P-ADIC ANALYSIS

K. OSKAR NEGRON

Abstract. p-adic numbers, which are produced by completing the field of rational numbers using the p-adic norm, non-Archimedean, instead of the traditional Archimedean norm, play a fundamental role in modern number theory and recently in analysis. This brief lecture will introduce the audience to the fascinating field of p-adic analysis from a topological perspective. Almost exclusively p will represent some fixed prime number, unless otherwise specified. This is will be a series of three, or four, talks I will give on this subject through the year.

1. Introduction

Definition 1.1. A field $\mathcal{X}$ is said to be a normed space if for every $x \in \mathcal{X}$ there is associated a nonnegative real number $||x||$, called the norm of x. A norm on $\mathcal{X}$ is a map $||\ || : \mathcal{X} \to \mathbb{R}_{\geq 0}$

(1) $||x|| > 0$ iff $x \neq 0$
(2) $||x * y|| = ||x|| * ||y||$ if $y \in \mathcal{X}$
(3) $||x + y|| \leq ||x|| + ||y|| \ \forall \ x, y \in \mathcal{X}$

Note we refer to this type of norm as Archimedean norm.

Definition 1.2. Every normed space may be regarded as a metric space, where we denote the metric as d such that $d(x, y) := ||x - y||$ where d has the following properties

(1) $0 \leq d(x, y) < \infty$
(2) $d(x, y) = 0$ iff $x = y$
(3) $d(x, y) = d(y, x) \ \forall \ x, y$
(4) $d(x, z) \leq d(x, y) + d(y, z)$

Note we call (4) the Triangle inequality. We denote the Metric Space as $(\mathcal{X}, d)$.

Example 1. $d(f, g) = \sup_{x\in[0,1]}\{f(x) - g(x)\}$.
$d(x, y) = \max\{|x_1 - y_1|, |x_2 - y_2|\}$.
$d(x, y) = |x_1 - y_1| + |x_2 - y_2|$.
$d(x, y) = \min\{|x_1 - y_1|, |x_2 - y_2|\}$. (Note this is not a metric space, fails the triangle inequality property.)

Definition 1.3. *Non-Archimedean Norm.* We say the norm is non-archimedean in a normed space $\mathcal{X}$ iff the addition property holds:

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

Date: January 24, 2012.
Key words and phrases. p-adic, metric spaces, topology of p-adic numbers.
I give thanks to my father for pushing me this far and Always supporting me. Also I give thanks to Dr. Ibragimov who has introduce me and guided me in this particular field.

$\forall\ x, y \in \mathcal{X}$. N.B. this satisfies the triangle inequality.

Definition 1.4. *Non-Archimedean Metric Norm.* We say the metric norm is non-archimedean in metric space $(\mathcal{X}, d)$ iff the addition property holds:

$$d(x,z) \leq \max\{d(x,y), d(y,z)\}$$

$\forall\ x, y, z \in \mathcal{X}$ Note, we call this property the Strong Triangle Inequality.

Definition 1.5. A topology on a set E is a subset T of $\mathcal{P}(E)$, i.e. a set of subsets of E, such that

(1) E, ϕ belong to T
(2) The union of every family of the sets in T is also a set in T
(3) The intersection of every finite family of sets in T is also a set in T

Proposition 1.6. The following states are equivalent:

- $||.||$ *is non-archimedean*
- $||n|| \leq 1$ *for every integer* n

Proof. The proof can be found in [Kat, pg. 11-12] □

Definition 1.7. *Ultrametric-Space.* Consider a norm space $\mathcal{X}$ with as metric d, i.e. a metric space denoted as $(\mathcal{X}, d)$, as $d : \mathcal{X} \times \mathcal{X} \to \mathbb{R}_{\geq 0}$. We define an Ultra-metric space as a metric space but with with the metric also following the property in definition 1.4.

Definition 1.8. In any metric space, the open ball with center at x and radius r is the set

$$B_{<r}(x) := \{y : d(x,y) < r\}.$$

The closed ball with center at x and radius r is the set

$$B_{\leq r}(x) := \{y : d(x,y) \leq r\}$$

The open balls of $\mathbb{C}$ with the usual metric are the open discs of the complex plane. They are all circular in shape.

Definition 1.9. Suppose that (X, d) is a metric space and A is a subset of X. The diameter of A, $diam(A) = \sup_{r,s\in A}\{d(r,s)\}$

Definition 1.10. Suppose that (X, d) is a metric space and A is a subset of X and $x \in X$. The distance from x to A, $dist(x, A) = \inf_{a\in A}\{d(x,a)\}$.

