8
Adic Numbers

8.1 The N-Adic Numbers

Convince yourself that the following lemma is true.

Lemma 8.1.1. *Let $N > 1$ be an integer. Then for any positive rational number α there exists unique $e \in \mathbb{Z}$ and positive integers a, b such that $\alpha = N^e \cdot \frac{a}{b}$ with $N \nmid a$, $\gcd(a,b) = 1$, and $\gcd(N,b) = 1$.*

Definition 8.1.2 (N-adic valuation). Let N be a positive integer. For any positive $\alpha \in \mathbb{Q}$, the *N-adic valuation* of α is e, where e is as in Lemma 8.1.1. If α is negative, the N-adic valuation of α is the valuation of $-\alpha$. The N-adic valuation of 0 is ∞.

We denote the N-adic valuation of α by $v_N(\alpha)$.

Definition 8.1.3 (N-adic metric). For $x, y \in \mathbb{Q}$ the *N-adic distance* between x and y is

$$d_N(x,y) = N^{-v_N(x-y)}.$$

We let $d_N(x,x) = 0$, since $v_N(x-x) = v_N(0) = \infty$.

For example, $x, y \in \mathbb{Z}$ are close in the N-adic metric if their difference is divisible by a large power of N. E.g., if $N = 10$ then 93427 and 13427 are close because their difference is 80000, which is divisible by a large power of 10.

Definition 8.1.4 (Metric). A *metric* on a set X is a map

$$d : X \times X \to \mathbb{R}$$

such that for all $x, y, z \in X$,

1. $d(x,y) \geq 0$ and $d(x,y) = 0$ if and only if $x = y$,
2. $d(x,y) = d(y,x)$, and
3. $d(x,z) \leq d(x,y) + d(y,z)$.

We recall from a basic analysis course the following facts about completion with respect to a metric. A *Cauchy sequence* is a sequence (x_n) in X such that for all $\varepsilon > 0$ there exists M such that for all $n, m > M$ we have $d(x_n, x_m) < \varepsilon$. The *completion* of X is the set of Cauchy sequences (x_n) in X modulo the equivalence relation in which two Cauchy sequences (x_n) and (y_n) are equivalent if $\lim_{n\to\infty} d(x_n, y_n) = 0$. A metric space is *complete* if every Cauchy sequence converges, and one can show that the completion of X with respect to a metric is complete.

For example, $d(x,y) = |x - y|$ defines a metric on $\mathbb{Q}$. The completion of $\mathbb{Q}$ with respect to this metric is the field $\mathbb{R}$ of real numbers. In certain parts of number theory the N-adic numbers, which we introduce shortly, are just as important as $\mathbb{R}$.

Proposition 8.1.5. *The distance d_N on $\mathbb{Q}$ defined above is a metric. Moreover, for all $x, y, z \in \mathbb{Q}$ we have*

$$d(x,z) \leq \max(d(x,y), d(y,z)).$$

Proof. The first two properties of Definition 8.1.4 are immediate. For the third, we first prove that if $\alpha, \beta \in \mathbb{Q}$ then

$$v_N(\alpha + \beta) \geq \min(v_N(\alpha), v_N(\beta)).$$

Assume, without loss, that $v_N(\alpha) \leq v_N(\beta)$ and that both α and β are nonzero. Using Lemma 8.1.1 write $\alpha = N^e(a/b)$ and $\beta = N^f(c/d)$ with a or c possibly negative. Then

$$\alpha + \beta = N^e\left(\frac{a}{b} + N^{f-e}\frac{c}{d}\right) = N^e\left(\frac{ad + bcN^{f-e}}{bd}\right).$$

Since $\gcd(N, bd) = 1$ it follows that $v_N(\alpha+\beta) \geq e$. Now suppose $x, y, z \in \mathbb{Q}$. Then

$$x - z = (x - y) + (y - z),$$

so

$$v_N(x - z) \geq \min(v_N(x - y), v_N(y - z)),$$

hence $d_N(x,z) \leq \max(d_N(x,y), d_N(y,z))$. $\square$

We can finally define the N-adic numbers.

Definition 8.1.6 (The N-adic Numbers). The set of *N-adic numbers*, denoted $\mathbb{Q}_N$, is the completion of $\mathbb{Q}$ with respect to the metric d_N.

The set $\mathbb{Q}_N$ is a ring, but it need not be a field as you will show in Exercises 4 and 5. Also, $\mathbb{Q}_N$ has a bizarre topology, as we will see in Section 8.4.

