2021

Arizona Winter School

p-adic Lecture 3: Topolalgebra

Background: Samuel Velasco

3.1: Keeping the Ball Rolling $\equiv 0$

- Last time, we defined

$$\mathbb{Q}_p := \text{the completion of } \mathbb{Q} \text{ wrt } |\cdot|_p$$

$$= \text{Cauchy sequences of rational \#s / equivalence}$$

- $|\cdot|_p$ extends to $\mathbb{Q}_p$ via

$$|(x_n)_{n\in\mathbb{N}}| := \lim_{n\to\infty} |x_n|$$

- Example: for $|\cdot|_\infty$, $-\sqrt{2}$ is the limit of

$$-1,\ -1.4,\ -1.41,\ -1.414,\ \ldots$$

so $|-\sqrt{2}|_\infty$ is the limit of

$$|-1|_\infty,\ |-1.4|_\infty,\ |-1.41|_\infty,\ |-1.414|_\infty,\ \ldots$$

$$\parallel$$

$$1,\ \ 1.4,\ \ 1.41,\ \ 1.414,\ \ldots$$

so $|-\sqrt{2}|_\infty = \sqrt{2}$.

- In Lecture 1, we computed <u>a</u> square root of 2, x, in $\mathbb{Q}_7$. We calculate $|x|_7$:

$$|x|_7 = |3 + 1\cdot 7 + 2\cdot 7^2 + 3\cdot 7^3 + \ldots|$$

$$= \lim\ |3|_7,\ |3+1\cdot 7|_7,\ |3+1\cdot 7+2\cdot 7^2|_7,\ |3+1\cdot 7+2\cdot 7^2+3\cdot 7^3|_7, \ldots$$

$$= \lim\ 1,\ \ 1,\ \ 1,\ \ 1,\ \ \ldots$$

$$= 1.$$

- We have only seen powers of p occur as abs. vals of elts of $\mathbb{Q}_p$. $|p^n| = p^{-n}$ $\forall n \in \mathbb{Z}$, so all powers of p occur. And if $r \in \mathbb{R}_{>0}$ is <u>not</u> a power of p, $\exists i: p^i < r < p^{i+1}$, so r

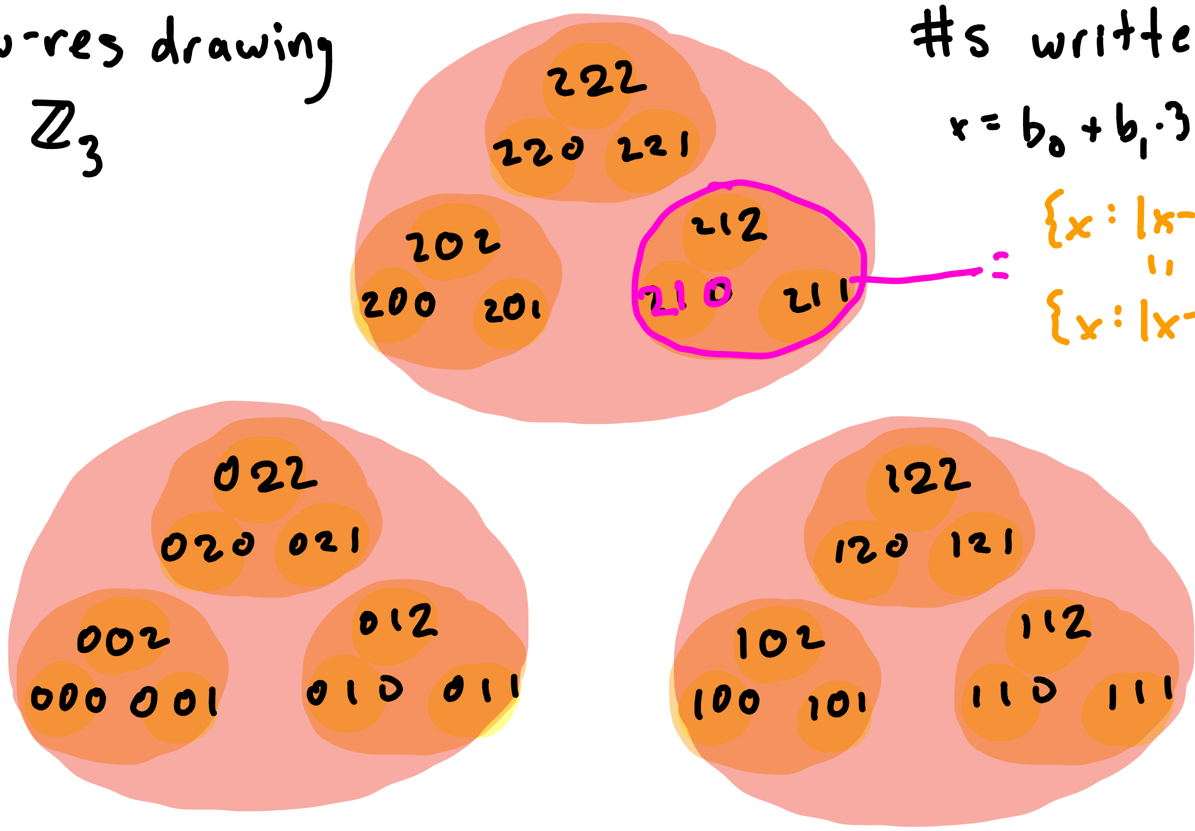
cannot occur as a limit of $|x_n|_p$ with $x_n \in \mathbb{Q}$. Hence,

