Lecture 5: Relearning how to Function 😊

Background image: Fernando Villegas Negrete

NB: Throughout this lecture, $\ell_1$ will denote $\ell_1^p$

5.1 Functions and Continuity

- We have built up $\mathbb{Q}_p$ as an analogue of $\mathbb{R}$. We want to develop a theory of functions on $\mathbb{Q}_p$
We define continuity derivatives like for \( \mathbb{R} \):

**Definition**

Let \( U \subseteq \mathbb{Q}_p \) be an open set. A function \( f: U \to \mathbb{Q}_p \) is **continuous** at \( x_0 \in U \) if \( \forall \varepsilon > 0 \ \exists \delta > 0 \) s.t.

\[
|x - x_0| < \delta \implies |f(x) - f(x_0)| < \varepsilon.
\]

- Ex: polynomials in \( X \) cts everywhere, same proof as in \( \mathbb{R} \)
- Nonex: \( f(x) = \frac{1}{x} \) for \( x \neq 0 \) and \( f(0) = 0 \), a.e. \( \lim_{n \to \infty} p^n = 0 \) but \( |\frac{1}{p^n}| \to \infty \)

**Definition**

Let \( U \subseteq \mathbb{Q}_p \) be an open set. A function \( f: U \to \mathbb{Q}_p \) is **differentiable** at \( x_0 \in U \) if the limit

\[
f'(x_0) = \lim_{h \to 0} \frac{f(x_0 + h) - f(x_0)}{h}
\]

exists.

If \( f'(x_0) \) exists \( \forall x_0 \in U \) we say \( f \) is differentiable in \( U \).

- Ex: polynomials in \( X \) differentiable everywhere, same proof as in \( \mathbb{R} \),
  and for \( f(X) = X^n \), \( f'(X) = nX^{n-1} \)

- We can also state the mean value theorem, but it's false!

- Also, there are functions which are not loc. constant, but...
whose deriv. is the zero function!

\[ f : \mathbb{Z}_p \to \mathbb{Q}, \quad f\left( \frac{\mathbb{Z}_p}{i} \right) = \sum_{i=0}^{\infty} a_i p^i \]

12121 ... \to 10201 ...

- We can't do calculus etc the same way as in \( \mathbb{R} \).

5.2 A Series of Fortunate Events

- We focus now on functions defined by power series (in \( \mathbb{R} \) this is how \( e^x \) and \( \sin x \) arise)

- Given a power series, we want to determine where it defines a function (i.e. where it converges, the region of convergence)

**Theorem 5.3**

Let \( f(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Q}_p [[x]] \) and define

\[ \rho = \frac{1}{\limsup \sqrt[n]{|a_n|}} \]

1. If \( \rho = 0 \), then \( f(x) \) converges iff \( x = 0 \).
2. If \( \rho = \infty \), then \( f(x) \) converges \( \forall x \in \mathbb{Q}_p \).
3. If \( 0 < \rho < \infty \), and \( \lim \ln |a_n| = 0 \), then \( f(x) \) converges iff \( |x| \leq \rho \).
4. If \( 0 < \rho < \infty \), and \( \lim \ln |a_n| \neq 0 \), then \( f(x) \) converges.
5. Let $D_f = \{ x \in \mathbb{Q}_p : f(x) \text{ converges} \}$. The function $f: D_f \to \mathbb{Q}_p, x \mapsto f(x)$ is continuous.

Proof:

Caution! If the series $\sum_{n=1}^{\infty} x_n$ converges, then $(x_n)_{n \in \mathbb{N}}$ is a null sequence, but the converse is false!

$\mathbb{Q}_p$:

Follows from the fact that $\sum_{n=1}^{\infty} a_n x^n$ converges iff

$\lim |a_n x^n| = 0$.

The proof for 5 is identical to the proof over $\mathbb{R}$. ◼

Example: $f(X) = \sum_{n=1}^{\infty} p^n X^n$.

$p = \limsup \frac{1}{2^n(r^n)} = \limsup \frac{1}{|r|^n} = p$, and $|a_n| \to 0$ so $D = B_{e_1}(0,p)$. 

Courtesy of Joanne Beckford
- Example: \( g(x) = \sum x^n, \ p = 1, |a_n| \neq 0 \)
  
  Region of convergence for \( g \): \( B(0,1) = p \mathbb{Z}_p \)

- We can define sum \& product power series, and they are sum \& product as functions.

