Dyadic Harmonic Analysis and the p-adic numbers

Taylor Dupuy

July, 5, 2011

Abstract

Notes from a talk given in Sevilla in 2012. These are incomplete and probably contain errors. If someone find errors or wants to suggest a re-organization of this material please email me: `taylor.dupuy@gmail.com`. Also email me if you want to talk about p-adic Harmonic analysis. The basic idea is that anything you can do in "dyadic harmonic analysis" you can also do with a complete distrete valuation field. This can also be viewed as a friendly introduction to p-adic numbers for analysts – Taylor Dupuy (Summer 2012)

0.1

An **absolute value** on a domain R is a map $|-|: R \to \mathbb{R}_{\geq 0}$ such that

1. $|x| = 0 \iff x = 0$
2. $|xy| = |x| \cdot |y|$
3. $|x + y| \leq |x| + |y|$

We will be focusing on **non-archimedean** or **ultra metric** absolute values, these are absolute values which satisfy the stronger triangle inequality:

$$|x + y| \leq \max\{|x|, |y|\}. \tag{1}$$

Remark 0.1.
- The are called non-archimedean because they destroy the ordering of the fields. We will see this later.
- Every absolute value extends uniquely to its field of fractions.

0.2

For every prime number p we can define a norm $|-|_p$ on $\mathbb{Z}$ which is distinct from usual norm. For example if $p = 5$ we will have

$$|14|_5 = 1, \quad |25|_5 = \tfrac{1}{5^2}, \quad |-10|_5 = \frac{1}{5},$$

The idea is that the more divisible by 5 the number is the smaller the 5-adic absolute value. Here is the general setup: For any prime p and any natural number n we can write $n = p^e n'$ where $p \nmid n'$. We then define the p-**adic absolute value** by

$$|p^e n'| = p^{-e}. \tag{2}$$

The exponent e is called the **order** or **valuation** of n at p as is sometimes denoted by $\nu_p(n)$ or $\mathrm{ord}_p(n)$. We can extend the absolute value to the rational numbers as we stated before. Here are some examples:

$$|1/14|_5 = 1, \quad |3/25|_5 = 5^2, \quad |\frac{1}{10}|_5 = 5.$$

0.3

With every absolute value there comes a metric. The p-adic metric on $\mathbb{Q}$ is

$$d(x, y) = |x - y|_p$$

and if we complete $\mathbb{Q}$ with respect to this metric a complete vector space $\mathbb{Q}_p$ called the p-adic numbers.

How do we write down p-adic numbers? We can represent any p-adic integer as a power series in p

$$a = \sum_{j>-N}^{\infty} a_j p^j \tag{3}$$

where $a_j \in \{0, 1, \ldots, p-1\}$. This is very similar to a decimal, binary or n-ary exansion of a real number only this times the decimal point is going the other way! For example

$$\sum_{j=0}^{n} 3^j = \ldots 111.0$$

Notice that even negative numbers are represented as power series as in 3

$$\frac{1}{1-p} = 1 + p + p^2 + \cdots$$

which means

$$-1 = \frac{p-1}{1-p} = (p-1) + (p-1)p + (p-1)p^2 + \cdots .$$

Proposition 0.2. *The p-adic norm on the p-adic numbers is non-archimedean.*

0.4

The p-adic numbers have some properties which may be peculiar to people who haven't worked with them before.

- Balls have no centers.
- The unit ball is a subring.
- $\sum_{j\geq 0} a_j$ converges in $\mathbb{Q}_p$ if and only if $|a_j|_p \to 0$ as $j \to \infty$.

0.4.1 Balls Have No Centers

This is actually just a property of any **non-archimedean (or ultrametric)** metric spaces. These are metric which satisfy the stronger triangle inequality

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

It is easy to check that the metric induced by the p-adic norm is ultrametric.

