Elementary Analysis in $\mathbb{Q}_p$

Hannah Hutter, May Szedlák, Philipp Wirth

November 17, 2011

This report follows very closely the book of Svetlana Katok[1].

1 Sequences and Series

In this section we will see some properties of sequences and series in $\mathbb{Q}_p$. Recall from the first presentation that $\mathbb{Q}_p$ is a complete metric space. Hence every Cauchy sequence converges and therefore the set of the convergent sequences is the set of the Cauchy sequences.
We will also see that we have some much better properties in $\mathbb{Q}_p$, than we are used to in the real case. The first example is the characterization of the Cauchy sequences.

Theorem 1. *A sequence $\{a_n\}$ in $\mathbb{Q}_p$ is a Cauchy sequence (i.e. converges), if and only if*

$$\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0.$$

Remark. This is obviously not true in $\mathbb{R}$. For example take $a_n = \sum_{k=1}^{n} \frac{1}{k}$ the n-th harmonic number. Then $\lim_{n\to\infty} |a_{n+1} - a_n|_p = \lim_{n\to\infty} \frac{1}{n+1} = 0$ but as we know the a_n is not Cauchy.

Proof. Remember that if $\{a_n\}$ is a Cauchy sequence, then

$$\lim_{m,n\to\infty} |a_m - a_n|_p = 0.$$

The first direction follows immediately for $m = n + 1$. Note that this is true for Cauchy sequences in any metric space.

[1] Katok, Svetlana; p-adic Analysis Compared with Real, American Mathematical Society, 2007

For the converse assume $\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0$. This means that for any $\epsilon > 0$ there exists $N \in \mathbb{N}$ s.t. for $n > N$

$$|a_{n+1} - a_n|_p < \epsilon.$$

Then for any $m > n > N$, using the strong triangle inequality, we get

$$\begin{aligned} |a_m - a_n|_p &= |a_m - a_{m-1} + a_{m-1} - a_{m-2} + \cdots - a_n|_p \\ &\leq \max(|a_m - a_{m-1}|_p, \ldots, |a_{n+1} - a_n|_p) < \epsilon, \end{aligned}$$

which completes the proof. □

Definition 1. *Let the series* $\sum_{n=1}^{\infty} a_n$ *be in* $\mathbb{Q}_p$.
The sum converges *if the sequence of its partial sums converges in* $\mathbb{Q}_p$*, i.e. if* $\lim_{N\to\infty} |S_{N+1} - S_N|_p = 0$ *where* $S_N = \sum_{n=1}^{N} a_n$.
The sum converges absolutely *if* $\sum_{n=1}^{\infty} |a_n|_p$ *converges in* $\mathbb{R}$.

Example. We have

$$\sum_{n=1}^{\infty} n^2 \cdot (n+1)! = 2$$

in $\mathbb{Q}_p$, for any p.
By induction we will show that for the N partial sum one has

$$\sum_{n=1}^{N} n^2 \cdot (n+1)! = 2 + (N-1) \cdot (N+2)!.$$

Then

$$\Big| \sum_{n=1}^{\infty} n^2 \cdot (n+1)! - 2 \Big|_p = \lim_{N\to\infty} |2 + (N-1) \cdot (N+2)! - 2|_p = 0$$

since $|(N+2)!|_p \to 0$ for $N \to \infty$. The proof by induction is simple calculus:
Case $N = 1$:

$$\sum_{n=1}^{1} n^2 \cdot (n+1)! = 1 \cdot 2 = 2 = 2 + (1-1) \cdot (1+2)!,$$

hence the induction base holds. For $N \to N+1$:

$$\begin{aligned} \sum_{n=1}^{N+1} n^2 \cdot (n+1)! &= \sum_{n=1}^{N} n^2 \cdot (n+1)! + (N+1)^2 \cdot (N+2)! \\ &= 2 + (N-1) \cdot (N+2)! + (N+1)^2 \cdot (N+2)! \\ &= 2 + (N+2)! \cdot (N - 1 + N^2 + 2N + 1) \\ &= 2 + N \cdot (N+3)!. \end{aligned}$$

As we are used to in $\mathbb{R}$, convergence follows from absolute convergence by the triangle inequality.

Proposition 1. *If the series $\sum_{i=1}^{\infty} |a_i|_p$ converges absolutely (in $\mathbb{R}$), then $\sum_{i=1}^{\infty} a_i$ converges in $\mathbb{Q}_p$.*

Proof. Suppose that $\sum_{i=1}^{\infty} |a_i|_p$ converges. Then the sequence of its partial sums is Cauchy i.e. for any $\epsilon > 0$ there exists $N \in \mathbb{N}$ s.t. for all $m > n > N$, we have $\sum_{i=n+1}^{m} |a_i|_p < \epsilon$. By the usual triangle inequality we get

$$|S_m - S_n|_p = \Big| \sum_{i=n+1}^{m} a_i \Big|_p \leq \sum_{i=n+1}^{m} |a_i|_p < \epsilon.$$

Therefore $\{S_n\}$ is a Cauchy sequence and by definition $\sum_{i=1}^{\infty} a_i$ converges in $\mathbb{Q}_p$. $\square$

We however can get a much better result in $\mathbb{Q}_p$ as seen in the next proposition.

Proposition 2. *A series $\sum_{i=1}^{\infty} a_i$ in $\mathbb{Q}_p$ converges in $\mathbb{Q}_p$ if and only if $\lim_{i\to\infty} a_i = 0$ and in this case*

$$\Big| \sum_{i=1}^{\infty} a_i \Big|_p \leq \max_n |a_i|_p.$$

Remark. The last property can be considered as the *strongest wins property* for converging series.
Remark. We again know that this proposition is not true in $\mathbb{R}$. By taking $a_i = \frac{1}{i}$, we can see that $\lim_{i\to\infty} a_i = 0$ but again the corresponding series does not converge.

