UNIVERSIDAD SAN FRANCISCO DE QUITO

Colegio de Ciencias e Ingenierías

Construcción y propiedades de los números p-ádicos

Pablo Joaquín Serrano Santos

John Skukalek, Ph.D., Director de Tesis

Tesis de grado presentada como requisito para la obtención del título de Licenciado en Matemáticas

Quito, mayo de 2015

UNIVERSIDAD SAN FRANCISCO DE QUITO

ACTA DE PRESENTACION FINAL DEL TRABAJO DE TESIS

REQUISITO PARA OBTENER EL TITULO DE

LICENCIADO EN MATEMÁTICAS

El día de hoy, 11 de mayo de 2015, comparece el Señor Pablo Joaquín Serrano Santos con el No. de Estudiante 00024830, ante el panel de Profesores del Departamento de Matemáticas, para presentar su Trabajo de Tesis, requisito previo para la obtención del título de Licenciado en la especialidad Matemáticas, en la Universidad San Francisco de Quito.

Una vez finalizada la presentación, absueltas satisfactoriamente las preguntas planteadas por el panel de profesores, y realizada la reunión final entre los profesores del panel, la nota que se otorga al trabajo es de A en la Preparación de la Tesis; de A en la Presentación y Defensa de la Tesis. Por lo tanto la nota final es de A.

Por lo tanto se recomienda que si se le otorgue el Título de Licenciado en Matemáticas.

Quito, 11 de mayo de 2015

Director de la Tesis

John Skukalek

Panel de Profesores

David Hervas

Andrea Moreira

Eduardo Alba

Cesar Zambrano
Decano de la Escuela de Ciencias

Firma: Pablo Serrano

Nombre: Pablo Serrano

C. I.: 0926691288

Fecha: 11 de mayo de 2015

Dedicado a Lucero, que me molestó por casi dos años para que termine la tesis.

Resumen

Los número p-ádicos son un sistema de numeración basado en una métrica distinta a la usual (euclidiana). El estudio de los números p-ádicos está motivado por la teoría de números, en particular la aritmética modular. Se explora la representación p-ádica de los elementos de los conjuntos $\mathbb{N}$, $\mathbb{Z}$ y $\mathbb{Q}$ (los números naturales, los enteros y los racionales respectivamente) dentro de la métrica p-ádica (de la cual también mostramos la definición y propiedades), y finalmente cómo llegar a la completación de los racionales mediante esta métrica, el cuerpo $\mathbb{Q}_p$ de los números p-ádicos y el subanillo $\mathbb{Z}_p$ de los enteros p-ádicos.

Abstract

The p-adic numbers are a numeric system based on a metric that is different from the usual metric (euclidean). The study of p-adic numbers is motivated by number theory, in particular modular arithmetic. We explore the p-adic expansion of elements from the sets $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ (the natural, integer and rational numbers respectively) using the p-adic metric, and finally we reach the completion of the rationals using this metric, the field $\mathbb{Q}_p$ of p-adic numbers and its subring $\mathbb{Z}_p$ of p-adic integers.

Tabla de contenidos:

Introducción

Partiendo de la teoría de números, se busca explorar y entender a los números p-ádicos como extensiones de los números racionales que responden a una pregunta simple: ¿se puede generalizar la solución a una ecuación modular módulo p^n para cualquier n? A pesar de que existen maneras puramente algebráicas de definir a los números p-ádicos, aquí la idea es volver (siempre que sea posible) a la teoría de números. Usamos álgebra y nuestro conocimiento previo de la construcción de los números reales para mostrar las similitudes entre estos y los números p-ádicos, así como hacer observaciones sobre las diferencias.

Objetivos:

Objetivos generales:

Explicar qué son los números p-ádicos y demostrar que son un cuerpo algebráico.

Objetivos específicos:

Describir las propiedades básicas de los números p-ádicos con una aproximación basada en teoría de números.

Sección 1: Definiciones generales y notación.

Notación posicional: Una notación numérica en que la posición de los dígitos afecta su valor. La numeración en base 10 que usamos cotidianamente es un ejemplo de esto. De derecha a izquierda las posiciones significan potencias de 10. También existen otras bases, como base 2 (que se denota con un subíndice), así $101_2 = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 = 5$. Como veremos más adelante, la representación p-ádica de un número también es posicional.

Periodicidad: Un número real periódico tiene una representación posicional infinita que se que se repite. Por ejemplo, $\frac{1}{7} = 0,142857142857\ldots$ donde los dígitos 142857 (que forman el periodo) se repiten indefinidamente. Para expresar la periodicidad usamos una barra superior, por ejempo $\frac{1}{7} = 0,\overline{142857}$. En los números p-ádicos también hay números periódicos, y usaremos la misma notación. Siempre usaremos la barra sobre el número periódico $\overline{0}$ para diferenciarlo del dígito 0. De esta manera, podemos representar una fracción como una suma infinita. En el ejemplo de $\frac{1}{7}$ que estamos usando, una sumatoria posible es $\frac{1}{7} = \sum_{i=1}^{\infty} 142857 \cdot 10^{-6i}$. La igualdad tiene sentido porque la sumatoria converge en los números reales: para todo $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que para todo $n > n_0$ se cumple $\left| \frac{1}{7} - \sum_{i=1}^{n} 142857 \cdot 10^{-6n} \right| < \varepsilon$.

Congruencias modulares: Una congruencia módulo p, con $p \in \mathbb{Z}$ es una relación de equivalencia. Para $a, b \in \mathbb{Z}$ se define $a \equiv b$ (mód p) si p divide a $a - b$ (lo que se denota por una raya vertical: $p|(a-b)$). Para un entero a, se puede definir su clase de equivalencia $[a]_p = \{n,\ a \equiv n \text{ (mód } p)\}$. Esta clase de equivalencia tiene un único representante $b \in [a]$ tal que $0 \leq b \leq p-1$.

Las congruencias módulo p primo tienen algunas propiedades que no necesariamente se cumplen si p es compuesto:

i) Todo entero tiene inverso multiplicativo. Es decir, para todo $a \in \mathbb{Z}$, existe $b \in \mathbb{Z}$ tal que $a \cdot b \equiv 1$ (mód p).

ii) Si $a \not\equiv 0 \pmod{p}$ y $b \not\equiv 0 \pmod{p}$, entonces $ab \not\equiv 0 \pmod{p}$.

Número p-ádico: Los números p-ádicos son una extensión de los números racionales mediante una métrica $\|\cdot\|_p$ distinta a la usual, en la que las potencias altas de p tienen una medida pequeña. La p es la base que se va a usar para la métrica. Por ejemplo, números 3-ádicos, 7-ádicos, etc. A diferencia de los números reales, donde la base en la que uno escribe es solo una elección de notación, los números p-ádicos son distintos para cada p. Es decir, estamos trabajando con una familia de extensiones de los racionales para cada valor de p. Generalmente se escoge una p prima, aunque es posible usar bases compuestas a cambio de perder algunas propiedades algebráicas.