  For \( f(x) = \sum a_n x^n \), \( g(x) = \sum b_n x^n \),

  \[
  (f+g)(x) = \sum (a_n + b_n)x^n
  \]

  \[
  (fg)(x) = \sum \sum a_n b_{n-k} x^n
  \]

- Can the composition \( fog \) be written as a power series? If so, how?

  - Solve recursively for what the coefficients of \( h(x) = (f \circ g)(x) \) would have to be, call that the formal composition.

---

**Proposition 5.4**

Let \( f, g, h \in \mathbb{Q}_p [[x]] \) be as above. Let \( x \in \mathbb{Q}_p \) and suppose

1. \( g(x) \) converges
2. \( f \) converges at \( g(x) \)
3. \( \forall n \ |b_n x^n| \leq |g(x)| \)

Then \( h(x) \) converges and \( f(g(x)) = h(x) \)

- Note: false without 1, 2, 3!
What else might we want to do? Recenter a power series. Where would the new series converge?

**Theorem 5.5**

Let \( f(x) = \sum a_n x^n \), and let \( d \in D_f \) (\( f \) converges at \( d \)). For each \( m \geq 0 \), define

\[
b_m := \sum_{n=m}^{\infty} \binom{n}{m} a_n d^{n-m}
\]

\[
g(x) := \sum_{m=0}^{\infty} b_m (x - d)^m.
\]

1. The series defining \( b_m \) converges \( b_m \).
2. \( D_f = D_g \) (same region of convergence!)
3. For any \( x \in D_f \), \( f(x) = g(x) \).

**Proof:** omitted (see Gouvea 5.4.2)

But we note: ETS \( f, g \) have same radii of convergence since \( x \in D_f \land D_g \) and \( p \)-adic disks "are either concentric or disjoint, like drops of mercury" — Yves Andrès
• This is a cool fact, but it means we can't do analytic continuation like we do in $\mathbb{C}$.

• On to derivatives and differences:

\begin{theorem}
Let $f, g \in \mathbb{Q}_p[[X]]$, and suppose there is a non-stationary (i.e. not eventually constant) sequence $x_m \in \mathbb{Q}_p : \lim x_m = 0$ s.t. $f(x_m) = g(x_m) \forall m$. Then $f(x) = g(x)$ (same coefficients!)
\end{theorem}

Proof sketch: Same as for $\mathbb{R}$, WTS difference is 0 porer ans. ( $f, g \in \mathbb{Q}_p[[X]]$, $\lambda(x_m) \to \text{const. term of } h$.)

\begin{theorem}
Let $f(x) = \sum a_n x^n \in \mathbb{Q}_p[[x]]$ and let $f'$ be the formal derivative of $f(x)$. Let $x \in \mathbb{Q}_p$. If $x \in D_f$ then $x \in D_{f'}$, and
\[ f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h} \]
\end{theorem}

Proof: if $x \neq 0$, we see
\[ \left| a_n x^n \right| < \left| a_{n-1} x^{n-1} \right| = \frac{1}{\left| a_n \right|} \left| a_{n-1} \right| x^n \to 0 \]
Next, let \( r \in \mathbb{R} : D_f = B_0(0, r) \). Suppose \( 0 < |x| \leq r \), then
\[
\frac{f(x+h) - f(x)}{h} = \sum_{n=1}^{\infty} \sum_{m=1}^{n} a_n(n) x^{n-m} h^{m-1}.
\]
then
\[
|a_n(n) x^{n-m} h^{m-1}| \leq |a_n| r^{n-1}
\]
so we can set \( h=0 \) and
\[
f'(x) = \sum_{n=1}^{\infty} n a_n x^{n-1}
\]
Our coveted result follows immediately!

**Theorem 5.8**
Suppose \( f, g \in \mathbb{C}_p[0, X] \) and that \( f, g \) converge for \( |x| < p \).
If \( f'(x) = g'(x) \) \( \forall |x| < p \), then \( \exists \) a constant \( C \in \mathbb{C}_p : f(x) = g(x) + C. \)

**Proof:** \( f', g' \) have the same coefficients, hence so do \( f, g \) aside from potentially the constant term.

5.3 Rooting Around (because pigs root around)

* We now explore the zeros of functions defined by power...
But first, an important and useful topological fact:

**Theorem 5.9**

\[ \mathbb{Z}_p \text{ is compact} \]

**Proof:** \( \mathbb{Z}_p \) is a closed subset of \( \mathbb{Q}_p \), which is complete, so \( \mathbb{Z}_p \) is complete.