Proof. We know by definition that $\sum_{i=1}^{\infty} a_i$ converges if and only if the sequence of partial sums $S_n = \sum_{i=1}^{\infty} a_i$ converges. Since $a_n = S_n - S_{n-1}$ the series converges if and only if a_n goes to 0. For the second part we assume that $\sum_{i=1}^{\infty} a_i$ converges. In the case where $\sum_{i=1}^{\infty} a_i = 0$ the proof is trivial. Now suppose $\sum_{i=1}^{\infty} a_i \neq 0$. Then by the strong triangle inequality for any partial sum we have

$$\Big| \sum_{i=1}^{n} a_i \Big|_p \leq \max_{1\leq i\leq n} |a_i|_p.$$

Since $a_i \to 0$ for $n \to \infty$ for large enough N we have

$$\max_{1\leq i\leq N} |a_i|_p = \max_n |a_n|_p.$$

Since the partial sum $\sum_{i=1}^{n} a_i$ converges to $\sum_{i=1}^{\infty} a_i \neq 0$ and the p-adic norm can only take a discrete amount of values, for m large enough we have $\left|\sum_{i=1}^{m} a_i\right|_p = \left|\sum_{i=1}^{\infty} a_i\right|_p$. The claim follows by taking the maximum of m and n. $\square$

Definition 2. *A series $\sum_{n=0}^{\infty} a_n$ converges* unconditionally *if for any reordering of the terms $a_n \to a'_n$ the series $\sum_{n=0}^{\infty} a'_n$ also converges.*

Theorem 2. *If $\sum_{n=0}^{\infty} a_n$ converges, it converges unconditionally and the sum does not depend on the reordering.*

Remark. This is not true in $\mathbb{R}$. We can even prove that for any convergent but not absolutely convergent series $\sum_{n=0}^{\infty} a_n$ we have that for every $x \in \mathbb{R}$ there exists a reordering of the summands $a_n \to a'_n$ such that $\sum_{n=0}^{\infty} a'_n = x$.

Proof. Let $\epsilon > 0$ and let $N \in \mathbb{N}$ s.t. for any $n > N$ we have that $|a_n|_p < \epsilon$, $|a'_n| < \epsilon$ and

$$\left|\sum_{n=1}^{\infty} a_n - \sum_{n=1}^{N} a_n\right|_p < \epsilon.$$

We know that we can find such an N since by Proposition 2 the terms a_n tend to zero. Let $S = \sum_{n=1}^{N} a_n$ and $S' = \sum_{n=1}^{N} a'_n$ and define by S_1 and S'_1, respectively, the sum of all terms in S for which $|a_n|_p \geq \epsilon$ and the sum of all terms of S' for which $|a'_n|_p \geq \epsilon$. By construction it is clear that S_1 and S'_1 contain the same terms and therefore $S_1 = S'_1$. The sum S differs from S_1 only by the terms a_n satisfying $|a_n|_p < \epsilon$ and similarly S' from S'_1 by the terms a'_n satisfying $|a'_n|_p < \epsilon$. Hence by applying the strong triangle inequality we get $|S - S_1|_p < \epsilon$ and $|S' - S'_1|_p < \epsilon$ and therefore $|S - S'|_p < \epsilon$. Hence we have

$$\left|\sum_{n=1}^{\infty} a_n - \sum_{n=1}^{N} a'_n\right|_p = \left|\sum_{n=1}^{\infty} a_n - \sum_{n=1}^{N} a_n + \sum_{n=1}^{N} a_n - \sum_{n=1}^{N} a'_n\right|_p < \epsilon.$$

Now for $\epsilon \to 0$ we see that the series $\sum_{n=1}^{\infty} a'_n$ converges and

$$\sum_{n=1}^{\infty} a_n = \sum_{n=1}^{\infty} a'_n$$

as desired. $\square$

Remark. As in $\mathbb{R}$, convergence does not imply absolute convergence. Consider the following series: 1; p repeated p times; p^2 repeated p^2 times; .... Since the terms converge to 0 the series converges but

$$\sum_{i=1}^{\infty} |a_n|_p = 1 + p \cdot p^{-1} + p^2 \cdot p^{-2} + \cdots = \infty,$$

and hence the series does not converge absolutely.
Conclusion. Summing up the previous theorems and remarks we can conclude the following properties.
In $\mathbb{Q}_p$ one has the follwing implications:
absolute convergence $\Rightarrow$ convergence $\Leftrightarrow$ unconditional convergence.
On the other hand in $\mathbb{R}$ one has:
absolute convergence $\Rightarrow$ unconditional convergence $\Rightarrow$ convergence.
Note that different from $\mathbb{Q}_p$ in $\mathbb{R}$: convergence $\not\Rightarrow$ unconditional convergence.
In both cases one has:
convergence, unconditional convergence $\not\Rightarrow$ absolute convergence.

The next proposition is pretty subtle in the real case and stated here because it will be used later.

Theorem 3. *Let $b_{ij} \in \mathbb{Q}_p$, $i, j = 1, 2, \ldots,$ such that for any $\epsilon > 0$ there exists $N \in \mathbb{N}$ such that*

$$max(i, j) \geq N \Rightarrow |b_{ij}|_p < \epsilon$$

i.e. $|b_{ij}|_p$ tends to zero if either i or j goes to infinity. Then the two series

$$\sum_{i=1}^{\infty} (\sum_{j=1}^{\infty} b_{ij}) \text{ and } \sum_{j=1}^{\infty} (\sum_{i=1}^{\infty} b_{ij})$$

converge, and their sums are equal.

