Lecture 15.1

Last time:

- A (p-adic) coherent sequence is a sequence of integers (x_n) satisfying

  * $0 \leq x_n \leq p^n - 1$
  * $x_n \equiv x_{n-1} \pmod{p^{n-1}}$.

- The p-adic valuation of $\frac{a}{b} \in \mathbb{Q}$ is

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$$

where $v_p(a) = n$ if $p^n \mid a$ but $p^{n+1} \nmid a$,

and $v_p(0) = \infty$.

- The p-adic absolute value $|\cdot|_p$ is defined as $\quad |x|_p := p^{-v_p(x)}$.

This allows us to measure distances p-adically:

$$\mathrm{dist}_p(x,y) := |x-y|_p .$$

Informally, x and y are p-adically "close" if $x-y$ is highly divisible by p (and x is "small" if it is highly divisible by p).

Prop For any rational numbers x, y,

(1) If x has p-adic expansion

$$\sum^{\infty}$$

$$x = \sum_{i=-N} a_i p^i$$

with $a_{-N} \neq 0$, then $v_p(x) = -N$.

(2) $v_p(xy) = v_p(x) + v_p(y)$.

(3) $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$.

$\boxed{\text{Prop}}$ Fix p and let x, y be rational.

(1) $|x|_p = 0$ if and only if $x = 0$.

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

(3) $|x+y|_p \leq |x|_p + |y|_p$. In fact,

$|x+y|_p \leq \max\{|x|_p, |y|_p\}$.

This says $|\cdot|_p$ is an absolute value function on the field $\mathbb{Q}$ of rationals.

(4) $|1|_p = 1$ and $|-1|_p = 1$.

(5) $|n|_p \leq 1$ if and only if $n \in \mathbb{Z}$.

Exercise 1: Prove the Proposition.

With a notion of distance, we also get a new notion of convergence.

$\boxed{\text{Def}}$ Fix an absolute value function $|\cdot|$. A sequence of rational numbers (x_n) **converges** with respect to $|\cdot|$ if for every $\varepsilon > 0$, there's an $N \geq 1$ such that for all $n \geq N$,

