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.

4 de junio de 2020

Pontificia Universidad Javeriana, Facultad de Ciencias
Departamento de Matemáticas

Notación

Unidades, decenas y centenas...

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 $543{,}89_{10}$.

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 $743{,}22_8$.

Representación que usamos

- Particularmente, estamos interesados en expansiones sobre bases primas.

Representación que usamos

- Particularmente, estamos interesados en expansiones sobre bases primas.
- Por ejemplo con $p = 2$, el ¡Sistema binario!

Representación que usamos

- 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

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

Representación que usamos

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

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

será

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

- ¿Deberíamos llamar a las expansiones, expansiones pesimales?

Representación que usamos

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

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

será

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

- ¿Deberíamos llamar a las expansiones, expansiones pesimales?
- Ni idea. Usaremos los términos: expansión (representación) p-ádica ó *Código de Hensel.*

Representación que usamos

- 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

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

- ¿Deberíamos llamar a las expansiones, expansiones pesimales?
- Ni idea. Usaremos los términos: expansión (representación) p-ádica ó *Código de Hensel*.
- Siendo así, ahora sí empecemos.

El campo de los números p-ádicos

Norma

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:

- $|x| \geqslant 0, |x| = 0 \iff x = 0,$

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

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:

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

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

Norma

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

Equivalencia entre normas

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

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

Observación

Dado que

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

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

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 $\mathrm{Ord}(0) = +\infty$.

Ejemplo

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

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

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.

No equivalencia de normas en $\mathbb{Q}$

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 $(x_n) + \mathcal{N} \in \hat{\mathbb{K}}$:

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

Completaciones de $\mathbb{Q}_p$

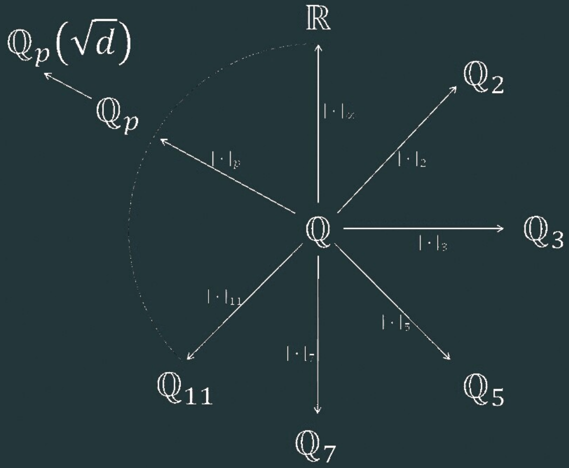

Figura 1: Completaciones respecto a las distintas normas en $\mathbb{Q}$

$\mathbb{Q}$ no es completo :c

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 $\mathbb{Q}$

$\mathbb{Q}$ no es completo :c

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 $\mathbb{Q}$
- $p \nmid a$

$\mathbb{Q}$ no es completo :c

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.

$\mathbb{Q}$ no es completo :c

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 $x^2 \equiv a \pmod p$

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 $x_n \to \sqrt{a} \notin \mathbb{Q}$.

$\mathbb{Q}$ no es completo :c

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 $x_1^2 \equiv a \pmod{p^2}$

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 $x_n \to \sqrt{a} \notin \mathbb{Q}$.

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 $x_n \to \sqrt{a} \notin \mathbb{Q}$.

Topología en $\mathbb{Q}_p$

El espacio $\mathbb{Q}_p^n$

Podemos definir en $\mathbb{Q}_p^n$ una norma como:

$$\|x\|_p := \max_{1\leqslant i\leqslant n} \|x_i\|_p, \qquad \text{para } x = (x_1, \ldots, x_n) \in \mathbb{Q}_p^n.$$

Así, $(\mathbb{Q}_p^n, d = \|x - y\|_p)$ es un espacio métrico, donde las distancias están en el conjunto $\{p^\gamma : \ \gamma \in \mathbb{Z}\} \cup \{0\}$. Luego, tiene sentido definir los abiertos básicos por:

$$B_\gamma^n(a) = \{x \in \mathbb{Q}_p : \|x - a\|_p < p^\gamma\}, \ \gamma \in \mathbb{Z}.$$

Observación

$B_\gamma^n(a)$ es un grupo aditivo.