8.2 The 10-Adic Numbers

It's a familiar fact that every real number can be written in the form

$$d_n \dots d_1 d_0 . d_{-1} d_{-2} \dots = d_n 10^n + \dots + d_1 10 + d_0 + d_{-1} 10^{-1} + d_{-2} 10^{-2} + \cdots$$

where each digit d_i is between 0 and 9, and the sequence can continue indefinitely to the right.

The 10-adic numbers also have decimal expansions, but everything is backwards! To get a feeling for why this might be the case, we consider Euler's nonsensical series

$$\sum_{n=1}^{\infty} (-1)^{n+1} n! = 1! - 2! + 3! - 4! + 5! - 6! + \cdots .$$

You will prove in Exercise 2 that this series converges in $\mathbb{Q}_{10}$ to some element $\alpha \in \mathbb{Q}_{10}$.

What is α? How can we write it down? First note that for all $M \geq 5$, the terms of the sum are divisible by 10, so the difference between α and $1! - 2! + 3! - 4!$ is divisible by 10. Thus we can compute α modulo 10 by computing $1! - 2! + 3! - 4!$ modulo 10. Likewise, we can compute α modulo 100 by compute $1! - 2! + \cdots + 9! - 10!$, etc. We obtain the following table:

α	mod 10^r
1	mod 10
81	mod 10^2
981	mod 10^3
2981	mod 10^4
22981	mod 10^5
422981	mod 10^6

Continuing we see that

$$1! - 2! + 3! - 4! + \cdots = \dots 637838364422981 \qquad \text{in } \mathbb{Q}_{10} \text{ !}$$

Here's another example. Reducing $1/7$ modulo larger and larger powers of 10 we see that

$$\frac{1}{7} = \dots 857142857143 \qquad \text{in } \mathbb{Q}_{10}.$$

Here's another example, but with a decimal point.

$$\frac{1}{70} = \frac{1}{10} \cdot \frac{1}{7} = \dots 85714285714.3$$

We have

$$\frac{1}{3} + \frac{1}{7} = \dots 66667 + \dots 57143 = \frac{10}{21} = \dots 23810,$$

which illustrates that addition with carrying works as usual.

8.2.1 FLT in $\mathbb{Q}_{10}$

An amusing observation, which people used to endlessly argue about on USENET back in the 1990s, is that Fermat's last theorem is false in $\mathbb{Q}_{10}$. For example, $x^3 + y^3 = z^3$ has a nontrivial solution, namely $x = 1$, $y = 2$, and $z = \ldots 60569$. Here z is a cube root of 9 in $\mathbb{Q}_{10}$. Note that it takes some work to prove that there is a cube root of 9 in $\mathbb{Q}_{10}$ (see Exercise 3).

8.3 The Field of p-Adic Numbers

The ring $\mathbb{Q}_{10}$ of 10-adic numbers is isomorphic to $\mathbb{Q}_2 \times \mathbb{Q}_5$ (see Exercise 5), so it is not a field. For example, the element $\ldots 8212890625$ corresponding to $(1, 0)$ under this isomorphism has no inverse. (To compute n digits of $(1, 0)$ use the Chinese remainder theorem to find a number that is 1 modulo 2^n and 0 modulo 5^n.)

If p is prime then $\mathbb{Q}_p$ is a field (see Exercise 4). Since $p \neq 10$ it is a little more complicated to write p-adic numbers down. People typically write p-adic numbers in the form

$$\frac{a_{-d}}{p^d} + \cdots + \frac{a_{-1}}{p} + a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots$$

where $0 \le a_i < p$ for each i.

8.4 The Topology of $\mathbb{Q}_N$ (is Weird)

Definition 8.4.1 (Connected). Let X be a topological space. A subset S of X is *disconnected* if there exist open subsets $U_1, U_2 \subset X$ with $U_1 \cap U_2 \cap S = \emptyset$ and $S = (S \cap U_1) \cup (S \cap U_2)$ with $S \cap U_1$ and $S \cap U_2$ nonempty. If S is not disconnected it is *connected*.

The topology on $\mathbb{Q}_N$ is induced by d_N, so every open set is a union of open balls

$$B(x, r) = \{y \in \mathbb{Q}_N : d_N(x, y) < r\}.$$

Recall Proposition 8.1.5, which asserts that for all x, y, z,

$$d(x, z) \le \max(d(x, y), d(y, z)).$$

This translates into the following shocking and bizarre lemma:

Lemma 8.4.2. *Suppose* $x \in \mathbb{Q}_N$ *and* $r > 0$. *If* $y \in \mathbb{Q}_N$ *and* $d_N(x, y) \ge r$, *then* $B(x, r) \cap B(y, r) = \emptyset$.

