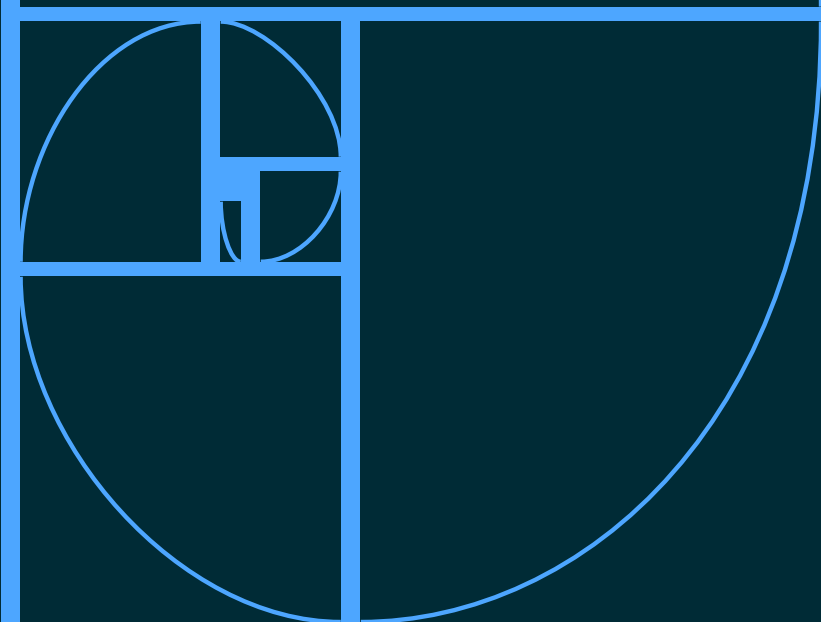
Números p-ádicos

Noviembre, 17



Micaela Yataz
Seminario
Universidad del Valle de Guatemala

Idea

La construcción de estos nuevos valores absolutos en $\mathbb{Q}$ es la siguiente:

- Dado un número p, se quiere decir cuándo dos números racionales estan cerca, en un sentido que involucre a este primo.
- En particular que tan cerca está un número racional $x \in \mathbb{Q}$ del cero $0 \in \mathbb{Q}$

Formalmente

El primo p asociado a la función $||_p$ que asigna a cada racional $x \in \mathbb{Q}$ su valor absoluto $|x|_p \in \mathbb{Q}$

$$||_p : x \to |x|_p$$

Nota

Dada la función $||_p$

- Si $x = 0 \in \mathbb{Q} \implies |0|_p = 0$
- Si $x = \frac{a}{b} \neq 0 \in \mathbb{Q}$
  Se puede escribir de forma única

$$x = \frac{a}{b} = p^r \frac{a'}{b'}, \quad \text{con } r, a', b' \in \mathbb{Z}$$

$$\text{y } p \nmid a'b'$$

Norma p-ádica

Valuación p-ádica

$$|\cdot|_p = p^{-v_p(x)}$$

donde el orden p-ádico: $v_p(x)$ es el exponente de mayor potencia de p que divide a x.

Ejemplo

Para $p = 5$ $x = 10$

Ya que $10 = 5^1 * 2$ entonces $v_5(10) = 1$

$$|10|_5 = 5^{-1} = \frac{1}{5}$$

Norma p-ádica

Distancia: Real vs p-ádica

Distancia Real $|\cdot|$

$$|6-1| = |5| = 5$$

$$|26-1| = |25| = 25$$

Distancia $|\cdot|_p$ con $p = 5$

$$|6-1|_5 = |5|_5 = \frac{1}{5}$$

$$|26-1|_5 = |25|_5$$

Ya que $25 = 5^2$ entonces $v_5(25) = 2$ Por lo que

$$|25|_5 = 5^{-2} = \frac{1}{5^2} = \frac{1}{25}$$

En $\mathbb{Q}_5$ el número 26 está mas cerca de 1 que 6. Ya que $\frac{1}{25} < \frac{1}{5}$

Norma p-ádica

Propiedades

La función $|\cdot|_p$ satisface las propiedades siguientes, para $x, y \in \mathbb{Q}$

1. $|x|_p = 0$ ssi $x = 0$
2. $|xy|_p = |x|_p |y|_p$
3. $|x + y|_p \leq \max\{|x|_p, |y|_p\}$

La norma p-ádica no es arquimediana

- Por el axioma de arquímides, dado $a \neq 0$ y b racionales. Para el valor absoluto usual:

$$|na| > |b|$$

para algún n suficientemente grande.