Análogamente pordemos definir la esfera n-dimensional con centro en a:

$$S_r^n(a) = \{x \in \mathbb{Q}_p^n : \|x - a\|_p = p^r\}, \ r \in \mathbb{Z}.$$

Además

- $S_\gamma^n(a) = \left\{x : \|x - a\|_p = p^\gamma\right\} = B_\gamma^n(a) \backslash B_{\gamma-1}^n(a).$

Análogamente pordemos definir la esfera n-dimensional con centro en a:

$$S_r^n(a) = \{x \in \mathbb{Q}_p^n : \|x - a\|_p = p^r\}, \ r \in \mathbb{Z}.$$

Además

- $S_\gamma^n(a) = \left\{x : \|x - a\|_p = p^\gamma\right\} = B_\gamma^n(a) \backslash B_{\gamma-1}^n(a)$.
- $B_\gamma^n(a) \subset B_{\gamma'}^n(a)$ siempre que $\gamma < \gamma'$.

Algunas propiedades topológicas de $\mathbb{Q}_p^n$

Análogamente pordemos definir la esfera n-dimensional con centro en a:

$$S_r^n(a) = \{x \in \mathbb{Q}_p^n : \|x - a\|_p = p^r\}, \; r \in \mathbb{Z}.$$

Además

- $S_\gamma^n(a) = \left\{x : \|x - a\|_p = p^\gamma\right\} = B_\gamma^n(a) \setminus B_{\gamma-1}^n(a)$.
- $B_\gamma^n(a) \subset B_{\gamma'}^n(a)$ siempre que $\gamma < \gamma'$.
- $B_{\gamma-1}^n(a) = \left\{x : \|x - a\|_p < p^\gamma\right\}$.

Análogamente pordemos definir la esfera n-dimensional con centro en a:

$$S_r^n(a) = \{x \in \mathbb{Q}_p^n : \|x - a\|_p = p^r\}, \ r \in \mathbb{Z}.$$

Además

- $S_\gamma^n(a) = \left\{x : \|x - a\|_p = p^\gamma\right\} = B_\gamma^n(a) \setminus B_{\gamma-1}^n(a)$.
- $B_\gamma^n(a) \subset B_{\gamma'}^n(a)$ siempre que $\gamma < \gamma'$.
- $B_{\gamma-1}^n(a) = \left\{x : \|x - a\|_p < p^\gamma\right\}$.
- $B_\gamma^n(a) = \bigcup_{\gamma' \leqslant \gamma} S_{\gamma'}^n(a)$.

Algunas propiedades topológicas de $\mathbb{Q}_p^n$

Análogamente pordemos definir la esfera n-dimensional con centro en a:

$$S_r^n(a) = \{x \in \mathbb{Q}_p^n : \|x - a\|_p = p^r\}, \ r \in \mathbb{Z}.$$

Además

- $S_\gamma^n(a) = \left\{x : \|x - a\|_p = p^\gamma\right\} = B_\gamma^n(a) \backslash B_{\gamma-1}^n(a)$.
- $B_\gamma^n(a) \subset B_{\gamma'}^n(a)$ siempre que $\gamma < \gamma'$.
- $B_{\gamma-1}^n(a) = \left\{x : \|x - a\|_p < p^\gamma\right\}$.
- $B_\gamma^n(a) = \bigcup_{\gamma' \leqslant \gamma} S_{\gamma'}^n(a)$.
- $\bigcup_\gamma B_\gamma^n(a) = \bigcup_\gamma S_\gamma^n(a) = \mathbb{Q}_p^n - \{0\}$.

Análogamente pordemos definir la esfera n-dimensional con centro en a:

$$S_r^n(a) = \{x \in \mathbb{Q}_p^n : \|x - a\|_p = p^r\}, \;\; r \in \mathbb{Z}.$$

Además

- $S_\gamma^n(a) = \left\{x : \|x - a\|_p = p^\gamma\right\} = B_\gamma^n(a) \backslash B_{\gamma-1}^n(a)$.
- $B_\gamma^n(a) \subset B_{\gamma'}^n(a)$ siempre que $\gamma < \gamma'$.
- $B_{\gamma-1}^n(a) = \left\{x : \|x - a\|_p < p^\gamma\right\}$.
- $B_\gamma^n(a) = \bigcup_{\gamma' \leqslant \gamma} S_{\gamma'}^n(a)$.
- $\bigcup_\gamma B_\gamma^n(a) = \bigcup_\gamma S_\gamma^n(a) = \mathbb{Q}_p^n - \{0\}$.
- $\bigcap_\gamma B_\gamma^n(a) = \{a\}$.

