Una introducción a los números p-ádicos, su aritmética y algunas simulaciones en Python

Trabajo de grado presentado para optar por el título de Matemático

Autor: Edgar Baquero
Supervisor: Leonardo Chacón. PhD.

30 de mayo de 2020

Pontificia Universidad Javeriana, Facultad de Ciencias
Departamento de Matemáticas

Notación

Notación

En la escuela nos enseñaron a separar los números por unidades, decenas y centenas. Por ejemplo el número 437 tiene 7 unidades, 3 decenas y 4 centenas. Es decir que podemos representar 437 como:

$$437 = 7 \cdot 10^0 + 3 \cdot 10^1 + 4 \cdot 10^2,$$

El número 543,89 como:

$$543{,}89 = 9 \cdot 10^{-2} + 8 \cdot 10^{-1} + 3 \cdot 10^0 + 4 \cdot 10^1 + 5 \cdot 10^2.$$

Que también se puede denotar como $543{,}89_{10}$.

Notación

Así:

- Se puede expandir un número por cualquier base q.
- Ejemplos conocidos de sistemas de numeración son el *octal*, *hexadecimal y binario*, entre otros.

Ejemplo

Podemos representar el siguiente número:

$$2 \cdot 8^{-2} + 2 \cdot 8^{-1} + 3 \cdot 8^{0} + 4 \cdot 8^{1} + 7 \cdot 8^{2},$$

por 743,22 ($q = 8$), o también $743{,}22_8$.

Notación

- Particularmente, estamos interesados en expansiones sobre bases primas.
- Por ejemplo con $p = 2$, el ¡Sistema binario!
- En general, una expansión de la forma.

$$x = \sum_{k=-\gamma}^{l} a_k p^k, \text{ con } \gamma \in \mathbb{Z}, \, a_k \in \{0, \ldots, p-1\} \, ,$$

será

$$a_l \ldots a_2 a_1 a_0, a_{-1} a_{-2} \cdots a_{-\gamma}{}_p. \tag{1.1}$$

- Siendo así, ahora sí empecemos.

El campo de los números p-ádicos

Definición

Sea K un cuerpo. Una *norma* en K es una función $|\cdot| : K \to \mathbb{R}_{\geqslant 0}$ tal que para todo $x, y \in K$ satisface las siguientes propiedades:

- $|x| \geqslant 0$, $|x| = 0 \iff x = 0$,
- $|xy| = |x|\,|y|$,
- $|x + y| \leqslant |x| + |y|$.

Además, una norma $|\cdot|$ en K define una métrica natural dada por $d(x, y) = |x - y|$.

Definición

Dos normas $|\cdot|_1, |\cdot|_2$ sobre un cuerpo K se dicen *equivalentes* si inducen la misma topología sobre K, i.e., todo abierto con respecto a una topología también lo es con respecto a la otra. Por notación decimos que $|\cdot|_1 \sim |\cdot|_2$.

Proposición

Sea K un cuerpo con dos normas $|\cdot|_1, |\cdot|_2$. Entonces $|\cdot|_1 \sim |\cdot|_2$ si, y sólo si, existe $c \in \mathbb{R}_{>0}$ tal que $|\cdot|_1 = |\cdot|_2^c$.

Proposición (Equivalencia Lipschitz)

Sea K un cuerpo con dos normas $|\cdot|_1, |\cdot|_2$. Entonces $|\cdot|_1 \sim |\cdot|_2$ si, y sólo si existen constantes k_1, k_2 positivas tales que:

$$k_1|x|_1 < |x|_2 < k_2|x|_1 \,,$$

para todo $x \in K$.

Proposición

Sea K un cuerpo con dos normas $|\cdot|_1, |\cdot|_2$ tales que $|\cdot|_1 \sim |\cdot|_2$, entonces una sucesión (x_n) es de Cauchy respecto a $|\cdot|_1$ si, y sólo si es de Cauchy respecto a $|\cdot|_2$.

