Radical Pi : Lines in p-adic geometry

§1. What are p-adic numbers?

- First introduced by Kurt Hensel (1861-1941)
- Motivation : $\mathbb{Z} \rightsquigarrow \mathbb{Q}$ = field of fractions (ratios in $\mathbb{Z}$ with an equiv rln. $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$.)

$\mathbb{C}[X] \rightsquigarrow \mathbb{C}(X) =$ _____ $(a,b) \sim (c,d)$ $ad - bc = 0$

= ratios of polynomials with non-zero denom

Convention : $\frac{a}{b}$ $b > 0$ & $\frac{P(x)}{Q(x)}$ $Q(x)$ monic ($Q(x) = x^n + a_{n-1}x^{n-1} + \dots$ ↳ leading coeff = 1)

Common features : $\mathbb{Z}$ & $\mathbb{C}[X]$ are rings with unique factorizations

$m = \pm p_1^{k_1} \cdots p_s^{k_s}$ $p_1, \dots p_s$ prime numbers (>0), $k_1, \dots k_s > 0$.

$P(x) = a(x-\alpha_1)^{k_1} \cdots (x-\alpha_s)^{k_s}$ $a, \alpha_1, \dots \alpha_s$ in $\mathbb{C}$, $k_1, \dots k_s > 0$.

Primes in $\mathbb{Z}$ $\longleftrightarrow$ linear polynomials $x - \alpha$

- Expansions of polynomials & rational functions

$P(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_0 = b_n(x-\alpha)^n + b_{n-1}(x-\alpha)^{n-1} + \dots + b_0$

base = 0 base = α

($b_0 = P(\alpha)$)

$b_n = a_n$

$\frac{P(x)}{Q(x)} = ?$

$\frac{P(x)}{Q(x)}$ ($Q(x)$ monic) $= \frac{(x-\alpha)^m (a_s(x-\alpha)^s + \dots + a_1(x-\alpha) + a_0}{(x-\alpha)^l ((x-\alpha)^r + b_{r-1}(x-\alpha)^{r-1} + \dots + b_0)}$

with $a_0, b_0 \neq 0$

$= (x-\alpha)^{m-l} \frac{(a_s(x-\alpha)^s + \dots + a_0)}{(x-\alpha)^r + \dots + b_0}$

- Obs 1 : $m - l$ is any integer, so we can have neg. exponents.
- Obs 2 : $a_0, b_0 \neq 0 \Rightarrow f(x) = \frac{a_s(x-\alpha)^s + \dots + a_0}{(x-\alpha)^r + \dots + b_0}$ is a well-defined, cont. differentiable function near $x = \alpha$, so it has a Taylor expansion.

$f(x) = \frac{a_0}{b_0} + \square(x-\alpha) + \square(x-\alpha)^2 + \dots$ Q: Behavior of $\square$?

A: Coefficients satisfy a linear recursion (after some point onwards)

Why? $C(x) = (c_0 + c_1 x + c_2 x^2 + \cdots)\,(x-\alpha)^{-m}$ (Laurent series)

Assume: $c_N = \sum_{l=1}^{k} \alpha_l c_{N-l} \quad \forall N \geq M$

Then set $Q(x) = -1 + \sum_{l=1}^{k} \alpha_l x^l$

$$Q(x)\frac{C(x)}{(x-\alpha)^m} \rightsquigarrow \text{coeff of } x^N \text{ for } N \geq M = \sum_{l=0}^{N} \text{coeff}_{x^l}(Q)\,\text{coeff}_{N-l}(C)$$

$$= -1\,c_N + \alpha_1 c_{N-1} + \cdots + \alpha_k c_{N-k} + 0 + \cdots$$

$$= -c_N + \alpha_1 c_{N-1} + \cdots + \alpha_k c_{N-k} = 0$$

So $Q(x)\frac{C(x)}{(x-\alpha)^m}$ is a polynomial of degree $\leq M$. $\Rightarrow Q(x)C(x)$ is a Laurent poly.