Proposition 3.1

$$\{ |x|_p : x \in \mathbb{Q}_p \} = \{ p^n : n \in \mathbb{Z} \} \cup \{0\}$$

- This implies that $B(x, p^n) = B_{cl}(x, p^{n-1})$ $\forall n \in \mathbb{Z}$!

Low-res drawing of $\mathbb{Z}_3$



#s written $b_0 b_1 b_2$:

$x = b_0 + b_1 \cdot 3 + b_2 \cdot 3^2$

$= \{x : |x-5| \le \frac{1}{27}\}$

$\shortparallel$

$\{x : |x-5| < \frac{1}{81}\}$

- We can give a new def. of $\mathbb{Z}_p$ as a ball!

Definition:

$$\mathbb{Z}_p := \{ x \in \mathbb{Q}_p : |x|_p \le 1 \}$$

Examples:

- $\sqrt{2} \in \mathbb{Z}_7$ since $|\sqrt{2}|_7 = 1$
- $1/3 \in \mathbb{Z}_5$ since $|1/3|_5 = 1$ $\Bigg\}$ lecture 1
- $\sqrt{-1} \in \mathbb{Z}_7$ since $|\sqrt{-1}|_7 = 1$
- $p \in \mathbb{Z}_p$ since $|p|_p = \frac{1}{p}$
- $1/p \notin \mathbb{Z}_p$ since $|1/p|_p = p$

3.2 Wearing Many Hats

- We will now unveil $\widehat{\mathbb{Q}}_p$! We first need some topological results.

Theorem 3.3

i) $\mathbb{Q}$ is dense in $\widehat{\mathbb{Q}}_p$

ii) $\mathbb{Z}$ is dense in $\widehat{\mathbb{Z}}_p$

iii) Every element of $\widehat{\mathbb{Z}}_p$ can be written <u>uniquely</u> in the form

$$b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots \quad \text{with } b_i \in \{0, 1, \dots, p-1\} \ \forall i$$

and every such series represents an elt. of $\widehat{\mathbb{Z}}_p$.

That is, $\widehat{\mathbb{Z}}_p = \mathbb{Z}_p$

iv) Every element of $\widehat{\mathbb{Q}}_p$ can be written <u>uniquely</u> in the form

$b_{n_0} + b_{n_0+1} p^{n_0+1} + b_{n_0+2} p^{n_0+2} + \dots$ with $b_i \in \{0, 1, \dots, p-1\}\ \forall i$
for some $n_0 \in \mathbb{Z}$,
and every such series represents an elt. of $\widehat{\mathbb{Q}}_p$
That is, $\widehat{\mathbb{Q}}_p = \mathbb{Q}_p$

Note: different from $\mathbb{R}$! In $\mathbb{R}$,

i ....

ii . . . .

iii, iv : $.9999\ldots = 1.000\ldots$ not unique!

Proof:

i: - $\mathbb{Q} \hookrightarrow \widehat{\mathbb{Q}}_p$ via $a \mapsto a, a, a, a, a, \dots$

WTS if $x \in \widehat{\mathbb{Q}}_p$, $\forall \varepsilon > 0$, $\exists a \in \mathbb{Q} : |x - a|_p < \varepsilon$.

- $x = (x_n)_{n \in \mathbb{N}}$ is Cauchy. Then
$\exists N : |x_n - x_m| < \varepsilon$ for all $n, m > N$

- Let $a = x_N$. Then
$$|x - a| = \lim_{n \to \infty} |x_n - x_N| < \varepsilon.$$

ii: Exercise.

iii: Let $x \in \widehat{\mathbb{Z}}_p$. Let $n \geq 0$

By ii, $\exists a \in \mathbb{Z} : |x - a| \leq p^{n+1}$.

Let $b \in \mathbb{Z}$. We have $|x - a + b| = \max\{|x-a|, |b|\}$ if $|b| > p^{n+1}$

so $|x - a + b| \leq p^{n+1}$ iff $|b| \leq p^{n+1}$ iff $p^{n+1} \mid b$

Hence, a is unique mod p^{n+1}

Let $a_n = a \bmod p^{n+1}$. Then $\lim_{n \to \infty} a_n = x$ and

decomposing $a_n = \sum_n b_i p^i$ gives the series.

iv: Let $x \in \mathbb{Q}_p$, and suppose $|x| = p^{-m}$. Then $p^m x \in \mathbb{Z}_p$, apply iii.

Proposition 3.4 $|\cdot|_p$ of a series

For $x \in \mathbb{Q}_p$: $x = \sum_{i=n_0}^{\infty} b_i p^i$ with $b_{n_0} \neq 0$ (so n_0 is the lowest power of p with a nonzero coefficient), $|x|_p = p^{-n_0}$.