- Si consideramos en $\mathbb{Q}$ el valor absoluto p-ádico, entonces $\forall n \in \mathbb{Z}$ se tiene que:

$$n = 1 + \cdots + 1 \in \mathbb{Q}$$

satisface que:

$$|n|_p = |1 + \cdots + 1|_p \leq \max\{|1|_p\} = 1$$

Por tanto, $\forall a \in \mathbb{Q}$ y $n \in \mathbb{N}$:

$$|na|_p = |n|_p |a|_p \leq |a|_p$$

De esta forma, incumple el axioma de Arquímedes.

Resultados interesantes

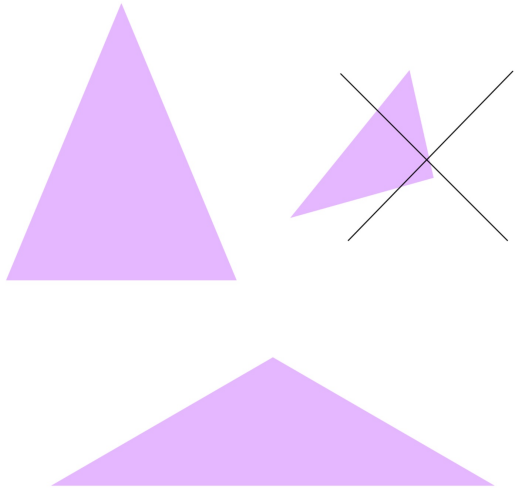


Figure: **Propiedad del triángulo isósceles:** En la métrica p-ádica, la longitud del tercer lado es $\leq max$ de los otros dos, forzando a al triángulo a ser isósceles o equilátero.

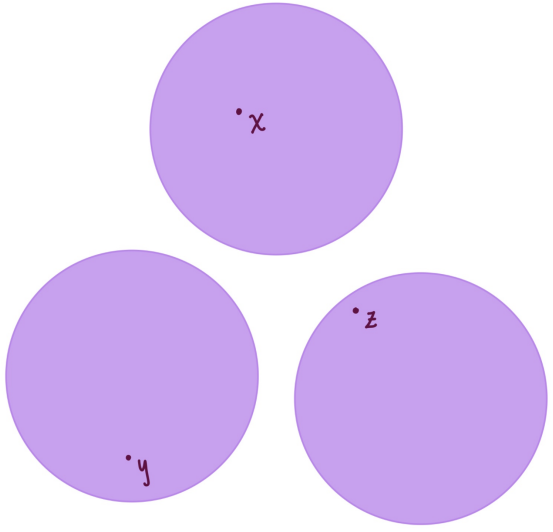


Figure: **Todo punto es centro:** Cualquier punto y dentro de una bola abierta $B(a, r)$ es centro de la misma bola ($B(a, r) = B(y, r)$.)

Propiedad del triángulo isósceles

Prueba:
Definimos los lados:

- $L_1 = d_p(x, y) = |x - y|_p$
- $L_2 = d_p(y, z) = |y - z|_p$
- $L_3 = d_p(x, z) = |x - z|_p$
  Podemos expresar L_3 usando L_1 y L_2:

$$x - z = (x - y) + (y - z)$$

Propiedad del triángulo isósceles

Aplicando la desigualdad ultra-métrica con $a = (x - y)$ *y* $b = (y - z)$*:*

$$|x - z|_p \leq \max\{|x - y|_p, |y - z|_p\}$$

$$L_3 \leq \max\{L_1, L_2\} \quad (1.1)$$

Ahora, debemos demostrar que la igualdad se cumple si $L_1 \neq L_2$*.*

Propiedad del triángulo isósceles

Sea $L_1 < L_2$. *Esto implica que* $\max\{L_1, L_2\} = L_2$.
La desigualdad (1.1) *se convierte en:*

$$L_3 \leq L_2$$

Ahora, examinamos la relación entre L_2 *y los otros dos lados. Podemos escribir:*