Propiedades bonitas de $\mathbb{Q}_p$:o

Teorema

- Si $b \in B_r(a)$, entonces $B_r(a) = B_r(b)$. En otras palabras: ¡Todo punto de una bola abierta es centro de la misma!

Propiedades bonitas de $\mathbb{Q}_p$:o

Teorema

- Si $b \in B_r(a)$, entonces $B_r(a) = B_r(b)$. En otras palabras: ¡Todo punto de una bola abierta es centro de la misma!
- Toda bola es a su vez, un conjunto cerrado y abierto.

Teorema

- Si $b \in B_r(a)$, entonces $B_r(a) = B_r(b)$. En otras palabras: ¡Todo punto de una bola abierta es centro de la misma!
- Toda bola es a su vez, un conjunto cerrado y abierto.
- Dos bolas en $\mathbb{Q}_p$ son disyuntas o una contiene a la otra; es decir, si $a, b \in \mathbb{Q}_p$, y $r, s \in \mathbb{Z}$, se tiene que $B_r(a) \cap B_s(b) \neq \emptyset$ si, y sólo si, $B_r(a) \subseteq B_s(b)$ o $B_s(b) \subseteq B_r(a)$.

Más propiedades de $\mathbb{Q}_p$

Teorema

$\mathbb{Q}_p$ es un espacio de *Hausdorff*

Teorema

$\{B_\gamma(a) \colon r \in \mathbb{Z}, a \in \mathbb{Q}_p\}$ es contable.

Teorema

$\mathbb{Q}_p$ es un espacio localmente compacto.

Algunas definiciones de Topología

Definición

Decimos que un espacio topológico es *conexo* si no puede ser escrito como la unión de dos abiertos disyuntos no vacíos. Por otro lado, decimos que un espacio es *disconexo* si es la unión de dos abiertos disyuntos no vacíos.

Definición

Los subconjuntos conexos maximales de un espacio topológico son llamados *componentes conexos*.

Definición

Decimos que un espacio topológico es *totalmente disconexo* si todas sus componentes conexos son singletons.

Un corolario simple y bonito

Teorema

$\mathbb{Q}_p$ es totalmente disconexo.

Teorema

$\mathbb{N}$ es denso en $\mathbb{Z}_p$.

Lema

Sean $x, y \in \mathbb{Q}_p$ tales que $\|x\|_p \neq \|y\|_p$. Entonces:

$$\|x + y\|_p = \text{máx}\{\|x\|_p, \|y\|_p\}$$

Corolario

Todos los triángulos en $\mathbb{Q}_p$ son isósceles.

Un corolario simple y bonito

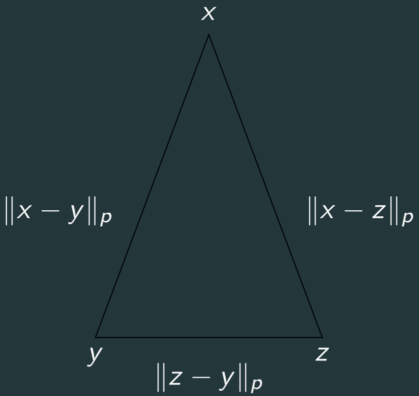

Figura 2: Todos los triángulos en $\mathbb{Q}_p$ son isósceles

Relación de $\mathbb{Q}_p$ con $\mathbb{R}$

- Existe una correspondencia con los *Conjuntos de Cantor*.
- También podemos relacionarlos mediante una función $\rho\colon \mathbb{Q}_p \to \mathbb{R}_+$ conocida como *Monna map*, definida por

$$\rho : \sum_{j=\gamma}^{\infty} x_j p^j \mapsto \sum_{j=\gamma}^{\infty} x_j p^{-j-1}, \quad x_j = 0, 1, \ldots, p-1, \quad \gamma \in \mathbb{Z}, \tag{3.1}$$

Propiedades de ρ

- ρ es una función continua, sobreyectiva, pero no inyectiva.