Proof. Suppose $z \in B(x, r)$ and $z \in B(y, r)$. Then

$$r \le d_N(x, y) \le \max(d_N(x, z), d_N(z, y)) < r,$$

a contradiction. □

You should immediately draw a picture that illustrates Lemma 8.4.2.

Lemma 8.4.3. *The open ball $B(x,r)$ is also closed.*

Proof. Suppose $y \notin B(x,r)$. Then $r < d(x,y)$ so

$$B(y, d(x,y)) \cap B(x,r) \subset B(y, d(x,y)) \cap B(x, d(x,y)) = \emptyset.$$

Thus the complement of $B(x,r)$ is a union of open balls. □

The lemmas imply that $\mathbb{Q}_N$ is *totally disconnected*, in the following sense.

Proposition 8.4.4. *The only connected subsets of $\mathbb{Q}_N$ are the singleton sets $\{x\}$ for $x \in \mathbb{Q}_N$ and the empty set.*

Proof. Suppose $S \subset \mathbb{Q}_N$ is a nonempty connected set and x, y are distinct elements of S. Let $r = d_N(x,y) > 0$. Let $U_1 = B(x,r)$ and U_2 be the complement of U_1, which is open by Lemma 8.4.3. Then U_1 and U_2 satisfies the conditions of Definition 8.4.1, so S is not connected, a contradiction. □

8.5 The Local-to-Global Principle of Hasse and Mikowski

Section 8.4 might have convinced you that $\mathbb{Q}_N$ is a bizarre pathology. In fact, $\mathbb{Q}_N$ is omnipresent in number theory, as the following two fundamental examples illustrate.

A "nontrivial" solution to a homogeneous equation is a solution where not all indeterminates are 0.

Theorem 8.5.1 (Hasse-Minkowski). *The quadratic equation*

$$a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2 = 0 \tag{8.1}$$

with $a_i \in \mathbb{Q}^\times$ has a nontrivial solution with $x_1, \ldots, x_n$ in $\mathbb{Q}$ if and only if (8.1) has a solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all primes p.

This theorem is very useful in practice because the p-adic condition turns out to be easy to check. For more details, including a complete proof, see IV.3.2 of Serre's *A Course In Arithmetic.*

The analogue of Theorem 8.5.1 for cubic equations is false. For example, Selmer proved that the cubic

$$3x^3 + 4y^3 + 5z^3 = 0$$

has a nontrivial solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all primes p but has no solutions in $\mathbb{Q}$.

Open Problem 8.5.2. *Give an algorithm that decides whether or not a cubic $ax^3 + by^3 + cz^3 = 0$ has a nontrivial solution in $\mathbb{Q}$.*

This open problem is closely related to the Birch and Swinnerton-Dyer Conjecture for elliptic curves. The truth of the conjecture would follow if we knew that "Shafarevich-Tate Groups" of elliptic curves are finite.

Exercises

8.1 Compute the first 5 digits of the 10-adic expansions of the following rational numbers:

$$\frac{13}{2}, \quad \frac{1}{389}, \quad \frac{17}{19}, \qquad \text{the 4 square roots of 41.}$$

8.2 Let $N > 1$ be an integer. Prove that the series

$$\sum_{n=1}^{\infty} (-1)^{n+1} n! = 1! - 2! + 3! - 4! + 5! - 6! + \cdots .$$

converges in $\mathbb{Q}_N$.

8.3 Prove that -9 has a cube root in $\mathbb{Q}_{10}$ using the following strategy (this is a special case of "Hensel's Lemma").

(a) Show that there is $\alpha \in \mathbb{Z}$ such that $\alpha^3 \equiv 9 \pmod{10^3}$.

(b) Suppose $n \geq 3$. Use induction to show that if $\alpha_1 \in \mathbb{Z}$ and $\alpha^3 \equiv 9 \pmod{10^n}$, then there exists $\alpha_2 \in \mathbb{Z}$ such that $\alpha_2^3 \equiv 9 \pmod{10^{n+1}}$. (Hint: Show that there is an integer b such that $(\alpha_1 + b10^n)^3 \equiv 9 \pmod{10^{n+1}}$.)

(c) Conclude that 9 has a cube root in $\mathbb{Q}_{10}$.

8.4 Let $N > 1$ be an integer.

(a) Prove that $\mathbb{Q}_N$ is equipped with a natural ring structure.

(b) If N is prime, prove that $\mathbb{Q}_N$ is a field.

8.5 (a) Let p and q be distinct primes. Prove that $\mathbb{Q}_{pq} \cong \mathbb{Q}_p \times \mathbb{Q}_q$.

(b) Is $\mathbb{Q}_{p^2}$ isomorphic to either of $\mathbb{Q}_p \times \mathbb{Q}_p$ or $\mathbb{Q}_p$?