An Introduction to p-adic Numbers

Geoff Vooys
University of Calgary

November 3, 2017

The p-adic Valuation and some Properties

Definition

Let $\mathbb{Z}^\times := \{n \in \mathbb{Z} \mid n \neq 0\}$ and let $p \in \mathbb{Z}$ be a fixed prime. Then define the p-adic valuation on $\mathbb{Z}$ to be the function $v_p : \mathbb{Z}^\times \to \mathbb{R}$ given by, for all $a \in \mathbb{Z}^\times$,

$$v_p(a) := \max\{n \in \mathbb{N} \ : \ p^n | a\}.$$

Properties of the p-adic Valuation

Properties of the p-adic Valuation

The mapping v_p satisfies the following:

1. For all $n \in \mathbb{Z}^\times$ we have $v_p(n) = v_p(-n)$;
2. For all $n \in \mathbb{Z}^\times$ we have $v_p(n) \geq 0$;
3. for all $m, n \in \mathbb{Z}^\times$ we have $v_p(mn) = v_p(m) + v_p(n)$;
4. For all $m, n \in \mathbb{Z}^\times$ we have

$$\inf\{v_p(m), v_p(n)\} \leq v_p(m+n) \leq \sup\{v_p(m), v_p(n)\}.$$

Proof of Properties (1) and (3)

UNIVERSITY OF CALGARY

Proof.

(1): Begin by letting $a \in \mathbb{Z}$ be arbitrary. Then

$$v_p(a) = \max\{n \in \mathbb{N} \ : \ p^n | a\} = \max\{n \in \mathbb{N} \ : \ p^n | -a\} = v_p(-a).$$

(3): Let $m, n \in \mathbb{Z}^\times$ and assume that $v_p(m) = a$ and $v_p(n) = b$. Now write $m = kp^a$ and $n = \ell p^b$ for $\gcd(k, p) = 1 = \gcd(\ell, p)$. Then

$$mn = (kp^a)(\ell p^b) = k\ell p^{a+b}$$

so that $p^{a+b} | mn$. Since a and b are the maximum integers such that $p^a | m$ and $p^b | n$, $a + b$ is the maximum integer such that $p^r | mn$. Thus

$$v_p(m) + v_p(n) = a + b = \max\{r \in \mathbb{N} \ : \ p^r | mn\} = v_p(mn).$$

$\square$

Extending v_p and the p-adic Norm

UNIVERSITY OF CALGARY

Definition

Extend v_p from $\mathbb{Z}^\times$ to $\mathbb{Q}^\times := \{a \in \mathbb{Q} \ : \ a \neq 0\}$ via, for all $a = m/n \in \mathbb{Q}^\times$ written such that $m, n \in Z^\times$ and $\gcd(m,n) = 1$,

$$v_p(a) = v_p\left(\frac{m}{n}\right) = v_p(m) - v_p(n).$$

Definition

Define the map $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ via the assignment

$$|a|_p := \begin{cases} 0 & \text{if } a = 0; \\ p^{-v_p(a)} & \text{if } a \in \mathbb{Q}^\times. \end{cases}$$

This defines the p-adic norm on $\mathbb{Q}$.

The p-adic Norm is Actually a Norm!

UNIVERSITY OF CALGARY

Theorem

Let $a, b \in \mathbb{Q}$. Then the following hold:

1. $|a|_p \geq 0$ and $|a|_p = 0$ if and only if $a = 0$;
2. $|ab|_p = |a|_p |b|_p$;
3. $|a + b|_p \leq \max\{|a|_p, |b|_p\}$.

Proof (of Selected Facts)

UNIVERSITY OF CALGARY

Proof.

(1): Begin by noting that for all real numbers $x, p^x > 0$. Thus $|x|_p \geq 0$ for all $x \in \mathbb{Q}$ and $|x|_p > 0$ for all $x \in \mathbb{Q}^\times$. Then $|x|_p = 0$ if and only if $x = 0$.