Espacio métrico: Un espacio métrico es un par ordenado (X, d) que contiene un conjunto y una función de distancia sobre ese conjunto. Ejemplos de esto son el plano cartesiano $\mathbb{R}^2$ con la medida euclidiana o $\mathbb{R}$ con la distancia absoluta $d(x, y) = |x - y|$.

Norma (de un espacio lineal V): Es una función $\|\cdot\| : V \to \mathbb{R}$ que cumple con 3 propiedades para todo $a \in \mathbb{R}$ y $v, w \in V$

1) $\|av\| = |a| \, \|v\|$.

2) $\|v + w\| \leq \|v\| + \|w\|$.

3) $\|v\| \geq 0$ con igualdad si y solo si v es el elemento neutro de V.

Función de distancia o métrica (de un conjunto V): Es una función $d : V \times V \to \mathbb{R}$ que cumple al menos 3 propiedades para todo $x, y, z \in V$.

1) Simetría: $d(x, y) = d(y, x)$.

2) No negatividad:$d(x, y) \geq 0$, y $d(x, y) = 0$ si y solo si $x = y$.

3) Desigualdad triangular: $d(x, z) + d(z, y) \geq d(x, y)$

Sucesión convergente: Dado un espacio métrico $(A, d())$ y una sucesión a_n con $a_i \in A, \forall i \in \mathbb{N}$, se dice que a_n converge a a si para todo real $\varepsilon > 0$ existe $N \in \mathbb{N}$ tal que $d(a_k, a) < \varepsilon$ para todo $k > N$. Es importante notar que la convergencia depende de la función de distancia escogida, de modo que una sucesión puede converger con una métrica y no con otra. Un ejemplo de una sucesión convergente es la progresión geométrica $(1, \frac{1}{2}, \frac{1}{4}, \ldots)$, que converge a 0 con la métrica usual en $\mathbb{R}$.

Anillo: Es una estructura algebráica $(A, +, \cdot)$ donde A es un conjunto con dos operaciones, una de suma $(+)$ y una de multiplicación $(\cdot)$, tales que $(A, +)$ es un grupo abeliano y la multiplicación tiene las propiedades de asociatividad y distributividad con respecto a la suma. Un ejemplo de un anillo es el conjunto de los enteros con la suma y multiplicación usuales.

Cuerpo: Es un anillo no trivial que además contiene la inversa multiplicativa de todos sus elementos no nulos. Un ejemplo de un cuerpo algebráico es el conjunto de los números complejos con las operaciones de suma y multiplicación.

Sección 2: Definición, motivación y construcción de los números p-ádicos.

Antes de definir formalmente lo que es un número p-ádico, vamos a explicar cuál fue el motivo de su creación y sus utilidades. Consideremos las ecuaciones modulares de la forma $bx \equiv a$ (mód p) con p primo y a, b coprimos con p (estas condiciones garantizan que el sistema tenga solución, y nos ayudarán luego de definir una métrica). Por ejemplo, digamos que queremos resolver $2x \equiv 1$ (mód 3). Usando nuestra definición de $a \equiv b$ (mód p) $\Leftrightarrow p \mid (a-b)$, podemos hallar infinitas soluciones -1, 2, 5, 8,... todas de la forma $3k+2$ con $k \in \mathbb{Z}$. La razón de esto es que $2(3k+2)-1 = 6k+3$, lo cual es múltiplo de 3 para k entero. Sin embargo, algunas de estas también satisfacen $2x \equiv 1$ (mód 9) (5, 14, 23) que son de la forma $9k + 3 \cdot 1 + 2$ (es fácil de comprobar que $2(9k+5)-1$ es múltiplo de 9). Podemos continuar resolviendo la ecuación $2x \equiv 1$ (mód 3^n) para valores crecientes de n, y encontrando el patrón que siguen las soluciones. La pregunta que viene a la mente es ¿existe, de alguna manera, una solución límite válida cuando $n \to \infty$? De manera más general, se busca una expresión que satisfaga $ax \equiv b$ (mód p^n) para $n = 1, 2, 3, \ldots$ y p primo, que esté bien definida en algún sentido.

Vamos a encontrar las soluciones parciales de algunos tipos de ecuaciones modulares separando casos, en orden creciente de dificultad, y con ellas formamos sucesiones. El objetivo es encontrar el límite de la sucesión cuando n tiende a infinito. Para escoger los términos de la sucesión, vamos a escoger la solución positiva más pequeña a cada ecuación modular.

Caso 1: Si $0 \leq a < p-1$ tenemos que la solución de la ecuación $x \equiv a$ (mód p^n) es a para todo n, lo que resulta en la secuencia constante $(a, a, a, \ldots)$. El límite entonces es a, por lo que podemos concluir que evidentemente $x = a$.

Caso 2: Pasamos a ecuaciones del tipo $x \equiv a$ (mód p^n) con $a \geq 0$. Sabemos que existe

n suficientemente grande tal que $p^n > a$, de modo que la menor solución positiva de la ecuación $x \equiv a \pmod{p^n}$ es a. Lo mismo ocurre para potencias mayores de p. En este caso, la secuencia se vería así: $(x_1, \ldots x_{n-1}, a, a, \ldots)$, donde todos los términos a partir del enésimo son a. El límite en este caso es nuevamente a.

Caso 3: $x \equiv -1 \pmod{p^n}$. Las soluciones parciales son $p-1$, p^2-1, etc. Aquí nos topamos con el primer problema: la secuencia no es eventualmente constante y los valores van creciendo ilimitadamente. La sucesión $(p-1, p^2-1, \ldots)$ no tiene un límite en los números reales.

Caso 4: $x \equiv -a \pmod{p^n}$ con $a > 0$. De manera similar al caso 2, sabemos que existe n tal que $p^n - a > 0$, de modo que la sucesión tendrá una forma $(x_1, \ldots x_{n-1}, p^n - a, p(p^n - a), \ldots)$. Como este caso es una generalización del anterior, no es sorprendente que tampoco converja en los reales.

Caso 5: $bx \equiv a \pmod{p^n}$ donde $p \mid a$ y $p \nmid b$. Sabemos entonces que $a \equiv 0 \pmod{p}$ pero $b \not\equiv 0 \pmod{p}$. Como las equivalencias modulares no tienen divisores de cero cuando el módulo es primo, podemos ver que el primer término de la secuencia es 0, lo que daría $(0, x_2, x_3, \ldots)$.

Caso 6: $bx \equiv a \pmod{p^n}$ donde $p^n \mid a$ y $p \nmid b$. Muy similar al anterior, ahora tenemos que las primeras n soluciones son 0, y la secuencia se vería así $(0, \ldots 0, x_{n+1}, x_{n+2}, \ldots)$.

