n is bounded from above, as we don't have a null sequence. It follows that there is a smallest integer N such that $e_n = N$ for infinitely many n. If we throw out the finitely many n such that $e_n < N$ we may assume that $e_n \geq N$ for all n. Let e be the largest exponent and let $f = e - N \geq 0$ be the difference.

As c_n is coprime to p we may pick an integer f_n such that

$$b_n - c_n f_n \equiv 0 \mod p^n.$$

Let $g_n = p^{e_n - N} f_n \in \mathbb{Z}$. In this case

$$\begin{aligned}
\left|\alpha_n - p^N g_n\right|_p &= \left|p^{e_n}\frac{b_n}{c_n} - p^{e_n} f_n\right|_p \\
&= \left|p^{e_n}\left(\frac{b_n}{c_n} - f_n\right)\right|_p \\
&= \frac{1}{p^{e_n}}\left|\frac{b_n}{c_n} - f_n\right|_p \\
&= \frac{1}{p^{e_n+n}} \\
&\leq \frac{1}{p^{N+n}}.
\end{aligned}$$

It follows that the Cauchy sequences $\alpha_1, \alpha_2, \dots$ and $p^N g_1, p^N g_2, \dots$ have the same limit. Replacing α_n by $p^N g_n$ we may assume that $c_n = 1$. Replacing α_m by $p^{-N}\alpha_n$ we may assume α_n is an integer. We will construct a p-adic integer

$$\beta = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \dots,$$

where $0 \leq a_i < p$ are integers, whose image is the Cauchy sequence $\alpha_1, \alpha_2, \dots$. As

$$|\alpha_m - \alpha_n| < \frac{1}{p^k}.$$

the difference is divisible by p^k so that

$$\alpha_m = a_0 + a_1 p + \dots + a_k p^k + \alpha'_m,$$

where the coefficients $a_0 a_1 \dots a_k$ don't depend on m and $\alpha'_m \in \mathbb{Z}$ is divisible by p^k. This defines β and it is clear that the image of β is the Cauchy sequence $\alpha_1, \alpha_2, \dots$. □

In the course of the proof of (10.7) we established that every element of $\mathbb{Q}_p$ has a unique representation in the form

$$\alpha = p^N(a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \dots).$$

In fact this allows us to extend the p-adic absolute value to the whole of $\mathbb{Q}_p$,

$$\nu_p(\alpha) = N \qquad \text{and} \qquad |\alpha| = \frac{1}{p^N}.$$

If $\nu_p(\alpha) \geq 0$ then we say that we have a p-adic integer.

Given the rational numbers $\mathbb{Q}$ we now have more than one way to complete $\mathbb{Q}$. If we use the usual absolute value, we get the real numbers $\mathbb{R}$, which we can either think of using their decimal expansion, or as equivalence classes of Cauchy sequences. If we use a p-adic absolute value, we get the p-adic numbers $\mathbb{Q}+p$ which we can think of either as a p-adic integer, multiplied by a power of p, or as equivalence classes of Cauchy sequences.

All of these fields give information about the rational numbers. One beautiful result is that the product of all of the absolute values is one:

$$|a|\prod_{p}|a|_{p}=1.$$

Another is the Hasse-Minkowski principle. Consider the problem of trying to solve a a Diophantine equation

$$F(x_1,x_2,\ldots,x_n)=0.$$

Here we are looking for integer solutions. If there is an integer solution then there must be a real solution and a p-adic integer solution. Conversely, if there is no real solution or no p-adic integer solution then there is no integer solution.

Sometimes, we can reverse this implication. For example, the homogeneous quadratic equation

$$\sum_{i\leq j}a_{ij}x_ix_j=0$$

has a non-trivial integer solution, if and only if it has a real solution and p-adic solutions for all primes p.

In fact Legendre's theorem is one particular case of this. Part of the hypothesis for Legendre's theorem is that there is a real solution. The other implies that there is a solution modulo p. If p is odd, we can use the method of Newton Raphson to get a p-adic solution. If $p=2$ the situation is more complicated and a little bit more work is needed.