Theorem 1.11. Suppose (X, d) is a metric space, $z \in X$ and (x_n) is a sequence in X. Then (x_n) converges to $z \in X$ if, and only if, the real sequence $(d(x_n, z))_{n\in\mathbb{N}}$ converges to 0 in $\mathbb{R}$.

2. p-adic Integers

Definition 2.1. *p-adic Ordinal.* We define the p-adic ordinal of x, r, as

$$ord_p(x) := max\{r : p^r \mid x\} \geq 0$$

$\forall\ x \in \mathbb{Z} - \{0\}$ and a fixed $p \in \mathbb{P}$. If $x = \{0\}$, then $ord_p(x) = \infty$. This means is for $x \in \mathbb{Z}_{>0}$ we have defined the ordinal of x, r, to be the highest order of p that divides x. Notice that if $ord_p(x) = n \Rightarrow p^n \mid x$ but p^{n+1} does not divide x.

Definition 2.2. Let $x = \frac{a}{b}$ $\forall$ $x \in \mathbb{Q}$ and $a, b \in \mathbb{Z} \ni b \neq 0$, then $ord_p(x) = ord_p(a) - ord_p(b)$.

Definition 2.3. We have defined the p-adic norm of $x \in \mathbb{Q}$ by

$$|x|_p = \begin{cases} p^{-ord_p(x)}, & \text{if } x \neq 0; \\ 0, & x = 0. \end{cases}$$

Remark, notice that $|.|$ can only take up a discrete set of values, $\{p^n, n \in \mathbb{Z}\} \cup \{0\}$. Also we have defined the norm to be zero since by definition $ord_p(0) = \infty$

Proposition 2.4. $\forall$ $x, y \in \mathbb{Q} - \{0\}$

$$ord_p(x * y) = ord_p(x) + ord_p(y)$$

Proof. ($\Rightarrow$) Let $x = \frac{a}{b}$ and $y = \frac{c}{d}$ then $ord_p(\frac{a}{b} * \frac{c}{d}) = ord_p(\frac{a*c}{b*d}) = ord_p(a * c) - ord_p(b * d) = ord_p(a) + ord_p(c) - ord_p(b) - ord_p(d) = ord_p(a) - ord_p(b) + ord_p(c) - ord_p(d) = ord_p(a/b) + ord_p(c/d) = ord_p(x) + ord_p(y)$

($\Leftarrow$)If $ord_p(x) = n$ and $ord_p(y) = m \Rightarrow x = p^n * r$ and $y = p^m * s$ where p does not divide r and $s \Rightarrow$ that p does not divide $r * s$ then $x * y = p^{n*m} rs$ and $p^{n+m} \mid xy$. Thus $ord_p(x * y) = n + m$ as expected. $\square$

Theorem 2.5. For all $x, y \in \mathbb{Q}$ we have that

(1) $|x|_p = 0$ *iff* $x = 0$
(2) $|x * y|_p = |x|_p * |y|_p$
(3) $|x + y|_p \leq \max\{|x|_p, |y|_p\}$

Proof. The first property is obvious. The second property follows directly from Proposition 2.4. For the third one if either $x, y = 0$ then it's trivial. Assume hat $x, y \neq 0$. Let $x = \frac{a}{b}$ and $y = \frac{c}{d}$ then $x + y = \frac{ad+bc}{bd}$ and

$$ord_p(x + y) = ord_p(ad + bc) - ord_p(bd)$$

$$\geq \min\{ord_p(ad), ord_p(bc)\} - [ord_p(b) + ord_p(d)].$$

If $ord_p(ad) > ord_p(bc)$ then $\{ord_p(ad), ord_p(bc)\} - ord_p(b) - ord_p(d) = \{ord_p(a) - ord_p(b)\}$. If $ord_p(bc) > ord_p(ad)$ then $\{ord_p(ad), ord_p(bc)\} - ord_p(b) - ord_p(d) = \{ord_p(c) - ord_p(d)\}$. So $min\{ord_p(ad), ord_p(bc)\} - ord_p(b) - ord_p(d) =$

$$min\{ord_p(a) - ord_p(b), ord_p(c) - ord_p(d)\}$$

$$min\{ord_p(x), ord_p(y)\}$$

So, $|x+y|_p = p^{-ord_p(x+y)} = p^{-min\{ord_p(x), ord_p(y)\}} \leq \max\{p^{-ord_p(x)}, p^{-ord_p(y)} = \max\{|x|_p, |y|_p\}$ $\square$

3. The Ring $\mathbb{Z}_P$ of p-adic Integers

Definition 3.1. *Cauchy Sequence.* In any metric space X we have the notion of a Cauchy sequence $\{a_1, a_2, a_3, \ldots\}$ of elements of X. This means that for any $\varepsilon > 0$ there exists an N such that $d(a_m, a_n) < \varepsilon$ whenever both $m > N$ and $n > N$.

