p-adic functions on $\mathbb{Z}_p$. Lecture 1.

<u>Outline</u>: Introduction to p-adic numbers, $\mathbb{Z}_p$

Hensel's lemma

p-adic valuations & p-adic norms

An important philosophy in number theory

$$\begin{tikzcd}
\mathbb{Q}_2 & & \\
\mathbb{Q}_3 & \mathbb{Q} \arrow[ul, hook] \arrow[l, hook] \arrow[r, hook, "\text{completion}"] & \mathbb{R} \\
\mathbb{Q}_5 \arrow[ur, hook] & &
\end{tikzcd}$$

$\ddots$ one for each prime number p

<u>Slogan</u>: Many theories over $\mathbb{R}$ have analogues over $\mathbb{Q}_p$ & they are equally important for arithmetic applications.

* Define $\mathbb{Z}_p$

"definition of $\mathbb{Z}_p, \mathbb{Q}_p$" "definition of $[0,1)$, $\mathbb{R}$"

Example of numbers?

$2 + 3p + 4p^2 + 0\cdot p^3 + 6p^4 + \cdots$

A <u>p-adic integer</u> is an infinite formal sum with coeffs in $\{0, \cdots, p-1\}$

$0.275689\ldots\ldots$

any infinite sequence with coeffs in $\{0, \cdots, 9\}$

$= 2\cdot 10^{-1} + 7\cdot 10^{-2} + 5\cdot 10^{-3} + \cdots\cdots$

How to add two numbers?

$p=5$ $\quad (2 + 3\times 5 + 4\times 5^2 + 5^4 + \cdots)$

$\quad + (2 + 4\times 5 + 5^3 + \cdots)$

$= 4 + 7\times 5 = 5\times 5^2 = 5^3 \quad 2\cdot 5^3 + \cdots$

$2\times 5 + 5^2$

$= 4 + 2\times 5 + 2\cdot 5^3 + \cdots$

sweep terms to higher & higher p-powers

slightly different

bring terms to earlier terms

Multiplication ?

$p=5$ $\quad (2+3\times5+4\times5^2+\cdots)(2+4\times5+5^3+\cdots)$

$14\times5 \to 2\times5^2$ $\quad 22\times5^2 \to 4\times5^3$

2 $\quad 4 + 6\times5 + 8\times5^2$

4×5 $\quad + 8\times5 \quad 12\times5^2$

5^3 $\quad + 0 \quad +$

2×5^3

Simplify $= 4 + 4\times5 + 2\times5^2 + \cdots$

Another point of view:

A p-adic integer is the collection of

$$(a_1 \bmod p,\ a_2 \bmod p^2,\ a_3 \bmod p^3,\ \cdots)$$

$$\text{s.t. } a_{n+1} \equiv a_n \bmod p^n$$

e.g. $p=5$ the 5-adic integer $2+3\times5+4\times5^2+1\times5^3$

$$2 \bmod 5,\ 17 \bmod 5^2,\ 117 \bmod 5^3,\ \cdots$$

Addition from this point of view:

$$(a_n \bmod p^n)_n + (b_n \bmod p^n)_n = (a_n + b_n \bmod p^n)$$

Hiding behind this is:

$$2+3\times5+4\times5^2+\cdots \to (2 \bmod 5,\ 17 \bmod 25,\ 117 \bmod 5^3,\ \cdots)$$

$$+\ 2+4\times5+5^2+\cdots \to (2 \bmod 5,\ 22 \bmod 25,\ 45 \bmod 5^3,\ \cdots)$$

$$+)$$

$$(4 \bmod 5,\ \underbrace{39 \bmod 25}_{\substack{\parallel \\ 14 \bmod 25}},\ \underbrace{162 \bmod 5^3}_{\substack{\parallel \\ 39 \bmod 5^3}},\ \cdots$$

This was the sweeping step earlier.

Theorem: If a is an integer relatively prime to p, then a is invertible in $\mathbb{Z}_p$

Example: This amounts to proving e.g. $p=7$ solve $10x=1$ in $\mathbb{Z}_7$.

Instead of proving this, we prove something much cooler

e.g. $p=7$ solve $x^2=2$ in $\mathbb{Z}_7$.

<u>Step 1</u>: Solve $x^2 \equiv 2 \mod 7$.

Fix this $\longrightarrow$ $\boxed{x \equiv 3}$ or $x \equiv 4 \mod 7$.

<u>Step 2</u>: Solve $x^2 \equiv 2 \mod 7^2$

Write $x = 3 + 7a$

$$(3+7a)^2 \equiv 2 \mod 7^2$$

$$9 + 42a + \cancel{49a^2} \equiv 2 \mod 49$$

$$7 + 42a \equiv 0 \mod 49$$

$$1 + 6a \equiv 0 \mod 7 \quad \Rightarrow a \equiv 1 \mod 7$$

So $x \equiv 10 \mod 7^2$

Step 3. Solve $x^2 \equiv 2 \mod 7^{3=343}$

Write $x = 10 + 49b$

$$(10+49b)^2 \equiv 2 \mod 7^3$$

$$\parallel$$

$$100 + 980b + \cancel{7^4 b^2}$$

$$98 + 980b \equiv 0 \mod 7^3 \quad \ldots\ldots$$

Continuing this way, we get $3 \bmod 7$, $10 \bmod 7^2$, $108 \bmod 7^3$, ...

This gives a sol'n of $x^2=2$ in $\mathbb{Z}_7$.