Proof: Induction on partial sums.

$$\begin{aligned} |b_{n_0} p^{n_0} + b_{n_0+1} p^{n_0+1} + \dots + b_k p^k|_p &= \max\{|b_{n_0} p^{n_0}|_p, |b_{n_0+1} p^{n_0+1} + \dots + b_k p^k|_p\} \\ &= \max\{p^{-n_0}, p^{-n_0-1}\} \\ &= p^{-n_0} \end{aligned}$$

So $|x|_p = \lim_k |b_{n_0} p^{n_0} + b_{n_0+1} p^{n_0+1} + \dots + b_k p^k|_p = p^{-n_0}$ $\square$

Examples:

- $|2 \cdot 3^{-2} + 3^{-1} + 0 + 1 \cdot 3^1 + \dots|_3 = 3^2$
- $|4 \cdot 5^3 + 2 \cdot 5^4 + 3 \cdot 5^5 + \dots|_5 = 5^{-3}$

3.3 A More Algebraic Viewpoint

- For $n \in \mathbb{Z}$, let

Def(/prop)

$$\boxed{\begin{aligned} p^n\mathbb{Z}_p &:= \{x\in\mathbb{Q}_p : x = p^n y \text{ for some } y\in\mathbb{Z}_p\} \\ &= \{b_n p^n + b_{n+1}p^{n+1} + \dots : b_i\in\{0,1,\dots,p-1\}\}\end{aligned}}$$

Ex:

$3^{-1}\mathbb{Z}_3 \ni 2\cdot 3^{-1} + 1 + 0\cdot 3 + 2\cdot 3^2 + \dots$

$5^2\mathbb{Z}_5 \ni 4\cdot 5^2 + 1\cdot 5^3 + 3\cdot 5^4 + \dots$

- If $n\geq 0$, $p^n\mathbb{Z}_p$ is an ideal of $\mathbb{Z}_p$.
- By prop 3.4, $p^n\mathbb{Z}_p = B_{cl}(0, p^{-n})$ for all $n\in\mathbb{Z}$!

Prop 3.5 Algebraic Criterion for closeness in $\mathbb{Q}_p$

$b_i(x) = b_i(y)$ for $i < p^n$ (series agreement)

$$\begin{tikzcd}[column sep=small] & b_i(x)=b_i(y) \text{ for } i<p^n \arrow[dl, Leftrightarrow] \arrow[dr, Leftrightarrow] & \\ \lvert x-y\rvert \leq p^{-n} \arrow[rr, Leftrightarrow] \arrow[d, Leftrightarrow] & & x-y\in p^n\mathbb{Z}_p \\ x\in B_{cl}(y, p^{-n}) & & \end{tikzcd}$$

Example: $x := \sqrt{2}$ in $\mathbb{Q}_7$, $x = 3 + 1\cdot 7 + 2\cdot 7^2 + 6\cdot 7^3 + \dots$

let $y := 3 + 1\cdot 7 + 2\cdot 7^2 + 1\cdot 7^3$.

$x = 3 + 1\cdot 7 + 2\cdot 7^2 + 6\cdot 7^3 + \dots$

$y := 3 + 1\cdot 7 + 2\cdot 7^2 + 1\cdot 7^3$

$|x-y|_7 \le \frac{1}{7^3}$

$\Updownarrow$

$x \in B_{cl}(y, \frac{1}{7^3})$

$x-y \in 7^3\mathbb{Z}_7$

- Let $x = \sum_{i=0}^{\infty} b_i p^i \in \mathbb{Z}_p$, series expansion. Let $a_n = \sum_{i=0}^{n} b_i p^i$. Let $n \in \mathbb{N}$. Then