Proof. We know from Proposition 2 that $\sum_{j=1}^{\infty} b_{ij}$ converges for all i and $\sum_{i=1}^{\infty} b_{ij}$ converges for all j. By the same proposition we know that for all $i \geq N$

$$\Big| \sum_{j=1}^{\infty} b_{ij} \Big|_p \leq \max_j |b_{ij}|_p < \epsilon$$

and for all $j \geq N$

$$\Big| \sum_{i=1}^{\infty} b_{ij} \Big|_p \leq \max_i |b_{ij}|_p < \epsilon.$$

This implies that both double series converge, again by Proposition 2. It is therefore left to show that both sums are equal. We know that

$$\begin{aligned}
&\Big|\sum_{i=1}^{\infty}\Big(\sum_{j=1}^{\infty} b_{ij}\Big) - \sum_{i=1}^{N}\Big(\sum_{j=1}^{N} b_{ij}\Big)\Big|_p \\
=&\Big|\sum_{i=1}^{N}\Big(\sum_{j=N+1}^{\infty} b_{ij}\Big) + \sum_{i=N+1}^{\infty}\Big(\sum_{j=1}^{\infty} b_{ij}\Big)\Big|_p \\
\leq &\max\Big\{\Big|\sum_{i=1}^{N}\Big(\sum_{j=N+1}^{\infty} b_{ij}\Big)\Big|_p, \Big|\sum_{i=N+1}^{\infty}\Big(\sum_{j=1}^{\infty} b_{ij}\Big)\Big|_p\Big\} < \epsilon,
\end{aligned}$$

where the last inequality follows from Proposition 2. Since this is true for any ϵ, the series must be equal. □

2 p-adic Power Series

Definition 3. *As in the real case a* formal power series *is of the form*

$$f(X) = \sum_{n=0}^{\infty} a_n X^n,$$

where the coefficients a_n are in $\mathbb{Q}_p$ and X is the indeterminate.
The set of all power series *in X with coefficients in $\mathbb{Q}_p$ are denoted by $\mathbb{Q}_p[[X]]$ and the set of all* polynomials *by $\mathbb{Q}_p[X]$.*

Let $x \in \mathbb{Q}_p$ and $f \in \mathbb{Q}_p[[\cdot]]$. Then the corresponding power series $f(x)$ is $\sum_{n=0}^{\infty} a_n x^n$. From Proposition 2 we know that $f(x)$ converges if and only if $|a_n x^n|_p \to 0$. Therefore if for a $0 \leq r \in \mathbb{R}$ we have that $|a_n|_p r^n \to 0$, our series $\sum_{n=0}^{\infty} a_n x^n$ converges for any $x \in \mathbb{Q}_p$ s.t. $|x|_p \leq r$.

Definition 4. *For a power series $f(X) = \sum_{n=0}^{\infty} a_n X^n$ with $a_n \in \mathbb{Q}_p$ the* radius of convergence *is defined as the extended real number $0 \leq r_f \leq \infty$ s.t.*

$$r_f = \sup\{r \geq 0 : |a_n|_p r^n \to 0\}.$$

The extended real numbers are defined as $\mathbb{R} \cup \{\infty\}$.

The convergence radius can be computed as in the Archimedian case.

Proposition 3. *For a power series $f(X) = \sum_{n=0}^{\infty} a_n X^n$ the radius of convergence is*

$$r_f = \frac{1}{\limsup_n |a_n|_p^{\frac{1}{n}}}.$$

Proof. The proof works as in the real case. Suppose that $|x|_p > r_f$ (in the case where $r_f < \infty$). We have

$$\limsup |x|_p |a_k|_p^{\frac{1}{k}} = |x|_p \limsup |a_k|_p^{\frac{1}{k}} = |x|_p \cdot \frac{1}{r_f} > 1.$$

Therefore for infinitely many values k we have that $|a_k|_p |x|_p^k > 0$ i.e. $a_k x^k$ does not converge to 0 and hence the series diverges.
Now suppose that $|x|_p < r_f$ (in the case where $r_f > 0$). Then we can choose $r \in \mathbb{R}$ such that $|x|_p < r < r_f$. Then

$$\limsup r|a_k|_p^{\frac{1}{k}} = r \limsup |a_k|_p^{\frac{1}{k}} = \frac{r}{r_f} < 1.$$

Hence there exists an $N \in \mathbb{N}$ such that

$$\sup_{k \geq N} r|a_k|_p^{\frac{1}{k}} < 1.$$

Therefore for $k > N$ we have $|a_k|_p r^k < 1$ and

$$|a_k x^k|_p = |a_k|_p r^k \left(\frac{|x|_p}{r}\right)^k < \frac{|x|_p^k}{r^k} \to 0 \text{ for } k \to \infty.$$

Since the terms of the series go to 0 it follows that the series converges. □

The natural question that arises is, whether the series converges on the boundary or not.

Proposition 4. *The domain of convergence of a p-adic power series $f(X) \in \mathbb{Q}_p[[X]]$ is a ball $D = \{|x|_p \leq R\}$ where $R \in \{p^k, k \in \mathbb{Z}\} \cup \{0\} \cup \{\infty\}$, and the series converges uniformly in D.*

Remark. We know that in the Archemedian case we can not make a statement about the convergence on the boundary. Take for example the power series of ln. We know that $\ln(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} x^n / n$. One can find the the radius of convergence is 1, but for $x = -1$ the series diverges and for $x = 1$ the series converges.