Propiedades de ρ

- ρ es una función continua, sobreyectiva, pero no inyectiva.
- $|\rho(x)-\rho(y)| \leqslant \|x-y\|_p$, para todo $x, y \in \mathbb{Q}_p$. Es decir, ρ satisface la desigualdad de Hölder,

Propiedades de ρ

- ρ es una función continua, sobreyectiva, pero no inyectiva.
- $|\rho(x) - \rho(y)| \leqslant \|x - y\|_p,$ para todo $x, y \in \mathbb{Q}_p$. Es decir, ρ satisface la desigualdad de Hölder,
- $\rho\left(p^{\gamma} x\right) = p^{-\gamma} \rho(x),$ para todo $x \in \mathbb{Q}_p$.

Aritmética p-ádica

Expansiones p-ádicas de enteros

- Podemos expandir por cualquier base p un número $n \in \mathbb{Z}$

Expansiones p-ádicas de enteros

- Podemos expandir por cualquier base p un número $n \in \mathbb{Z}$
- El procedimiento es algorítmico:

$$\begin{aligned}
a_0 = n \bmod p \quad &\implies \quad n_1 = \frac{n - a_0}{p}, \\
a_1 = n_1 \bmod p \quad &\implies \quad n_2 = \frac{n_1 - a_1}{p}, \\
a_2 = n_2 \bmod p \quad &\implies \quad n_3 = \frac{n_2 - a_2}{p}, \\
&\vdots
\end{aligned}$$

Expansiones p-ádicas de enteros

- Podemos expandir por cualquier base p un número $n \in \mathbb{Z}$
- El procedimiento es algorítmico:

$$\begin{aligned}
a_0 = n \bmod p \quad &\Longrightarrow \quad n_1 = \frac{n - a_0}{p}, \\
a_1 = n_1 \bmod p \quad &\Longrightarrow \quad n_2 = \frac{n_1 - a_1}{p}, \\
a_2 = n_2 \bmod p \quad &\Longrightarrow \quad n_3 = \frac{n_2 - a_2}{p}, \\
&\vdots
\end{aligned}$$

- Así, la representación de un entero p-ádico por dígitos está dada por 1.1

$$n = a_l \dots a_3 a_2 a_1 {a_0}_p,$$

Expansiones p-ádicas de enteros

- Podemos expandir por cualquier base p un número $n \in \mathbb{Z}$
- El procedimiento es algorítmico:

$$\begin{aligned} a_0 &= n \bmod p &\implies&& n_1 &= \frac{n - a_0}{p}, \\ a_1 &= n_1 \bmod p &\implies&& n_2 &= \frac{n_1 - a_1}{p}, \\ a_2 &= n_2 \bmod p &\implies&& n_3 &= \frac{n_2 - a_2}{p}, \\ &&\vdots&& \end{aligned}$$

- Así, la representación de un entero p-ádico por dígitos está dada por 1.1

$$n = a_l \dots a_3 a_2 a_1 {a_0}_p,$$

- La representación es conocida como el *Código de Hensel* de n.

Expansiones p-ádicas de enteros

Ejemplo

Sea $n = 5353$ y sea $p = 5$, entonces la representación p-ádica de 5353 en base 5 está dada por:

$$
\begin{aligned}
a_0 &= 5353 \bmod 5 = 3 &\implies&& n_1 &= \frac{5353-3}{5} = 1070,\\
a_1 &= 1070 \bmod 5 = 0 &\implies&& n_2 &= \frac{1070-0}{5} = 214,\\
a_2 &= 214 \bmod 5 = 4 &\implies&& n_3 &= \frac{214-4}{5} = 42,\\
a_3 &= 42 \bmod 5 = 2 &\implies&& n_4 &= \frac{42-2}{5} = 8,\\
a_4 &= 8 \bmod 5 = 3 &\implies&& n_5 &= \frac{8-3}{5} = 1,\\
a_5 &= 1 \bmod 5 = 1 &\implies&& n_6 &= \frac{1-1}{5} = 0.
\end{aligned}
$$

En otras palabras, el código de Hensel de 5353 es 132403_5.