$$x = \left(\sum_{i=0}^{n} b_i p^i\right) + b_{n+1} p^{n+1} + \cdots$$

$$x - a_n = b_{n+1} p^{n+1} + b_{n+2} p^{n+2} + \cdots$$

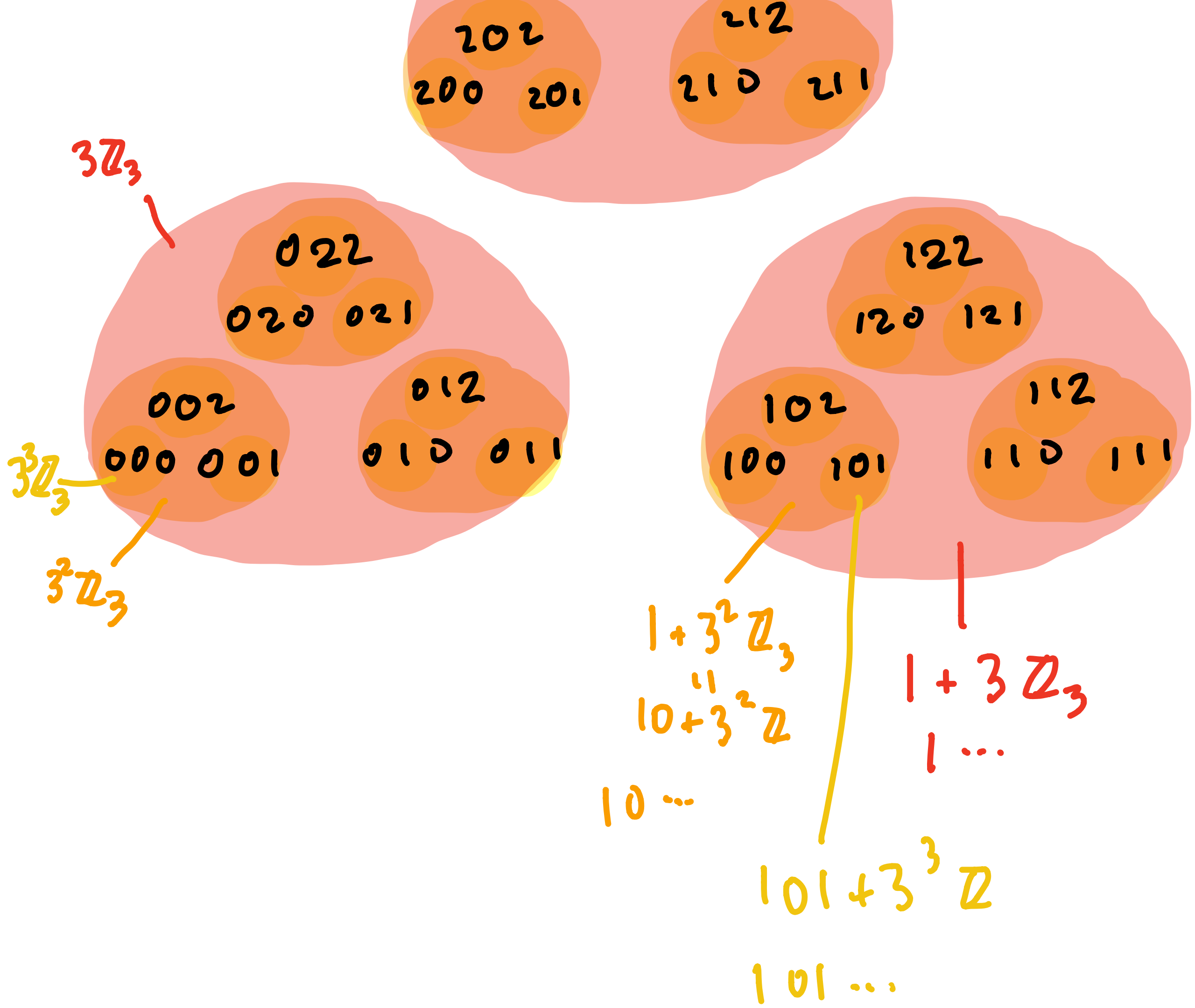
$x \in B_{cl}(a_n, p^{-(n+1)})$

$x - a_n \in p^{n+1}\mathbb{Z}_p$

- $x \notin B_{cl}(a, p^{-(n+1)})$ for any other $0 \le a < p^{n+1}$. Hence

$$\boxed{\text{Prop 3.6: Disjoint balls \& cosets. Let } n \in \mathbb{N}. \quad \mathbb{Z}_p = \bigsqcup_{a=0}^{p^n-1} B_{cl}(a, p^{-n}) = \bigsqcup_{a=0}^{p^n-1} (a + p^n\mathbb{Z}_p)}$$

