p-adic functions on $\mathbb{Z}_p$. Lecture 2.

Outline: Cauchy sequences in $\mathbb{Z}_p$
Topology of $\mathbb{Z}_p$.
Exponential & logarithmic functions in $\mathbb{Z}_p$
Structure of $\mathbb{Z}_p^\times$

Recall: $\mathbb{Z}_p$ = completion of $\mathbb{Z}$ with respect to the p-adic norm
if $p^\beta \| n$, then $|n|_p = \frac{1}{p^\beta}$ & $v_p(n) := \beta$

Theorem 1 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
$$d(x,y) = |x-y|_p.$$
Then $\mathbb{Z}_p$ = the completion of $\mathbb{Z}$ with respect to this p-adic metric.
(something to be proved about the metric space; later.)

Theorem 2 Every $a \in \mathbb{Z}$ s.t. $p \nmid a$ is invertible in $\mathbb{Z}_p$.
$a \in \mathbb{Z}_p$ s.t. $p \nmid a$ ($\Leftrightarrow v_p(a)=0$) $\Rightarrow a \in \mathbb{Z}_p^\times$.

Corollary: $\mathbb{Z}_p$ is a PID & has a unique maxl ideal (p).

Define: $\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p) = \mathbb{Z}_p[\frac{1}{p}]$
$= \{ \sum_{n \gg -\infty} a_n p^n , a_n \in \{0, \cdots, p-1\} \}$
$\Rightarrow \mathbb{Z}_p = \{ a \in \mathbb{Q}_p , v_p(a) \geq 0 \}$ $\Leftrightarrow |a|_p \leq 1$.
As $\mathbb{Z} \subseteq \mathbb{Z}_p$, $\mathbb{Q} \subseteq \mathbb{Q}_p$.

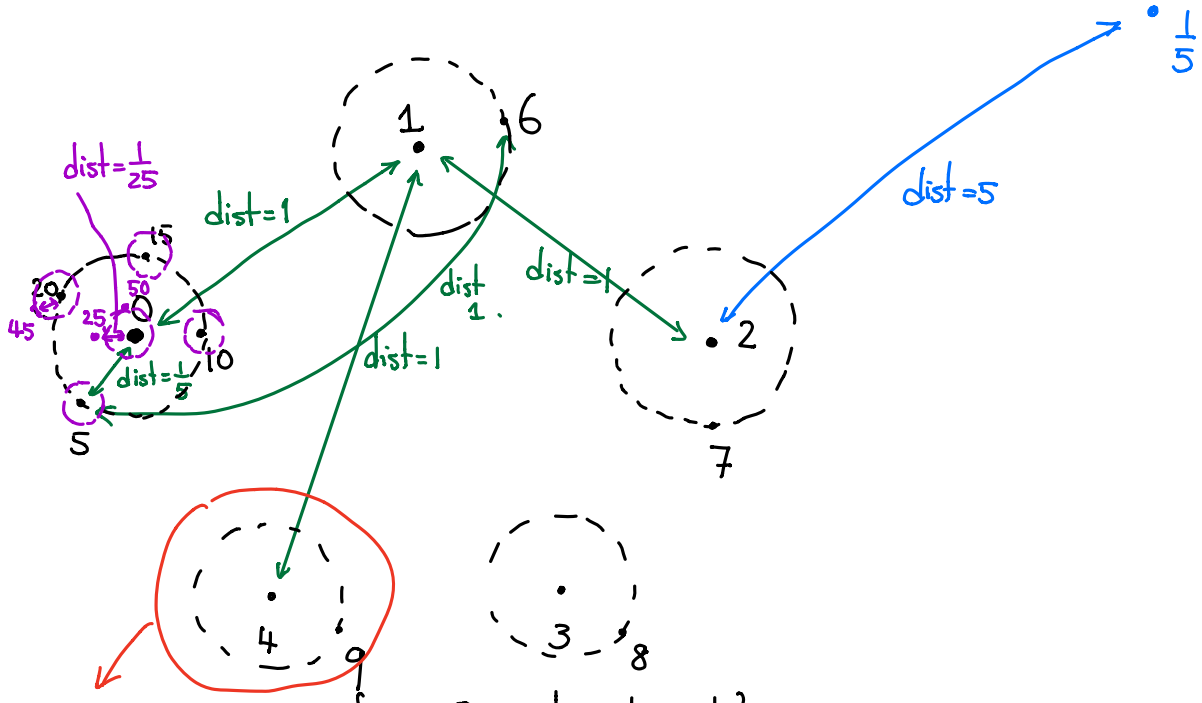
Obvious fact: $v_p(n \cdot m) = v_p(n) + v_p(m)$. & $|nm|_p = |n|_p \cdot |m|_p$ for $n, m \in \mathbb{Z}$ & $\mathbb{Z}_p$