Definition 3.2. Fix a prime number p. We consider the sequences of rational numbers, which are Cauchy with respect to the p-adic norm $|\ |_p$. We say two Cauchy sequences $\{a_i\}$, $\{b_i\}$ are equivalent if $|a_i - b_i|_p \to 0$ as $i \to \infty$. For any $x \in \mathbb{Q}$, let $\{x\}$ denote the constant Cauchy sequence all of whose terms equal x. We define the set $\mathbb{Q}_p$ to be the set of equivalence classes of Cauchy sequences.

Definition 3.3. Define addition and multiplication of sequences as:

$$\{a_i\} + \{b_i\} = \{a_i + b_i\}$$
$$\{a_i\} * \{b_i\} = \{a_i * b_i\}$$

i.e. componentwise addition and multiplication.

Definition 3.4. The norm $|\cdot|_p$ on $\mathbb{Q}_p$ is defined to be

$$|\{a_i\}|_p = \lim_{i\to\infty} |a_i|_p.$$

Definition 3.5. The integers θ and e are called the additive identity and the multiplicative identity, respectively. i.e. $n + \theta = \theta + n = n$ and $n * e = e * n = n$ for all $n \in \mathbb{Z}$.

Remark 1. We have two binary operations $(+, *)$ defined on $\mathbb{Z}$. The triple $(\mathbb{Z}, +, *)$ is referred to as the ring of integers.

Remark 2. The ring of integers is a commutative ring because $n*m = m*n$ for all $n, m \in \mathbb{Z}$.

Definition 3.6. *Integral Domain.* For $n, m \in \mathbb{Z}$ and $n * m = 0$; then $n = 0$ or $m = 0$. If $(\mathbb{Z}, +, *)$ follows this property then we say this is integral domain.

Remark 3. The ring of integers, $(\mathbb{Z}, +, *)$, is not a field since it lacks the following property: for each $n \in \mathbb{Z}$ and $n \neq 0$ the equation $n * x = 1$ has a solution in $\mathbb{Z}$.

Definition 3.7. The set of p-adic integers is denoted by $\mathbb{Z}_p$

$$\mathbb{Z}_p = \{\sum_{i\geq 0} a_i p^i\}$$

where $a_i \in \mathbb{Z}$ and $0 \leq a_i \leq p - 1$.

Remark 4. With definition 3.7 a p-adic integer $a = \sum_{i\geq 0} a_i p^i$ can be identified with the sequence $\{a_i\}_{i\geq 0}$ of it coefficients.

Definition 3.8. The set of p-adic integers coincide with the Cartesian product

$$\mathcal{X} = X_p = \prod_{i\geq 0} \{0, 1, \ldots, p-1\} = \{0, 1, \ldots, p-1\}^{\mathbb{N}}.$$

Proposition 3.9. The set of p-adic integers is NOT countable.

Proof. Consider a sequence of p-adic numbers: $a = \sum_{i\geq 0} a_i p^i$, $b = \sum_{i\geq 0} b_i p^i$, $c = \sum_{i\geq 0} c_i p^i$, $\ldots$, we can define a p-adic integer $x = \sum_{i\geq 0} x_i p^i$ by choosing $x_0 \neq a_0$, $x_1 \neq b_1$, $x_3 \neq c_3$, $\ldots$, thus constructing a p-adic integer different than $a, b, c, \ldots$. $\square$

Definition 3.10. Let $a = \sum_{i\geq 0} a_i p^i$, $b = \sum_{i\geq 0} b_i p^i$ be two p-adic integers. Then $a + b = \sum_{i\geq 0}(a_i + b_i)p^i = \sum_{i\geq 0} c_i p^i$ where $c_i = a_i + b_i$ such that

- $c_i \in \{0, 1, 2, \ldots, p-1\}$ for all i
- $m \in \mathbb{N} \cup \{0\}$ then $\sum_{i=0}^{m} c_i p^i = \sum_{i=0}^{m} (a_i + b_i) p^i \ (mod p^{m+1})$

Remark 5. i.e. $c_0 = a_0 + b_0$ (mod$p$) and $c_0 + c_1 p = a_0 + b_0 + (a_1 + b_1)p$ (mod$p$).