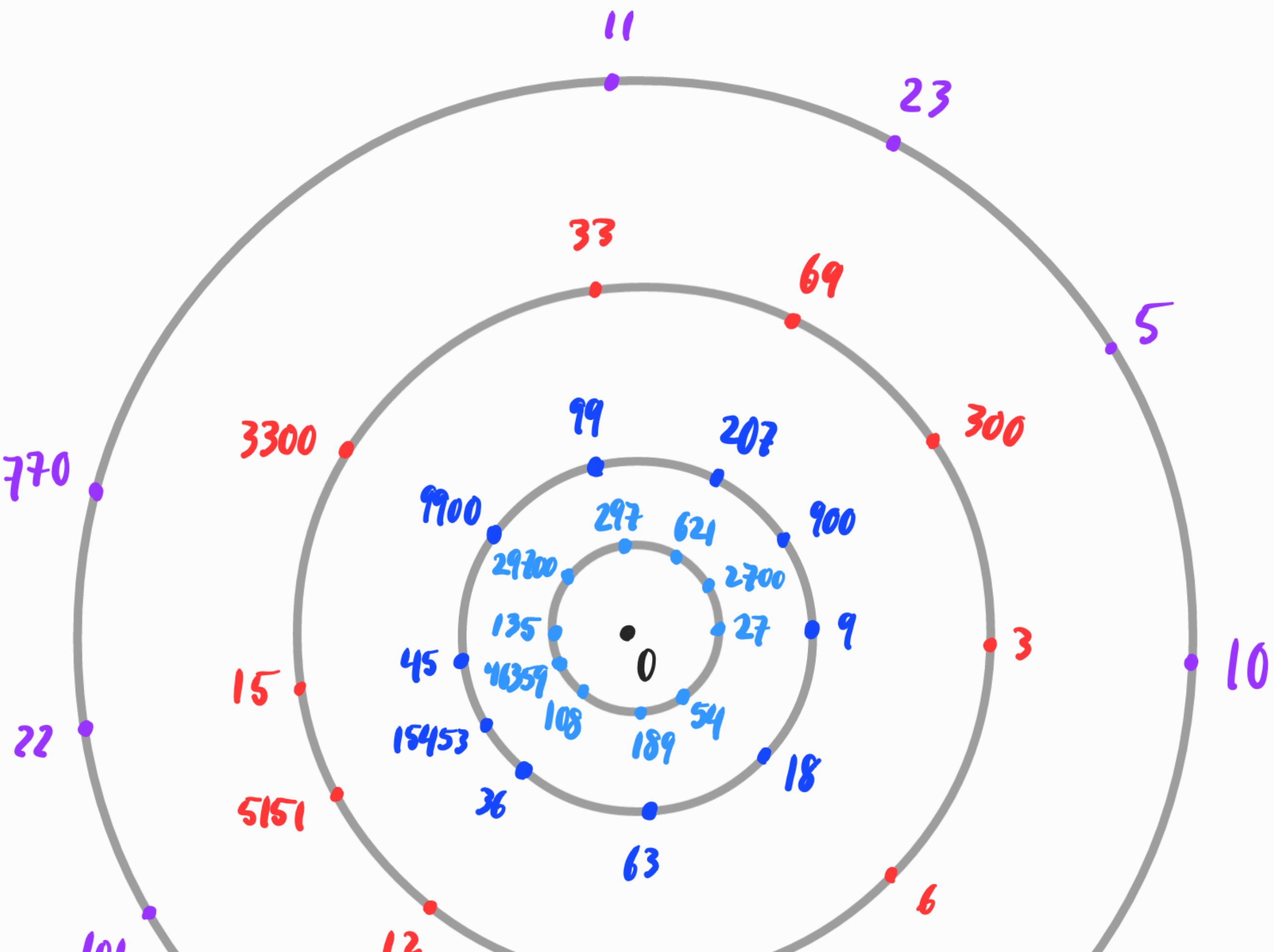
$$|x_n - L| < \varepsilon$$

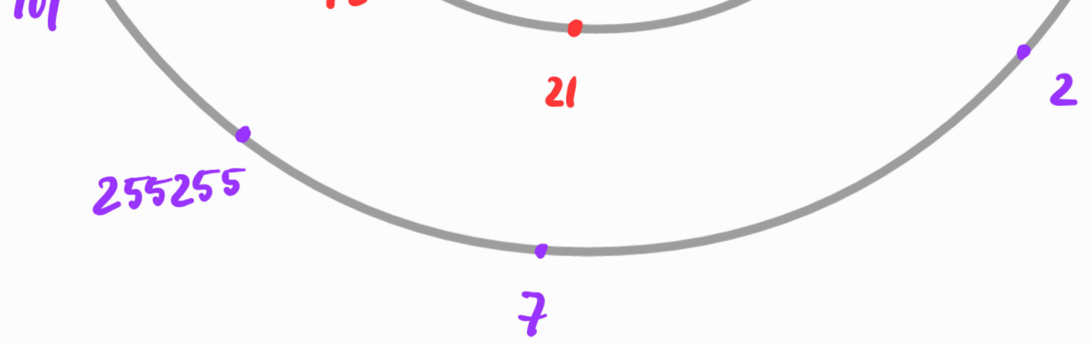
for some $L \in \mathbb{Q}$, called the limit of (x_n), written

$$L = \lim_{n \to \infty} x_n .$$

Remark: There is an absolute value called the trivial absolute value, defined by

$$|x|_0 = 0 \quad \text{for all } x \in \mathbb{Q}.$$





Circles in the 3-adic system

Theorem (Ostrowski) Every nontrivial absolute value on $\mathbb{Q}$ is, up to rescaling*, one of the p-adic absolute values $|\cdot|_p$ or the usual absolute value $|\cdot| = |\cdot|_\infty$.

$$\left(\quad |x|_\infty = \begin{cases} x, & x \geq 0 \\ -x, & x < 0. \end{cases} \right.$$

* "Rescaling" $|\cdot|_1$ means defining a new absolute value $|\cdot|_2$ by

$$|x|_2 = |x|_1^a \quad \text{for some real number } a > 0.$$

This has the property that convergent sequences in $|\cdot|_1$ are the same as convergent sequences in $|\cdot|_2$.

Theorem (Product Formula) For any nonzero rational number x,

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

Idea of proof: If $x = q$ is prime itself,

$$|x|_p = \begin{cases} 1, & p \neq q, \infty \\ \frac{1}{q}, & p = q \\ q, & p = \infty. \end{cases}$$

$\square$

Exercise 2: Verify the Product Formula for each $x \in \mathbb{Q}$.

(a) 400

(b) 902

(c) 621

(d) $\frac{123}{48}$

(e) $\frac{180}{3}$

Next, we need to identify which sequences of rational numbers "should" converge with respect to $|\cdot|_p$ and then enlarge $\mathbb{Q}$

to include the "limits" of such sequences.