Definición

Una norma $\|\cdot\|$ sobre un cuerpo K se dice *no-arquimediana o ultramétrica*, si la condición (3) (en la definición 1) es reemplazada por

$$\|x+y\| \leq \max\{\|x\|, \|y\|\}, \forall x, y \in K. \tag{2.1}$$

Observación

Dado que

$$\|x+y\| \leq \max\{\|x\|, \|y\|\} \leqslant \|x\| + \|y\|, \forall x, y \in \mathbb{Q},$$

la condición 2.1 es también llamada *desigualdad triangular fuerte*.

El campo de los números p-ádicos

Definición

Fijemos un primo p, sea $x \in \mathbb{Q} \setminus \{0\}$ expresado de forma única como $x = p^v \frac{a}{b}$, donde v es un entero y a, b son primos relativos con p. Definimos la función $\|\cdot\|_p$ de la siguiente manera:

$$\|x\|_p = p^{-v},$$

donde el entero $v = v(x)$ se denomina el orden *p-ádico de x* y será denotado por $\mathrm{Ord}(x)$. Por definición $\|0\|_p = 0$, y $\mathrm{Ord}(0) = +\infty$.

El campo de los números p-ádicos

Ejemplo

Cálculo de la función $\|\cdot\|_p$ para distintos p's.

$$\left|-\frac{66}{500}\right|_p = \left|-\frac{33}{250}\right|_p = \left|-\frac{3\cdot 11}{2\cdot 5^3}\right|_p = \begin{cases} \frac{33}{250} & \text{si} \quad p=\infty; \\ 2 & \text{si} \quad p=2; \\ \frac{1}{3} & \text{si} \quad p=3; \\ 5^3 & \text{si} \quad p=5; \\ 1 & \text{si} \quad p=7; \\ \frac{1}{11} & \text{si} \quad p=11; \\ & \vdots \\ 1 & \text{otro caso.} \end{cases}$$

El campo de los números p-ádicos

Nuestros 3 mosqueteros:

Teorema (Fórmula Adélica del producto)

Sea $x \in \mathbb{Q}$ tal que $x \neq 0$, entonces:

$$\prod_{p}^{\infty} \|x\|_p = 1, \text{ con } \|x\|_\infty = |x| \text{ y } p \text{ primo.}$$

Teorema

$\|\cdot\|_p$ es una norma no arquimediana.

Teorema (Ostrowski)

Cualquier norma no trivial sobre $\mathbb{Q}$ es equivalente al valor absoluto usual, o a una norma p-ádica $\|\cdot\|_p$, para algún primo p.

El campo de los números p-ádicos

Observación

Las normas $\|\cdot\|_p$ y $\|\cdot\|_q$ no son quivalentes si p y q son primos distintos. Por ejemplo, sea $p = 5$ y $q = 7$, la sucesión $x_n = \left(\frac{5}{7}\right)^n$ se tiene que

$$\|x_n\|_5 = 5^{-n} \to 0 \text{ y } \|x_n\|_7 = 7^n \to \infty,$$

cuando $n \to \infty$.

El valor absoluto usual sobre $\mathbb{Q}$ tampoco es equivalente a una norma p-ádica. Por ejemplo, considérese la sucesión $x_n = (\frac{1}{p})^n$, entonces

$$|x_n| = p^{-n} \to 0 \text{ y } \|x_n\|_p = p^n \to \infty,$$

cuando $n \to \infty$. Lo cual contradice la proposición 3.

El campo de los números p-ádicos

Observación

Las normas $\|\cdot\|_p$ y $\|\cdot\|_q$ no son quivalentes si p y q son primos distintos. Por ejemplo, sea $p = 5$ y $q = 7$, la sucesión $x_n = \left(\frac{5}{7}\right)^n$ se tiene que

$$\|x_n\|_5 = 5^{-n} \to 0 \text{ y } \|x_n\|_7 = 7^n \to \infty,$$

cuando $n \to \infty$.