Caso 7: $bx \equiv a \pmod{p^n}$ donde $p \nmid a$ y $p \mid b$. Este sistema no tiene solución en los enteros, ya que al ser $b \equiv 0 \pmod{p}$, se tiene también $bx \equiv 0 \pmod{p}$ y por lo tanto se debería tener que $a \equiv 0 \pmod{p}$, lo que contradice que p no divide a a. Este caso lo dejaremos pendiente.

La idea de las sucesiones funciona bien para los casos más simples, pero no para la mayoría. Una alternativa es trabajar con una segunda sucesión, cuyas sumas parciales sean iguales a los términos correspondientes de la primera. Lo que buscamos es poder expresar las soluciones parciales como una sumatoria, de manera que en cada paso se añade un

término y se mantiene todos los anteriores. Esto es muy simple: dada una sucesión $S_1 = (a_1, a_2, a_3, \ldots)$ podemos formar la sucesión de diferencias $S_2 = (a_1, a_2 - a_1, a_3 - a_2, \ldots)$. La idea es que la suma de los primeros n términos de S_2 es igual al n-ésimo término de S_1. De esta manera, las sucesiones para cada caso respectivamente son:

1) $(a, 0, 0, 0, \ldots)$

2) $(s_1, \ldots, s_{n-1}, a, 0, 0, \ldots)$

3) $(p-1, p^2 - p, p^3 - p^2, \ldots)$

4) $(s_1, \ldots, s_{n-1}, p^n - a, p^{n+1} - ap, \ldots)$

5) $(0, s_2, s_3, \ldots)$

6) $(0, \ldots, 0, s_{n+1}, \ldots)$

7) Pendiente.

A pesar de que no hemos podido expresar todas las sucesiones en términos de a y p, al menos tenemos algunos patrones para la mayoría. Por el momento, vamos a hacer la siguiente afirmación:

Se puede expresar la solución del sistema infinito $bx \equiv a \pmod{p^n}$, $n = 1, 2, 3, \ldots$ mediante una sumatoria infinita $\sum_{i=k}^{\infty} d_i p^i$ con $k, d_i \in \mathbb{Z}$ y $0 \leq d_i \leq p-1$ para todo i. La idea con estas sumatorias, que serán definidas de manera más rigurosa adelante, es hacer un paralelismo con los números reales, que pueden ser expresados mediante una sumatoria infinita y una base entera mayor a 1. Pero para que hablar del límite de todas esas sucesiones (y no solo de algunas) tenga sentido, necesitamos primero establecer una métrica en la que estas sean convergentes.

Sección 3: Métrica.

Para poder dar un sentido estricto a las sucesiones de la sección anterior, necesitamos definir una métrica, que llamaremos la métrica p-ádica. Antes de eso, vamos a introducir algunos conceptos previos.

Valuación p-ádica:

Definición La valuación p-ádica de un número racional está dada por:

$$\begin{cases} v_p(n) = \max\{k \in \mathbb{N} \cup \{0\} : p^k | n\} & \text{si } n \in \mathbb{Z} \setminus \{0\} \\ v_p(q) = v_p(a) - v_p(b) & \text{si } q = \frac{a}{b} \in \mathbb{Q} \\ v_p(0) = \infty & \text{por convención} \end{cases}$$

La valuación p-ádica nos será útil para definir un norma p-ádica, que a su vez es la base de la distancia d_p de los números p-ádicos. Para esto, vamos a demostrar algunas propiedades.

lema 1 *Si $a, b \in \mathbb{N}$ y p es primo, tenemos $v_p(ab) = v_p(a) + v_p(b)$.*

Podemos escribir a a y b de manera única de la forma $a = p^k \cdot n$ y $b = p^l \cdot m$, donde m y n son coprimos con p. Al multiplicarlos obtenemos $a \cdot b = p^{k+l} \cdot mn$, cuya valuación p-ádica es $k + l = v_p(a) + v_p(b)$. Nótese que esto no es necesariamente cierto si p no es primo. Por ejemplo $v_6(12) = 1$ y $v_6(18) = 1$ pero $v_6(12 \cdot 18) = 3$. ∎

lema 2 *Si p es primo, la valuación p-ádica está bien definida para los racionales incluso si tomamos en cuenta las distintas maneras de representar la misma fracción.*

Si tenemos $\frac{a_1}{b_1} = \frac{a_2}{b_2}$, usando el hecho de que para enteros $v_p(ab) = v_p(a) + v_p(b)$ se tiene:

$$\begin{aligned} \frac{a_1}{b_1} &= \frac{a_2}{b_2} \\ \Rightarrow a_1 b_2 &= a_2 b_1 \\ \Rightarrow v_p(a_1) + v_p(b_2) &= v_p(a_2) + v_p(b_1) \\ \Rightarrow v_p(a_1) - v_p(b_1) &= v_p(a_2) - v_p(b_2) \end{aligned}$$

Como queríamos demostrar. ∎

lema 3 *Podemos extender la propiedad del lema 1 a todos los racionales, de modo que* $\forall x, y \in \mathbb{Q}, \quad v_p(xy) = v_p(x) + v_p(y)$

Sean $x = \frac{a}{b}$, $y = \frac{c}{d}$. Entonces

$$\begin{aligned} v_p(x) + v_p(y) &= v_p(a) - v_p(b) + v_p(c) - v_p(d) \\ &= v_p(a) + v_p(c) - [v_p(b) + v_p(d)] \\ &= v_p(ac) - v_p(bd) \\ &= v_p(\frac{ac}{bd}) \\ &= v_p(xy) \end{aligned}$$

lo que termina la demostración ∎

lema 4 *Sean x y y racionales. Entonces $v_p(x+y) \geq \inf\{v_p(x), v_p(y)\}$ (y la igualdad solo es posible si $v_p(x) \neq v_p(y)$)*

Sean $x = p^k \frac{a}{b}$, $y = p^n \frac{c}{d}$, donde a, b,c y d son coprimos con p. Sin pérdida de generalidad, sea $k \geq n$.

Entonces:

$$\begin{aligned} x+y &= p^n\left(p^{k-n}\frac{a}{b}+\frac{c}{d}\right) \\ &= p^n\left(\frac{adp^{k-n}+cb}{bd}\right) \end{aligned}$$

Si $k > n$ entonces se tiene que p divide a adp^{k-n} y por lo tanto no divide a $adp^{k-n}+cb$. De ahí que $v_p(x+y) = n = \inf\{v_p(x), v_p(y)\}$. Si $k = n$, es posible que $v_p > \inf\{v_p(x), v_p(y)\}$ si p divide a $ad + cb$. ∎

Norma p-ádica:

Para un número primo positivo p definimos la norma p-ádica $\|\cdot\|_p : \mathbb{Q} \to \mathbb{R}$ de la siguiente manera:

Definición

$$|q|_p = \begin{cases} p^{-v_p(q)} & \text{si } q \neq 0 \\ 0 & \text{si } q = 0 \end{cases}$$

Como consecuencia inmediata de la definición, podemos ver que $|x|_p \geq 0$ con igualdad ssi $x = 0$.