Conversely, for $\frac{P(x)}{Q(x)}$, write $Q(x)$ as $a\left(-1 + \sum_{l=1}^{k} \alpha_l x^l\right)(x-\alpha)^m$

$$\Rightarrow \frac{P(x)}{Q(x)} = (x-\alpha)^{-m}\frac{P(x)}{a}.$$ Power series with recurrence $c_N = \sum_{l=1}^{N} \alpha_l c_{N-l}$

Exercise: $C(x)$ is finite expansion $\Leftrightarrow Q(x) = (x-\alpha)^m$

- **Question**: What would the analog be for $\mathbb{Z}$?

Let's do some examples, starting with positive integers.

- $(x-\alpha) \rightsquigarrow p$ positive prime as our building block.

① **Claim**: Any pos. integer m can be written as:

$$m = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n = \sum_{i=0}^{n} a_i p^i$$

where $a_0, \ldots, a_n$ integers $0 \leq a_i \leq p-1$.

How? Long division in succession.

Ex: $320 = 5 + 3\cdot 7 + 6\cdot 7^2$

$p=7$

320	⌊7
40	45 ⌊7
⑤	③ ⑥ , (6<7 STOP)

← # divisions = 2 = highest power of 7 we need.

Record it as **635**.

(lowest powers come last!)

Alt: $320 \equiv 5 \pmod 7$, meaning $7 \mid 320-5$

$320 \equiv 5 + 3\cdot 7 \pmod{7^2}$ — $7^2 \mid (320-5-3\cdot 7)$

$320 \equiv 5 + 3\cdot 7 + 6\cdot 7^2 \pmod{7^3}$ — $7^3 \mid (320-5-3\cdot 7-6\cdot 7^2)$

After that, we only get to add 0's.

② What about negative integers? Can't expect a finite sum... (finite sums are ≥ 0)

Use the algorithm (remainders!)

$-1 \equiv \square \pmod 7$ $\quad 7 \mid \square + 1$ $\quad \square \in \{0,1,\dots,6\} \Rightarrow \square = 6$

$-1 \equiv 6 + \square\, 7 \pmod{7^2}$ $\quad 7^2 \mid \underbrace{1+6}_{=7} + \square\, 7 = 7(1+\square)$ $\quad$ so $\square = 6$

$-1 \equiv 6 + 6\cdot 7 + \square\, 7^2 \pmod{7^3}$ $\quad$ same idea gives $\square = 6$.

So $-1 = 6 + 6\cdot 7 + 6\cdot 7^2 + 6\cdot 7^3 + \cdots = \sum_{i\geq 0}^{\infty} 6\cdot 7^i$

Here: we need to interpret the = sign!

- Same idea works in general! $-1 = \sum_{i\geq 0}^{\infty} (p-1)\, p^i$ for all primes $p > 0$.

Other integers? { . $-m = m(-1)$ & multiply in base p carrying the excess (*)
. run the algorithm for $-m$ directly:

Operations: ① Addition: term-by-term + carry over Subtraction = add its negative

Need a table to add digits mod p (pigits, pits?)

$p=7$

$0+i = i$
$1+1 = 2$
$1+2 = 3$
$1+3 = 4$
$1+4 = 5$
$1+5 = 6$
$1+6 = 10$

$2+2 = 4$
$2+3 = 5$
$2+4 = 6$
$2+5 = 10$
$2+6 = 11$

$3+3 = 6$
$3+4 = 10$
$3+5 = 11$
$3+6 = 12$

$4+4 = 11$
$4+5 = 12$
$4+6 = 13$

$5+5 = 13$
$5+6 = 14$
$6+6 = 15$

Eg:
$$\begin{array}{r} \cdots 6\,6666 \\ 635 \\ \hline \cdots\cdots 00634 \end{array} \quad \text{carries: } 1\,1\,1\,1$$

$\hookrightarrow$ $320 + (-1)$ in base 7.