Can extend this definition to $\mathbb{Q}$ & $\mathbb{Q}_p$
$v_p(\frac{a}{b}) := v_p(a) - v_p(b)$, e.g. $p=5$, $v_p(\frac{25}{3}) = 2$, $v_p(\frac{7}{15}) = -1$
& $|\frac{a}{b}|_p = p^{-v_p(\frac{a}{b})}$ $|\frac{25}{3}|_5 = \frac{1}{25}$, $|\frac{7}{15}|_5 = 5$.

Cor: $\mathbb{Q}_p$ = completion of $\mathbb{Q}$ w.r.t. the p-adic norm.

What does $\mathbb{Z}_p$ or $\mathbb{Q}_p$ look like?

$p=5$



Remark: $4+5\mathbb{Z}_5 = 9+5\mathbb{Z}_5 = \{a \in \mathbb{Q}_5,\ |a-4|_5 \le \frac{1}{5}\}$

Proof: $9+5\mathbb{Z}_5 = 4+5+5\mathbb{Z}_5 = 4+5\mathbb{Z}_5$.

- For $a \in \mathbb{Q}_5$, $|a-4|_5 \le \frac{1}{5} \iff v_5(a-4) \ge 1$.

$\iff v_5\left(\frac{a-4}{5}\right) \ge 0 \iff \frac{a-4}{5} \in \mathbb{Z}_5 \iff a \in 4+5\mathbb{Z}_5$.

Topology: each disk above is open: a subset $a+p^n\mathbb{Z}_p$ (for $a \in \mathbb{Z}_p$) is an open & closed subset of $\mathbb{Q}_p$.

So $\mathbb{Q}_p$ and $\mathbb{Z}_p$ are very very disconnected!

Fact: $\mathbb{Z}_p$ is compact. (and Hausdorff).

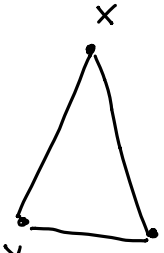
Proof of the $\mathbb{Z}_p$-version of Theorem 1.

Need to check: $\begin{cases} d(x,y)=0 \iff x=y. & \checkmark \\ d(x,z) \le d(x,y)+d(y,z) & \text{(triangle inequality)} \end{cases}$

In fact, we have a stronger triangle inequality:

$$d(x,z) \le \max\{d(x,y), d(y,z)\}$$

$$\left(\iff |x-z|_p \le \max\{|x-y|_p, |y-z|_p\}\right)$$



Setting $a = x-y$, $b = y-z$

$(\Leftrightarrow \quad |a+b|_p \le \max\{|a|_p, |b|_p\}$ ⇔ b/c $|\cdot|_p = p^{-v_p(\cdot)}$ order reversing

Claim: $v_p(a+b) \ge \min\{v_p(a), v_p(b)\}$

Pf: WLOG, $v_p(a) \ge v_p(b)$

then $p^{v_p(b)} \mid b$ & $p^{v_p(b)} \mid p^{v_p(a)} \mid a$

$\Rightarrow p^{v_p(b)} \mid a+b \Rightarrow v_p(a+b) \ge v_p(b)$ □.

This is just a fancy way to say

$p^n \mid a$ & $p^n \mid b \Rightarrow p^n \mid a+b$

Also $p^n \| a$ & $p^{n+1} \mid b \Rightarrow p^n \| a+b$

↳ if $|x-y|_p > |y-z|_p$ then $|x-z|_p = |x-y|_p$

All triangles in p-adic world are isoceles.

Corollary of the stronger triangle inequality:

An infinite sum $x_1 + x_2 + \cdots$ with $x_i \in \mathbb{Z}_p$ (absolutely) converges in $\mathbb{Z}_p$

if $\lim_{n\to\infty} |x_n|_p = 0$ ← analogue of Cauchy criterion

Compare to the real story: need $\lim_{n,m\to\infty} |x_n + \cdots + x_m| = 0$

i.e. $\forall \varepsilon > 0$, $\exists N > 0$ s.t. for any $m \ge n \ge N$, $|x_n + \cdots + x_m| < \varepsilon$.

"Proof": For any $\varepsilon > 0$, $\exists N > 0$ s.t. for any $n \ge N$, we have $|x_n|_p < \varepsilon$.