Proposición 5 $\forall\, x, y \in \mathbb{Q}$ *se tiene que* $|x|_p \cdot |y|_p = |x \cdot y|_p$

Usando la definición tenemos

$$\begin{aligned} |x|_p \cdot |y|_p &= p^{-v_p(x)} \cdot p^{-v_p(y)} \\ &= p^{-v_p(x)-v_p(y)} \\ &= p^{-v_p(xy)} \\ &= |x \cdot y|_p \quad ∎ \end{aligned}$$

Proposición 6 $\forall\, x, y$ *se tiene que* $\|x+y\|_p \leq \|x\|_p + \|y\|_p$, *y más aún,* $\|x+y\|_p \leq \max\left\{|x|_p, |y|_p\right\}$

Sabiendo que $v_p(x+y) \geq \inf\{v_p(x), v_p(y)\}$ tenemos que $p^{-v_p(x+y)} \leq \sup\left\{p^{-v_p(x)}, p^{-v_p(y)}\right\}$. Como ya no tenemos valores infinitos, podemos reemplazar el supremo por el máximo sin inconvenientes. ∎

Extensión de la norma p-ádica a series infinitas:

De la **proposición 6** se tiene que $\left|\sum_{i=k}^{k+n} d_i p^i\right|_p = \max\left\{|d_i p^i|_p\right\} = p^{-k}$ para cualquier $n \in \mathbb{N}$. Con esto podemos definir la norma para una sumatoria infinita por continuidad, de manera que la norma del límite sea el límite de la norma:

$$\begin{aligned}\left|\lim_{n\to\infty}\sum_{i=k}^{k+n} d_i p^i\right|_p &= \lim_{n\to\infty}\left|\sum_{i=k}^{k+n} d_i p^i\right|_p \\ &= \lim_{n\to\infty} p^{-k} \\ &= p^{-k}\end{aligned}$$

De aquí que la norma p-ádica de cualquier sucesión finita o infinita está dada por el exponente más pequeño en la descomposición en base p.

Distancia d_p en los números p-ádicos:

Con la norma p-ádica, definimos la métrica p-ádica mediante la fórmula de distancia $d_p(x,y) = |x-y|_p$. La norma p-ádica nos será útil al momento de definir de manera rigurosa la expansión p-ádica de un número.

La distancia p-ádica cumple las propiedades necesarias. Para todo x, y, $z \in \mathbb{Q}$:

$|x-y|_p \geq 0$ con igualdad si y solo si $x = y$.

$|x-y|_p = |y-x|_p$.

$|x-z|_p \leq |x-z|_p + |z-y|_p$.

Sección 4: Convergencia y sucesiones de Cauchy.

Definimos una sucesión (x_n) como Cauchy si cumple que para todo $\varepsilon > 0$ existe $N \in \mathbb{N}$ tal que para todo $m, n \geq N$ se tiene $d(x_n, x_m) < \varepsilon$. Esta definición depende de la función de distancia, de modo que una sucesión puede ser Cauchy bajo una métrica pero no bajo otra. Nosotros nos enfocaremos en las sucesiones de Cauchy bajo la norma p-ádica. El objetivo es volver a las sucesiones que introdujimos en la segunda parte y definirlas de una manera rigurosa mediante sucesiones de Cauchy usando la norma p-ádica.

En esta sección nos vamos a referir siempre a x_n como la sucesión de soluciones del sistema $bx \equiv a \pmod{p^n}$ a menos que se diga lo contrario.

Consideramos primero el caso $bx \equiv a \pmod{p^n}$ con a y b coprimos con p. Sean $x_1, x_2, \ldots$ las soluciones del sistema $bx_n \equiv a \pmod{p^n}$ con $0 \leq x_n \leq p^n - 1$. Primero queremos saber si esta es una sucesión de Cauchy con la métrica p-ádica. Recordemos que la proposición $bx_n \equiv a \pmod{p^n}$ es equivalente a $bx_n - a = p^n \cdot l$ para algún l entero coprimo con p. Escojamos $N > \log_p \varepsilon^{-1}$. Luego, para todo $m, n \geq N$ (sin pérdida de generalidad, asumimos $m \geq n$) tenemos que

$$\begin{aligned} |x_n - x_m|_p &= |p^n \cdot a - p^m \cdot b|_p \\ &\leq p^{-n} \\ &\leq p^{-N} \\ &< \varepsilon \end{aligned}$$

Entonces, las soluciones del sistema $bx \equiv a \pmod{p^n}$, $n = 1, 2, \ldots$ forman una sucesión de Cauchy bajo la norma p-ádica. La pregunta que surge ahora es ¿cuál es el límite de una de estas sucesiones?

Vamos a demostrar que el límite de la sucesión generada por $bx \equiv a \pmod{p^n}$ es justamente $\dfrac{a}{b}$.

Queremos demostrar que $\lim_{n\to\infty} \left|x_n - \frac{a}{b}\right|_p = 0$. De manera similar a la demostración anterior, nos valemos de que $bx_n - a = p^n \cdot l$ con l entero. Así,

$$\begin{aligned} \left|x_n - \frac{a}{b}\right|_p &= \left|\frac{bx_n - a}{b}\right|_p \\ &= \left|p^n \frac{l}{b}\right|_p \\ &= p^{-n} \to 0 \end{aligned}$$

Lo que hemos logrado es hallar una sucesión que converge a un número racional cualquiera con la norma p-ádica. Finalmente tiene sentido escribir algo como $\lim_{n\to\infty} x_n = \frac{a}{b}$. Los términos parciales x_1, x_2, etc. que encontramos son los términos de la expansión p-ádica de un número, del mismo modo que un número real se puede escribir mediante una expansión decimal finita o infinita.

Propiedades de la sucesión x_n:

Proposición 7 *Para todo $n \in \mathbb{N}$ se cumple que p^{n-1} divide a $x_n - x_{n-1}$*

Por definición de x_n y x_{n-1} tenemos que $x_n - a = l_n \cdot p^n$ y $x_{n-1} - a = l_{n-1} \cdot p^n$ donde l_i es un entero coprimo con p para todo i. Luego $x_n - x_{n-1} = p^{n-1}(pl_n - l_{n-1})$, que es múltiplo de p^{n-1} pero no de p^n. ∎.