Expansiones p-ádicas de racionales

Consideremos x tal que su serie de expansión es

$$\begin{aligned} x &= 2 + 3p + p^2 + 3p^3 + p^4 + 3p^5 + p^6 + \cdots \\ &= 2 + 3p\left(1 + p^2 + p^4 + \cdots\right) + p^2\left(1 + p^2 + p^4 + \cdots\right) \\ &= 2 + \left(3p + p^2\right)\left(1 + p^2 + p^4 + \cdots\right). \end{aligned}$$

Como $1 + p^2 + p^4 + \cdots$ converge a $\left(1 - p^2\right)^{-1}$, tenemos

$$x = 2 + \frac{3p + p^2}{1 - p^2}.$$

Como caso particular, tomando $p = 5$, tenemos que

$$x = 2 + \frac{3 \cdot 5 + 5^2}{1 - 5^2} = \frac{1}{3},$$

por lo tanto, la expansión 5-ádica de $\frac{1}{3}$ es $\cdots 1313132_5$.

Ejemplos de expansiones p-ádicas sobre racionales

Ejemplo

$$14{,}31_5 = 1 \cdot 5^{-2} + 3 \cdot 5^{-1} + 4 \cdot 5^0 + 1 \cdot 5^1 = 241/25$$
$$1413_5 = 1 \cdot 5^0 + 3 \cdot 5^1 + 4 \cdot 5^2 + 1 \cdot 5^3 = 241$$
$$14310_5 = 0 \cdot 5^0 + 1 \cdot 5^1 + 3 \cdot 5^2 + 4 \cdot 5^3 + 1 \cdot 5^4 = 1205$$

Suma

Sean $\alpha = (a_i)$ y $\beta = (b_i)$ dos enteros p-ádicos. Definimos la suma como una sucesión (c_i) de dígitos p-ádicos apoyados de una sucesión (ϵ_i) en $\{0, 1\}$ (*carries*), tales que:

- $\epsilon_0 = 0$,

Suma

Sean $\alpha = (a_i)$ y $\beta = (b_i)$ dos enteros p-ádicos. Definimos la suma como una sucesión (c_i) de dígitos p-ádicos apoyados de una sucesión (ϵ_i) en $\{0, 1\}$ (*carries*), tales que:

- $\epsilon_0 = 0$,
- $c_i = a_i + b_i + \epsilon_i$ ó $c_i = a_i + b_i + \epsilon_i - p$, donde alguno de los dos es un dígito p-ádico; es decir, $c_i \in \{0, \ldots, p-1\}$. Dado el caso de c_i se tendrá que $\epsilon_{i+1} = 0$ o $\epsilon_{i+1} = 1$.

Suma

Ejemplo

- Tomando $p = 7$, se tiene:

$$\begin{array}{cccccccc} & \cdots & 2 & 5 & 1 & 4 & 1 & 3 \\ + & \cdots & 1 & 2 & 1 & 1 & 0 & 2 \\ \hline & \cdots & 4 & 0 & 2 & 5 & 1 & 5 \end{array}$$

- $0 - 1$ en los 7-ádicos:

$$\begin{array}{cccccccc} & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \\ - & \cdots & 0 & 0 & 0 & 0 & 0 & 1 \\ \hline & \cdots & 6 & 6 & 6 & 6 & 6 & 6 \end{array}$$

Esto quiere decir que $-1 = \cdots 666_7$.

Representación de números negativos

Si $x = \sum_{i=\gamma}^{\infty} a_i p^i$, entonces $-x = \sum_{i=\gamma}^{\infty} b_i p^i$, donde $b_\gamma = p - a_\gamma$ y $b_i = (p-1) - a_i$ con $i > \gamma$.

Ejemplo

Con $p = 5$

$$\frac{1}{3} = \cdots 1313132_5 \Rightarrow -\frac{1}{3} = \cdots 3131313_5,$$
$$\frac{5}{3} = \cdots 13131320_5 \Rightarrow -\frac{5}{3} = \cdots 31313130_5.$$

Numeros unidades

Definición

Un número p-ádico es llamado *unidad* si no es múltiplo de una potencia negativa de p y su primer dígito no es 0.

Ejemplo

Los números $\cdots 314_5$ y $\cdots 24_5$ son unidades, mientras que $\cdots 310_5$ y $\cdots 1321{,}24_5$ no lo son.