$$y - z = (y - x) + (x - z)$$

Propiedad del triángulo isósceles

Aplicando la desigualdad ultra-métrica con $a = (y - x)$ *y* $b = (x - z)$*:*

$$|y - z|_p \leq \max\{|y - x|_p, |x - z|_p\}$$

$$L_2 \leq \max\{L_1, L_3\} \quad (1.2)$$

Propiedad del triángulo isósceles

Si $L_3 < L_2$, *entonces, como asumimos que* $L_1 < L_2$, *el máximo en* 1.2) *sería:*

$$\max\{L_1, L_3\} = \textit{el mayor de dos números menores que } L_2$$

Esto llevaría a la contradicción $L_2 \leq \max\{L_1, L_3\} < L_2$.*Por lo tanto, la única posibilidad compatible con las suposiciones y las desigualdades es que* L_3 *debe ser igual a* L_2*:*

$$L_3 = L_2$$

Propiedad del triángulo isósceles

Si $L_1 < L_2$, hemos demostrado que $L_3 = L_2$.Los tres lados del triángulo son:

$$L_1, L_2, L_3 \implies L_1, L_2, L_2$$

Dado que $L_1 \neq L_2$, el triángulo tiene dos lados iguales (L_2 y L_3), lo que demuestra que todo triángulo en un espacio p-ádico es isósceles.

Todo punto es centro: B(a, r) = B(y, r)

Bola abierta en la norma p-ádica

Sea $|\cdot|_p$ la norma p-ádica. La bola abierta de centro a y de radio p^{-n} es:
$B(a, p^{-n}) = \{x : |x - a|_p < p^{-n}\}$
En $\mathbb{Q}_p$ esta bola significa que las primeras n cifras $p-$ádicas de x coinciden con las de a.

Prueba:

- $B(a, r) \subseteq B(y, r)$

  Dado que y es un punto interior de $B(a, r)$, por definición se cumple que:

  $$d(y, a) < r \quad (2.1)$$

Todo punto es centro: B(a, r) = B(y, r)

Tomemos un punto arbitrario $x \in B(a, r)$. *Por definición se cumple que:*

$$d(x, a) < r \quad (2.2)$$

Queremos demostrar que x *también está en* $B(y, r)$, *lo que requiere probar que* $d(x, y) < r$.*Usamos la propiedad de la desigualdad triangular fuerte para los puntos* x, y, a*:*

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

Todo punto es centro: B(a, r) = B(y, r)

Sustituyendo las condiciones (1) y (2) en la desigualdad ultramétrica, tenemos:

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

Esto prueba que $x \in B(y,r)$. *Así,* $B(a,r) \subseteq B(y,r)$.

Todo punto es centro: B(a, r) = B(y, r)

- $B(y,r) \subseteq B(a,r)$

  Sabemos que $d(a,y) = d(y,a) < r$. *Esto significa que a es un punto interior de la bola* $B(y,r)$.
  Tomemos un punto arbitrario $z \in B(y,r)$. *Por definición se cumple que:*

  $$d(z,y) < r \quad (2.3)$$

  Queremos demostrar que z también está en $B(a,r)$, *es decir, que* $d(z,a) < r$.*Aplicamos la desigualdad ultramétrican a los puntos* z, y, a:

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

Todo punto es centro: B(a, r) = B(y, r)

Sustituyendo las condiciones (2.2) y (2.3) en la desigualdad ultra-métrica, tenemos:

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

Esto prueba que $z \in B(a,r)$. *Así,* $B(y,r) \subseteq B(a,r)$.
se concluye que:

$$\mathbf{B(a,r) = B(y,r)}$$

□

Todo punto es centro: B(a, r) = B(y, r)

Dentro de una bola abierta, todos los puntos son igual de p-cercanos entre sí como lo son al centro original, porque la proximidad está dictada por las primeras cifras idénticas de sus expansiones p-ádicas. Si dos puntos comparten las cifras que definen el radio de la bola, cualquiera de ellos puede ser el centro de ese conjunto de cifras.

Cifras de un entero p-ádico $x \in \mathbb{Z}_p$

$$x = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots = \sum_{i=0}^{\infty} a_i p^i$$

Para $\mathbb{Z}_3 : x = a_0 3^0 + a_1 3^1 + a_2 3^2 + a_3 3^3 + \ldots$

Analogías

Con la norma $p-$ádica podemos definir en forma análoga, los conceptos como: sucesión de Cauchy, límite de una sucesión, etc.

