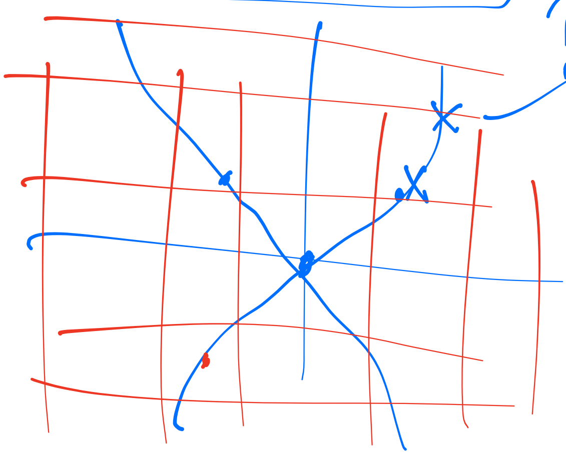
Diophantus 300 CE:

$$\underbrace{\boxed{x^2}}_{x} + \underbrace{\boxed{x^4}}_{x^2} + \underbrace{\boxed{x^8}}_{x^4} = \underbrace{\boxed{y^2}}_{y}$$

$$\underline{x^2 + x^4 + x^8 = y^2}. \quad / \mathbb{Q}.$$



?

$/ \mathbb{R}$

Hensel: If there were a rational solution, there would be solutions mod p^n for almost all p's & n's.

Try: look for solutions mod 3^{100}.

Better: Randomly / Exhaustively search mod 3 & try to "lift" solutions mod 3 to solutions mod 9, 27, 81, ---

mod 3:

$x^2+x^4+x^8$	x^8	x^4	x^2	x	$y \backslash y^2$: 0	1	1
					0	1	2
0	0	0	0	0	~~0~~		
0	1	1	1	1	~~0~~		
0	1	1	1	2	~~0~~		

(0, 0)

(1, 0) ←

(2, 0).

Look for solutions mod 9 which when reduced mod 3 give (1, 0)

i.e. $x = 1 + 3\cdot x_1$, $y = 0 + 3\cdot y_1$.

$x^2 = 1 + 2\cdot 3x_1$, $y^2 = 0$.

$x^4 = 1 + 3\cdot x_1$

$x = 1$ (1, …

$$\left.x^8 = 1 + 6x_1\right.$$

$$= 3 + 6x_1 \equiv 0 \ (9)$$

$$\Rightarrow 1 + 2x_1 \equiv 0 \ (3).$$

$(4, 0)$ mod 9.

Try to find solution mod 27, s.t. mod 9!

$$x = 4 + 9 \cdot x_2, \quad y = 0 + 9 \cdot y_2.$$

$$\left[\begin{array}{l} x^2 = 16 + 18x_2, \quad y^2 = 0, \\ x^4 = 13 + 9x_2 \\ x^8 = 7 + 18x_2 \end{array}\right.$$

$x_2 = 1$

$$= 9 + 18x_2 \equiv 0 \ (27)$$

$$1 + 2x_2 \equiv 0 \ (3)$$

Exercise: Continue calculation;

$$x = 1 + \underbrace{1\cdot 3 + 1\cdot 3^2 + 1\cdot 3^3 + 1\cdot 3^4 + \dots}_{3\cdot x}$$

If we could make any sense of this,

then $x = 1 + 3\cdot x$, $x = -\frac{1}{2}$.

$$1 + \lambda + \lambda^2 + \lambda^3 + \dots = \frac{1}{1-\lambda}, \quad |\lambda| < 1$$

In $\mathbb{C}$-analysis, $f(\lambda)$ on $\underline{D}$,

$$g(\lambda) = \frac{1}{1-\lambda}, \text{ on } \lambda \neq 1.$$

$\boxed{f(3)}$ " = " $\underline{g(3)}$ unique analytic Cont.

$x = \frac{1}{2} \Rightarrow x^2 + x^4 + x^8$

$$= \frac{1}{4} + \frac{1}{16} + \frac{1}{256}$$

$$= \frac{1}{256}\left(\underline{64} + \underline{16} + \underline{1}\right) = \frac{81}{256}$$

On V: $x^2 + x^4 + x^8 = y^2 / \mathbb{Q}$

$\left(\frac{1}{2}, \frac{9}{16}\right)$.