Proof. Suppose the radius of convergence of $f(X)$ is r_f. As seen before the series converges on the open ball $D = \{|x|_p < R\}$. We know that on the boundary i.e. where $|x|_p = r_f$, $f(X)$ converges if and only if $|a_n x^n|_p \to 0$. We can observe that this depends only on the norm of x and not the specific value of x, hence either for all points with $|x|_p = r_f$ the series converges or it does for none. If the series converges for all points with $|x|_p = r_f$ then we

have $R = r_f$. If the series diverges for all points with $|x|_p = r_f$, then we have $R = p^{-1} r_f$.
Finally for any $|x|_p \leq R$ we have

$$|a_n x^n|_p \leq |a_n R^n|_p \to 0$$

and therefore the uniform convergence on D follows. □

3 p-adic Logarithm and Exponential

Definition 5. *Similar as in the real setting, we define the* p-adic logarithm *by the series*

$$ln_p(x) := \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}.$$

This series converges for all $x \in B := \left\{ x \in \mathbb{Z}_p | \, |x-1|_p < 1 \right\} = 1 + p\mathbb{Z}_p$.

Note that the p-adic logarithm corresponds to the formal power series

$$log(1+X) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n} \in \mathbb{Q}[[X]].$$

Theorem 4. *The p-adic logarithm satisfies the fundamental property*

$$ln_p(xy) = ln_p(x) + ln_p(y)$$

for all $x, y \in B$ *such that* xy *is in* B *as well.*

Proof. Consider the following identity of formal power series:

$$log(1+X) + log(1+Y) - log(1+X+Y+XY) = 0.$$

Clearly, this holds for the real logarithmic function, i.e. the left hand side of the above identity vanishes for all real numbers x, $y \in (-1, 1)$. We also know that all the series converge absolutely, which means that we can rearrange the terms such that the left side is of the form $\sum c_{i,j} x^i y^j$ with $c_{i,j} = 0$ for all $i, j \in \mathbb{N}$.
Now we choose any $\alpha, \beta \in p\mathbb{Z}_p$. Clearly, $\alpha + \beta + \alpha\beta \in p\mathbb{Z}_p$ and by applying Theorem 3, the expression

$$ln_p(1+\alpha) + ln_p(1+\beta) - ln_p((1+\alpha)(1+\beta))$$

can be written in the form $\sum c_{i,j} \alpha^i \beta^j$ where all $c_{i,j} = 0$. This implies the theorem. □

Definition 6. *Consider the formal power series*

$$exp\,(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}$$

the corresponding power series in $\mathbb{Q}_p$ *is called the* p-adic exponential *and is denoted by* $exp_p\,(x)$.

Unfortunately, the radius of convergence of the p-adic exponential is not as obvious as the one of the p-adic logarithm. To find this, we need the following

Lemma 1. *For any positive integer* $n \in \mathbb{N}$, *let*

$$n = \sum_{i=0}^{k} a_i p^i$$

be its expansion in base p. *We then have*

$$ord_p\,(n!) = \frac{n - S_n}{p-1},$$

where $S_n = a_0 + a_1 + ... + a_k$.

Proof. If $p > n$, we have $S_n = n$ and therefore $\frac{n-S_n}{p-1} = 0$. Of course this is true since $p \nmid n!$ and therefore $ord_p\,(n!) = 0$. Now let us assume $p \leq n$ and let $n = \sum_{i=0}^{k} a_i p^i$ be the expansion of n in base p. For any $1 \leq i \leq k$ there are exactly

$$\left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^{i+1}} \right\rfloor$$

numbers between 1 and n such that p^i is the is the greatest power of p dividing each. So we get

$$ord_p\,(n!) = \sum_{i=1}^{k} i \left(\left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^{i+1}} \right\rfloor \right) = \sum_{i=1}^{k} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Here the last equation holds because for $i \geq 2$, each term appears twice in the sum, once with coefficient i and once with coefficient $-(i+1)$. Further, $\left\lfloor \frac{n}{p^{k+1}} \right\rfloor = 0$ by the definition of k.

On the other hand we have

$$\begin{aligned}
\frac{n-S_n}{p-1} &= \frac{\left(a_0+a_1p+...+a_kp^k\right)-\left(a_0+a_1+...+a_k\right)}{p-1} \\
&= \frac{a_1\left(p-1\right)+a_2\left(p^2-1\right)+...+a_k\left(p^k-1\right)}{p-1} \\
&= \sum_{i=1}^{k} a_i\left(\sum_{j=0}^{k-1} p^j\right) = \sum_{1\le j<i\le k} a_ip^j \\
&= \left(a_1+a_2p+...+a_kp^{k-1}\right) \\
&+ \left(a_2+a_3p+...+a_kp^{k-2}\right) \\
&+ ... \\
&+ a_k \\
&= \left\lfloor\frac{n}{p}\right\rfloor + \left\lfloor\frac{n}{p^2}\right\rfloor + \left\lfloor\frac{n}{p^k}\right\rfloor = \sum_{i=1}^{k}\left\lfloor\frac{n}{p^i}\right\rfloor
\end{aligned}$$

as desired. □

Theorem 5. *The p-adic exponential exp_p converges in the disc*

$$D_p := \left\{x\in\mathbb{Q}_p \middle| \left|x\right|_p < p^{-1/(p-1)}\right\}.$$