And for \( i > 0 \), \( \exists \ N \in \mathbb{N} : p^{-N} < \varepsilon \). And

\[
\mathbb{Z}_p = \bigcup_{i=0}^{n-1} i + p^n \mathbb{Z}_p
\]

is a covering of \( \mathbb{Z}_p \) by finitely many balls of radius \( < \varepsilon \), so \( \mathbb{Z}_p \) is also totally bounded. \( \Box \)
Back to the zeros:

**Strassman’s Theorem**

Let \( f(x) = \sum_{n=0}^{\infty} a_n x^n \) be a nonzero elt of \( \mathbb{Q}_p[[x]] \). Suppose \( \lim_{n \to \infty} a_n = 0 \) (so \( f(x) \) converges for \( x \in \mathbb{Z}_p \)).

Let \( N \) be the integer s.t.

\[
|a_N| = \max \{ |a_n| : n \leq N \} \quad \text{and} \quad |a_n| < |a_N| \quad \forall \ n > N.
\]

Then the function \( f: \mathbb{Z}_p \to \mathbb{Q}_p \), \( x \mapsto f(x) \) has at most \( N \) zeros.

Also, if \( \{a_1, \ldots, a_m\} \) are the zeros of \( f \), then \( \exists g \in \mathbb{Q}_p[[x]]: \)

\[
f(x) = (x-a_1) \cdots (x-a_m) g(x)
\]

so \( g \) converges on \( \mathbb{Z}_p \) and has no zeros in \( \mathbb{Z}_p \).

Proof sketch: Induct on \( N \), rearrange series to factor out \( x-a \) for \( a \) a root (Gouvea 5.4.6).

- Consequences: \( f \) has fin. many zeros in \( \mathbb{Z}_p \).
- If $f, g$ agree on infinitely many points in some disk $p^{-n} \mathbb{Z}$, then $f = g$ as power series

- $f$ cannot be periodic if $f$ is nonconstant!
  
  If $\exists x \in \mathbb{N}$: $f(x+p) = f(x)$ for all $x \in p^{-n} \mathbb{Z}$, $f$ is constant. **No!**

- Next: roots beyond $\mathbb{Q}_p$

- We'll take the following theorem as a black box:

Theorem 5.11: Complex #s but make it $p$-adic

There exists a field $\mathbb{C}_p$ and a valuation $v_p(\cdot)$ on $\mathbb{C}_p$

1. $\mathbb{Q}_p \subset \mathbb{C}_p$ and $1:1$ extends $1:1$
2. $\mathbb{C}_p$ is complete \& algebraically closed
3. $\mathbb{Q}_p$ is dense in $\mathbb{C}_p$
4. $\text{Ev}_p(x): x \in \mathbb{C}_p \to \mathbb{Q}$
Tool for investigating roots:

**Definition:** Let \( K = \mathbb{C}_p \) or a fin. ext. of \( \mathbb{Q}_p \). Let \( f = a_0 + a_1 x + \ldots + a_n x^n \in K[x] \). Then the Newton polygon of \( f \), denoted \( NP_p(f) \), is the lower convex hull in \( \mathbb{R}^2 \) of the points

\[
S = \{(i, v_p(a_i)) : i = 0, 1, \ldots, n \text{ and } a_i \neq 0\}
\]

- Procedure: let rope hang below points of \( S \), pull upward until it is taut.

- Example: \( NP_5(f) \)

\[
f(x) = 1 + 5x + \frac{1}{2}x^2 + 3\frac{5}{4}x^3 + 2\frac{5}{4}x^5 + 625x^6
\]

\[
S = \{(0, 0) \quad (1, 1) \quad (2, -1) \quad (3, 1) \quad (5, 2) \quad (6, 4) \}
\]
We define the "width" of a line segment as the length of its projection onto the x-axis.

This simple drawing gives us a ton of information about the roots of $f$.

**Theorem 5.13**
Let $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in K[X]$. Let $m_1, \ldots, m_r$ be the slopes of $NP_p(f)$, with corresponding widths $w_1, \ldots, w_r$. Then for each $k : 1 \leq k \leq r$, $f(X)$ has exactly $w_k$ roots (in $\overline{F}$, counting multiplicity) with abs. val $p^{-m_k}$ (so valuation $-m_k$).