Así, un número p-ádico no-unidad $x = \sum_{j=-N}^{\infty} a_j p^j$ es un número que puede escribirse de la forma $x = u \cdot p^{-N}$ donde u es un número unidad. Por ejemplo

$$\cdots 410_5 = \cdots 41_5 \cdot 5^1$$
$$\cdots 1321{,}24_5 = \cdots 132124_5 \cdot 5^{-2}.$$

Multiplicación p-ádica

Sean $x = u \cdot p^{-N_1}$ y $y = v \cdot p^{-N_2}$ con u, v unidades. Definimos la multiplicación $x \cdot y = u \cdot v \cdot p^{-(N_1+N_2)}$

Ejemplo

$$
\begin{array}{cccccc}
 & \cdots & 5 & 1 & 4 & 1 & 3 \\
\times & \cdots & 2 & 1 & 1 & 0 & 2 \\
\hline
 & \cdots & 3 & 3 & 1 & 2 & 6 \\
 & \cdots & 0 & 0 & 0 & 0 & \\
 & \cdots & 4 & 1 & 3 & & \\
 & \cdots & 1 & 3 & & & \\
+ & \cdots & 6 & & & & \\
\hline
 & \cdots & 1 & 0 & 4 & 2 & 6
\end{array}
$$

Así, con $p = 7$, $u \cdot v = \cdots 251413_7 \times \cdots 123102_7 = \cdots 310426_7$.

División p-ádica

Los cálculos de divisiones en los enteros p-ádicos no difieren de los métodos tradicionales de división.

Ejemplo

$$
\begin{array}{r|l}
 & 5\;1\;6\cdots \\ \hline
3\;5\;1 & 1\;2\;4\cdots \\
 & 1\;6\;1\cdots \\ \hline
 & \;3\;2\cdots \\
 & \;3\;5\cdots \\ \hline
 & \;\;4\cdots \\
 & \;\;4\cdots \\ \hline
 & \;\;\;\cdots
\end{array}
$$

Así, con $p = 7$, $\frac{\cdots 421_7}{\cdots 153_7} = \cdots 615_7$.

Observación

Los anteriores procedimientos de multiplicación y división, hechos sobre $\mathbb{Z}_p$ pueden ser extendidos de manera natural a $\mathbb{Q}_p$, pues el problema se reduce a operar números unidades.

Ejemplo

Al momento de multiplicar los números no-unidades, sean

$$x = \cdots 2514{,}13_7 = \cdots 251413_7 \cdot 7^{-2} = u \cdot 7^{-2},$$
$$y = \cdots 121{,}102_7 = \cdots 121102_7 \cdot 7^{-3} = v \cdot 7^{-3},$$

Luego

$$x \cdot y = u \cdot v \cdot 7^{-(2+3)}.$$

Por el ejemplo 34, tenemos que $u \cdot v = \cdots 310426_7$, entonces:

$$x \cdot y = \cdots 310426_7 \cdot 7^{-5} = 3{,}10426_7.$$

Sucesiones y series de números p-ádicos

Estabilización de sucesiones y series

Teorema

Si

$$\lim_{n\to\infty} x_n = x, \text{ con } x_n, x \in \mathbb{Q}_p \text{ y } \|x\|_p \neq 0,$$

entonces la sucesión $(\|x_n\|_p)_{n\in\mathbb{N}}$ se estabiliza, es decir, existe $N \in \mathbb{N}$ tal que:

$$\|x_n\|_p = \|x\|_p, \text{ para todo } n \geqslant N.$$

Teorema

Una serie $\sum_{j=1}^{\infty} x_j,\ x_j \in \mathbb{Q}_p$ converge en $\mathbb{Q}_p$, si, y sólo si, $\lim_{n\to\infty} x_n = 0$. En tal caso:

$$\|\sum_{j=1}^{\infty} x_j\|_p \leqslant \max_j \|x_j\|_p.$$

Ejemplo

En $\mathbb{Q}_p$ tenemos que:

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

Problema abierto

Desde el año 1971 se abrió el siguiente problema: ¿Puede ser $\sum_{n=0}^{\infty} n!$ un número racional para algún primo p? Por ahora, se sabe que $\sum_{n=0}^{\infty} n!$ converge en cada $\mathbb{Q}_p$. Pero nada se sabe de su valor.

Proposición

Todo número p-ádico se puede escribir de manera única como la suma de una serie convergente en $\mathbb{Q}_p$ de la forma:

$$\sum_{k=-\infty}^{\infty} a_k p^k, \text{ con } a_k \in \{0, \ldots, p-1\} \tag{5.1}$$

y en donde $a_k = 0$, para $k \leqslant -N$ y $a_{-N} \neq 0$. A $-N$ se le denomina el *orden* del número.