El valor absoluto usual sobre $\mathbb{Q}$ tampoco es equivalente a una norma p-ádica. Por ejemplo, considérese la sucesión $x_n = (\frac{1}{p})^n$, entonces

$$|x_n| = p^{-n} \to 0 \text{ y } \|x_n\|_p = p^n \to \infty,$$

cuando $n \to \infty$. Lo cual contradice la proposición 3.

Teorema (Caracterización de sucesiones de Cauchy)

Una sucesión $(x_n)_{n\in\mathbb{N}}$ en $\mathbb{Q}$ es de Cauchy, si, y sólo si:

$$\lim_{n\to\infty} \|x_{n+1} - x_n\|_p = 0. \tag{2.2}$$

Definición

Sea $(\mathbb{K}, \|\cdot\|)$ un cuerpo métrico. Sea $\mathbb{K}^{\mathbb{N}}$ el anillo de todas las sucesiones en $\mathbb{K}$. Definimos $\mathcal{C}, \mathcal{N}$ como el subanillo de todas las sucesiones de Cauchy y el subanillo de todas las sucesiones finalmente nulas, respectivamente.

Definición (Completación de un cuerpo métrico)

Sea $(\mathbb{K}, \|\cdot\|)$ un cuerpo métrico. Sean $\mathcal{C}, \mathcal{N}$ los subanillos de todas las sucesiones de Cauchy y de todas las sucesiones finalmente nulas, respectivamente. Definimos el cociente de anillos $\hat{\mathbb{K}} := \mathcal{C}/\mathcal{N}$ como la completación de $\mathbb{K}$.

Observación

La norma $\|\cdot\| : \hat{\mathbb{K}} \to \mathbb{R}_+$, sobre la completación de $\mathbb{K}$ está definida tal que para todo $(x_n) + \mathcal{N} \in \hat{\mathbb{K}}$:

$$\left\|(x_n) + \mathcal{N}\right\| = \lim_{n\to\infty} \|x_n\| .$$

El campo de los números p-ádicos

El siguiente teorema es importante, pues caracteriza a $\mathbb{Q}$ como un cuerpo no completo.

Teorema

$(\mathbb{Q}, d(x,y) = \|x-y\|_p)$ y $(\mathbb{Q}, d(x,y) = |x-y|)$ no son espacios completos.

Ejemplo

Un procedimiento para construir una sucesión de Cauchy en $(\mathbb{Q}, d(x,y) = \|x-y\|_p)$ podría hacerse, tomando $a \in \mathbb{Q}$ tal que:

- a no es cuadrado en $\mathbb{Q}$
- $p \nmid a$
- a es residuo cuadrático módulo p. i.e., $x^2 \equiv a \pmod{p^n}$ tiene solución.

Continuación...

Podemos hallar a tal que sea cuadrado en $\mathbb{Z}$ y sumarle un múltplo de p; para así construir la sucesión como sigue:

- Tomamos x_0 solución de $x^2 \equiv a \pmod{p}$
- Construimos a x_1 tal que $x_1 \equiv x_0 \pmod{p}$ y además $x_1^2 \equiv a \pmod{p^2}$
- Recursivamente, construimos x_n tal que:

$$x_n \equiv x_{n-1} \pmod{p^n} \text{ y } x_n^2 \equiv a \pmod{p^{n+1}}$$

Es de cauchy: $\|x_{n+1} - x_n\|_p = \|kp^n\|_p \leqslant \|p^n\|_p = p^{-n} \to 0$.
No converge: $\|x_n^2 - a\|_p = \|sp^{n+1}\|_p \leqslant \|p^{n+1}\|_p \leqslant p^{-(n+1)} \to 0$, luego $x_n \to \sqrt{a} \notin \mathbb{Q}$.