③ Multiplication: again, need multiplication table for "pigits":

$0\cdot i = 0$
$1\cdot i = i$
$2\cdot 2 = 4$
$2\cdot 3 = 6$
$2\cdot 5 = 13$
$2\cdot 6 = 15$

$3\cdot 3 = 12$
$3\cdot 4 = 15$
$3\cdot 5 = 21$
$3\cdot 6 = 24$

$4\cdot 4 = 22$
$4\cdot 5 = 26$
$4\cdot 6 = 33$
$5\cdot 5 = 34$
$5\cdot 6 = 42$
$6\cdot 6 = 51$

$4^2 4^2 5$

$$\begin{array}{r} \cdots 6666 \\ 635 \\ \hline \cdots\cdots 662 \\ \cdots\cdots 6640 \\ \cdots 66100 \\ \hline \cdots\cdots 66032 \end{array} \quad \begin{array}{l} \text{carries: } 2\,2\,2\,1 \\ \\ \\ \\ \\ \\ \end{array} \quad \begin{array}{l} 1 \\ 15 \\ 2 \\ 20 \end{array}$$

mod 7

$= (-320)_7$.

Check: Add (320) to ... and ... 7.

⑤ What about rationals? Positive ones, then multiply by series for -1.

• Easy if denom is a power of p. Just shift exponents of numerator's exp.

Eg: $\frac{320}{49} = \frac{5+3\cdot 7+6\cdot 7^2}{7^2} = 5\cdot 7^{-2}+3\cdot 7^{-1}+6 = \boxed{6.35}$ ←

⇝ Neg exponents, but fin. many!

$\frac{-1}{49} = \frac{6+6\cdot 7+6\cdot 7^2+\cdots}{49} = 6\cdot 7^{-2}+6\cdot 7^{-1}+6+6\cdot 7+6\cdot 7^2+\cdots$

$= \cdots 6\cdots 6.66$

• For general denominators: → divide formally ($\frac{P(x)}{Q(x)}$ & evaluate?) ←
→ use repeated division with remainder

We expect: $\frac{a}{b} = c_{-n}p^{-n}+c_{-n+1}p^{-n+1}+\cdots+c_0+c_1p+\cdots$

Example $p=3$ $\frac{a}{b} = \frac{24}{17} = \frac{2\cdot 3+2\cdot 3^2}{2+2\cdot 3+3^2} = \frac{2p+2p^2}{2+2p+p^2}$

$= p\left(\frac{2+2p}{2+2p+p^2}\right)$

↳ expect only positive powers (as in $\mathbb{Q}(x)$)

Write $\frac{2+2p}{2+2p+p^2} = c_0+c_1p+c_2p^2+\cdots$ $\quad c_0,c_1,\ldots \in \{0,1,\ldots,6\}$

$2+2p = (2+2p+p^2)(c_0+c_1p+c_2p^2+c_3p^3+\cdots$

$= 2\cdot c_0+(2c_1+2c_0)p+(2c_2+2c_1+c_0)p^2+$

$+(2c_3+2c_2+c_1)p^3+(2c_4+2c_3+c_2)p^4+\cdots$

Equate term by term & carry on!

p^0 $\quad 2 \equiv 2c_0 \ (3) \Rightarrow c_0=1$ nothing to carry!

p^1 $\quad 2 \equiv 2c_1+2c_0 = 2c_1+2 \ (3) \Rightarrow 2c_1 \equiv 0 \ (3) \Rightarrow c_1=0$

p^2 $\quad 0 \equiv 2c_2+2c_1+c_0 = 2c_2+1 \ (3) \Rightarrow c_2=1$

$2c_2+1=3$

p^3 $\quad 0 \equiv 1+2c_3+2c_2+c_1 \ (3)$ so carry a 1 to p^3 term

$= 1+2\cdot c_3+2\cdot 1 = 3+2\cdot c_3 \ (3) \Rightarrow c_3=0$

$= 3 = p$ carry a 1 to p^4 term!

p^4: $0 = 1 + 2c_4 + 2c_3 + c_2$ (3)

$= 1 + 2c_4 + 0 + 1 = 2 + 2c_4$ (3) $\Rightarrow c_4 = 2$ & we must carry a 2 to p^5

$= 6 = 2 \cdot p$

p^5: $0 = 2 + 2 \cdot c_5 + 2 \cdot c_4 + c_3 = 2 + 2c_5 + 2 \cdot 2 + 0 = 6 + 2c_5$ (3)

