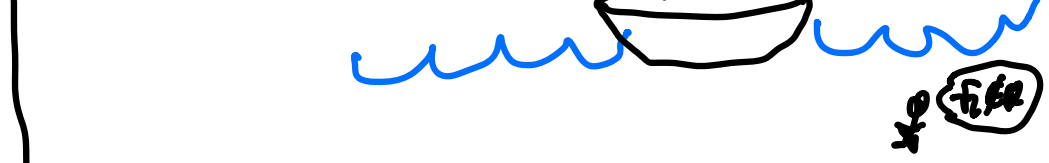
AWS 2021

Strange new landscape:
An exploration of the p-adic numbers and modular forms

1.1 Getting Real

"God made the integers, all else is the work of man" - Leopold Kronecker

- Anold question: what is a real number?
  (a) $3.1415\ldots$ $(=\pi)$
  (b) $0.3333\ldots$ $(1/3)$
  (c) $1.4142\ldots$ $(\sqrt{2})$



Notation is shorthand for:

$$\sqrt{2} = 1\cdot\left(\tfrac{1}{10}\right)^0 + 4\cdot\left(\tfrac{1}{10}\right)^1 + 1\cdot\left(\tfrac{1}{10}\right)^2 + 4\cdot\left(\tfrac{1}{10}\right)^3 + \cdots$$

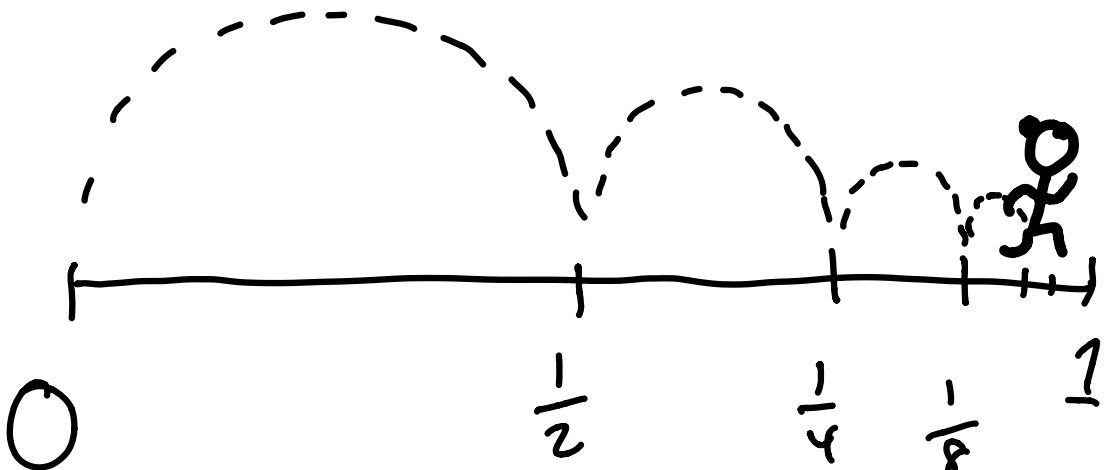
$\sqrt{2} \approx 1$

≈ 1.4

≈ 1.41 ← calculated up to $1/100000$ place

800BC, Shulba Sutras

- Zeno's Paradox
  - Suppose Atalanta has to run a mile.
  - She must first run half a mile,
  - Next, she runs an additional $\frac{1}{4}$ mile
  - " " " " " $\frac{1}{8}$ mile
  - ...



- This is an infinite number of tasks, a "paradox"

- Atalanta runs

$$\sum_{i=1}^{\infty} \frac{1}{2^i} = 1 \text{ mile}$$

- Why? Geometric series:

$$\sum_{i=0}^{\infty} p^i = \frac{1}{1-p}$$

↑ doesn't make sense if $p \geq 1$.
OR DOES IT?!