$\pi = \underline{3}.\underline{14}\boxed{1}5 \ldots$ $\quad d\left(\pi, \frac{22}{7}\right) = \left|\pi - \frac{22}{7}\right| \simeq 10^{-3}$.

$\frac{22}{7} = \underline{3}.\underline{14}\boxed{2}8 \ldots$

$x = 1 + 1\cdot 3 + 1\cdot 3^2 + 1\cdot 3^3 + 1\cdot 3^4 \ldots$

$x' = 1 + 1\cdot 3 + 1\cdot 3^2 + 1\cdot 3^3 + 2\cdot 3^4 \ldots$

want "d_3"$(x, x') = \underbrace{|x - x'|_3 = 3^{-4}}$.

$$\mathbb{R} = \{\underbrace{\text{Cauchy seq in } \mathbb{Q}}_{\{r_n\} \subset \mathbb{Q},\ \forall \varepsilon > 0,\ \exists N\ \forall n, m > N,\ |r_n - r_m| < \varepsilon}\}/\sim.$$

p-adic numbers

$$\mathbb{Q}_p = \{\text{Cauchy seq in } \mathbb{Q} \text{ with } |\cdot|_p\}/\sim.$$

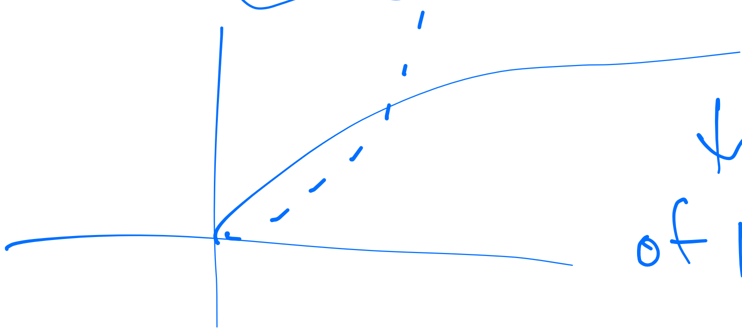
What are possible abs vals on $\mathbb{Q}$?

Def: $|\cdot| : \mathbb{Q} \to \mathbb{R}$ is an abs val if:

- (0) pos def, $|x| \geq 0$, & $|x| = 0 \Leftrightarrow x = 0$.
- (1) mult, $|xy| = |x| \cdot |y|$.
- (2) triangle: $|x+y| \leq |x| + |y|$.

Obs: If $|\cdot|$ is an abs val, & $c<1$, then $|\cdot|^c$ is also an abs val.

$y = x^c$



triangle ineq of $|\cdot| \Rightarrow$ same for $|\cdot|^c$.

Def: $|\cdot|_1$ & $|\cdot|_2$ are equivalent if $\exists\ c>0$ s.t. $|\cdot|_1 = |\cdot|_2^c$.

Want: $|\cdot|_\infty^{0.7}$ & $|\cdot|_\infty^{0.8}$ to be equivalent.

Note: equiv norms ($\subseteq$ abs vals) give same Cauchy seq structure.

Given arbitrary abs val $|\cdot|$ on $\mathbb{Q}$

what is it? $|0|=0$, $|1|=|1^2|=|1|\cdot|1|$

$\Rightarrow |1|(|1|-1)=0$

$|1| \neq 0$

$|1|=1=|1|$

If you know $|\cdot|$ on $\mathbb{N}$, can work out $|\cdot|$ on $\mathbb{Q}$ from multiplicativity.

To know $|\cdot|$ on $\mathbb{N}$, need to know it on just primes. (unique factorization).

<u>Case 1:</u> $\exists\, n \geq 2$, s.t. $|n|>1$. ($n \in \mathbb{N}$)

Let $m \in \mathbb{N}$ be arbitrary. Fix $k \geq 1$. Write

$$n^k = n_0 + n_1 \cdot m + n_2 m^2 + \dots + n_{\ell-1} \cdot m^{\ell-1}$$ (in base m.)