Parte entera y parte fraccionaria

- La *parte fraccionaria de* $x \in \mathbb{Q}_p$, denotada como $\{x\}_p$, es el siguiente número racional:

$$\{x\}_p := \begin{cases} 0 & \text{si} \quad x = 0, \text{ u } \operatorname{Ord}(x) \geqslant 0 \\ p^v \displaystyle\sum_{j=0}^{|v|-1} x_j p^j & \text{si} \quad \operatorname{Ord}(x) < 0. \end{cases}$$

Parte entera y parte fraccionaria

- La *parte fraccionaria de* $x \in \mathbb{Q}_p$, denotada como $\{x\}_p$, es el siguiente número racional:

$$\{x\}_p := \begin{cases} 0 & \text{si} \quad x = 0, \text{ u } \operatorname{Ord}(x) \geqslant 0 \\ p^v \displaystyle\sum_{j=0}^{|v|-1} x_j p^j & \text{si} \quad \operatorname{Ord}(x) < 0. \end{cases}$$

- Así, para todo $x \in \mathbb{Q}_p$

$$\begin{aligned} x &= \sum_{i=v}^{-1} a_i p^i + \sum_{i=0}^{\infty} a_i p^i \\ &=: \{x\}_p + [x]_p. \end{aligned}$$

Una mirada algebraica de los números p-ádicos

Definición

El conjunto

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leqslant 1\} = \{x \in \mathbb{Q}_p : x = \sum_{i=i_0}^{\infty} a_i p^i, i_0 \geqslant 0\},$$

es llamado el conjunto de los *enteros p-ádicos*.

Teorema

$\mathbb{Z}_p$ es un subanillo de $\mathbb{Q}_p$.

Números invertibles

Proposición

Un entero p-ádico $x = \sum_{i=i_0}^{\infty} a_i p^i$, $i_0 \geqslant 0$ es invertible en $\mathbb{Z}_p$ si, y sólo si, $a_0 \neq 0$.

- Así, el grupo de los números invertibles en $\mathbb{Z}_p$ está dado por:

$$\mathbb{Z}_p^{\times} = \{x \in \mathbb{Z}_p : \|x\|_p = 1\} = \left\{x \in \mathbb{Z}_p : x = \sum_{k=0}^{\infty} x_k p^k, \quad x_0 \neq 0\right\},$$

  que es un grupo multiplicativo del anillo $\mathbb{Z}_p$.
- Estos elementos son llamados *unidades* de $\mathbb{Q}_p$ ¡Tal como lo vimos en la sección de aritmética!

Ejemplo

$1 - p$ es invertible en $\mathbb{Z}_p$, pues su inverso es $\sum_{k=0}^{\infty} p^k = \frac{1}{1-p}$.

Ideales en $\mathbb{Z}_p$

- El anillo $\mathbb{Z}_p$ es un *dominio de ideales principales*.

Ideales en $\mathbb{Z}_p$

- El anillo $\mathbb{Z}_p$ es un *dominio de ideales principales*.
- Más exactamente, cualquier ideal de $\mathbb{Z}_p$ tiene la forma

$$p^m\mathbb{Z}_p = \left\{x \in \mathbb{Z}_p : x = \sum_{i \geqslant m} a_i p^i\right\}, \ m \in \mathbb{N}.$$

Ideales en $\mathbb{Z}_p$

- El anillo $\mathbb{Z}_p$ es un *dominio de ideales principales*.
- Más exactamente, cualquier ideal de $\mathbb{Z}_p$ tiene la forma

$$p^m\mathbb{Z}_p = \left\{x \in \mathbb{Z}_p : x = \sum_{i \geqslant m} a_i p^i\right\}, \; m \in \mathbb{N}.$$

- $\mathbb{Z}_p \supset p\mathbb{Z}_p \cdots \supset p^k\mathbb{Z}_p \supset \cdots \supset \bigcap_{k \geqslant 0} p^k\mathbb{Z}_p = \{0\}$

Ideales en $\mathbb{Z}_p$

- El anillo $\mathbb{Z}_p$ es un *dominio de ideales principales*.
- Más exactamente, cualquier ideal de $\mathbb{Z}_p$ tiene la forma

$$p^m\mathbb{Z}_p = \left\{x \in \mathbb{Z}_p : x = \sum_{i \geqslant m} a_i p^i\right\}, \ m \in \mathbb{N}.$$