Example 2. $1 = 1 + 0p + 0p^2 + \ldots = \sum_{i \geq 0} a_i p^i$. Let $b = (p-1) + (p-1)p + (p-1)p^2 + \ldots$, then $1 + b = c_0 + c_1 + c_2 p^2 + \ldots$, where $c_0 = 1 + (p-1)$ modulus p

4. Topology of p-adic Numbers

Definition 4.1. An ultrametric field is said to be complete if it is complete as a metric space, that is, every Cauchy sequence in $\mathcal{X}$ converges to an element of $\mathcal{X}$. Note that the strong triangle inequality implies that a sequence $\{a_n\}$ in $\mathcal{X}$ is a Cauchy sequence iff $|a_n - a_{n+1}| \to 0$ for $n \to \infty$. As a consequence, over a complete ultrametric field a series

$$\Sigma_{i=1}^{\infty}(a_i)$$

converges if and only if $|a_i| \to 0$ for $i \to \infty$.

Like all metric spaces, an ultrametric field $\mathcal{X}$ may be completed, its completion $\widehat{\mathcal{X}}$ again an ultrametric field with absolute value obtained from that of $\mathcal{X}$ by continuity.

Proposition 4.2. If $b \in B_r(a, r)$, then $B_r(a, r) = B_r(b, r)$. Every point of a ball is its center.

Proof. Let $x \in B_r(b, r)$. Then by assumption, $|a - b|_p < r$, $|b - x|_p < r$, and therefore by Strong Triangle Inequality,

$$|a - x|_p = |a - x + b - b|_p = |(a - b) + (b - x)|_p \leq \max\{|a - b|_p + |b - x|_p\} < r;$$

$\Rightarrow B(b, r) \subset B(a, r)$. Since $|a - b|_p < r$ for b to lie in $B(a, r)$ is identical with that for a to lie in $B(b, r)$, we obtain $B(a, r) \subset B(b, r)$ which implies that the balls coincide. □

Proposition 4.3. The sphere $S(a, r)$ is an open set in $\mathbb{Q}_p$. Where $S(a, r) := \{x \in \mathbb{Q}_p : |x - a|_p = r\}$

Proof. Let $x \in S(a, r)$ $\epsilon < r$. Let $y \in B(x, \epsilon)$. Then, $|x - y|_p < |x - a| = r \Rightarrow |y - a|_p = |x - a| = r$, which means that $y \in S(a, r)$. □

Proposition 4.4. The open balls in $\mathbb{Q}_p$ are both open and closed.

Proof. Can be found in [Kat, pg 55] □

Proposition 4.5. Two balls in $\mathbb{Q}_p$ have a nonempty intersection iff one is contained in the other.

Proof. Can be found in [Kat, pg 56] □

Proposition 4.6. The sphere $S(a, r)$ is both open and closed.

Proof. Can be found in [Kat, pg 56] □

5. Isometries in Metric Spaces

Definition 5.1. A function $f : X \to Y$ between two topological spaces (X, D_X) and (Y, T_Y) is called a homeomorphism if it has the following properties

(1) f is a bijection
(2) f is continuous
(3) the inverse function f^{-1} is continuous, i.e. f is an open mapping.

A function with these three properties is sometimes called bicontinuous. If such a function exists, we say X and Y are homeomorphic.

Definition 5.2. Isometry of a metric space (X, d) is a homeomorphism f of X that preserves distance. That is, an isometry of (X, d) is a homeomorphism f of X for which

$$d(x, y) = d(f(x), f(y))$$

for every pair x, y of points of X.

Proposition 5.3. Let $f : X \to X$ be any function that preserves distance. Prove that f is injective and continuous.

Proof. If $f(x) = f(y)$, then $d(f(x), f(y)) = 0$. Hence, $d(x, y) = 0$, and so $x = y$ by the first of the three conditions describing a metric. Hence, f is injective. WNTS f is continuous at x, take some $\varepsilon > 0$. We need to find $\delta > 0$ such that $f(U_\delta(x)) \subset U_\varepsilon(f(z))$. However, because $d(x, y) = d(f(x), f(y))$, we see that if $y \in U_\delta(x)$, then $d(x, y) < \delta$, and so $d(f(x), f(y)) < \delta$, and so $f(y) \in U_\delta(f(x))$. Hence, take $\delta = \varepsilon$. □

Proposition 5.4. A function $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(z) = az$ is an isometry of the metric space $(\mathbb{Z}, n)$ if and only if $|a| = 1$. Here, $n(z, w) = |zw|$.