The 3-adic topology looks something like this:

Proposition 0.3. *Suppose that (X,d) is a non-archimedean metric space. Then for all x, y and r*

$$y \in B_r(x) \implies B_r(x) = B_r(y).$$

Proof. We will show that $B_r(x) \subset B_r(y)$. If $y \in B_r(x)$ then $d(x,y) \leq r$. For all $z \in B_r(x)$ we have

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

which implies that $z \in B_r(y)$ and hence $B_r(x) \subset B_r(y)$. The reverse inclusion follows from symmetry. □

any Ultra metric space has a property of dyadic intevals that you are probably familiar with:

Proposition 0.4. *Let (X,d) be an Ultrametric space. For all balls B and B' we have*

$$B \cap B' = \emptyset \text{ or } B \subset B' = \emptyset \text{ or } B' \subset B.$$

Proof. Let $B = B_r(x)$ and $B' = B_{r'}(x')$. Without loss of generality we can assume that $r' \leq r$. Clearly we have $B_{r'}(x') \subset B_r(x)$. If $B_r(x) \cap B_r(x')$ is not empty for any element y in the intersection we have

$$B_r(x) = B_r(y) = B_r(x')$$

by the previous proposition. In the case that the intersection is nonempty we have $B' \subset B$. Otherwise the intersection is empty. □

Remark 0.5. We will see shortly that the dyadic intervals used in dyadic harmonic analysis actually come from an non-archimedean norm placed on the set of real numbers.

0.4.2 The Unit Ball is a Subring

The unit ball in the p-adics

$$B_1(0) = \{x \in \mathbb{Q}_p : |x|_p \leq 1\} := \mathbb{Z}_p$$

is sometimes called the ring of ***p*-adic integers** and is denoted by $\mathbb{Z}_p$.

Proposition 0.6. *Let F be a complete field with a non-archimedean valuation*

1. *The closed unit ball in F is a subring.*
2. *The open unitball in F is a maximal ideal in the subring.*

Proof. $|x+y|_F \leq \max\{|x|_F, |y|_F\}$ □

0.5 The Dyadic Reals

[1] We want to explain the following claim

Proposition 0.7. *The dyadic intervals on the set* $\mathbb{R}$ *are balls on the "approximate reals"* $\widetilde{\mathbb{R}} = (\mathbb{R}, \widetilde{+}, \widetilde{*}, |\cdot|)$ *which has an ultrametric topology.*

The approximate reals are the completion of the approximate integers. The approximate integers are essentially the integers where we drop don't carry. In order to explain $\widetilde{ZZ}$ we need to explain

- The addition
- The multiplication
- The norm

Every number can be written in binary

$$n = \sum_{j=0}^{N} b_j 2^{-j}$$

where $b_j \in \{0, 1\}$. For example

$$10 = 0 \cdot 1 + 1 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3.$$

When we add two numbers we can usually using rounding:

$$5 + 11 = 101_2 + 11 = 1011_2 = 10000_1 = 16$$

If we forget about the rounding get a kind of approximate addition

$$5 + 11 = 101_2 \widetilde{+} 1011_2 = 1110_2 = 14.$$

The worst thing that happens here is $n \widetilde{+} n = 0$. What we really have done is identified the binary expansion with elements of the ring of polynomials $\mathbb{F}_2[t]$ with $\mathbb{R}$ by plugging in $t = 2$.

$$5 \leftrightarrow 1 + t^2 \text{ and } 11 \leftrightarrow 1 + t + t^3$$

Given that, the natural multiplcation $n \widetilde{*} m$ should be given by the multiplcation in the polynomial ring. So for example we have

$$5 \widetilde{*} 11 = 39.$$

In general the coefficients for multiplcation are given by

$$b_r(n \widetilde{*} m) = \sum_{i+j=r} b_j(n) b_i(m).$$

This explains the addition and the multiplication. It remains to explain the norms. For every integer n the norm $|n|$ is equal to the number of elements

[1]The following (awesome) observation was brought to my attention by Terrence Tao's blog.

in the abelian group $\mathbb{Z}/\langle n\rangle$. We define a norm similarly for the approximate integers: if $n \in \mathbb{F}_2[t] = \widetilde{\mathbb{Z}}$ then we will define

$$|n|_{\widetilde{\mathbb{R}}} = \#\widetilde{\mathbb{Z}}/\langle n\rangle = (\#\mathbb{F}_2)^{\deg(n)} = 2^{\deg(n)}.$$

where $\deg(n)$ is the degree of n as a polynomial in $\mathbb{F}_2$. Using this definition we have

$$|5|_{\widetilde{\mathbb{R}}} = 4 \text{ and } |11|_{\widetilde{\mathbb{R}}} = 8$$

Remark 0.8. To get a sense of how these are actually "approximate" one could compute the probabilities by which they vary. Perhaps a relative error is the best estimate.