Then for any $m \ge n \ge N$,

$$|x_n + \cdots + x_m|_p \le \max\{|x_n|_p, |x_{n+1}|_p, \cdots, |x_m|_p\} < \varepsilon.$$

↑ stronger inequality

Slogan: Sequences are easier to converge in p-adic topology

Example: $\exp(p)$ makes sense in $\mathbb{Z}_p$ $\boxed{p \ge 3}$

In the real world, $e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$ Taylor expansion

- $\exp(p) = 1 + p + \frac{p^2}{2!} + \frac{p^3}{3!} + \cdots$

$\exp(p) = 1 + p + \frac{p^2}{2!} + \frac{p^3}{3!} + \cdots$

n^{th} term is $p^n/n!$

div. by p exactly n times

$v_p\left(p^n/n!\right) = n - \lfloor \frac{n}{p} \rfloor - \lfloor \frac{n}{p^2} \rfloor - \lfloor \frac{n}{p^3} \rfloor \cdots$

$\geq n - \frac{n}{p} - \frac{n}{p^2} - \cdots$

$= n - \frac{n}{p-1} \to \infty$ as $n \to \infty$

$n! = 1 \cdot \cdots \cdot n$

$\lfloor \frac{n}{p} \rfloor$ times the # is div by p

$\lfloor \frac{n}{p^2} \rfloor$ times the # is div by p^2 ....

So $\left| p^n/n! \right|_p \to 0$

So this infinite series converges.

Similarly, $\exp(p \cdot a) = 1 + pa + \frac{(pa)^2}{2!} + \cdots$ makes sense

Moreover, as formally $\exp(x+y) = 1 + (x+y) + \frac{(x+y)^2}{2!} + \cdots$

$\exp(x) \cdot \exp(y) = \left(1 + x + \frac{x^2}{2!} + \cdots\right)\left(1 + y + \frac{y^2}{2} + \cdots\right)$

So $\exp(p(a+b)) = \exp(pa) \cdot \exp(pb)$

Theorem. When $p \geq 3$. $(p\mathbb{Z}_p, +) \xrightarrow{\exp(x)} (1 + p\mathbb{Z}_p, \cdot)$ is a ~~homomorphism~~ an isomorphism

$p\mathbb{Z}_p = \{pa \,;\, a \in \mathbb{Z}_p\}$

$\log(x)$

$\log(1+pa) := pa - \frac{(pa)^2}{2} + \frac{(pa)^3}{3} - \cdots$

↑ by same argument, this converges as well.

Theorem. When $p \geq 3$, $(\mathbb{Z}_p^\times, \cdot) \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p)^\times \xrightarrow[\cong]{id \times \frac{1}{p}\log(x)} (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}_p, +)$

$\mathbb{Z}_p^\times = \{a \in \mathbb{Z}_p, p \nmid a\}$

Proof **Recall**: $x^{p-1} = 1$ has solns in $\mathbb{Z}_p^\times$

so $\mathbb{Z}_p^\times$ contains $(p-1)^{st}$ root of unity

This gives a map $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mu_{p-1} \longrightarrow \mathbb{Z}_p^\times$

$a \longmapsto [a]$ ← called Teichmüller lift.

By the uniqueness of the lift, $[ab] = [a] \cdot [b]$.

On the other hand, we have $\mathbb{Z}_p^\times \xrightarrow{\bmod p} (\mathbb{Z}/p\mathbb{Z})^\times$

Now, we can define the isomorphism.

$$\mathbb{Z}_p^\times \xrightarrow{\cong} (\mathbb{Z}/p\mathbb{Z})^\times \times (1+p\mathbb{Z}_p)^\times$$

$$[\bar{a}] \cdot (1+pb) \longleftarrow (\bar{a}, 1+pb)$$

$$c \longmapsto (c \bmod p, \; x)$$

x is so that $x \cdot [c \bmod p] = c \Rightarrow x = \dfrac{c}{[c \bmod p]}$

Example $p=7$ $\quad \mathbb{Z}_7^\times \longrightarrow (\mathbb{Z}/7\mathbb{Z})^\times \times (1+7\mathbb{Z}_7)^\times$

$$10 \longmapsto \left(\begin{matrix} \bmod 7 \\ \| \\ 3 \bmod 7 \end{matrix}, \; \frac{10}{[3]} \right)$$

Recall $[3] = 3 + 4 \cdot 7 + 6 \cdot 7^2 + \cdots$

or rather as $3 \cdot 5 \equiv 1 \bmod 7$, so. $[3]^{-1} = [5]$

$[5] = 5 + 2 \cdot 7 + 3 \cdot 7^3 + \cdots$

So $\dfrac{10}{[3]} = 10 \cdot (5 + 2 \cdot 7 + 3 \cdot 7^3 + \cdots)$