Proposición 8 *Para todo $n > 0$ enteros, se tiene $0 \leq \frac{x_n - x_{n-1}}{p^{n-1}} < p$*

En el punto anterior demostramos que $\frac{x_n - x_{n-1}}{p^{n-1}}$ es un entero. Necesariamente $x_n < p^n$, o de lo contrario $x_n - p^n$ sería una solución positiva menor a $bx_n \equiv a$ (mód p^n). De ahí que $\frac{x_n - x_{n-1}}{p^{n-1}} < \frac{p^n}{p^{n-1}} = p$. ∎

Esto nos permite crear la expansión p-ádica de un número. Por la proposición 1 podemos expresar los términos de la sucesión x_n mediante una sumatoria $\sum_{k=1}^{n} s_k$ donde $s_1 = x_1$ y $s_k = x_k - x_{k-1}$ para $k > 1$. La proposición 2 implica que podemos escribir esta sumatoria de la forma $\sum_{k=0}^{n} d_k p^k$ donde $d_i \in \mathbb{N}$ y $0 \leq d_i < p$ para todo i entre 1 y n, simplemente definiendo $d_i = s_i p^{-i}$. En la sección anterior mostramos que esa sumatoria converge bajo la métrica p-ádica. En resumen, del sistema de ecuaciones $bx \equiv a$ (mód p^n) obtenemos una sucesión de soluciones parciales x_n, de la cual derivamos una sucesión de diferencias s_n que cumple $\sum_{i=1}^{n} s_i = x_n$. Demostramos que podemos escribir $s_n = d_n \cdot p^{n-1}$ con $0 \leq d_i < p$ para todo i, de modo que podemos escribir las soluciones parciales $x_n = \sum_{i=1}^{n} d_i p^{i-1}$, y esta sumatoria converge bajo la métrica p-ádica, asi que podemos definir rigurosamente $x = \sum_{i=1}^{\infty} d_i p^{i-1}$, denominada la expansión p-ádica de x.

Sección 5: Representación p-ádica de un número.

En la sección anterior mostramos cómo los números racionales tienen una representación p-ádica por medio de series infinitas, de manera similar a cómo existen las representaciones decimales finitas. Vamos a ver cómo se representan varios subconjuntos de números racionales mediante expansiones p-ádicas.

El conjunto de los naturales ($\mathbb{N}$):

Como vimos en la sección 2, un número natural b es su propia solución al sistema $bx \equiv a \pmod{p^n}$ a partir de cierto valor de n, lo que nos da una representación p-ádica que eventualmente tiene una sucesión infinita de ceros. Por ejemplo

$$\begin{aligned} 17 &\equiv 2 \pmod 3 \\ 17 &\equiv 8 \pmod 9 \\ 17 &\equiv 17 \pmod{27} \end{aligned}$$

Lo que nos da una sucesión de soluciones $x_n = (2, 8, 17, 17, \ldots)$, una sucesión de diferencias $s_n = (2, 6, 9, 0, \ldots)$ y una sucesión de dígitos $d_n = (2, 2, 1, 0, \ldots)$

Es decir, la representación p-ádica de un número natural es la misma que su representación en base p.

El conjunto de los enteros ($\mathbb{Z}$):

En el caso de los números negativos, planteamos el sistema de ecuaciones

$$x_n \equiv -a \pmod{p^n}$$

con $a > 0$. Las x_n deben cumplir $|x_n + a|_p \equiv 0 \pmod{p^n}$. Para n suficientemente grande,

$p^n > a$ y las soluciones parciales son $x_n = p^n - a$. De este modo, al tomar las diferencias $x_{n+1} - x_n$ para la representación p-ádica , eventualmente todos los dígitos van a ser $p-1$. Es decir, los números enteros tienen todos representaciones eventualmente periódicas, en donde el dígito repetido es 0 si el número es positivo o $p-1$ si el número es negativo.

Por ejemplo, para hallar la representación 3-ádica de -17 tenemos

$$\begin{aligned} -17 &\equiv 1 \textbf{ (mód 3)} \\ &\equiv 1 \textbf{ (mód 9)} \\ &\equiv 10 \textbf{ (mód 27)} \\ &\vdots \end{aligned}$$

Con estos números formamos la sucesión $x_n = \{1, 1, 10, 64, 226, \ldots\}$. La sucesión s_n de las diferencias queda

$$\begin{aligned} s_n &= \{1, 0, 9, 54, 162, \ldots\} \\ &= \{1 \cdot 3^0 + 0 \cdot 3^1 + 1 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \ldots\} \end{aligned}$$

Finalmente, la sucesión de dígitos queda $d_n = \{1, 0, 1, 2, 2, \ldots\}$. A partir del cuarto término todos los dígitos van a ser 2, puesto que $n = 3$ es el primer exponente que satisface $3^n - 17 > 0$. Entonces, la representación 3-ádica de -17 es $\overline{2}101, 0$

El conjunto de los racionales ($\mathbb{Q}$):

En la sección 2 no encontramos ningún patrón evidente para la representación p-ádica de un racional cualquiera, pero eso no quiere decir que no exista. Partamos del caso más simple, suponiendo que tenemos el sistema de ecuaciones $bx \equiv a$ (mód p^n) donde b es

coprimo con p. El número p-ádico asociado es la expresión p-ádica de $\frac{a}{b}$, digamos $\sum_{n=1}^{\infty} d_i p^i$. Si esta representación es periódica, es decir, existe un k tal que $d_{n+k} = d_n$ para todo n, entonces

Supongamos que la representación p-ádica de $\frac{a}{b}$ no es periódica. Llamemos $\sum_{n=1}^{\infty} d_i p^i$ a esta representación. Es decir, no existe un entero positivo k tal que $d_{n+k} = d_n$ para todo $n \in \mathbb{N}$. Esto implica que no existe k tal que $(p^k - 1)\frac{a}{b}$ es un entero, o lo que es lo mismo, $b \nmid p^k - 1$ para todo k. Esto es equivalente a decir que $p^k \equiv 1$ (mód b) no tiene solución, pero esto es imposible por el teorema de Euler-Fermat (Martinez 47). Por contradicción, la representación p-ádica de un racional debe ser periódica.

Ejemplo: para hallar $\frac{1}{4}$ en 3-ádicos resolvemos $4x \equiv 1$ (mód 3^n), lo que nos da la sucesión de soluciones $x_i = (1, 7, 7, 61, 61, \ldots)$, la sucesión de diferencias $s_n = (1, 6, 0, 54, 0, \ldots)$ y finalmente la sucesión de dígitos $d_n = (1, 2, 0, 2, 0, \ldots)$. Finalmente, podemos escribir la representación 3-ádica de $\frac{1}{4}$ como

$$\sum_{n=1}^{\infty} d_i \cdot 3^{i-1} \quad = \quad 1 + 2 \cdot 3 + 0 \cdot 3^2 + 2 \cdot 3^3 + 0 \cdot 3^4 \ldots$$

El período es 2. Ahora, notemos que la expansión de $3^2 \cdot \frac{1}{4}$ debe ser $\sum_{n=2}^{\infty} d_i \cdot 3^i$. Si hacemos la diferencia, el resultado es $1 + 2 \cdot 3^1 - 1 \cdot 3^2 = -2$. Efectivamente, $\frac{1}{4} - \frac{9}{4} = -2$. Este método es igual al que usamos con la expansión decimal de un racional para encontrar la forma fraccionaria.