$\Rightarrow c_5 = 0$ & $6 = 2 \cdot p$ so carry a 2 to p^6

p^6: $0 = 2 + 2c_6 + 2c_5 + c_4 = 2 + 2c_6 + 0 + 2 = 4 + 2c_6$ (3)

$\Rightarrow c_6 = 1$ & $6 = 2 \cdot p$ so carry a 2 to p^7.

p^7: $0 = 2 + 2c_7 + 2c_6 + c_5 = 2 + 2c_7 + 2 = 4 + 2c_7$ (3)

$\Rightarrow c_7 = 1$ & $6 = 2 \cdot p$ so carry a 2 to p^8

p^8: $0 = 2 + 2 \cdot c_8 + 2c_7 + c_6 = 2 + 2c_8 + 2 + 1 = 5 + 2c_8$ (3)

$\Rightarrow c_8 = 2$ & $9 = p^2$ so carry a 1 to p^{10}

p^9: $0 = 2c_9 + 2c_8 + c_7 = 2 \cdot c_9 + 5 \Rightarrow c_9 = 2$

& $9 = p^2$ so carry a 1 to p^{11}

$\vdots$

we get $\frac{2+2p}{2+2p+p^2} = 1 + 0 \cdot p + 1 \cdot p^2 + 2p^4 + 1p^6 + 1p^7 + 2p^8 + 2p^9 + \ldots$

$= 1 + p^2 + 2p^4 + p^6 + p^7 + 2p^8 + 2p^9 + 2p^{10} + \ldots$

$= \ldots 2\,2\,2\,1\,1\,0\,2\,0\,1\,0\,1$

$\Rightarrow \frac{24}{17} = p\left(\frac{2+2p}{2+2p+p^2}\right) = \ldots 2\,2\,2\,1\,1\,0\,2\,0\,1\,0\,1\,0$

Check: $(2+2p+p^4)(p + p^3 + 2p^5 + p^7 + p^8 + 2p^9 + \ldots$

$= 2p + 2p^2 + \underbrace{p^3 + 2p^3}_{= p^4} + 2p^4 + p^5 + 4p^5 + 4p^6 + 2p^7 + 2p^8 + \ldots$

$\underbrace{\qquad\qquad}_{= p^5}$

$\underbrace{\qquad\qquad\qquad}_{2p^6}$

$\underbrace{\qquad\qquad\qquad\qquad}_{2p^7}$

$p^8 + p^9 \ldots$

In the end, all terms with $p^3, p^4, \ldots$ cancel out!

Def: A *p-adic number* is an expression

$$x = a_{n_0} p^{n_0} + a_{n_0+1} p^{n_0+1} + \cdots \qquad (x \in \mathbb{Q}_p)$$

where $n_0 \in \mathbb{Z}$ is a fixed integer, and all a_i are in $\{0, \dots p-1\}$, with $a_{n_0} \neq 0$.

FACT 1: Such an expression corresponds to a rational number if and only if the sequence (a_i) is eventually periodic.

FACT 2: For positive integers, the sequence is ultimately constant $= 0$.

Example: $p=3$

$$\cdots 201201 = 1 + 2\cdot 3^2 + 1\cdot 3^3 + 2\cdot 3^5 + \cdots$$

$$= \underbrace{(1+2\cdot 3^2)}_{=19} \underbrace{(1 + 3^3 + 3^6 + \cdots)}$$

$$= \text{geom series with } x = 3^3$$

$$\text{"}=\text{"} \quad \frac{1}{1-3^3} = \frac{1}{1-27} = \frac{1}{-26}$$

$$\text{So } \cdots 201201 = \frac{-19}{26}$$

Similarly: $\cdots 2012011 = 1 + 3(\cdots 201201) \text{"}=\text{"} 1 + 3\left(\frac{-19}{26}\right) = \frac{-31}{26}$

- We get $\mathbb{Q} \subset \mathbb{Q}_p$ & operations translate nicely to operations among Laurent series in p if we carry appropriately.

Question: What is the meaning of number = power series in p?