Proof. The convergence radius r_p of a power series $\sum a_nX^n$ is given by the formula

$$r_p = \frac{1}{\limsup\left|a_n\right|_p^{1/n}}.$$

In our case, $a_n = 1/n!$. Thus we get by Lemma 1

$$ord_p\left(r_p\right) = -\liminf\frac{1}{n}ord_p\left(a_n\right) = \liminf\left(\frac{n-S_n}{n\left(p-1\right)}\right) = \frac{1}{p-1},$$

where S_n is the same as in Lemma 1 and the last equality holds since

$$\lim_{n\to\infty} -\frac{n-S_n}{n} = -1+\lim_{n\to\infty}\frac{S_n}{n} = -1.$$

Since r_p is a power of p, we have

$$r_p = p^{ord_p(r_p)} = p^{-1/(p-1)}.$$

□

Remark. If $|x|_p = p^{-1/(p-1)}$ then we have

$$ord_p\left(\frac{x^n}{n!}\right) = -\frac{n-S_n}{p-1} + \frac{n}{p-1} = \frac{S_n}{p-1}.$$

Now consider the subsequence $n_k = p^k$. Then $S_{n_k} = 1$ and $ord_p\left(x^{n_k}/n_k!\right) = \frac{1}{p-1}$. Hence we have

$$\lim_{k\to\infty}\left|\frac{x^{n_k}}{n_k!}\right|_p \neq 0 \text{ for } |x|_p = p^{-1/(p-1)}.$$

This means that $exp_p(x)$ diverges on ∂D_p.

Proposition 5. *The p-adic exponential satisfies the fundamental property*

$$exp_p(x+y) = exp_p(x)\, exp_p(y)$$

for all $x, y \in D_p$.

Proof. Similar as in Theorem 4, the result is true for formal power series. Therefore we can conclude the result exactly the same way as in Theorem 4. □

Example. Let $p = 2$. Since $|-1-1|_p = 1/2 < 1$, we know that $-1 \in B = \left\{x \in \mathbb{Z}_p \middle| \, |x-1|_p < 1\right\}$. So the 2-adic logarithm of -1 can be computed:

$$ln_2(-1) = ln_2(1-2) = -\left(\frac{2^1}{1} + \frac{2^2}{2} + \frac{2^3}{3} + ...\right).$$

On the other hand, we know from the fundamental property of the p-adic logarithm that

$$0 = ln_2(1) = ln_2(-1) + ln_2(-1) = 2 * ln_2(-1).$$

This means that the sum $2 + \frac{2^2}{2} + \frac{2^3}{3} + ...$ converges to 0 as $n \to \infty$.

The next goal is to show that the p-adic logarithm and the p-adic exponential are inverse to each other in some sense. Again, let $D_p = \left\{x \in \mathbb{Z}_p \middle| \, |x|_p < r_p\right\}$ be the region of convergence of exp_p, where $r_p = p^{-1/(p-1)}$. Before we can prove the main result, we need the following estimates:

Lemma 2. *Let* $n \geq 2$ *and let* $0 < |x|_p < r_p$. *Then the following estimate holds:*

$$\left|\frac{x^n}{n}\right|_p \leq \left|\frac{x^n}{n!}\right|_p < |x|_p < r_p.$$

Proof. From Lemma 1 we know that for any integer $n \geq 1$,

$$ord_p(n!) = \frac{n - S_n}{p-1} \leq \frac{n-1}{p-1}.$$

But since $ord_p(n) \leq ord_p(n!)$, we clearly have

$$|n|_p \geq |n!|_p \geq p^{-\frac{n-1}{p-1}} = r_p^{n-1}.$$

Therefore, by combining these two estimates, we get

$$\left|\frac{x^n}{n}\right|_p \leq \left|\frac{x^n}{n!}\right|_p \leq \left(\frac{|x|_p}{r_p}\right)^{n-1} |x|_p < |x|_p < r_p.$$

□

Proposition 6. *The maps*

$$exp_p : D_p \to 1 + D_p \text{ and } ln_p : 1 + D_p \to D_p$$

are inverse to each other. This means that for all $x \in D_p$,

$$ln_p(exp_p(x)) = x \text{ and } exp_p(ln_p(1+x)) = 1 + x.$$

Proof. By considering the corresponding formal power series, we know that the relations in the Proposition hold. So the only thing we have to make sure is that all involved power series converge. In other words, we have to show that $exp_p(x) \in 1 + D_p$ and $ln_p(1+x) \in D_p$ for any $x \in D_p$. Then the convergence follows from the discussion above. By applying the estimate form the previous Lemma and the *strongest wins* property for series, we have

$$|exp_p(x) - 1|_p = \left|x + \sum_{n=2}^{\infty} \frac{x^n}{n!}\right|_p \leq |x|_p < r_p.$$

The last equality holds because all the terms in the sum are less than $|x|_p$ by Lemma 2. Therefore, $exp_p(x) \in 1 + D_p$ and $exp_p : D_p \to 1 + D_p$.
The same argument works for the p-adic logarithm. Let $1 + x \in 1 + D_p$. Then

$$|ln_p(1+x)|_p = \left|x + \sum_{n=2}^{\infty} (-1)^{n+1} \frac{x^n}{n}\right|_p \leq |x|_p < r_p.$$

Again, the last equality follows from Lemma 2 and the *strongest wins* property for series. Thus we have $ln_p(1+x) \in D_p$ for all $x \in D_p$ and therefore $ln_p : 1 + D_p \to D_p$. □

Now let $x, y \in D_p$ and let $z \in \mathbb{Z}_p$. Then $|x+y|_p \leq max\left\{|x|_p, |y|_p\right\}$ and $|zx|_p \leq |x|_p$. Therefore, $x+y$ and zx are in D_p as well, which means that D_p is an ideal in $\mathbb{Z}_p$. In particular, D_p is an additive subgroup of $\mathbb{Z}_p$. Further, $x+y+xy \in D_p$, which means that $(1+x)(1+y) = 1+x+y+xy \in 1+D_p$. This means that $1+D_p$ is a multiplicative subgroup of $\mathbb{Z}_p$.