*(partial) Proof:* we will show that if $f(d) = 0$,
If the min is uniquely attained, it becomes a contradiction.

We minimize \( g(x,y) \), where \( g(x,y) = (v, a) \cdot x + y \).

Claim: the min of \( g \) over points of \( S \) must occur at an extremal point of \( NP_\alpha(f) \).

\[ v_\alpha(0) = v_\alpha(f(0)) = v_\alpha \left( \sum_{i=0}^{N} a_i \cdot \alpha^i \right) \geq \min \left\{ v_\alpha(a_i \cdot \alpha^i) \right\} \]

\[ = \min \left\{ (v_\alpha \cdot \alpha^i) \cdot x + y \mid (x,y) \in S \right\} \]

\( \Box \)

---

Corollary 5.14: Eisenstein's Criterion

\( (v_\alpha \cdot \alpha^i) \cdot x + y = c \) is a line of slope \( -v_\alpha \cdot \alpha^i \).

Points s.t. \( g(x,y) = c \).

\( (v_\alpha \cdot \alpha^i) \cdot x + y = c' < c \)

\( (v_\alpha \cdot \alpha^i) \cdot x + y = c'' < c \)

\( g \) smaller at \( \Box \).
Let $p \in \mathbb{Z}$ be a prime and let
\[ f(X) = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} + X^n \in \mathbb{Z}[X] \]
such that $p \mid a_i$ for $i < n$ and $p^2 \nmid a_0$. Then $f$ is irreducible over \( \mathbb{Q} \).

Proof:

- By theorem, all roots of $f$ have valuation $\frac{1}{n}$.
- But if $\alpha$ is a root of $g \in \mathbb{Q}[X]$ and $g$ has degree $d$, then $v_p(d) \leq \frac{1}{d} \mathbb{Z}$.

\[ \text{(ex: if } \alpha^2 = p^3, 2v_p(d) = 3 \text{ so } v_p(d) = \frac{3}{2}) \]

5.41 Connecting the Dots (another way)

- We will now step back and talk about how to construct $p$-adic functions via interpolation

- Picture in \( \mathbb{N} \):
Example in \( \mathbb{Q}_p \): if \( c \in \mathbb{Z}_p \) and \( a \in \mathbb{Z} \), we can define \( f(a) = c^a = (\underbrace{c \cdot c \cdots c}_{a \text{ times}}) \) (or \( f(a) = \frac{1}{c} \cdots \frac{1}{c} - a \text{ times if } a < 0 \)).

- Want to extend \( f \) to a function defined on more of \( \mathbb{Q}_p \).
Definition
For a valued field $K$ and set $S \subseteq K$, a function $f : S \to K$ is uniformly continuous if $\forall \varepsilon > 0 \exists \delta > 0$ s.t. $\forall x, y \in S$,
$$|x - y| < \delta \implies |f(x) - f(y)| < \varepsilon.$$ 

Proposition 5.16
Let $S \subseteq \mathbb{Z}_p$ be a dense subset, and let $f : S \to \mathbb{Q}_p$ be a function. Then $\exists$ a continuous extension $\tilde{f} : \mathbb{Z}_p \to \mathbb{Q}_p$ of $f$ to $\mathbb{Z}_p$ iff $f$ is bounded and uniformly continuous. If $\tilde{f}$ exists, it is unique.

Proof: any extension $\tilde{f}$ is unique by density of $S$.
$\implies$: If $\tilde{f}$ is cts, it is bounded and uniformly continuous by compactness of $\mathbb{Z}_p$. 
If \( x \in \mathbb{Z}_p \), then \( k \to \lim x_n \) for \( x \in S \).

so \( \lim (f(x_{n+1}) - f(x_n)) = 0 \) since \( f \) add. unif. cts,

some define:

\[
\forall \epsilon > 0 \exists N \in \mathbb{N} : \forall n \geq N \quad |f(x_{n+1}) - f(x_n)| < \epsilon
\]

. What does this look like in \( \mathbb{Q}_p \)?

**Proposition 5.17**

For a set \( S \subseteq \mathbb{Q}_p \), a function \( f : S \to K \) is uniformly continuous if \( \forall m \in \mathbb{Z} \exists N \in \mathbb{Z} : \]

\[
d \equiv b \pmod{p^N} \implies f(d) \equiv f(b) \pmod{p^m}
\]

. Hence \( f \) boundedness on a dense set is enough to check for existence of extension of \( f \) on \( S \).