- $\mathbb{Z}_p \supset p\mathbb{Z}_p \cdots \supset p^k\mathbb{Z}_p \supset \cdots \supset \bigcap_{k \geqslant 0} p^k\mathbb{Z}_p = \{0\}$
- $\mathbb{Z}_p$ es un *anillo local*, cuyo ideal maximal es:

$$p\mathbb{Z}_p = \{x \in \mathbb{Z}_p : \|x\|_p < 1\}.$$

Homomorfismos

- Podemos definir el homomorfismo de anillos:

$$\begin{aligned} \pi_n : \mathbb{Z}_p &\to \mathbb{Z}/p^n\mathbb{Z} \\ x &\mapsto \sum_{k=0}^{n-1} a_k p^k \pmod{p^n}, \end{aligned}$$

Homomorfismos

- Podemos definir el homomorfismo de anillos:

$$\begin{aligned} \pi_n : \mathbb{Z}_p &\to \mathbb{Z}/p^n\mathbb{Z} \\ x &\mapsto \sum_{k=0}^{n-1} a_k p^k \pmod{p^n}, \end{aligned}$$

- Y en general, definimos el homomorfismo:

$$\begin{aligned} \pi : \mathbb{Z}_p &\to \prod_{n=0}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \\ x &\mapsto (\pi_1(x), \pi_2(x), \dots). \end{aligned}$$

Homomorfismos

- Podemos definir el homomorfismo de anillos:

$$\begin{aligned} \pi_n : \mathbb{Z}_p &\to \mathbb{Z}/p^n\mathbb{Z} \\ x &\mapsto \sum_{k=0}^{n-1} a_k p^k \pmod{p^n}, \end{aligned}$$

- Y en general, definimos el homomorfismo:

$$\begin{aligned} \pi : \mathbb{Z}_p &\to \prod_{n=0}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \\ x &\mapsto (\pi_1(x), \pi_2(x), \dots). \end{aligned}$$

- Si nos restringimos a la imagen de este homorfismo, esta es conocida como el *límite proyectivo* de los $\mathbb{Z}/p^n\mathbb{Z}$, y se denota por

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

- Se puede ver que π restringida al rango, es isomorfismo, y así:

$$\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

Definición de $\mathbb{Z}_p$ y $\mathbb{Q}_p$ vía álgebra

- Se puede ver que π restringida al rango, es isomorfismo, y así:

$$\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

- $\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p)$.

Definición de $\mathbb{Z}_p$ y $\mathbb{Q}_p$ vía álgebra

- Se puede ver que π restringida al rango, es isomorfismo, y así:

$$\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

- $\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p)$.
- $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$.

Sobre Diferenciación e Integración

Si $f : \mathbb{Q}_p \to \mathbb{C}$, estaríamos tentados a definir:

$$f'(a) = \lim_{h \to 0} \frac{f(a+h) - f(a)}{h}.$$

Definición

Una función $f : B_\gamma \subseteq \mathbb{Q}_p \to \mathbb{Q}_p$ se dice *analítica* si:

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

con $x \in B_\gamma$, $a_n \in \mathbb{Q}_p$.

Definición

Si $f : B_\gamma \subseteq \mathbb{Q}_p \to \mathbb{Q}_p$ es analítica, definimos

$$f^{(m)}(x) = \sum_{n=m}^{\infty} n(n-1)\cdots(n-m+1)a_n x^{n-m},$$

$$f^{(-m)}(x) = \sum_{n=0}^{\infty} \frac{1}{(n+1)(n+2)\cdots(n+m)} a_n x^{n+m},$$

como *derivadas* y *primitivas*, respectivamente.

Dado que $(\mathbb{Q}_p, +)$ es un grupo topológico localmente compacto, un resultado conocido en teoría de la medida establece que $(\mathbb{Q}_p, +)$ tiene una única medida *dx*, llamada la *medida de Haar* de $\mathbb{Q}_p$.

Definición

Decimos que una función $f : \mathbb{Q}_p \to \mathbb{C}$ es *integrable* en $\mathbb{Q}_p$ si existe

$$\lim_{N \to \infty} \int_{B_N} f(x)dx.$$

Por notación, decimos que $f \in \mathcal{L}^1(\mathbb{Q}_p)$.