En el caso de que b no sea coprimo con p, podemos escribir $b = p^l \cdot c$, donde p y c son enteros coprimos, resolver el sistema para $cx \equiv a$ (mód p^n) y dividir el p-ádico resultante para p^l. Por ejemplo, la expansión 3-ádica de $\frac{1}{12}$ no es más que $\frac{1}{3}\sum_{n=1}^{\infty} d_i \cdot 3^{i-1} = \sum_{n=1}^{\infty} d_i \cdot 3^{i-2}$.

¿El conjunto de los reales? ($\mathbb{R}$):

Hasta ahora hemos definido la serie p-ádica para un racional $\frac{a}{b}$ mediante las soluciones al sistema $bx \equiv a$ (mód p^n). Es lógico preguntarse si todos los reales tienen una representación p-ádica. Pues bien, la respuesta es que no, y es fácil encontrar un contraejemplo: Busquemos la expansión 3-ádica de $\sqrt{2}$. Si intentamos, análogamente a los problemas anteriores, resolver las equivalencias $x^2 \equiv 2$ (mód 3^n), nos topamos con un problema de inmediato: no existe ninguna solución para $x^2 \equiv 2$ (mód 3), pues 2 no es un residuo cuadrático módulo 3.

Antes de lanzarnos a la pregunta de si existen números no racionales con expansión p-ádica bien definida, vamos a ver una propiedad que los p-ádicos no comparten con los números reales.

Demostración Las expansión p-ádica de cualquier número es única.

En los números reales esto no es cierto. Si un racional tiene representación finita en base b, entonces también tiene una representación alternativa que es infinita en base b. Por ejemplo, $1 = 0,\overline{9}$. Vamos a demostrar por contradicción que un número no puede tener dos expansiones p-ádicas distintas.

Sean $\sum_{i=k}^{\infty} d_i p^i = \sum_{i=k}^{\infty} e_i p^i$ dos expansiones p-ádicas distintas del mismo número (esto es, $d_i \neq e_i$ para algun i, con $0 \leq e_i, d_i < p$). Claramente $\left|\sum_{i=k}^{\infty} d_i p^i - \sum_{i=k}^{\infty} e_i p^i\right|_p = 0$, de modo que debería cumplirse también que $\lim_{n\to\infty} \left|\sum_{i=k}^{n} d_i p^i - \sum_{i=k}^{n} e_i p^i\right|_p = 0$.

Empezando con $n = k$, deberíamos tener $\left\|d_k \cdot p^k - e_k \cdot p^k\right\|_p = 0$, de lo contrario $\left|\sum_{i=k}^{\infty} d_i p^i - \sum_{i=k}^{\infty} e_i p^i\right|_p = p^k$ (puesto que la norma está dada por el exponente más pequeño de p en la expansión). De ahí que $d_1 = e_1$. Por el mismo motivo, $\left|\sum_{i=k}^{k+1} d_i p^i - \sum_{i=k}^{k+1} e_i p^i\right|_p$ debe ser cero, de lo contrario el módulo de la diferencia seria p^{k-1} para todos los términos

subiguientes, lo que implica $d_2 = e_2$. Por inducción, si para todo entero l menor a n se tiene $\left|\sum_{i=k}^{l} d_i p^i - \sum_{i=k}^{l} e_i p^i\right|_p = 0$, entonces $d_{n+1} - e_{n+1}$ debe ser igual a cero, de lo contrario el módulo de la diferencia sería p^{n+1}. De ahí que $d_i = e_i$ para todo $i \in \mathbb{N}$. ∎

Sección 6: El cuerpo $\mathbb{Q}_p$ y el anillo $\mathbb{Z}_p$.

Ahora que hemos definido los racionales y una métrica, lo siguiente sería comprobar si es que $\left(\mathbb{Q}, \|\cdot\|_p\right)$ forma un cuerpo con la propiedad de clausura algebraica. La clausura algebraica implica que cualquier secuencia de Cauchy formada por los elementos de un conjunto tiene un límite dentro del conjunto mismo. Recordemos además que una secuencia es Cauchy si el límite de la norma de sus elementos tiende a cero.

La respuesta a la pregunta de si $\left(\mathbb{Q}, \|\cdot\|_p\right)$ cumple la clausura es que no: podemos encontrar una secuencia de Cauchy de p-ádicos racionales cuyo límite no es racional.

Demostración :

Los racionales con el módulo $\|\cdot\|_p$ no forman un espacio métrico completo.

Sea $x_n = a^{p^n}$ con $1 < a < p-1$, con $a,\ p,\ n \in \mathbb{N}$. Consideremos $\left|a^{p^{n+1}} - a^{p^n}\right|_p = \left|a^{p^n}(a^{p^n(p-1)} - 1)\right|_p$. El pequeño teorema de Fermat dice que $a^{p^n(p-1)} - 1 \equiv 0 \ (\text{mód } p^n)$, por lo tanto $\left|a^{p^n}(a^{p^n(p-1)} - 1)\right|_p \leq p^{-n} \underset{n\to\infty}{\longrightarrow} 0$. De aquí que x_n es una sucesión de Cauchy. Si definimos $x = \lim_{n\to\infty} x_n$ entonces tenemos:

$$\begin{aligned} x &= \lim_{n\to\infty} x_n \\ &= \lim_{n\to\infty} x_{n+1} \\ &= \lim_{n\to\infty} (x_n)^p \\ &= \left(\lim_{n\to\infty} x_n\right)^p \\ &= x^p \end{aligned}$$

Por otro lado,

$$\begin{aligned} |x-a|_p &= \left|x-a^{p^n}+a^{p^n}-a\right|_p \\ &\leq \max\left\{\left|x-a^{p^n}\right|_p, \left|a^{p^n}-a\right|_p\right\} \\ &= \left|a^{p^n}-a\right|_p \\ &= |a|_p \left|a^{p^n-1}-1\right|_p \\ &\leq \left|a^{p^n-1}-1\right|_p \\ &< 1 \end{aligned}$$

Como $\|x-a\| = p^{-v_p(x-a)} < 1$, se sigue que $p|(x-a)$. Como $a \neq 1$, $p-1$ se tiene que $x-a \neq 0$. Finalmente, dado que $x^p = x$ se tiene que x es una raíz $p-1$ no trivial de la unidad, de modo que $x \notin \mathbb{Q}$. ∎

Completación:

Dado que $\mathbb{Q}$ con la norma p-ádica es un espacio métrico incompleto, debe tener una completación única (excepto por isomorfismos). Podemos completar $\mathbb{Q}$ con la métrica p-ádica por el método de sucesiones de Cauchy. Esto se hace creando un espacio que contenga un subconjunto isomorfo a $\mathbb{Q}$ pero que además contenga a los límites de las sucesiones de Cauchy en los racionales.