(2): If $x = 0$ or $y = 0$ there is nothing to show, so take $x, y \neq 0$. Then

$$|xy|_p = p^{-v_p(xy)} = p^{-v_p(x)-v_p(y)} = p^{-v_p(x)}p^{-v_p(y)} = |x|_p|y|_p.$$

$\square$

Making a Metric from the p-adic Norm

UNIVERSITY OF CALGARY

Definition

Define a function $d : \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}$ via the assignment, for all $x, y \in \mathbb{Q}$,

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

Proving that this is a Metric

Proof

Symmetry: Let $x, y \in \mathbb{Q}$. Then since $v_p(a) = v_p(-a)$ for all $a \in \mathbb{Z}$, if $z \in \mathbb{Q}$ with $z = m/n$ in lowest terms we have

$$v_p(z) = v_p(m/n) = v_p(m) - v_p(n) = v_p(-m) - v_p(n) = v_p(-m/n) = v_p(-z)$$

so it follows that

$$d(x, y) = |x - y|_p = p^{-v_p(x-y)} = p^{-v_p(y-x)} = |y - x|_p = d(y, x).$$

Nondegeneracy: Let $x, y \in \mathbb{Q}$. Then

$$d(x, y) = 0 \iff |x - y|_p = 0 \iff x - y = 0 \iff x = y.$$

Proof, cont.

UNIVERSITY OF CALGARY

Proof.

(Strong) Triangle Inequality: Let $x, y, z \in \mathbb{Q}$. Then set $\alpha = x - y$ and $\beta = y - z$ so that $x - z = x - y + y - z = \alpha + \beta$. It then follows that

$$\begin{aligned} d(x,z) &= |x-z|_p = |\alpha+\beta|_p \leq \max\{|\alpha|_p, |\beta|_p\} = \max\{|x-y|_p, |y-z|_p\} \\ &= \max\{d(x,y), d(y,z)\} \leq d(x,y) + d(y,z) \end{aligned}$$

□

Ultrametric Spaces

Definition

Let (M, ∂) be a metric space. We then say that M is ultrametric if M satisfies the strong triangle inequality, i.e., for all $x, y, z \in M$ we have

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

Remark

Note that this above condition states that the distance between x and y is less than the maximum distance between x, y, and any "intermediate" point z. We can use this to show that in any ultrametric space M, if $\partial(x, y) < r$ for some $r > 0$, then $B_r(x) = B_r(y)$.

Facts About Ultrametric Spaces

Theorem

Let (M, ∂) be an ultrametric space. Then if (x_n) is a sequence in M such that $\partial(x_n, x_{n+1}) \to 0$ as $n \to \infty$, (x_n) is a Cauchy sequence in M.

Theorem

Let (M, ∂) be an ultrametric space. Then M is totally disconnected.

Is $(\mathbb{Q}, |\cdot|_p)$ Complete?

UNIVERSITY OF CALGARY

Theorem

The metric space $(\mathbb{Q}, |\cdot|_p)$ is not complete.

Sketch

Let $p \in \mathbb{N}$ be prime with and fix some $a \in \mathbb{Z}$ with $1 \leq a \leq p-1$ and consider the sequence

$$x_n := a^{p^n}.$$

Then (x_n) is Cauchy in the p-adic norm (use Fermat's Little Theorem to derive this) and set $x := \lim x_n$. It can be shown that x is a nontrivial $(p-1)^{th}$ root of unity. Because $\mathbb{Q}$ contains only a first and second root of unity, we conclude that $x \notin \mathbb{Q}$ and hence $(\mathbb{Q}, |\cdot|_p)$ is not complete.

Finally, the p-adic Numbers

UNIVERSITY OF CALGARY

Definition

Define the space $(\mathbb{Q}_p, |\cdot|_p)$ of p-adic numbers to be the completion of $\mathbb{Q}$ with respect to the p-adic norm.

Definition

Define the space $(\mathbb{Z}_p, |\cdot|_p)$ of p-adic integers to be the closed ball

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

Theorem

The space $(\mathbb{Q}_p, |\cdot|_p)$ is a topological field and $(\mathbb{Z}_p, |\cdot|_p)$ is a topological ring.

Fun p-adic Facts!

UNIVERSITY OF CALGARY

Theorem

The space $(\mathbb{Z}_p, |\cdot|_p)$ is homeomorphic to the Cantor set $C \subset \mathbb{R}$ for all primes $p \in \mathbb{N}$.

Theorem

Every p-adic number $x \in \mathbb{Q}_p$ can be represented as a power series

$$\sum_{n=m}^{\infty} a_n p^n$$

for some $m \in \mathbb{Z}$ and $a_n \in \{0, \cdots, p-1\}$ for all n. Furthermore, $x \in \mathbb{Z}_p$ if and only if

$$x = \sum_{n=0}^{\infty} a_n p^n.$$

Thanks For Coming!