p-Adic Numbers

Motivation: Analogy between $\mathbb{C}(X)$ and $\mathbb{Q}$

- Both are fields.
- $\mathbb{C}[X]$ works like $\mathbb{Z}$
  - Fractions
    - $x \in \mathbb{Q}$, then $x = \frac{a}{b}$ for $a, b, \in \mathbb{Z}$
    - $f \in \mathbb{C}$, then $f = \frac{g}{h}$for $g, h \in \mathbb{C}[X]$
  - Factorization
    - Fundamental Theorem of Arithmetics
    - Fundamental Theorem of Algebra

One particular useful technique used in $\mathbb{C}(X)$ is Taylor/Laurent Expansion around $(X - a)$.

$$f(X) = \sum_{i=-n}^{\infty} a_i (X - a)^i$$

Question: Can we do the same for $\mathbb{Q}$?

Introducing p-adic numbers

Well, we certainly can do similar things for positive integers, for example, the base 10 representation.

$$237 = 7 \times 10^0 + 3 \times 10^1 + 2 \times 10^2$$

BUT, 10 is not a prime in $\mathbb{Z}$. but this can be fixed by using base-p representation of integers.

Ex.

$$320 = 5 + 3 \times 7 + 6 \times 7^2$$

So,

$$320 = \overline{635}$$

How do we get this?

Division with remainder.

$$320 = 45 \times 7 + 5$$

$$45 = 6 \times 7 + 3$$

$$6 = 0 \times 7 + 6$$

Try 72 in base 3

$$72 = \overline{2200}$$

But we can do more in $\mathbb{C}(X)$ using laurent series! Ex.

$$f(X) = \frac{X}{X - 1}$$

Expanding at $X = 0$:

$$\frac{X}{X - 1} = -X - X^2 - ...$$

BUT we can also expand at a pole $X = 1$

$$\frac{X}{X-1} = \frac{1}{X-1} + 1$$

Ex. $\frac{320}{49}$ in 7-adic

$$\frac{320}{49} = 5 \times 7^{-2} + 3 \times 7^{-1} + 6 = \overline{6.35}$$

- What about generic positive rational numbers?

TRY DIVISON WITH REMAINDER

Ex. $\frac{1}{2}$ in 5-adic

$$\frac{1}{2} = 5 \times -\frac{1}{2} + 3$$

$$-\frac{1}{2} = 5 \times -\frac{1}{2} + 2$$

$$-\frac{1}{2} = 5 \times -\frac{1}{2} + 2$$

$$\frac{1}{2} = 3 + 2 \times 5 + 2 + 5^2 + ... = \overline{...222223}$$

Check

$$\overline{...222223} \times 2 = \overline{....000001} = 1$$

So, it sorta works.

Ex. $\frac{1}{3}$ in 5-adic.

$$\frac{1}{3} = \overline{...031312}$$

- What about negative numbers

Ex. -1 in 7-adic

Then $-1 = \overline{...66666}$

Check $\overline{...66666} + 1 = \overline{....000000} = 0$

In general, we can subtract each digit from p-1, and add one to the end.

Now, we know we can write all natural numbers in this representation.

Exercise:

Show the p-adic representations of rational numbers are eventually periodic.

BUT what does it mean?

Absolute Value, Topology and Convergence

What does base 10 representation mean?

$$x = \overline{a_n \ldots a_0 . a_{-1} \ldots}$$

is to say

$$x = \sum a_i 10^i$$

But this does not make any sense in p-adic as $p^i \to \infty$.

But does it?? or can we fix it?

Convergence depends on how we measure the distance, which in particular depends on how we define absolute value. So, we will try to redefine absolute value.

Absolute Value

Let k be a field

Then, $|\ .\ | : k \times k \to k$ s.t.
- $|x| \geq 0$ and equality hold iff $x = 0$
- $|xy| = |x|\ |y|$
- $|x + y| \leq |x| + |y|$

Ex. $(\mathbb{R}, |\ .\ |)$, trivial absolute value.

Prop. If k is a finite field, then the only absolute value is the trivial absolute value.

Once we have an absolute value, we can induce a metric from the absolute value:

$$d(x, y) = |x - y|$$

which then induces a topology.

By redefining an absolute value, we can try to make the p-adic representation converges like the base 10 representation.

p-adic Valuation

Let $x \in \mathbb{Z}$, define $\nu_p(x) = a$ s.t. $p^a \mid x, p^{a+1} \nmid x$

Let $x \in \mathbb{Q}$, write $x = \frac{a}{b}, a, b \in \mathbb{Z}$, define $\nu_p(x) = \nu_p(a) - \nu_p(b)$

We further define $\nu_p(0) = \infty$

Verify:
- $\nu_p(x) = \infty \Leftrightarrow x = 0$
- $\nu_p(xy) = \nu_p(x) + \nu_p(y)$
- $\nu_p(x + y) \geq \min\{\nu_p(x), \nu_p(y)\}$

p-adic Absolute Value

Define $|x|_p = p^{-\nu_p(x)}$ And we also use the convention $|x|_\infty = |x|$.

Verify these are absolute values.