-  $-1 = 2222\cdots$

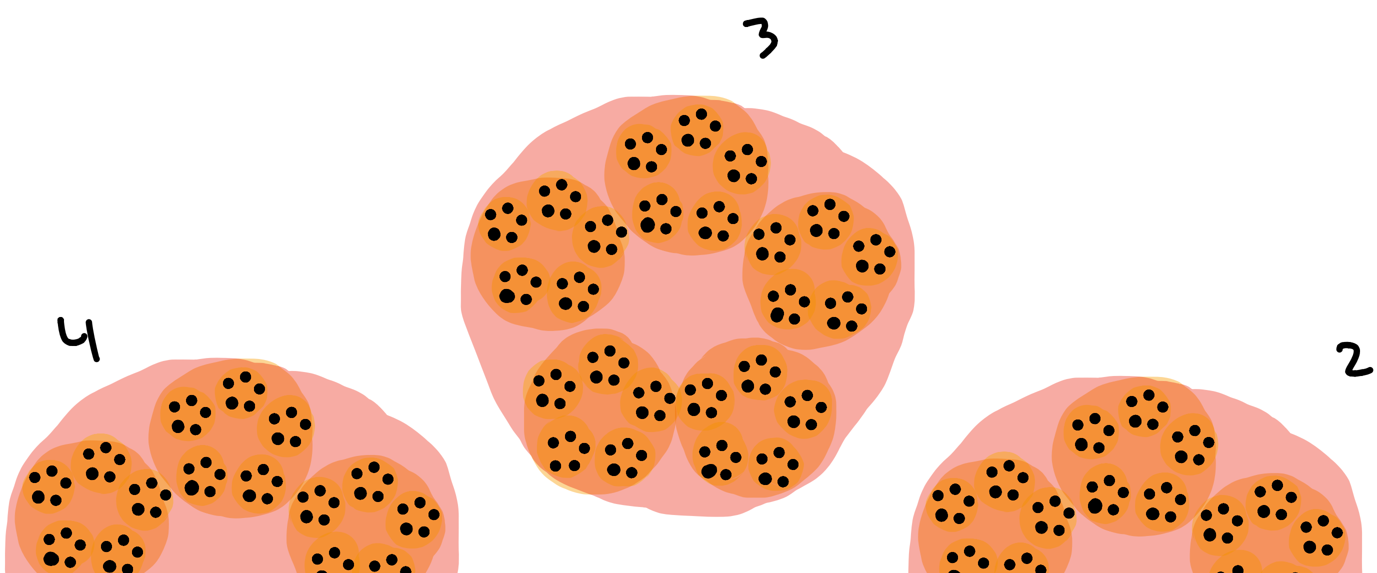


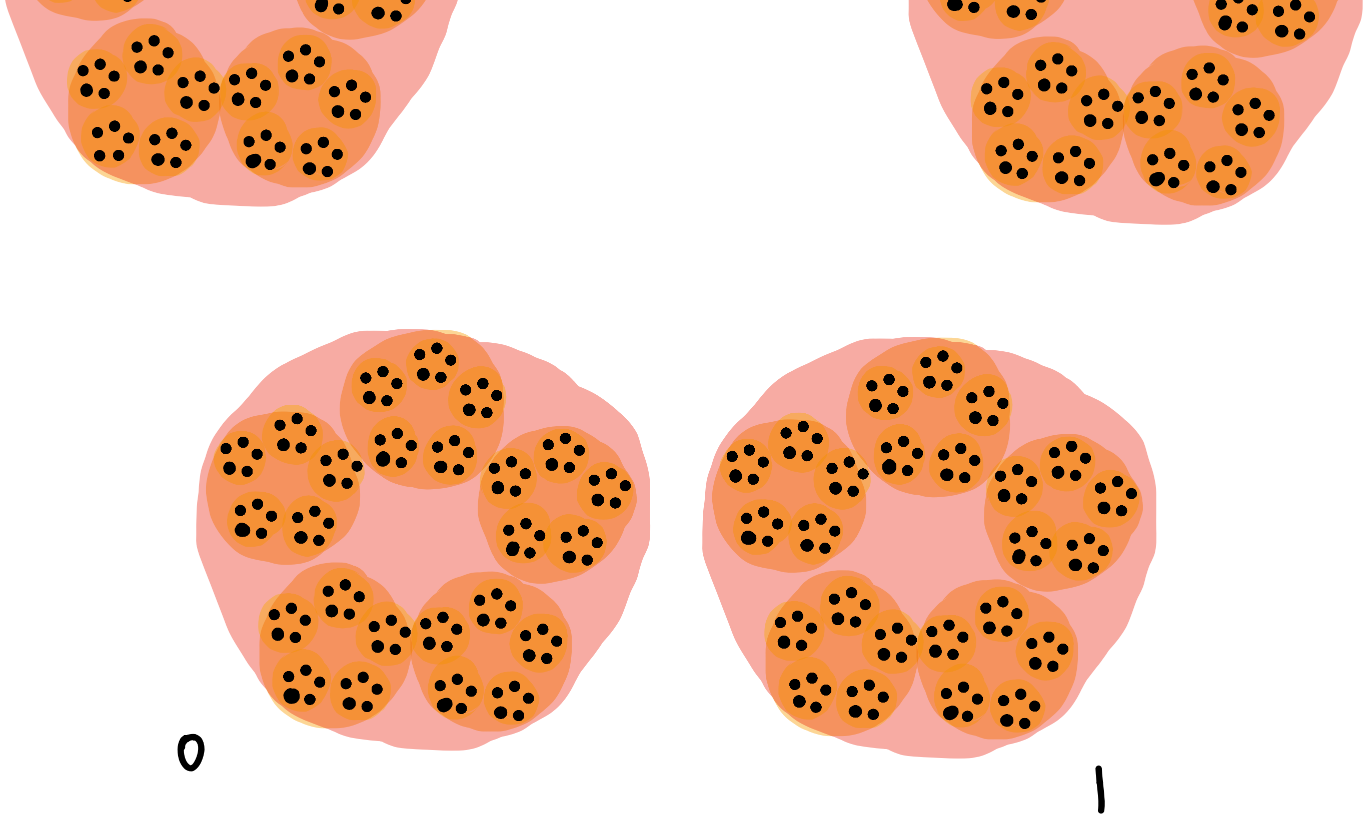
- $\sqrt{-1}$ in $\mathbb{Q}_5$

$a_0 = 3$

$a_1 = 3 + 3\cdot 5$

$a_2 = 3 + 3\cdot 5 + 2\cdot 5^2$





- For $n \in \mathbb{N}$, we define a map

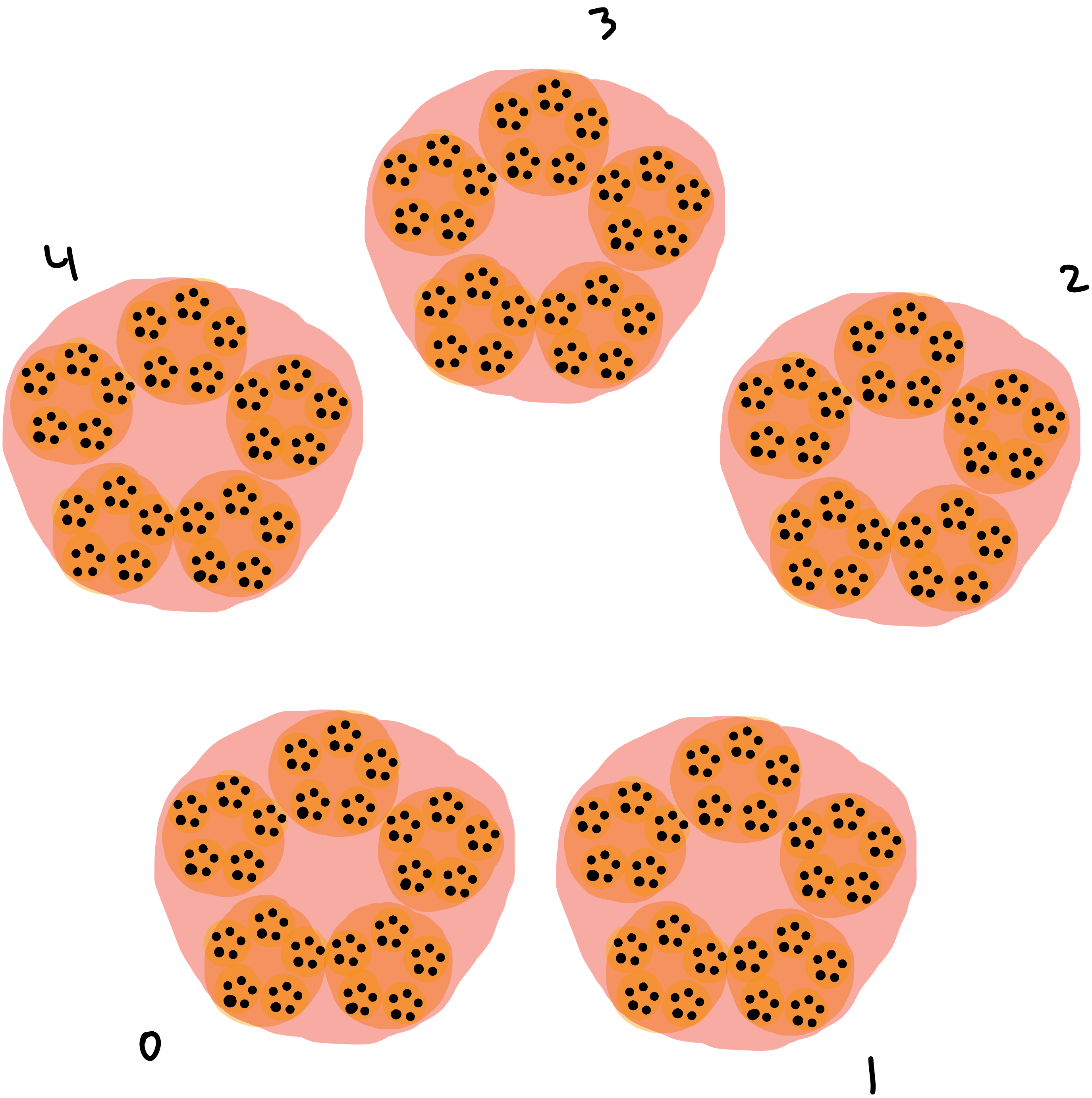
$$\boxed{\begin{aligned} \pi_n : \mathbb{Z}_p &\longrightarrow \mathbb{Z}/p^{n+1}\mathbb{Z} \\ x = \sum_{i=0}^{\infty} b_i p^i &\longmapsto \overline{\sum_{i=0}^{n} b_i p^i} \mod p^{n+1} \end{aligned}}$$

- π_n is surjective, and for $\bar{a} \in \mathbb{Z}/p^{n+1}\mathbb{Z}$,

$$\pi_n^{-1}(\bar{a}) = a + p^{n+1}\mathbb{Z}_p$$
$$= B_{<1}(a, p^{-(n+1)})$$

- Arithmetic with balls: for $a, b \in \mathbb{Z}_p$,

$$(a + p^n\mathbb{Z}_p) + (b + p^n\mathbb{Z}_p) = (a+b) + p^n\mathbb{Z}_p$$
$$(a + p^n\mathbb{Z}_p) \cdot (b + p^n\mathbb{Z}_p) = (a \cdot b) + p^n\mathbb{Z}_p$$



- π_n is a surjective ring homomorphism.
- $\ker \pi_n = p^{n+1}\mathbb{Z}_p$, so π_n is not injective. But $x \neq y \in \mathbb{Z}_p$ map to different elements under π_n for n large enough. So piecing together compatible elts of $\mathbb{Z}/p^n\mathbb{Z}$ "recovers" $\mathbb{Z}_p$.