$\rightsquigarrow$ We need a *metric* to say $\sum_{n=n_0}^{\infty} a_n p^n = \frac{a}{b}$

(sequence of partial sums are rational numbers & their *limit* is $\frac{a}{b}$)

2 Ultrametrics:

Intuitive idea: $\sum_{n=n_0}^{N} a_n p^n \xrightarrow[N\to\infty]{} \frac{a}{b}$ forces high powers of p to be small

(tails: $\sum_{n=N+1}^{\infty} a_n p^n = p^{N+1} \cdot \sum_{n=0}^{\infty} a_{N+1+n} p^n$)

Def: Given a number $\frac{a}{b}$ in $\mathbb{Q}$, write it as $p^n \frac{r}{s}$ with $p \nmid r$, $p \nmid s$. Then

$$\left|\frac{a}{b}\right|_p = p^{-n} \qquad \text{(p-adic absolute value)}$$

- For p-adic numbers we can do the same thing!

$$\left|\sum_{n=n_0}^{N} a_n p^n\right|_p = \left|p^{n_0}(a_{n_0} + a_{n_0+1} p + \cdots)\right|_p = p^{-n_0} \xrightarrow[n_0 \to \infty]{} 0$$

⇝ p-adic distance between x & y in $\mathbb{Q}_p$ is $= |x-y|_p$

Caveat: Need to show that if we write $\frac{a}{b}$ in it's p-adic expansion, we get the same value $\left|\frac{a}{b}\right|_p$ (Exercise)

- p-adic abs value is an ultrametric

Def: $|\ |: \mathbb{Q}_p \longrightarrow \mathbb{R}_{\geq 0}$ is an ultrametric if

(1) $|x|=0 \iff x=0$

(2) $|xy| = |x||y|$

(3) $|x-y| \leq \max\{|x-z|, |z-y|\}$ $\forall$ all z (Strong triangular ineq).

Moreover, if $|x-z| \neq |z-y|$, then $|x-y| = \max\{|x-z|, |z-y|\}$

(Observe: Strong Δ ineq forces usual one: $|x-y| \leq |x-z| + |z-y|$.)

- Consequence 1: If $|\ |$ is an ultrametric, any triangle is isosceles and the unequal side (if any exists) is the shortest one.
- Consequence 2: Any 2 balls are either disjoint or 1 is contained in the other!

Prop $|\ |_p$ is an ultrametric. & $(\mathbb{Q}_p, |\ |_p)$ is a complete metric spa

- With $|\ |_p$, we get an actual equality when representing $\frac{a}{b}$ in $\mathbb{Q}$ in it's p-series expansion.

§3. How to draw p-adic numbers? Example: p=3

Let's start with some numbers.