- We think of

$$a := \sum_{i=n_0}^{\infty} b_i \left(\frac{1}{10}\right)^i \quad \text{with } n_0 \in \mathbb{Z} \text{ and } b_i \in \{0, \dots, 9\}$$

as a real number to which the sum converges

- let $a_n := \sum_{i=n_0}^{n} b_i \left(\frac{1}{10}\right)^i$, finite approximations

$$- \lim_{n\to\infty} a - a_n = \lim_{n\to\infty} \underbrace{\sum_{i=n+1}^{\infty} b_i \frac{1}{10^i}}_{\text{small} \to \frac{1}{10^{n+1}}(\epsilon)} = 0$$

1.2 Zeno's p-aradox

- Let's look again at the geometric series
  $1 + p + p^2 + p^3 + \dots$

- Example: $p = 5$
  - p-atalanta starts at 0
  - Runs to 4
  - Runs 20miles to $4 + 4 \cdot 5^1$
  - " 100 miles to $4 + 4 \cdot 5^1 + 4 \cdot 5^2 + \dots$
  - culminates in
    $4 \cdot 5^0 + 4 \cdot 5^1 + 4 \cdot 5^2 + 4 \cdot 5^3 + \dots$

- We often consider 624, 124 to be "far", but they are "similar" arithmetically: 624, 124 have the same remainder when you divide by $5, 5^2, 5^3$.

1.3 A new perspective

- We will consider a <u>new notion of "similarity"</u>, of "<u>closeness</u>", of rational numbers, which will motivate a <u>new number system</u>!

Notation: for $a, b \in \mathbb{Z}$ and $a \neq 0$, we say a *divides* b and write $a \mid b$ if $\exists n \in \mathbb{Z}$ s.t. $b = na$

Examples: $2 \mid -6$ $25 \mid 625$, $m \mid 0$ $\forall m \in \mathbb{Z}$.

Notation: for $n \in \mathbb{N}_{>0}$, and $a, b \in \mathbb{Z}$, we write $a \equiv b \pmod{n}$ iff $n \mid (a-b)$

Examples $4 \equiv -1 \pmod{5}$

$3 \equiv 10 \pmod{7}$

$10 \equiv 108 \pmod{7^2}$

Arithmetic criterion for equality of rat'l #s:
Let p be a prime.

$\alpha, \beta \in \mathbb{Q}$ are equal iff
$\forall k \in \mathbb{Z}_{>0}$, p^k divides the numerator of the reduced form of $\alpha - \beta$

(a) α, β are "close" if $p^k \mid (\alpha - \beta)$ for "most" k

(b) $\gamma = 0$ iff $\forall k \in \mathbb{Z}_{>0}$, $p^k \mid \gamma$

$\rightsquigarrow$ γ is "close" to 0 if γ is highly divisible by p. γ "almost" satisfies the equality to 0 condition.

Ex: $p = 5$,
$5^4 \mid 625$ so 625 is "small 5-adically"
But $5^5 \nmid 625$.

- So p-atalanta is taking "smaller and smaller" steps, in this sense

Definition: We define the p-adic #s $\mathbb{Q}_p$ as

$$\mathbb{Q}_p := \left\{ \sum_{i=n_0}^{\infty} b_i p^i : n_0 \in \mathbb{Z}, b_i \in \{0, \ldots, p-1\} \right\}$$

Exercise: Show $\mathbb{Q}_p$ is uncountable.

1.4 Arithmetic in $\mathbb{Q}_p$

- For any prime p, we can write any natural # in base p by expanding it as a sum of powers of p with coeffs in $\{0, 1, \ldots, p-1\}$

Define

$: \mathbb{N} \to \mathbb{Q}_p$

$n \longmapsto$ "base p-expansion"

"expansion into pigits"

ex: $p = 7$ ← copy paste

$77 \mapsto 0 \cdot 7^0 + 4 \cdot 7^1 + 1 \cdot 7^2 + 0 \cdot 7^3 + \cdots$

$36 \mapsto 1 \cdot 7^0 + 5 \cdot 7^1 + 0 \cdots$

$113 \mapsto 1 \quad 2 \quad 2 \quad 0 \cdots$

- We define addition, multiplication in $\mathbb{Q}_p$ by extending the usual base p addition, multiplication. This is so  will be a homomorphism.