Proposition 7. *The p-adic logarithm is an isomorphism of groups*

$$exp_p : D_p \to 1 + D_p.$$

Proof. From the last Proposition, we already know that exp_p is bijective. Therefore it is enough to show that exp_p is a group homomorphism. But this follows directly from the fundamental property:

$$exp_p(x+y) = exp_p(x)\, exp_p(y).$$

□

Until now, the p-adic logarithm and exponential behave quiet similar as the corresponding maps in the setting of real numbers. But there is one property which is totally different in the p-adic setting. In fact, the p-adic exponential is an isometry! Recall that an isometry is a map that preserves the distance. To prove this, we need the following Proposition:

Proposition 8. *Let $x \in D_p$. Then the following holds:*

1. $|exp_p(x)|_p = 1$,
2. $|ln_p(1+x)|_p = |x|_p$,
3. $|1 - exp_p(x)|_p = |x|_p$.

Proof. Let $x \in D_p$. By the estimate of Lemma 2, the term of maximal norm in the series

$$exp_p(x) = 1 + x + \sum_{n=2}^{\infty} \frac{x^n}{n!}$$

is 1. By the *strongest wins* property for series we get that $|exp_p(x)|_p = 1$. Exactly the same way we see that in the series

$$exp_p(x) - 1 = x + \sum_{n=2}^{\infty} \frac{x^n}{n!},$$

the term of maximal norm is x and therefore $|1 - exp_p(x)|_p = |x|_p$.

Similarly, the term of maximal norm in the series

$$ln_p(1+x) = x + \sum_{n=2}^{\infty} (-1)^{n+1} \frac{x^n}{n}$$

is x and thus $|ln_p(1+x)|_p = |x|_p$. □

Corollary 1. *The maps*

$$exp_p : D_p \to 1 + D_p \text{ and } ln_p : 1 + D_p \to D_p$$

are isometries.

Proof. Let $x, y \in D_p$. Then we have

$$\begin{aligned} |exp_p(x) - exp_p(y)|_p &= |exp_p(y)|_p \, |exp_p(x-y) - 1|_p \\ &= |exp_p(x-y) - 1|_p = |x-y|_p, \end{aligned}$$

where the second equation follows from part 1 and the last equation follows from part 3 of the previous proposition. This shows that exp_p is an isometry. To show the same for the p-adic logarithm, we use that $exp_p(ln_p(1+x)) = 1 + x$ for $x \in D_p$. Then, since

$$\begin{aligned} |ln_p(1+x) - ln_p(1+y)|_p &= |exp_p(ln_p(1+x)) - exp_p(ln_p(1+y))|_p \\ &= |(1+x) - (1+y)|_p = |x-y|_p, \end{aligned}$$

the p-adic logarithm is an isometry. □

4 Strassman's Theorem

This last section is about the number of zeros of functions given by $\mathbb{Z}_p$-converging power series. First the Strassman's theorem is stated, which gives us an upper bound for the number of zeros for certain functions. Then some interesting corollaries will follow.

Theorem 6 (Strassman's theorem)**.** *Let $f : \mathbb{Z}_p \to \mathbb{Q}_p, x \mapsto f(x)$, be given by a nonzero power series $f(X) = \sum_{n \geq 0} a_n X^n \in \mathbb{Q}_p[[X]]$. Suppose that $\lim_{n\to\infty} a_n = 0$, so that $f(x)$ converges for all $x \in \mathbb{Z}_p$. Now let $N \in \mathbb{N}_0$ be defined by:*

1. *$|a_N|_p = \max_{n \geq 0} |a_n|_p$, (since $\lim_{n\to\infty} a_n = 0$ $|a_n|_p$ attains its maximum for a finite set of indices).*

2. *$|a_n|_p < |a_N|_p \ \forall n > N$, i.e., N is the largest index of a_n with maximum norm.*

Now one can conclude that f has at most N zeros.

Before proving Strassman's Theorem an example:
Example. Consider the power series $f(X) = \sum_{n\geq 0} n! X^n$. We want (1) to determine the radius of convergence and (2) to estimate the number of zeros from above.
(1) Set $a_n := n!$. $|a_n|_p = 1$ for all $n \in \{0, \dots, p-1\}$, $|a_n|_p \leq p^{-1}$ for all $n \in \{p, \dots, 2p-1\}$ and so on. So $\limsup_{n\geq 0} |a_n|_p = 1$, hence the convergence radius is 1. Since $|a_n 1^n|_p \overset{n\to\infty}{\longrightarrow} 0$, f converges in $\mathbb{Z}_p$.
(2) The number we are looking for is $N = p-1$. We are then able to conclude by applying Stassman that f has at most $p-1$ zeros.
Remark. In $\mathbb{R}$ this theorem is clearly not true. Consider to see this

$$f(X) = \sin(X) = \sum_{n\geq 0} \frac{(-1)^n}{(2n+1)!} X^{2n+1}.$$

The coefficients a_n are given by

$$a_n = \begin{cases} 0, & \text{if } n \text{ even,} \\ \frac{(-1)^{\frac{n-1}{2}}}{n!}, & \text{else.} \end{cases}$$

From this, one can see that $N = 1$. But we know that sine has infinitely many zeros and not at most one!