Ejemplo: Encontrando $\sqrt{2}$ con la Métrica p-ádica

Problema

La ecuación $x^2 = 2$ no tiene solución en $\mathbb{Q}$.

- Buscando en $\mathbb{Q}_7$: Queremos una solución p-ádica (en $p = 7$) que satisfaga $x^2 \equiv 2 \pmod{7^n}$ para toda n.
- $n = 1$: $x^2 \equiv 2 \pmod{7}$ tiene la solución $x_1 = 3$.

Ejemplo: Encontrando $\sqrt{2}$ con la Métrica p-ádica

Teorema (Lema de Hensel)

Sea $P(X)$ un polinomio con coeficientes en los enteros p-ádicos ($\mathbb{Z}_p[X]$).Supongamos que existe una solución aproximada $x_1 \in \mathbb{Z}_p$ tal que:

$$P(x_1) \equiv 0 \pmod{p}$$

La solución inicial es una "buena semilla" si la derivada evaluada en x_1 no es divisible por p:

$$\mathbf{v_p(P'(x_1)) = 0}$$

- Si la solución inicial no es degenerada ($f'(3) = 6 \not\equiv 0 \pmod{7}$), la Métrica $\boldsymbol{p}$-ádica garantiza que la solución existe y es única.

Ejemplo: Encontrando $\sqrt{2}$ con la Métrica p-ádica

- Polinomio: $P(x) = x^2 - 2 \implies P'(x) = 2x$
- Solución Mód 7: $x^2 \equiv 2 \pmod 7$. La solución es $x_1 = 3$.
- Verificación de No Singularidad: Evaluamos la derivada en $x_1 = 3$:

$$P'(3) = 2(3) = 6$$

Como $6 \not\equiv 0 \pmod 7$, se cumple la condición $v_7(P'(3)) = 0$.

Ejemplo: Encontrando $\sqrt{2}$ con la Métrica p-ádica

- Construcción de la Sucesión $\{x_n\}$: Usamos la fórmula $x_{n+1} = x_n + 7^n k$ para encontrar las cifras sucesivas de la raíz
- Buscamos $x_2 = x_1 + 7k$, donde $x_1 = 3$.

$$(3+7k)^2 \equiv 2 \pmod{49}$$

$$9 + 42k + 49k^2 \equiv 2 \pmod{49}$$

$$9 + 42k \equiv 2 \pmod{49} \implies 42k \equiv -7 \pmod{49}$$

$$6k \equiv -1 \pmod{7} \implies -k \equiv -1 \pmod{7} \implies k = 1$$

$$x_2 = 3 + 7(1) = \mathbf{10}$$

(Cifras 7-ádicas: $\mathbf{3}, \mathbf{1}$)

Ejemplo: Encontrando $\sqrt{2}$ con la Métrica p-ádica

Table: Construcción de $\sqrt{2}$ en $\mathbb{Z}_7$ (Lema de Hensel)

Etapa (n)	**Congruencia a Resolver**	**Solución x_n**
1	$x^2 \equiv 2 \pmod{7^1}$	$x_1 = 3$
2	$x^2 \equiv 2 \pmod{7^2}$	$x_2 = 10$
3	$x^2 \equiv 2 \pmod{7^3}$	$x_3 = 108$
4	$x^2 \equiv 2 \pmod{7^4}$	$x_4 = 2167$
$\dots$	$\dots$	$\dots$
$n \to \infty$	$P(\alpha) = 0$	$\alpha = \sqrt{2}$

- La sucesión $\{3, 10, 108, \dots\}$ es una sucesión de Cauchy en d_7 y converge al número p-ádico $\sqrt{2}$

Sucesiones

Recordatorio

Si $\{a_n\}$ es una sucesión de Cauchy de números reales, entonces $\lim_{n\to\infty} |a_n - a_{n+1}| = 0$ pero el recíproco es falso. Ejemplo: $\{a_n\} = \{\frac{1}{n}\}$