+ Addition

paste

ex: $p=7$

carry $+1+7^2$

$$\begin{array}{l} 0\cdot 7^0+\ 4\cdot 7^1+\ 1\cdot 7^2+0\cdot 7^3+\cdots = 77 \\ +\ 2\cdot 7^0+\ 5\cdot 7^1+\ 0\cdot 7^2+0\cdot 7^3+\cdots = 37 \\ \hline 2\cdot 7^0+\ 2\cdot 7^1+\ 2\cdot 7^2+0\cdot 7^3+\cdots = 114 \end{array}$$

🐷(77) + 🐷(36) = 🐷(77+36)

ex: $p=5$

carry $1\cdot 5^1$ carry $1\cdot 5^2$

$$\begin{array}{l} 4\cdot 5^0+\ 4\cdot 5^1+\ 4\cdot 5^2+\ 4\cdot 5^3+\cdots = -1 \\ +\ 1\cdot 5^0+\ 0\cdot 5^1+\ 0\cdot 5^2+\ 0\cdot 5^3+\cdots = 1 \\ \hline 0\cdot 5^0+\ 0\cdot 5^1+\ 0\cdot 5^2+\ 0+\cdots = 0 \end{array}$$

− Subtraction:

Exercise: If $a = \sum_{i=n_0}^{\infty} b_i p^i$, what is $-a$?

Multiplication:

Exp=7

$$\begin{array}{l} 0\cdot 7^0 + 4\cdot 7^1 + 1\cdot 7^2 + 0\cdot 7^3 + \cdots = 77 \\ \times\ 2\cdot 7^0 + 5\cdot 7^1 + 0\cdot 7^2 + 0\cdot 7^3 + \cdots = 37 \\ \hline 0\cdot 7^0 + 1\cdot 7^1 + 3\cdot 7^2 + 0\cdot 7^3 + 0\cdot 7^4 + \cdots \\ \qquad\quad 0\cdot 7^1 + 6\cdot 7^2 + 0\cdot 7^3 + 1\cdot 7^4 + \cdots \\ \hline 0\cdot 7^0 + 1\cdot 7^1 + 2\cdot 7^2 + 1\cdot 7^3 + 1\cdot 7^4 \end{array}$$

÷ Division?

- What's $\frac{1}{3}$ in $\mathbb{Q}_5$? We do long division

$$3\,(b_0\cdot 5^0 + b_1\cdot 5^1 + b_2\cdot 5^2 + b_3\cdot 5^3 + \cdots) = 1\cdot 5^0 + 0\cdot 5^1 + \cdots$$

$$3b_0 + 5(\cdots) = 1 + 5(\cdots)$$

$$-3\cdot 2$$

need $3 \cdot b_0 \equiv 1 \pmod 5 \rightsquigarrow b_0 = 2$

$$3(b_1 \cdot 5^1 + b_2 \cdot 5^2 + b_3 \cdot 5^3 + \cdots) = 1 - (1 + 1 \cdot 5^1)$$

$$5 \cdot 3(b_1 \cdot 5^0 + b_2 \cdot 5^1 + \cdots) = 5(-1)$$

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

Step 0

Step 1:

$3(b_1 \cdot 5^0 + \cdots) = 1 + 4 \cdot 5^1 + \cdots$

$3 \quad -9 \quad -(1 + 1 \cdot 5)$

Step 2:

$3(b_2 \cdot 5^0 + \cdots) = 3 \cdot 5^0 + 4 \cdot 5^1 + \cdots$

$1 \quad -3 \quad -3$

	b_0	b_1	b_2	b_3	
	2	3	1	3	$\cdots$
3 |	1	0	0	0	$\cdots$
$-$		1	1		
		4	4	4	$\cdots$
$-$		4	1		
			3	4	$\cdots$
$-$			3	0	0
				4	$\cdots$

$$\frac{1}{3} = \underbrace{2 \cdot 5^0}_{a_0} + \underbrace{3 \cdot 5^1}_{a_1} + 1 \cdot 5^2 + 3 \cdot 5^3 + \cdots$$

a_2

$\approx 2 \cdot 5^0$

$\approx 2 \cdot 5^0 + 3 \cdot 5^1$

$\approx 2 \cdot 5^0 + 3 \cdot 5^1 + 1 \cdot 5^2$

1.5 Rooting Around

$\sqrt{2}$ in $\mathbb{Q}_7$?