1 & $4 = 1+3$ are $|1-4|_3 = \frac{1}{3}$ apart

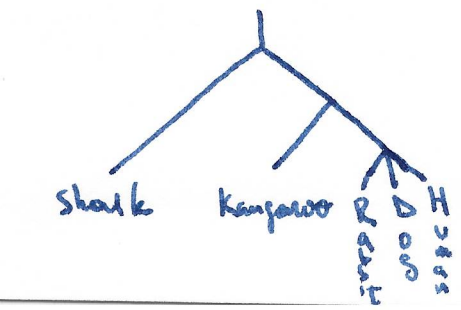
1 & 2 " $|1-2|_3 = 1$ —

1 & $5 = 2+1\cdot 3$ " $|1-5|_3 = |4|_3 = 1$ —

1 & $10 = 1+1\cdot 3^2$ are $|1-10|_3 = \frac{1}{9}$ —

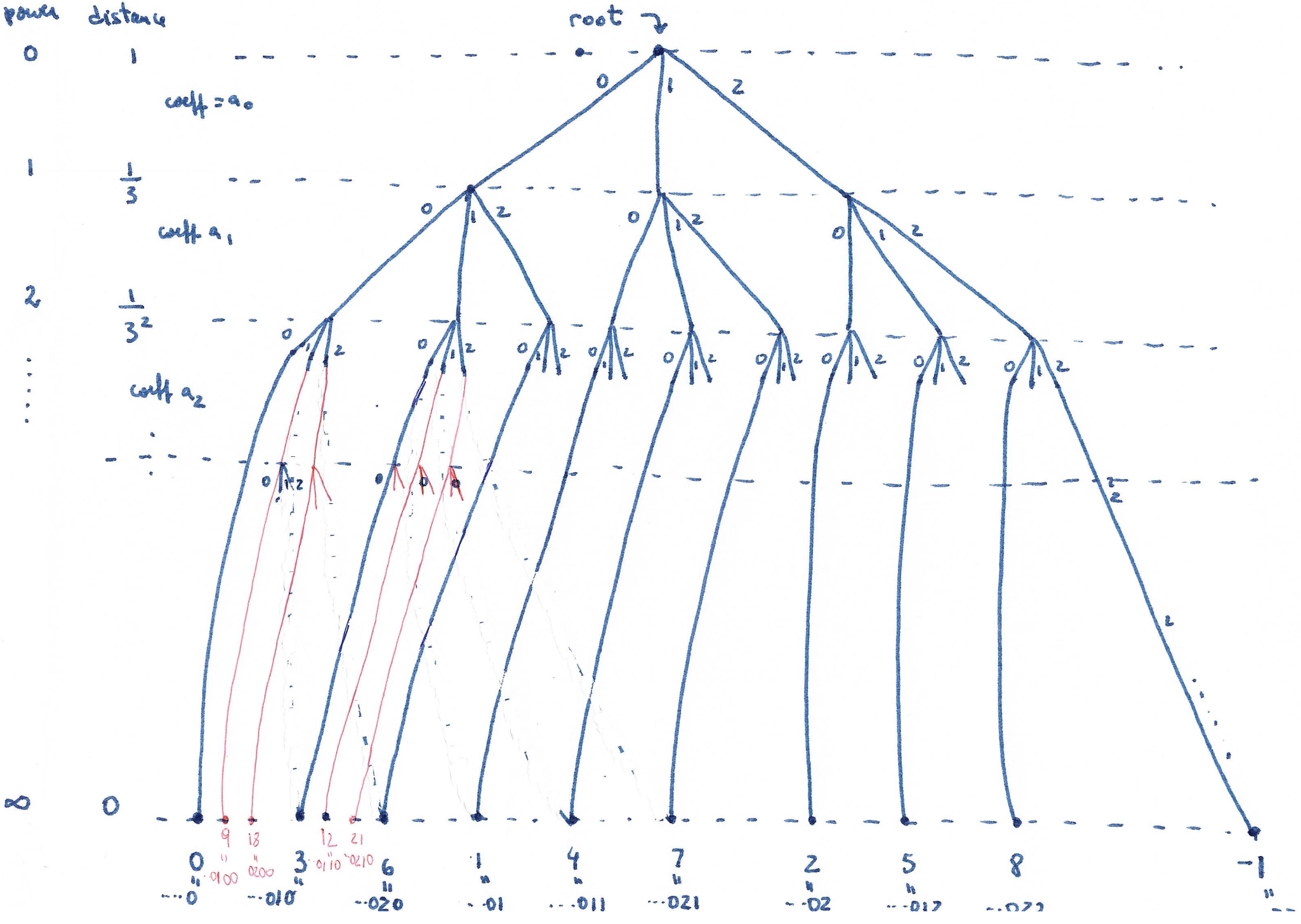
⇝ need to express each number in 3-adic expansion and pick 1st slot when they differ

⇝ This resembles what we do to classify species in the tree of life!