(the other sol'n is the negative of this.)

<u>Hensel's lemma</u>: Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$ be a monic polynomial.

Assume that $f(x) \bmod p \in \mathbb{F}_p[x]$ has a <u>simple</u> zero $\alpha \in \mathbb{F}_p$.

Then there <u>exists</u> a <u>unique</u> zero $\tilde{\alpha} \in \mathbb{Z}_p$ of $f(x)$ s.t. $\tilde{\alpha} \bmod p = \alpha$.

(In our earlier example, $f(x) = x^2 - 2$

& $f(x) \bmod 7$ has a simple zero $\alpha = 3$, i.e. $3^2 - 2 = 7 \equiv 0 \mod 7$

then we got a sol'n $\tilde{\alpha} \in \mathbb{Z}_7$ s.t. $\tilde{\alpha} \bmod 7 = 3$.)

Non-example: $f(x) = x^2 - 5$ with $p=5$. $f(x)$ mod 5 has a double zero at $x=0$ in $\mathbb{F}_5$

But $f(x) = x^2-5$ has no zero in $\mathbb{Z}_5$, see later

Corollary: Consider $f(x) = x^{p-1} - 1$.

Modulo p, it has precisely $p-1$ zeros: $1, 2, \cdots, p-1$.

(by Fermat's little thm: $a^{p-1} \equiv 1 \bmod p \quad \forall p \nmid a$

or $(\mathbb{Z}/p\mathbb{Z})^\times$ has order $p-1$ so $a^{p-1} \equiv 1 \bmod p$ by Lagrange thm.)

By Hensel's lemma, for each $a \in \{1, 2, \cdots, p-1\}$, there exists a unique $\tilde{a} \in \mathbb{Z}_p$

s.t. $\tilde{a} \equiv a \bmod p$ & $\tilde{a}^{p-1} = 1$.

In other words, $\mathbb{Z}_p$ contains all $(p-1)^{st}$ roots of unity.

Remark: If one spells out the proof of Hensel's lemma,

this amounts to solving $x^{p-1} = 1$ modulo higher & higher power of p.

E.g $p=7$. $x^6 \equiv 1 \bmod 7^3$ has sol'ns

$$
\begin{aligned}
1 &\longrightarrow 1 \\
2 &\longrightarrow 2 + 4\times 7 + 6\times 7^2 \\
3 &\longrightarrow 3 + 4\times 7 + 6\times 7^2 \\
4 &\longrightarrow 4 + 2\times 7 + 0 \\
5 &\longrightarrow 5 + 2\times 7 + 0 \\
6 &\longrightarrow 6 + 6\times 7 + 6\times 7^2
\end{aligned}
$$

This is -1 in its disguised form.

3rd way to think of $\mathbb{Z}_p$:

Think of $2 + 3p + 4p^2 + \cdots$

as limit of $\underset{=x_1}{2}, \underset{=x_2}{2+3p}, \underset{=x_3}{2+3p+4p^2}, \ldots$

as the difference between two number $x_n - x_m$ is div. by higher & higher

$0.275689\cdots$

is the limit of $\underset{=x_1}{0.2}, \underset{=x_2}{0.27}, \underset{=x_3}{0.275}, \cdots$

b/c the difference $|x_n - x_m|$ ← absolute value

with m, n large is small.

power of p

Definition: Fix p a prime number.

A <u>p-adic valuation</u> of an integer $n \in \mathbb{Z}$ is the max'l nonneg. integer $v_p(n)$ s.t. $p^{v_p(n)}$ divides n. & $v_p(0) := \infty$

E.g. $p=5$, $v_5(3)=0$, $v_5(25)=2$, $v_5(15)=1$.

The <u>p-adic norm</u> of n is $|n|_p := p^{-v_p(n)}$

E.g. $|3|_5 = 1$, $|4|_5 = 1$, $|25|_5 = \frac{1}{25}$, $|375|_5 = \frac{1}{125}$

So the more divisible by p a number is, the smaller its p-adic norm is.

Theorem. The p-adic norm defines a natural metric space structure on $\mathbb{Z}$.

i.e. for $x, y \in \mathbb{Z}$, their p-adic distance is

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

& $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to this p-adic metric.

Back to earlier example: $2 + 3p + 4p^2 + \cdots$ $(p \geq 5)$

the sequence 2, $2+3p$, $2+3p+4p^2$

$|(2+3p)-2|_p = \frac{1}{p}$ $|4p^2|_p = \frac{1}{p^2}$ ... getting smaller & smaller for the p-adic norm.

$v_p(\cdot)$, $|\cdot|_p$ extends naturally to $\mathbb{Z}_p$

e.g. $p=5$ $3\cdot 5^3 + 2\cdot 5^4 + 7\cdot 5^5 + \cdots$ has p-adic valuation 3

p-adic norm $1/p^3$

Remark: No solution of $x^2 = 5$ in $\mathbb{Z}_5$, b/c

$1 = v_5(5) = v_5(x^2) = 2\cdot v_5(x) \Rightarrow v_5(x) = \frac{1}{2}$. not possible!

Remark: For p-adic norm, $\mathbb{Z}$ is bounded! (as $v_p(n) \geq 0$ $|n|_p \leq 1$ for every n)

So our usual picture of $\mathbb{Z}$ on a line should be discarded.

Will show a picture of $\mathbb{Z}_p$ next lecture!

Also no orders on $\mathbb{Z}_p$! $\cancel{a<b}$