Proof. Note that $f(z) = az$ is a homeomorphism of $\mathbb{Z}$ for every $a \in \mathbb{Z} - \{0\}$. As $|f(z) - f(w)| = |az - aw| = |a||z - w|$, we see that f is an isometry iff $|a| = 1$. □

6. p-adic Functions

Definition 6.1. A function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is called continuous at the point $a \in \mathbb{Z}_p$ if for each $\varepsilon > 0$ there exists a $\delta > 0$ such that $|x - a|_p < \delta$ implies $|f(x) - f(y)|_p < \varepsilon$ for all $x \in \mathbb{Z}_p$. A function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is called continuous if it is continuous at all points $a \in \mathbb{Z}_p$. A function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is uniformly continuous if for each $\varepsilon > 0$ there exists a $\delta > 0$ such that $|x - y|_p < \delta$ implies $|f(x) - f(y)|_p < \varepsilon$ for all $x, y \in \mathbb{Z}_p$

Definition 6.2. A function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is called locally constant if for each $x \in \mathbb{Z}_p$ $\exists$ a neighborhood $U_x \ni x$, i.e. a ball of radius p^{-m} for some $m \in \mathbb{N}$ centered at x, $U_x = \{y \in \mathbb{Z}_p : |x - y|_p < p^{-m}\}$, such that f is continuous on U_x.

Notice that in $\mathbb{R}$ the only locally constant functions are constants.

Proposition 6.3. There exist an injective function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ whose derivative is zero.

Proof. Since f is injective it implies that f is not locally constant. Let $x = \Sigma_{n=0}^{\infty} a_n p^n \in \mathbb{Z}_p$ and set $f(x) = \Sigma_{n=0}^{\infty} a_n p^{2n}$. Now if $x = \Sigma_{n=0}^{\infty} a_n p^n \in \mathbb{Z}_p$ and $y = \Sigma_{n=0}^{\infty} b_n p^n \in \mathbb{Z}_p$ satisfy $|x - y|_p = p^{-j}$ for some $j = 0, 1, 2...$, then $a_0 = b_0, a_1 = b_1, ..., a_{j-1} - b_{j-1}, a_j \neq b_j$. Thus we have $|f(x)-f(y)|_p = p^{-2j}$. $|f(x)-f(y)|_p = |x-y|_p^2 \ \forall\ x,y \in \mathbb{Z}_p$ since f is injective, $f(x)=f(y) \Rightarrow x=y$, $|\frac{f(x)-f(y)}{x-y}|_p = |x-y|_p \to 0$ as $y \to x$ □

Proposition 6.4. Rolle's Theorem Fail. Recall Rolle's Theorem: Assume that f has a derivative (finite or infinite) at each point of the open interval (a,b) and assume that f is continuous at both the endpoints a,b. If $f(a)=f(b)$ there is at least one interior point c at which $f'(c)=0$.

Proof. Let $f:\mathbb{Z}_p \to \mathbb{Q}_p$ be given by $f(x)=x^p-x$. We have $f(0)=0, f(1)=0, f'(x)=px^{p-1}$. Since $|f'(x)+1|_p \le \frac{1}{p}$, i.e., $f'(x) \in -1+p\mathbb{Z}_p$ it follows that $f'(x) \neq o$ for all $x \in \mathbb{Z}_p$ □

Acknowledgements

The author would like to give thanks to his father for pushing him this far and for Always supporting him and also gives thanks to Dr. Ibragimov whom introduced him and is guiding him in this particular field.

References

[Mun] J. R. Munkres. *Topology 2nd Edition*, Prentice Hall, Upper Saddle River, 2000.
[Kat] S. Katok. *p-adic Analysis Compared with Real*, American Mathematical Society, Providence, 2007.
[Ked] K. S . Kedlaya. *p-adic Differential Equations*, Cambridge University Press, New York, 2010.
[Ru2] W. Rudin. *Functional Analysis.* McGraw-Hill, New York, 1973.
[Ru1] W. Rudin. *Principles of Mathematical Analysis*, McGraw-Hill, New York, 1953.
[Ro1] A. M. Robert. *A Course in p-adic Analysis*, Springer-Verlag, New York, 2000.
[Za1] Z. Ibragimov. *LECTURE NOTES ON p-ADIC NUMBERS*, Zair Ibragimov, Retrived 1-23-2012.

E-mail address: `koskar@csu.fullerton.edu`