$\boxed{\text{Def}}$ A sequence (x_n) in $\mathbb{Q}$ is called a **Cauchy sequence** if for every $\varepsilon > 0$, there's some $N \geq 1$ such that for all $n, m \geq N$,

$$|x_n - x_m| < \varepsilon.$$

Informally, Cauchy sequences "want to converge" because their terms eventually become close together.

Exercise 3: Show that every convergent

sequence is Cauchy.

Ex ① The sequence

$$(x_n) = (1, 1.4, 1.41, 1.414, 1.4142, 1.41421, \ldots)$$

is an example of a Cauchy sequence that does not converge with respect to $|\cdot|_\infty$.

In the real numbers however, it converges to $\sqrt{2}$.

Def The **completion** of $\mathbb{Q}$ with respect to an absolute value $|\cdot|$ is the set of equivalence classes of Cauchy sequences in $\mathbb{Q}$ with respect to $|\cdot|$, where two sequences (x_n) and (y_n) are equivalent if $\lim_{n\to\infty} |x_n - y_n| = 0$.

Exercise 4: (a) Check that this is an equivalence relation on Cauchy sequences.

(b) Show that for any equivalence class $x = [(x_n)]$, there is some $N \geq 1$ such that for all $n, m \geq N$, $|x_n| = |x_m|$.

(c) Define $|x| := |x_N|$ for N as above and check that this doesn't depend on the sequence (x_n) representing x.

For $|\cdot| = |\cdot|_\infty$, the completion of $\mathbb{Q}$ is precisely the real numbers, $\mathbb{R}$.

For a prime p, the completion of $\mathbb{Q}$ at $|\cdot|_p$ is called the field of p-adic numbers, $\mathbb{Q}_p$.

Much like with $\mathbb{R}$, the rationals $\mathbb{Q}$

$\mathbb{R}$, the rationals $\mathbb{Q}$

form a <u>dense</u> subset of each $\mathbb{Q}_p$, i.e.

there is a one-to-one map

$$\begin{aligned} \mathbb{Q} &\hookrightarrow \mathbb{Q}_p \\ x &\longmapsto [(x, x, x, \ldots)] \end{aligned}$$

such that every p-adic number is

arbitrarily close to some $x \in \mathbb{Q}$.

$\boxed{\text{Ex}}$ 2 In Lecture 14.1, we constructed

two coherent sequences

$$(x_1, x_2, x_3, x_4, \ldots) = (2, 7, 57, 182, \ldots)$$

$(y_1, y_2, y_3, y_4, \ldots) = (3, 18, 68, 443, \ldots)$

with the following 5-adic expansions:

$$(x_n) \longrightarrow \quad \ldots + 1\cdot 125 + 2\cdot 25 + 1\cdot 5 + 2\cdot 1 = \ldots 1212$$

$$(y_n) \longrightarrow \quad \ldots + 3\cdot 125 + 2\cdot 25 + 3\cdot 5 + 3\cdot 1 = \ldots 3233.$$

These are each Cauchy sequences with respect to $|\cdot|_5$, so they determine 5-adic numbers $x = [(x_n)]$ and $-x = [(y_n)]$ which are both solutions to

$$x^2 + 1 = 0$$

in $\mathbb{Q}_5$.

Exercise 5: Show that $x^2+1=0$ does not have a solution in $\mathbb{Q}_7$. Can you guess the primes p for which $x^2+1=0$ will have a solution in $\mathbb{Q}_p$?

Def The **p-adic integers** are the subset

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

In terms of the p-adic valuation,

$$x \in \mathbb{Z}_p \iff v_p(x) \geq 0.$$

This makes part of our number/function analogy clear:

p-adic integer	power series
$\sum_{i=0}^{\infty} a_i p^i$	$\sum_{i=0}^{\infty} a_i x^i$
p-adic number	**Laurent series**
$\sum_{i=-n}^{\infty} a_i p^i$	$\sum_{i=-n}^{\infty} a_i x^i$

(If $i=-n$ is the smallest index for which $a_i \neq 0$, then $v_p\left(\sum_{i=-n}^{\infty} a_i p^i\right) = -n$.)

More importantly, $\mathbb{Z}_p$ is exactly the

set of [illegible] sequences in $\mathbb{Z}$

set of p-adic coherent sequences in $\mathbb{Z}$.

Exercise 6: Prove this!

To summarize:

$$
\begin{tikzcd}
x \in \mathbb{Z}_p \arrow[rr, leftrightarrow] \arrow[dr, leftrightarrow] & & (x_n) \subseteq \mathbb{Z} \text{ coherent} \arrow[dl, leftrightarrow] \\
& x_n = \displaystyle\sum_{i=0}^{n} a_i p^i &
\end{tikzcd}
$$

Next time: applications of p-adic numbers.