Consideremos el conjunto de todas las sucesiones de Cauchy en $\mathbb{Q}$, al que llamamos $C[\mathbb{Q}]$. Definimos una relación de equivalencia en $C[\mathbb{Q}]$ de la siguiente manera: $\{x_n\} \sim \{y_n\}$ si y solo si $\lim_{n\to\infty} |x_n - y_n|_p = 0$. Ahora consideramos el conjunto $\mathbb{Q}^*$ de clases de equivalencia en $C[\mathbb{Q}]$ mediante $\sim$.

$\mathbb{Q}^* = \{[\{x_n\}], \{x_n\} \in C[\mathbb{Q}]\}$

Definimos una función de distancia $d^* : \mathbb{Q}^* \times \mathbb{Q}^* \to [0, \infty)$

$$d^*([\{x_n\}], [\{y_n\}]) = \lim_{n\to\infty} |x_n - y_n|_p$$

Demostramos que d^* es bien definida de la siguiente manera:

Dadas 4 sucesiones tales que $\{x_n\} \sim \{x'_n\}$ y $\{y_n\} \sim \{y'_n\}$. Por definición tenemos $\lim_{n\to\infty} |x_n - x'_n|_p = 0$ y $\lim_{n\to\infty} |y_n - y'_n|_p = 0$. Por la desigualdad triangular tenemos

$$\begin{aligned} |x_n - y_n|_p &\leq |x_n - x'_n|_p + |x'_n - y'_n|_p + |y'_n - y_n|_p \\ |x'_n - y'_n|_p &\leq |x'_n - x_n|_p + |x_n - y_n|_p + |y_n - y'_n|_p \end{aligned}$$

de donde $\left| |x_n - y_n|_p - |x'_n - y'_n|_p \right| \leq |x_n - x'_n|_p + |y'_n - y_n|_p \to 0$.

Como $|x_n - y_n|_p$ y $|x'_n - y'_n|_p$ son convergentes, tenemos $\lim_{n\to\infty} |x_n - y_n|_p = \lim_{n\to\infty} |x'_n - y'_n|_p$ de modo que d^* esta bien definida.

Ahora demostramos que d^* es una métrica:

i) $d^*([\{x_n\}], [\{y_n\}]) = 0 \iff \lim_{n\to\infty} |x_n - y_n|_p = 0 \iff \{x_n\} \sim \{y_n\} \iff [\{x_n\}] = [\{y_n\}]$

ii) $d^*([\{x_n\}], [\{y_n\}]) = \lim_{n\to\infty} |x_n - y_n|_p = \lim_{n\to\infty} |y_n - x_n|_p = d^*([\{x_n\}], [\{y_n\}])$

iii) Como $|x_n - z_n|_p \leq |x_n - y_n|_p + |y_n - z_n|_p$, entonces $\lim_{n\to\infty} |x_n - z_n|_p \leq \lim_{n\to\infty} |x_n - y_n|_p + \lim_{n\to\infty} |y_n - z_n|_p$ y finalmente $d^*([\{x_n\}], [\{z_n\}]) \leq d^*([\{x_n\}], [\{y_n\}]) + d^*([\{y_n\}], [\{z_n\}])$.

Este es un buen momento para definir un subconjunto de $\mathbb{Q}_p$ llamado los enteros p-ádicos:

$$\mathbb{Z}_p = \left\{ x \,|\, x \in \mathbb{Q}_p, |x|_p \leq 1 \right\}$$

Los enteros p-ádicos son los elementos del disco unitario en $\mathbb{Q}_p$. En términos de series, los enteros p-ádicos tienen la forma $\sum_{i=0}^{\infty} d_i p^i$, a diferencia de los p-ádicos en general, donde el índice i de la sumatoria puede empezar en un valor entero negativo.

Topología:

Hemos definido finalmente al conjunto de los p-ádicos. La pregunta que surge es

¿cómo son los números p-ádicos? Sabemos que podemos identificar a $\mathbb{R}$ con la recta numérica. En ese mismo sentido, los p-ádicos deben poder asociarse con un conjunto. Para esto recurrimos a la topología. Todo espacio métrico tiene una topología inducida cuya base son las bolas abiertas. En el caso de los números p-ádicos, debemos ver qué es una bola abierta. Dado un p-ádico q, una bola abierta de radio r serían el conjunto $B(q,r) = \left\{x, |q-x|_p < r\right\}$.

Proposición: El espacio $\mathbb{Q}_p$ de los números p-ádicos es totalmente disconexo.

Un espacio es totalmente disconexo si sus únicos subconjuntos conexos son el conjunto vacío y los conjuntos que contienen un solo punto. Una definición equivalente es que todo conjunto contiene un subconjunto clopen (abierto y cerrado). Recordemos que la norma $|\cdot|_p$ toma valores en el conjunto $\{0\} \cup \left\{p^k, k \in \mathbb{Z}\right\}$. Supongamos que $p^n \leq r < p^{n+1}$ entonces la bola $B(q,r)$ sería exactamente el conjunto $\left\{x, |q-x|_p \leq p^n\right\}$; el complemento de esta bola sería el conjunto $\left\{x, |q-x|_p > p^n\right\}$. Como la función de distancia a un punto es siempre continua, tenemos la preimagen del intervalo (p^{n+1}, ∞) es también abierta. De ahí que el complemento de la bola abierta $B(q,r)$ es también un conjunto abierto, y por lo tanto toda bola es un clopen. Ahora, La bola $B(q,r)$ contiene a la bola $B(q,p^{n-1})$ que es un clopen. De ahí que toda bola es disconexa. Es decir, $\mathbb{Q}_p$ es disconexo en todas partes. ∎

Ahora, consideramos a la bola abierta $B(q,r)$ con $p^{-n} \leq r < p^{-n+1}$ y $q = \sum_{i=0}^{\infty} d_i p^i$. En base a esto, busquemos qué característica debe tener un elemento x para pertenecer a $B(q,r)$. Como $|q-x|_p \leq p^{-n}$ se debe tener $q - x = \sum_{i=n}^{\infty} d_i p^i$. Esto solo es posible si $x = \sum_{i=0}^{\infty} e_i p^i$ con $e_i = d_i$ para $i = 1, \ldots, n-1$. Es decir, los discos alrededor de un p-ádico deben tener una cantidad de dígitos iguales al inicio que dependen del radio de disco.