Definition:

The **inverse limit** of the system $(\mathbb{Z}/p^n\mathbb{Z})_{n>0}$ is the ring

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} := \{ (\bar{a}_n)_{n>0} : \bar{a}_n \in \mathbb{Z}/p^n\mathbb{Z} \text{ and } \bar{a}_n \equiv \bar{a}_{n+1} \bmod p^n \ \forall n \}$$

where
$$(\bar{a}_n) + (\bar{\alpha}_n) := (\overline{a_n + \alpha_n})$$
$$(\bar{a}_n) \cdot (\bar{\alpha}_n) := (\overline{a_n \cdot \alpha_n})$$

Note: $k[[x]] = \varprojlim k[x]/x^n$

Theorem 3.8
The map
$$\pi : \mathbb{Z}_p \longrightarrow \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$
$$x \longmapsto (\pi_n(x))_n$$
is an isomorphism of rings.

3.4 The Incarnations of $x \in \mathbb{Z}_p$

$\boxed{\text{Series Expansion}}$

$b_0 + b_1 p + b_2 p^2 + \dots$

$b_i \in \{0, 1, \dots, p-1\}$

$a_n := \sum_{i=0}^{n} b_i p^i$

expand a_i out in p-ary

?

$a_n := \sum_{i=0}^{n} b_i p^i$

$x \in \mathbb{Z}_p$

$a_0, a_1, a_2, \dots$

$a_i \in \{0, 1, \dots, p^{i+1}-1\}$

$(a_i)_{i \in \mathbb{N}}$ cauchy wrt $|\cdot|_p$

$\bar{a}_0, \bar{a}_1, \bar{a}_2, \dots$

$\bar{a}_i \in \mathbb{Z}/p^{i+1}\mathbb{Z}$

$\bar{a}_i \equiv \bar{a}_{i+1} \pmod{p^{i+1}}$

$$\text{Cauchy seq. of Approximations} \underset{\text{Pick rep in } \{0,\dots,p^{i+1}-1\}}{\overset{a_i \mapsto \bar{a}_i \bmod p^{i+1}}{\rightleftarrows}} \text{Residues mod } p^n$$

Notes:

- Mult., addition of series $\sum b_i p^i$ is done with carrying, not componentwise
- Mult., addition of residue sequences is done componentwise:

$$(\bar{a}_0, \bar{a}_1, \bar{a}_2, \dots) \cdot (\bar{\alpha}_0, \bar{\alpha}_1, \bar{\alpha}_2, \dots) = (\overline{a_0\alpha_0}, \overline{a_1\alpha_1}, \overline{a_2\alpha_2}, \dots)$$

$$1 + 0\cdot p + 0 \cdot p^2 + \cdots$$

$$1 \in \mathbb{Z}_p$$

$$1, 1, 1, \dots \qquad \bar{1}, \bar{1}, \bar{1}, \dots$$

$$4+4\cdot 5+4\cdot 5^2+\cdots$$

$$-1\in\mathbb{Z}_5$$

$4, 24, 124, \ldots$ $\qquad$ $\overline{-1}, \overline{-1}, \overline{-1}, \ldots$

- In $\mathbb{Z}_5$, $(-1)+1$

$$= (4+4\cdot 5+4\cdot 5^2+\cdots)+(1+0+\cdots)$$

$$= (\overline{-1},\overline{-1},\overline{-1},\overline{-1},\ldots)+(\overline{1},\overline{1},\overline{1},\ldots)$$

$$= (\overline{0},\overline{0},\overline{0},\overline{0},\ldots)$$

3.5 Hensel's Lemma: p-adic Newton's Method

Theorem 3.8 Hensel's Lemma

Let $F(X)=c_0+c_1X+c_2X^2+\cdots+c_mX^m$ be a polynomial with $c_i\in\mathbb{Z}_p$ $\forall i$.

Let $F'(X)=c_1+2c_2X+3c_3X^2+4c_4X^3+\cdots+mc_mX^{m-1}$.

Suppose you have $\alpha_0\in\mathbb{Z}_p : F(\alpha_0)\equiv 0 \pmod{p\mathbb{Z}_p}$

and $F'(\alpha_0) \not\equiv 0 \pmod{p\mathbb{Z}_p}$. Then $\exists!\, \alpha \in \mathbb{Z}_p$:

$$F(\alpha) = 0 \quad \text{and} \quad \alpha \equiv \alpha_0 \pmod{p\mathbb{Z}_p}$$

- That is, if we find a root of F mod p, we can "lift" it to a root of F in $\mathbb{Z}_p$!

Proof: we will generalize the method we used to find $\sqrt{2}$ in $\mathbb{Q}_7$!