As with any normed space we can extend the norm the the field of fractions

$$\mathrm{Frac}(\mathbb{F}_2[t]) = \mathbb{F}_2(t) = \{\frac{f(t)}{g(t)} : f, g \in \mathbb{F}_2[t], g \neq 0\} := \widetilde{\mathbb{Q}}$$

and complete with respect to the norm to get

$$\widetilde{\mathbb{R}} \cong \mathbb{F}_2((1/t)) = \{\sum_{j>>-\infty}^{\infty} b_j t^{-j} : b_j \in \mathbb{F}_2\}.$$

Note that the degree of each element in this ring is finite. We would also like to observe that $\mathbb{R}$ is, in fact, in bijection with the real numbers (which can be seen by making the substitution $t \mapsto 2$).[2]. Now observe that in this topology that since the norm only depends on the degree we have

$$|x+y|_{\widetilde{\mathbb{R}}} \leq \max\{|x|_{\widetilde{\mathbb{R}}}, |y|_{\widetilde{\mathbb{R}}}\}.$$

By the ultrametric properties every x in a unique ball of radius r (which is the same as the ball of radius of some 2^n— the biggest power of 2 smaller than r). Observe that $|x-y|_{\widetilde{\mathbb{R}}} < 2^n$ means that these numbers only disagree at the smaller powers of 2. One can immediately see for example that

$$B_{2^n}(0) = [0, 2^n] \subset \mathbb{R}.$$

0.6

Proposition 0.9. *$\mathbb{Z}_2$ and $B_1(0)$ are homeomorphic (both are homeomorphic to the Cantor Set).*

Lemma 0.10. *For a topological space X the following are equivalent*

1. *X is homeomorphic to the cantor set.*
2. *X is homeomorphic to $\prod_{i\in\mathbb{N}}\{0,1\}$ where we give $\{0,1\}$ the discrete topology.*
3. *X is perfect, compact, hausdorff and totally disconnected.*

[2]It is more common in commutative algebra and algebraic geometry to work with (the isomorphic normed field) $\mathbb{F}_2((t))$ and the order of vanishing of t rather than the degree

0.7

Proposition 0.11. *There exists a ring homomorphism from* $\mathbb{Z}_2$ *to* $\widetilde{\mathbb{R}}$.

The main idea of this proposition is the that $\mathbb{Z}_2 \cong W_{2^\infty}(\mathbb{F}_2)$ where $W_{p^\infty}(R)$ is the ring of **p-typical Witt Vectors**. These consist of sequences $(a_0, a_1, \dots)$ to which we make up some addition and multiplication rules to give it a ring structure

$$\begin{aligned}(a_0, a_1, \dots) + (b_0, b_1, \dots) &= (a_0 + b_0, a_1 + b_1 + \frac{a_0^p + b_0^p - (a_0 + a_1)^p}{p}, \dots),\\ (a_0, a_1, \dots) * (b_0, b_1, \dots) &= (a_0 b_0, a_1 b_0^p + b_1 a_0^p + p a_1 b_1, \dots)\end{aligned}$$

we have only given the first two sum and product polynomials which define the addition and multiplication operations but they continue. We need some notation. If $x = (x_0, x_1, \dots)$ the the nth **Witt Polynomial** is defined by

$$w_n(x) := \sum_{j=0}^{n} p^j x_j^{p^{n-j}}. \tag{4}$$

The Witt Vectors are given the unique structure such that the map

$$w(x_0, x_1, x_2, \dots) := (w_0(x), w_1(x), w_2(x), \dots)$$

is a ring homomorphism. In other words

$$x +_W y = (s_0(x,y), s_1(x,y), \dots) := s \text{ and } x *_W y = (p_0(x,y), p_1(x,y), \dots) := p$$

are made so that

$$(w_0(s), w_1(s), \dots) = (w_0(x) + w_0(y), w_1(x) + w_1(y), \dots)$$

and

$$(w_0(p), w_1(p), \dots) = (p_0(x) p_0(y), p_1(x) + p_1(y), \dots).$$

the Witt polynomials are essentially the unique polynomials you can do this with. The homomorphism we were talking about is from $\mathbb{Z}_2$ to $B_1(0) \cong \mathbb{F}_2[[t]]$ comes from equation (4) and is called the **Ghost map**.

0.8

One can define Calderon-Zygmund operators. Maximal functions and Calderon-Zygmund decompositions in the same way you do for dyadic harmonic analysis. See Cristina Pereyra's notes.