Con esto, es fácil ver que todo punto es un punto de acumulación: Alrededor de un punto q puedo hacer una bola abierta de radio $\varepsilon < p^{-k}$. Esta bola sería el disco de radio

p^{-k-1}, que contiene a todos los p-ádicos cuyos primeros $k+1$ dígitos son iguales a los de q. Luego, no puede haber puntos aislados.

Compacidad de $\mathbb{Z}_p$ y $\mathbb{Q}_p$:

Un espacio métrico es localmente compacto si toda vecindad contiene un subconjunto cerrado. En $\mathbb{Q}_p$ toda bola es un clopen, de lo que sigue que una vecindad cualquiera de un punto dado contiene un clopen. Esto satisface la definición de un espacio localmente compacto. Más aún, $\mathbb{Z}_p$ pues es un espacio completo que además es totalmente acotado. Para verificar esto último, recordemos que $\mathbb{Z}_p = \left\{x, |x|_p \leq 1\right\}$ y que una bola de radio ε y centro O, donde $p^k \leq \varepsilon < p^{k+1}$, es el conjunto de números cuyos primeros $k+1$ dígitos coinciden con los primeros $k+1$ dígitos de O. Claramente podemos cubrir $\mathbb{Z}_p$ con p^{k+1} bolas de radio ε, luego $\mathbb{Z}_p$ es totalmente acotado, y por lo tanto compacto.

Por el otro lado, podemos ver que $\mathbb{Q}_p$ no es compacto. Podemos considerar el recubrimiento por bolas abiertas $\bigcup_{n=1}^{\infty} B(0, p^n)$. Este es un recubrimiento infinito de $\mathbb{Q}_p$, pero cualquier subconjunto finito sería insuficiente para contener a $\mathbb{Q}_p$. Luego, $\mathbb{Q}_p$ no es compacto. Sin embargo, cualquier bola es compacta, lo que hace que $\mathbb{Q}_p$ sea localmente compacto.

Sabiendo que $\mathbb{Z}_p$ es un subconjunto de un espacio métrico que es compacto, perfecto (no tiene puntos aislados) y totalmente disconexo, se tiene por necesidad que es homeomorfo a un conjunto de Cantor. Por otro lado, $\mathbb{Q}_p$ es la unión infinita contable de bolas abiertas que son homeomorfas a conjuntos de Cantor, cuyo resultado es homeomorfo a un conjunto de Cantor menos un punto..

$\mathbb{Q}_p$ es un cuerpo algebráico:

Ya hemos demostrado que $\mathbb{Q}_p$ es un espacio métrico completo con una operación de suma y multiplicación bien definidas. Lo único que falta demostrar para que sea un

cuerpo es que cada elemento no nulo tiene un inverso multiplicativo. Vamos a volver a la definición de los p-ádicos como clases de equivalencia de series de Cauchy. Un elemento no nulo corresponde a una sucesión convergente $\{x_n\}$ tal que $\lim_{n\to\infty} x_n \neq 0$ por definición, pero veamos qué implica eso. Primero, digamos que $a = \lim_{n\to\infty} x_n$, con $a \neq 0$. Esto quiere decir que existe $\delta > 0$ tal que para todo $N \in \mathbb{N}$ existe $n > N$ tal que $|0, x_n|_p > \delta$. Ahora, consideremos la sucesión $\left\{\frac{1}{x_n}\right\}$ debemos demostrar que esta sucesión también es Cauchy. Sin pérdida de generealidad, sean $m > n > N$. Queremos ver que $\lim_{n<m\to\infty} \left|\frac{1}{x_n} - \frac{1}{x_m}\right|_p = 0$.

$$\begin{aligned}
\lim_{n<m\to\infty} \left|\frac{1}{x_n} - \frac{1}{x_m}\right|_p &= \lim_{n<m\to\infty} \left|\frac{x_m - x_n}{x_n x_m}\right|_p \\
&\leq \frac{1}{\delta^2} \cdot \left(\lim_{n<m\to\infty} |x_m - x_n|_p\right) \\
&\to 0
\end{aligned}$$

$\mathbb{Z}_p$ no es un cuerpo algebráico, pues $\left|\frac{1}{q}\right|_p = \frac{1}{|q|_p}$ y sus elementos tienen todos módulo 1 o menos. Sin embargo, $\mathbb{Z}_p$ sí es un anillo algebráico, pues todo elemento tiene inversa aditiva.

$\mathbb{Q}_p$ cuando p no es primo:

Cabe recalcar que si p es un número compuesto con 2 o más divisores primos distintos, las métricas usadas no están bien definidas o no poseen todas las propiedades que demostramos en la sección 2. De hecho, en estos casos $\mathbb{Q}_p$ no es un cuerpo: tiene divisores de cero debido a que las ecuaciones $x \equiv x^2$ (mód p, p^2, ...) tienen soluciones adicionales aparte de 0 y 1.

Ejemplos:

$$\begin{aligned} 6 &\equiv 6^2 \text{ (mód 10)} \\ 76 &\equiv 76^2 \text{ (mód 100)} \\ 376 &\equiv 376^2 \text{ (mód 1000)} \\ &\vdots \end{aligned}$$

$$\begin{aligned} 5 &\equiv 5^2 \text{ (mód 10)} \\ 25 &\equiv 25^2 \text{ (mód 100)} \\ 625 &\equiv 625^2 \text{ (mód 1000)} \\ &\vdots \end{aligned}$$

Ambos sistemas tienen solución para potencias arbitrarias de 10. Las soluciones parciales del primer sistema son divisibles para 2, 4, 8, y asi sucesivamente, mientras que las de la segunda son divisibles para 5, 25, 125, (por el simple hecho de que $10 = 2 \cdot 5$). Por esto, las multiplicaciones de las soluciones parciales dan múltiplos de 10, 100, 1000, ..., cuyo límite en 10-ádicos es $\overline{0}$.

Conclusión:

Partiendo de la equivalencia modular $bx \equiv a$ (mód p) y el deseo de generalizar una solución a esta equivalencia para cualquier potencia de p, construimos una métrica que nos permita completar los racionales.

Una vez definidas las operaciones de suma y multiplicación de números p-ádicos así como sus respectivas inversas, demostramos que los p-ádicos forman un anillo (cuando p es compuesto) o un cuerpo (cuando p es primo). Junto con la métrica $\mathbb{Q}_p$ que también definimos forman un cuerpo algebráico.

Bibliografía:

Ireland, Rosen "Gruaduate Texts in Mathematics: A classic introduction to modern number theory". Segunda edición, Springer

LeVeque, William "Fundamentals of number theory" 1996

Martinez, Fabio Brochero et al "Teoria dos números". Rio de Janeiro: Projeto Euclides 2010.

Morris, Sidney "Topology without tears" 2015

<https://proofwiki.org/wiki/P-adic_Norm_not_Complete_on_Rational_Numbers>, revisado el 5 de mayo de 2015