Proof. The proof is done by induction on N.
$N = 0$: We know from the condition on N that $|a_n|_p > |a_0|_p$ for all $n > 0$. Now assume for the purpose of deriving a contradiction that there exists $x \in \mathbb{Z}_p$ such that

$$0 = f(x) = \sum_{n\geq 0} a_n x^n = a_0 + a_1 x + a_2 x^2 \dots.$$

We obtain that $|a_0|_p = |\sum_{n\geq 1} a_n x^n|_p$, which can be rewritten as the following since we can use the 'strongest wins'-property for sums:

$$|a_0|_p = |\sum_{n\geq 1} a_n x^n|_p \leq \max_{n\geq 1} |a_n x^n|_p.$$

Finally we get (since $|x|_p \leq 1$):

$$|a_0|_p \leq \max_{n\geq 1} |a_n x^n|_p \leq \max_{n\geq 1} |a_n|_p < |a_0|_p,$$

which is a contradiction. Our assumption was proved wrong so there exists no $x \in \mathbb{Z}_p$ such that $f(x) = 0$. This shows the base of induction.
$N \geq 1$: Assume the statement of the theorem holds for $m < N$. We show that it also holds for N. To do this we factor out one zero and show that we are allowed to use the induction hypothesis on our new power series. Assume that f has at least one zero in $\mathbb{Z}_p$ denoted by α. Otherwise the proof is trivial $(0 < N)$. Suppose N is given as in the assumption of the theorem. Choose $x \in \mathbb{Z}_p$ arbitrary. We get

$$f(x) = f(x) - f(\alpha) = \sum_{n\geq 0} a_n(x^n - \alpha^n) = (x-\alpha)\sum_{n\geq 0}\sum_{j=0}^{n-1} a_n x^j \alpha^{n-1-j},$$

where the last equality can be justified by multiplying out

$$(x-\alpha)\sum_{j=0}^{n-1} x^j \alpha^{n-1-j} = x^n - \alpha^n.$$

Since x and α are elements of $\mathbb{Z}_p$, we have $|x|_p, |\alpha|_p \leq 1$. Hence we obtain that $|a_n x^j \alpha^{n-1-j}|_p \leq |a_n|_p \overset{n\to\infty}{\longrightarrow} 0$. We can use Theorem 3(interchanging sums) and achieve that

$$\begin{aligned} f(x) &= (x-\alpha)\sum_{n\geq 0}\sum_{j=0}^{n-1} a_n x^j \alpha^{n-1-j} = (x-\alpha)\sum_{j\geq 0}\sum_{n=j+1}^{\infty} a_n x^j \alpha^{n-1-j} \\ &= (x-\alpha) g_1(x), \end{aligned}$$

where

$$g_1(x) = \sum_{j\geq 0} b_j x^j,\ b_j = \sum_{n=j+1}^{\infty} a_n \alpha^{n-1-j} = \sum_{k=0}^{\infty} a_{j+1+k}\alpha^k.$$

Now we show that (1) g_1 converges in $\mathbb{Z}_p$ and (2) the largest index of b_j with maximal norm is $N-1$.
(1) g_1 converges in $\mathbb{Z}_p$ if $|b_j|_p \overset{j\to\infty}{\longrightarrow} 0$ (theorem from before). This is indeed the case (again with the 'strongest wins'-property):

$$\begin{aligned} |b_j|_p &= |\sum_{k=0}^{\infty} a_{j+1+k}\alpha^k|_p \leq \max_{k\geq 0} |a_{j+1+k}\alpha^k|_p \\ &\leq \max_{k\geq 0} |a_{j+1+k}|_p \overset{j\to\infty}{\longrightarrow} 0. \end{aligned}$$

(2) We have

$$|b_j|_p \leq \max_{k\geq 0} |a_{j+1+k}|_p \leq |a_N|_p\ \forall j \in \mathbb{N}_0,$$

To obtain $|b_{N-1}|_p = |a_N|_p$ one has to work a bit more. We have:

$$|b_{N-1}|_p = |\sum_{k\geq 0} a_{N+k}\alpha^k|_p = \lim_{n\to\infty} |\sum_{k=0}^{n} a_{N+k}\alpha^k|_p,$$

where the last equality holds because of continuity of the norms. By the 'strongest-wins'-property from the first talk, i.e., if $|a|_p < |b|_p$ then $|a+b|_p = |b|_p$ and since $|a_{N+k}\alpha^k|_p \leq |a_{N+k}|_p < |a_N|_p$ $\forall k \geq 1$, we have that

$$|b_{N-1}|_p = \lim_{n\to\infty} |\sum_{k=0}^{n} a_{N+k}\alpha^k|_p = |a_N|_p.$$

$$\forall j \geq N : |b_j|_p \leq \max_{k\geq 0} |a_{j+1+k}|_p = \max_{n\geq N+1} |a_n|_p < |a_N|_p.$$

So b_{N-1} has maximal norm and $N-1$ is the largest index with maximal norm. We are now allowed to use the induction hypothesis on g_1, hence g_1 has at most $N-1$ zeros. We conclude that f has at most $N-1+1 = N$ zeros. □

So now we are able to derive some corollaries:

Corollary 2. *Let f again be given by a nonzero power series*

$$f(X) = \sum_{n\geq 0} a_n X^n,$$

that converges in $\mathbb{Z}_p$. Say $\alpha_1, \ldots, \alpha_m$ are all the zeros of $f(X)$ in $\mathbb{Z}_p$. Then there exists a power series $g(X)$ converging in $\mathbb{Z}_p$ with no zeros in $\mathbb{Z}_p$ and it holds that: $f(X) = (X-\alpha_1)\cdots(X-\alpha_m)g(X)$.