- We will show $\exists!$ sequence of integers $a_0, a_1, a_2, \ldots$ s.t.

0. $a_0 := \alpha_0 \bmod p$
1. $F(a_n) \equiv 0 \pmod{p^{n+1}}$
2. $a_{n+1} \equiv a_n \pmod{p^{n+1}}$
3. $0 \leq a_n < p^{n+1}$

- Then $\alpha := \lim_{n\to\infty}(a_n)$ will be our solution. It will be a root of F since for $n \in \mathbb{N}$,

$$F(\alpha) = F(a_n + p^{n+1} \underset{\text{in } \mathbb{Z}_p}{y}) \equiv F(a_n) + 0 \pmod{p^{n+1}\mathbb{Z}_p}$$
$$\equiv 0 \bmod p^{n+1}\mathbb{Z}_p \text{ by 1.}$$

- We'll denote by $\{b_i\}_{i\in\mathbb{N}}$ the sequence of integers $b_i \in \{0, 1, \ldots, p-1\}$ (the pigits) s.t

$$a_n = \sum_{i=0}^{n} b_i p^i$$

- We solve for b_{n+1} recursively, inducting on n.

- Base case: $n=0$. We define a_0 to be the ones term of the p-adic expansion of α_0; so a_0 is the unique integer in $\{0,1,\ldots,p-1\}$ s.t. $\alpha_0 \equiv a_0 \pmod{p\mathbb{Z}_p}$. And so $F(a_0) \equiv 0 \bmod p\mathbb{Z}_p$

- Suppose a_n satisfies 1, 2, 3. We will find $b_{n+1} \in \{0,\ldots,p-1\}$ s.t. $a_{n+1} := a_n + b_{n+1} p^{n+1}$ satisfies 1, 2, 3.

- Expanding out 1, we get

$$
\begin{aligned}
F(a_{n+1}) &= F(a_n + b_{n+1} p^{n+1}) \\
&= \sum_{i=0}^{m} c_i (a_n + b_{n+1} p^{n+1})^i \\
&= \sum_{i=0}^{m} c_i \left(a_n^i + i\, a_n^{i-1} b_{n+1} p^{n+1} + \text{terms divisible by } p^{n+2} \right) \\
&= F(a_n) + b_{n+1} F'(a_n) p^{n+1} + \text{terms divisible by } p^{n+2}
\end{aligned}
$$

- By ind., $\exists\, k \in \mathbb{Z}$: $F(a_n) = k p^{n+1}$. We want:

$$0 \equiv k p^{n+1} + b_{n+1} F'(a_n) p^{n+1} \pmod{p^{n+2}}$$

$$\Updownarrow$$

$$0 \equiv k + b_{n+1} F'(a_n) \pmod{p}.$$

- Since $F'(a_n) \equiv F'(\alpha_0) \not\equiv 0 \pmod p$, $\exists$ an integer which we call $(F'(a_n))^{-1}$ s.t. $(F'(a_n))(F'(a_n)^{-1}) \equiv 1 \pmod p$

- We can then define b_{n+1} to be the unique integer in $\{0, 1, \dots, p-1\}$ s.t. $b_{n+1} \equiv -t \cdot (F'(a_n))^{-1} \pmod p$. $\boxtimes$

$\sqrt{2}$ in $\mathbb{Q}_7$? $\quad F(x) = x^2 - 2$

$$\sqrt{2} = a = b_0 + b_1 \cdot 7 + b_2 \cdot 7^2 + b_3 \cdot 7^3 + \cdots$$

Step 0:

$b_0^2 - 2 \equiv 0 \ (7)$ $\quad b_0^2 \equiv 2 \bmod 7 \rightsquigarrow$ choose $b_0 = 3$ $\quad \alpha_0 = 3$

Note: $b_0^2 = 2 + \underline{1 \cdot 7^1}$ $\quad F(b_0) = b_0^2 - 2 \equiv 0 \bmod 7$

Step 1: $F(b_0 + b_1 7) \bmod 7^2$

$(3b_1 + 3b_1 + 1)7 \equiv 0 \bmod 7^2$

$\rightsquigarrow 3b_1 + 3b_1 + 1 \equiv 0 \bmod 7$

$\rightsquigarrow 6b_1 = -1 \bmod 7 \rightsquigarrow b_1 = (-1)(-1) = 1$

- Example(s): square roots in $\mathbb{Z}_p$ when $p \neq 2$.
  - Let $n \in \mathbb{Z} : p \nmid n$. $\sqrt{n} \in \mathbb{Z}_p$?
  - $F(X) = X^2 - n$.
  - Suppose $\exists \alpha_0 \in \mathbb{Z} : \alpha_0^2 \equiv n \pmod p$, so $F(\alpha_0) \equiv 0 \bmod p$
  - Then $F'(\alpha_0) = 2\alpha \not\equiv 0 \pmod p$.
  - Hensel's lemma $\rightsquigarrow \exists \alpha \in \mathbb{Z}_p : \alpha^2 = n$.

"n is a quadratic residue mod p"

p-uppy