Lema

Sea $\{a_n\}$ una sucesión en $\mathbb{Q}$ con el valor absoluto $p-$ádico. Entonces,

$$\{a_n\}$$

es de Cauchy si y solo si

$$\lim_{n\to\infty} |a_n - a_{n+1}|_p = 0$$

Demostración del lema:
($\leftarrow$) **Sólo necesitamos probar que** $\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0$ **entonces** $\{a_n\}$ **es de Cauchy.**
Para esto, notemos que como este límite es 0, entonces para todo $\varepsilon > 0$ existe un N tal que si $n \geq N$, entonces $|a_{n+1} - a_n|_p < \varepsilon$.
Podemos estimar la distancia entre dos términos cualesquiera a_m y a_n de la sucesión.
Escribamos $m = n + r$ y observemos que

$$\begin{aligned} |a_m - a_n|_p &= |a_{n+r} - a_{n+r-1} + a_{n+r-1} - a_{n+r-2} + \cdots + a_{n+1} - a_n|_p \\ &\leq \max\{|a_{n+r} - a_{n+r-1}|_p, |a_{n+r-1} - a_{n+r-2}|_p, \ldots, |a_{n+1} - a_n|_p\} \\ &< \varepsilon. \end{aligned}$$

$\square$

Nota

En el campo $\mathbb{Q}$ con el valor absoluto $p-$ádico le sucede algo similar a lo que sucede a $\mathbb{Q}$ con el valor absoluto usual: hay sucesiones de Cauchy en $\mathbb{Q}$ que no convergen en $\mathbb{Q}$.

Ejemplo

- La sucesión de soluciones es $\{x_n\} = \{3, 10, 108, \dots\}$.
- Por la forma en que se construye (y por el Lema de Hensel), la distancia entre términos sucesivos $|x_{n+1} - x_n|_7$ es $\leq 7^{-n}$.
- Esto prueba que $\{x_n\}$ es una sucesión de Cauchy.
- El límite de esta sucesión converge en $\mathbb{Q}_7$ a la raíz exacta ξ, la cual es $\sqrt{2}$.

La Raíz $\sqrt{2}$ en $\mathbb{Z}_7$ tiene la expansión:

$$\sqrt{2} = \dots 213_7$$

Nota

De forma análoga a como, usando el valor absoluto usual, en $\mathbb{Q}$ para obtener el campo $\mathbb{R}$ de los números reales, usando ahora el valor absoluto $p-$ádico $||_p$ se puede completar el campo $\mathbb{Q}$, para obtener un campo nuevo llamando el campo de los números $p-$ádicos $\mathbb{Q}_p$

$$\text{Completitud de } (\mathbb{Q}, |\cdot|) \to \mathbb{R}$$

$$\text{Completitud de } (\mathbb{Q}, |\cdot|_p) \to \mathbb{Q}$$

Anillo de enteros 3-ádicos

$\mathbb{Z}_3$ es el anillo de convergencia de todas las sucesiones de Cauchy en el espacio $p-$ádico
$\mathbb{Z}_3 = \{x \in \mathbb{Q}_3 : |x|_3 \leq 1\}$

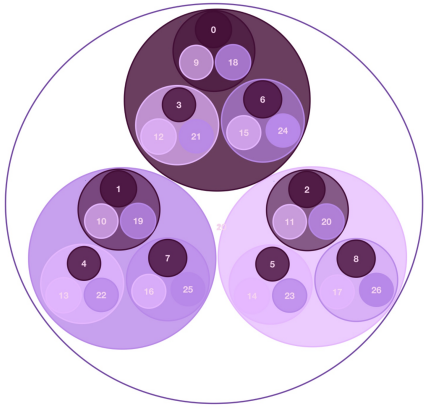


Figure: **Estructura jerárquica de $\mathbb{Z}_3$:** Los enteros p-ádicos se descomponen en p bolas disjuntas de radio p^{-n}.

Conclusiones

- Los números p-ádicos aclaran que concepto de distancia depende totalmente del métrica.
- Que la métrica $p-$ádica no sea arquimediana implica resultados como que todo triángulo es isósceles, que para todo punto contenido en una bola abierta es el centro de la bola.
- Este sistema de números además de ser muy llamativos, son aplicables en teoría de números moderna, física teórica, computación y criptografía.

Bibliografía


Zaldívar, F. (2003). *Fundamentos de álgebra.* Fondo de Cultura Económica.


Gouvêa, F. Q. (2003) *p-adic numbers: An introduction (2nd ed.)*. Springer.