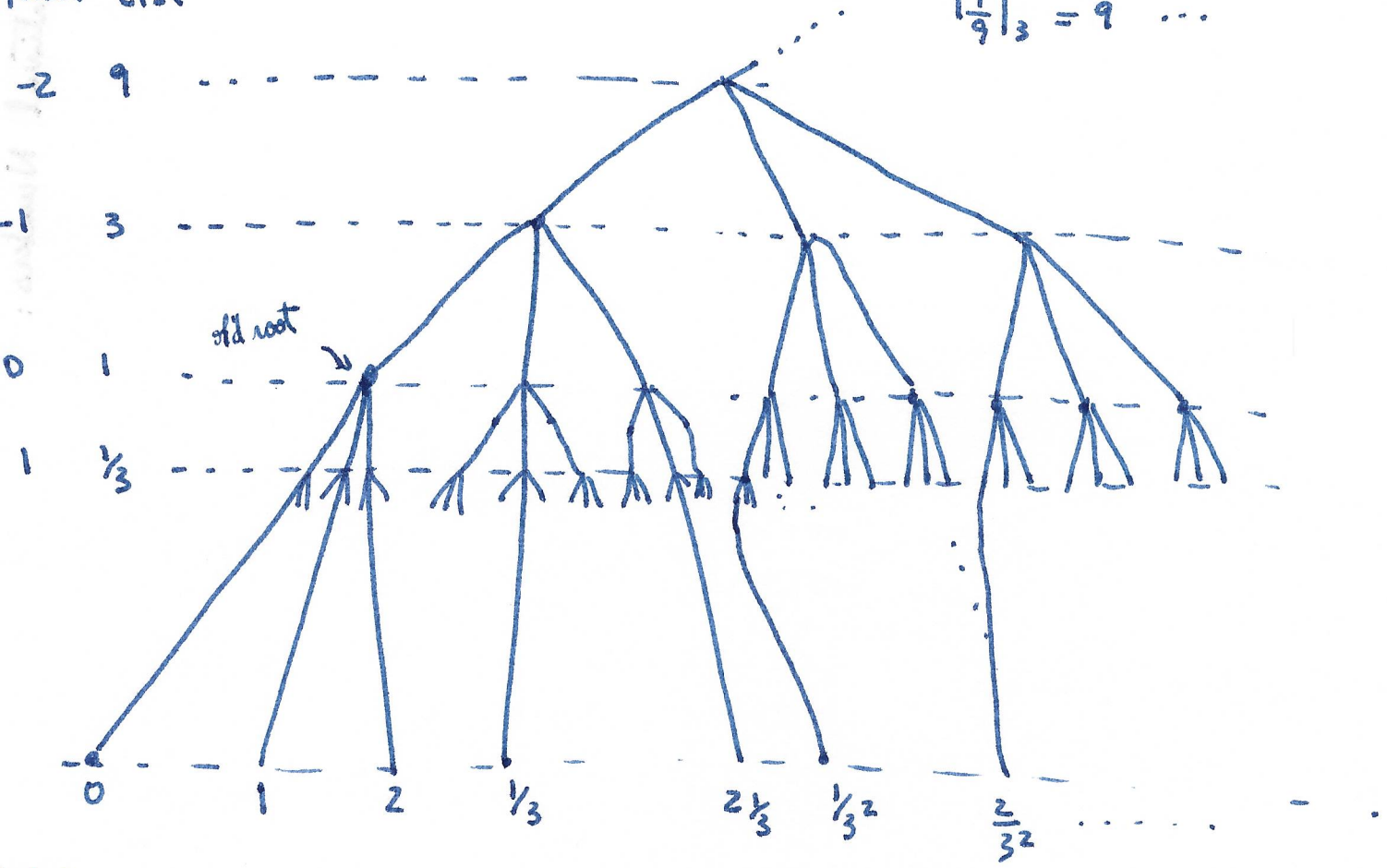
distance: amino acid differences.

① Integers in $\mathbb{Q}_p$:



② For rational numbers, distances increase $|\frac{1}{3}|_3 = (3^{-1})^{-1} = 3$

$|\frac{1}{9}|_3 = 9$ ...

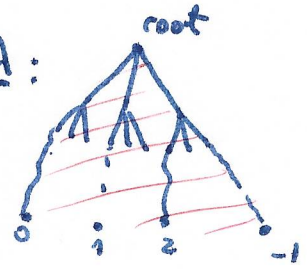


Q: Where are numbers that are in $\overline{B}(1,1)$?

Same as $\overline{B}(0,1)$!

(0 & 1 are centers of the same ball with closed $r=1$)

A:



- Leaves of the tree are 3-adics
- Only some leaves are rational numbers

} we need to add leaves to $\mathbb{Q}$ to get a complete tree.