$n_i \in \{0, \dots, m-1\}$. $n_{\ell-1} \neq 0$;

$$|n_j| = |1+1+\cdots+1| \le |1|+\cdots|1| \le m.$$

$$|m^j| \le \max(1, |m|^{\ell-1})$$ needed in case $|m| \le 1$.

$$1 < |n|^k = |n^k| \le \underline{\underline{\ell}} \cdot m \cdot \max(1, |m|^{\ell-1}).$$

Since $n_{\ell-1} \neq 0$, $n^k \geq m^{\ell-1}$

$$k \log n \geq (\ell-1) \log m$$

$$\Rightarrow \quad \ell-1 \le k \frac{\log n}{\log m}.$$

$$\Rightarrow 1 < |n|^k \le \left(k \frac{\log n}{\log m} + 1\right) \cdot m \cdot \max\left(1, |m|^{k \frac{\log n}{\log m}}\right).$$

$$\Rightarrow \quad |n| \le \left(\cancel{k \frac{\log n}{\log m} + 1}\right)^{\cancel{1/k}\, 1} \cdot \cancel{m}^{\cancel{1/k}\, 1} \cdot \max(1, |m|^{\log n / \log m})$$

True for any K, $K \to \infty$.

$$1 < |n| \le \max\left(\cancel{K}, |m|^{\log n/\log m}\right).$$

$$|n| \le |m|^{\log n/\log m}.$$

$$\Rightarrow \quad |n|^{1/\log n} \le |m|^{1/\log m}$$

m was arbitrary,

$$\Rightarrow \forall n, \cancel{m} \quad |n|^{1/\log n} = C.$$

$$|n| = C^{\log n} = e^{\alpha \log n} = n^{\alpha}.$$

$$= |n|_{\infty}^{\alpha}.$$

$$\Rightarrow |\cdot| \sim |\cdot|_{\infty}.$$

Case 2: $\forall n \in \mathbb{N}$, $|n| \leq 1$.

Case 2a: $\forall n \in \mathbb{N}^{\neq 0}$, $|n| = 1$. $\Rightarrow$ $\forall r \in \mathbb{Q}^{\neq 0}$, $|r| = 1$.

$\Rightarrow$ $|\cdot| = \text{trivial} = \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases}$.

$\Rightarrow$ Cauchy seq = eventually constant.

Case 2b: all $|n| \leq 1$, & $\exists n \in \mathbb{N}$, $|n| < 1$.

$$|n| = \prod_p |p|^{e_p(n)} < 1 \qquad p^{e_p(n)} \,\|\, n.$$

$\Rightarrow$ $\exists$ p with $|p| < 1$.

If $p \,\&\, q$ primes & $|p|, |q| < 1$,
$\neq$

$$|p^e| < \frac{1}{2}. \quad |q^f| < 1/2.$$

Chinese Remainder Thm (Bezout Thm)

$\exists\, x, y \in \mathbb{Z}$ s.t. $|p^e x + q^f y| = |1| = 1$

$$\not\leq |p^e| \cdot |x| + |q^f| \cdot |y| < \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 1$$

$\Rightarrow \exists!\ p_*$, with $\lambda = |p_*| < 1.$

$$|n| = \prod_p |p|^{e_p(n)} = |p_*|^{e_{p_*}(n)} = \lambda^{e_{p_*}(n)}.$$

$$|n|_p = \left(\frac{1}{p}\right)^{e_p(n)}$$

$\sim$

$n = 0 + 0p + 0p^2 + 1 \cdot p^3 + \cdots$

Thm (Ostrowski Thm): If $|\cdot|$ abs val on $\mathbb{Q}$, then

$$|\cdot| \sim \begin{cases} |\cdot|_\infty \\ |\cdot|_p \\ \text{triv.} \end{cases}$$

If we choose $|n|_p = \left(\frac{1}{p}\right)^{e_p(n)}$, $\forall q \in \mathbb{Q} \setminus 0$,

then

$$\prod_{p \leq \infty} |q|_p = 1 .$$