$\vdots$

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

part of a series, not nec. the coeff!

$b_0 + b_1 \cdot 7 + b_2 \cdot 7^2 + b_3 \cdot 7^3 + \cdots$

$\times \quad b_0 + b_1 \cdot 7 + b_2 \cdot 7^2 + b_3 \cdot 7^3 + \cdots$

$b_0^2 + 2b_0b_1 7 + 2b_0b_2 7^2 + \cdots$

$+ \quad b_0b_1 7 + b_1^2 7^2 + \cdots$

$+ \quad b_0b_2 7^2 + \cdots$

$\vdots$

$2 + 0 \cdot 7 + 0 \cdot 7^2 + 0 \cdot 7^3 + \cdots$

Step 0:

$b_0^2 \equiv 2 \bmod 7 \rightsquigarrow$ choose $b_0 = 3$

Note: $b_0^2 = 2 + 1 \cdot 7^1$

Step 1:

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

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

Step 2:

$b_2 = 2$

$\sqrt{-1}$ in $\mathbb{Q}_7$??

$\vdots$

$a = \sum b_i 7^i$

$-1 = 6 + 6 \cdot 7 + 6 \cdot 7^2 \cdots$

$\rightsquigarrow b_0^2 + 7(\cdots) = 6 + 7(\cdots)$

$\rightsquigarrow b_0^2 \equiv 6 \pmod 7$ DNE!

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

$$
\begin{array}{rl}
 & b_0 + b_1\cdot 5 + b_2\cdot 5^2 + b_3\cdot 5^3 + \cdots \\
\times & b_0 + b_1\cdot 5 + b_2\cdot 5^2 + b_3\cdot 5^3 + \cdots \\
\hline
 & b_0^2 \quad b_0b_1 \quad b_0b_2 \quad b_0b_3 \quad \cdots \\
+ & \quad\; b_0b_1 \quad b_1^2 \quad b_1b_2 \quad \cdots \\
+ & \quad\; 1 \quad b_0b_2 \quad b_1b_2 \quad \cdots \\
 & \quad\; \vdots \\
\hline
 & 4 \quad 4 \quad 4 \quad 4
\end{array}
$$

0) $b_0^2 \equiv 4 \pmod 5$ choose $b_0 = 3$

$\rightsquigarrow b_0 = 4 + 1\cdot 5$

1) $(6b_1 + 1)5 \equiv 4 \pmod{25}$

$\rightsquigarrow b_1 + 1 \equiv 4 \pmod 5 \rightsquigarrow b_1 = 3$

2) ---- $b_2 = 2$

⋮

1.6 A coherent explanation

- We have been doing all these calculations by computing "approximations" to solutions in $\mathbb{Q}_p$.

  - If $a = \sum_{i=0}^{\infty} b_i p^i$, let $a_n = \sum_{i=0}^{n} b_i p^i$

  - Ex: for $\sqrt{-1}$ in $\mathbb{Q}_5$

    $3 = a_0 = b_0$

    $3 + 3 \cdot 5 = a_1 = b_0 + b_1 p$

    $3 + 3 \cdot 5 + 3 \cdot 5^2 = a_2 = b_0 + b_1 p + b_2 p^2$

refining by adding mult. of p^i

Def: a sequence of integers α_n s.t. $0 \leq \alpha_n \leq p^n - 1$ is <u>coherent</u> if $\forall n \geq 1$,

$$\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$$

- $a_0, a_1, a_2, \ldots$ was a <u>coherent</u> sequence of solutions mod $p, p^2, p^3, \ldots$