Proof. From the proof of Strassman's Theorem we know that we can construct $g_1(X)$ a power series in $\mathbb{Z}_p[[X]]$ with at most $m-1$ zeros and

$$f(X) = (X-\alpha_1)g_1(X).$$

Applying the same procedure to g_1 we get g_2 with at most $m-2$ zeros and

$$f(X) = (X-\alpha_1)(X-\alpha_2)g_2(X).$$

Repeating this process we can find g_m with no zeros and

$$f(X) = (X-\alpha_1)\cdots(X-\alpha_m)g_m(X).$$

Setting $g := g_m$ finishes the proof. □

Corollary 3. *Let $f(X) = \sum_{n\geq 0} a_n X^n$ be a nonzero power series converging in $p^m\mathbb{Z}_p$ for some $m \in \mathbb{Z}$. Then $f(X)$ has finitely many zeros in $p^m\mathbb{Z}_p$. The number of zeros is bounded from above by N, where N satifies*

$$|p^{mN} a_N|_p = \max_{n\geq 0} |p^{mn} a_n|_p \text{ and } |p^{mn} a_n|_p < |p^{mN} a_N|_p \ \forall n > N.$$

Proof. Define $g(X) := f(p^m X) = \sum_{n\geq 0} a_n p^{mn} X^n$. As f converges in $p^m\mathbb{Z}_p$, g converges in $\mathbb{Z}_p$. We show that the number of zeros of g in $\mathbb{Z}_p$ is the same as the number of zeros of f in $p^m\mathbb{Z}_p$: If $x \in \mathbb{Z}_p$ is a zero of g, then $p^m x$ is a zero of f in $p^m\mathbb{Z}_p$. Conversely if $y \in p^m\mathbb{Z}_p$ is a zero of f, then $p^{-m}y$ is a zero of g in $\mathbb{Z}_p$. If we apply Strassman to g and the result follows immediately. □

Corollary 4. *Let $f(X) = \sum_{n\geq 0} a_n X^n$ and $g(X) = \sum_{n\geq 0} b_n X^n$ two p-adic nonzero power series converging in $p^m\mathbb{Z}_p$. Assume there exist infinitely many numbers $\alpha \in p^m\mathbb{Z}_p$ such that $f(\alpha) = g(\alpha)$, then $a_n = b_n$ for all $n \in \mathbb{N}_0$.*

Proof. Define $h(X) = f(X) - g(X)$ converging in $p^m\mathbb{Z}_p$. If h were nonzero, it would have a finite number of zeros in $p^m\mathbb{Z}_p$ by Corollary 3. But it has infinitely many zeros in $p^m\mathbb{Z}_p$ as all the α's are zeros of h. So h has to represent the zero power series. Therefore we get $a_n = b_n$ for all $n \in \mathbb{N}_0$. □

Remark. Corollaries 2 and 4 have a real respectively complex counterpart.

Corollary 5. *Let $f(X) = \sum_{n\geq 0} a_n X^n$ be nonzero and convergent in $p^m\mathbb{Z}_p$. If $f(x)$ is periodic, i.e., there exists $\tau \in p^m\mathbb{Z}_p$ such that $f(x+\tau) = f(x)$ for all $x \in p^m\mathbb{Z}_p$, then f(X) is constant.*

Remark. This is not at all what we expect and know in real analysis. For example we know that sine and cosine are periodic power series converging everywhere on $\mathbb{R}$ but are not at all constant. The difference comes from the fact that for power series in $\mathbb{R}$ if τ is a period, then $n\tau$ for $n \in \mathbb{Z}$ do not belong to a bounded interval (but in p-adic analysis they do).

Proof. Set $h(X) = f(X) - f(0)$. h has zeros at τn for all $n \in \mathbb{Z}$ because f is periodic. Since $\tau \in p^m\mathbb{Z}_p$ and $p^m\mathbb{Z}_p$ is an ideal, we have that $n\tau \in p^m\mathbb{Z}_p$. So h has infinitely many zeros in $p^m\mathbb{Z}_p$. By Corollary 4 this leads us to $h(X) = 0$ and thus $f(X) = f(0) = const.$ □

Corollary 6. *Let $f(X) = \sum_{n\geq 0} a_n X^n$ be a nonzero power series converging for all $x \in \mathbb{Q}_p$. Then $f(x)$ has at most a countable set of zeros. If the set of zeros $\{z_n\}_{n\geq 1}$ is not finite, then it forms a sequence with $|z_n|_p \overset{n\to\infty}{\longrightarrow} \infty$.*

Proof. We know from the second and third talk that if $x \in \mathbb{Q}_p$ then there exists $m \in \mathbb{Z}$ such that $x \in p^m\mathbb{Z}_p$. So we get that

$$\{x \in \mathbb{Q}_p \mid f(x) = 0\} \subseteq \bigcup_{m \in \mathbb{Z}} \{x \in p^m\mathbb{Z}_p \mid f(x) = 0\}.$$

From Corollary 3 we know that in $p^m\mathbb{Z}_p$, f has only finitely many zeros. So the set of all zeros in $\mathbb{Q}_p$ is a countable union of finite sets, thus countable. Let the set of zeros not be finite and assume that $\sup_{n\geq 1} |z_n|_p \leq C < \infty$. Then there exists $m \in \mathbb{Z}$ such that $\{z_n\}_{n\geq 1} \subseteq p^m\mathbb{Z}_p$ and by Corollary 3 $\{z_n\}_{n\geq 1}$ is finite, which is the desired contradiction. So $|z_n|_p \overset{n\to\infty}{\longrightarrow} \infty$. $\square$