In fact, from $\nu_p(x + y) \geq \min\{\nu_p(x), \nu_p(y)\}$, $|x|_p$ satisfies the strong triangle inequality:

$|x + y| \leq \max\{|x|, |y|\}$ we call such absolute value non-archimedean.

Now, we can see the p-adic representation gives converges sequences similar to base 10 representation.

Ultra metric

A metic satisfies $d(x,y) \leq \max\{d(x,z), d(y,z)\}$ is called a ultra metic.

Prop:

- All triangles are isosceles
- All open balls are closed
- All closed balls are open

Pf.

If $|x| \neq |y|$,then $|x+y| = \max\{|x|, |y|\}$

WLOG $|x| > |y|$, then $|x+y| \leq |x|$ and $|x| \leq \max\{|x+y|, |-y| = |x+y|$

The other proposition follows.

Cauchy Sequences

A sequence $\{a_n\}$ is Cauchy,if $\forall \varepsilon > 0$, $\exists N$ s.t. $m, n > N$ implies $|a_n - a_m| < \varepsilon$

A metric space is called complete if all Cauchy sequences converges.

Note: $\left(\mathbb{Q}, |\ .\ |_p\right)$ is not complete, because the exercise above.

Similar to $\mathbb{R}$, $\left(\mathbb{Q}, |\ .\ |_p\right)$ has a completion and we call the completion (up to isometry) $\mathbb{Q}_p$.

Brief construction:

We take all Cauchy sequences and mod out the null sequences.

More algebraically, we can consider the ring

$$R = \prod_{\mathbb{N}} \mathbb{Q}$$

the product ring of $\mathbb{Q}$

The Ideal $I \coloneqq \{\text{null sequences}\}$ is a maximal ideal.

Therefore, R/I is a field, and we can embed $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ by sending $x \mapsto \{x\}_{\mathbb{N}}$.

Prop: n-th term test in $\mathbb{Q}_p$

Because $\mathbb{Q}_p$ has stronger triangle inequality, $\sum x_i$ converges iff $x_i \to 0$

Pf. Apply triangle inequality.

Definition: $|\ .\ |_1$ is equivalent to $|\ .\ |_2$ if $|x|_1 = |x|_2^s$ for $s \in \mathbb{R}$ for all $x \in k$

Ostrowski's Theorem: Every non-trivial absolute value on the rational numbers $\mathbb{Q}$ is equivalent to either the usual real absolute value or a p-adic absolute value.

We will only prove for the non-Archimedean case, archimedean case is more complicated in calculation but not very difficult.

Pf.

It is enough to find the absolute value on $\mathbb{Z}$.

we know $|x| \leq 1$ for all $x \in \mathbb{Z}$. Because it is not trivial absolute value, $\exists\ |x| < 1$.

Let $I = \{x|\ |x| < 1\}$. verify I is an non-empty maximal ideal.

Therefore, $I = (p)$ as $\mathbb{Z}$ a PID.

Let $k = |p|$, we can reconstruct the absolute value for $\mathbb{Z}$, therefore, for $\mathbb{Q}$.

So, why is $\mathbb{Q}_p$ useful?

Valuation Ring, Valuation Ideals.

In $\mathbb{Q}_p$, there is a ring similar to the role of $\mathbb{Z}$ in $\mathbb{Q}$, the valuation ring.

The $\mathbb{Z}_p := \{x : |x| < 1\}$

Verify $\mathbb{Z}_p$ is a ring.

In fact, $\mathbb{Z}_p$ is a discrete valuation ring.

Therefore, it has only a unique prime/maximal ideal (the valuation ideal) $\mathfrak{M} = p\mathbb{Z}_p$.

This allows us to study one prime at a time, allowing easier way to study many questions in ANT.

This is similar to taylor/laurent expansion because it gives the local information about a prime $p \in \mathbb{Z}$.

Hensel's Lemma

$f \in \mathbb{Z}_p[X]$, $f(\alpha_1) = 0 \bmod p$, $f'(\alpha_1) \neq 0$, then there is a unique α s.t. $f(\alpha) = 0$ and $\alpha = \alpha_1 \bmod p$.

Pf.

we will construct a Cauchy sequence s.t.:

- $f(a_n) = 0 \bmod (p^n)$
- $a_{n+1} = a_n \bmod (p^n)$

$a_2 = a_1 + pb$

$f(a_2) = f(a_1 + pb) = f(a_1) + bf'(a_1)p \bmod (p^2)$ let we know $f(a_1) = px$,

so we have $x + bf'(a_1) = 0 \bmod p$

so, $b = -x(f'(a_1))^{-1}$

Applications

Hasse-Minkowski

Let

$$F(X_1, ..., X_n) = \sum c_{ij} X_i X_j$$

be a quadratic form. The equation $F = 0$ has non-trivial solutions in $\mathbb{Q}$ iff it has non-trivial solutions in $\mathbb{Q}_p$ for all $p \leq \infty$.

Local Kronecker-Webber implies Global

All Abelian extension of $\mathbb{Q}_p$ is contained in $\mathbb{Q}_p(\zeta_m)$

Implies

All Abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_m)$