Una introducción a los números P-ádicos

Sergio Carrillo Torres
Estudiante Universidad Sergio Arboleda
Bogotá D.C, Colombia
sergio_carrillo30@hotmail.com

Carlos Hurtado Amaya
Estudiante Universidad Sergio Arboleda
Bogotá D.C, Colombia
carlos.hurtado@usa.edu.co

Resumen

EL objetivo del presente artículo es mostrar los números p-ádicos, obteniéndolos a partir de la completación topológica de los números racionales $\mathbb{Q}$, por medio de una métrica, que no coincide con la inducida por el valor absoluto, y describir el lema de Hensel que permite resolver ecuaciones en dicha estructura.

1. Preliminares algebraicos y topológicos

Definición 1.1. Sea R un anillo con unidad, una función

$$N : R \longrightarrow \mathbb{R}^+$$

se dice una norma sobre R si satisface:

1. $N(x) = 0$ si y sólo si $x = 0$.
2. $N(xy) = N(x)N(y)$ para todo x, y en R.
3. $N(x + y) \leq N(x) + N(y)$ para todo x, y en R.

si además tenemos que

$$N(x + y) \leq \text{máx}\{N(x), N(y)\} \qquad \forall x, y \in R$$

decimos que N es no arquimediana.

Definición 1.2. Sea $x \in \mathbb{Z}$ el ordinal p-ádico (o valuación) de x es:

$$\text{ord}_p(x) = \text{máx}\{r : p^r | x\} \geq 0$$

ahora, si $a/b \in \mathbb{Q}$ entonces

$$\text{ord}_p\left(\frac{a}{b}\right) = \text{ord}_p(a) - \text{ord}_p(b)$$

y definimos $\text{ord}_p(0) = \infty$

Teorema 1.1. Si x, y estan en $\mathbb{Q}$ el ord_p satisface:

1. $\text{ord}_p(x) = \infty$ si y sólo si $x = 0$.
2. $\text{ord}_p(xy) = \text{ord}_p(x) + \text{ord}_p(y)$.
3. $\text{ord}_p(x + y) \geq \text{mín}\{\text{ord}_p(x), \text{ord}_p(y)\}$ con la igualdad si $\text{ord}_p(x) \neq \text{ord}_p(y)$

Demostración:

2)
$$\begin{aligned}\mathrm{ord}_p(xy) &= \mathrm{ord}_p(x \cdot 1/(1/y)) \\ &= \mathrm{ord}_p(x) - \mathrm{ord}_p(1/y) \\ &= \mathrm{ord}_p(x) - (\mathrm{ord}_p(1) - \mathrm{ord}_p(y)) \\ &= \mathrm{ord}_p(x) + \mathrm{ord}_p(y) \quad \square\end{aligned}$$

3) escribamos a x y y de la siguiente forma:

$$x = p^r \frac{a}{b} \quad \text{y} \quad x = p^s \frac{c}{d}$$

donde $a, b, c, d \in \mathbb{Z}$ con $p \not| a, b, c, d$ y $r, s \in \mathbb{Z}$. Ahora si $r = s$, tenemos que

$$\begin{aligned}x + y &= p^r \left(\frac{a}{b} + \frac{c}{d}\right) \\ &= p^r \left(\frac{ad + bc}{bd}\right)\end{aligned}$$

de donde $\mathrm{ord}_p(x + y) \geq r$ porque $p \not| bd$.
Si $r \neq s$, supongamos que $s > r$. entonces

$$\begin{aligned}x + y &= p^r \left(\frac{a}{b} + p^{s-r}\frac{c}{d}\right) \\ &= p^r \left(\frac{ad + p^{s-r}bc}{bd}\right)\end{aligned}$$

como $s - r > 0$ y $p \not| ad$, entonces

$$\mathrm{ord}_p(x + y) = r = \text{mín}\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}. \square$$

Definición 1.3. Sea $x \in \mathbb{Q}$ la norma p-ádica de x se define como:

$$|x|_p = \begin{cases} \frac{1}{p^{\mathrm{ord}_p(x)}} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases}$$

Teorema 1.2. La función $|\ |_p : \mathbb{Q} \longrightarrow \mathbb{R}^+$ satisface:

1. $|x|_p = 0$ si y sólo si $x = 0$.
2. $|xy|_p = |x|_p|y|_p$;
3. $|x + y|_p \leq \text{máx}\{|x|_p, |y|_p\}$ con la igualdad si $|x|_p \neq |y|_p$.

Luego $|\ |_p$ es una norma no arquimedeana sobre $\mathbb{Q}$. Tomemos $p = 3$, y evaluemos la norma 3-ádica de 12, 27, 14 y 68

- $|12|_3 = \dfrac{1}{3^{\mathrm{ord}_3(12)}} = \dfrac{1}{3^{\mathrm{ord}_3(4\cdot 3)}} = \dfrac{1}{3^{\mathrm{ord}_3(4)+\mathrm{ord}_3(3)}} = \dfrac{1}{3^1}$
- $|27|_3 = \dfrac{1}{3^{\mathrm{ord}_3(27)}} = \dfrac{1}{3^{\mathrm{ord}_3(3^3)}} = \dfrac{1}{3^3} = \frac{1}{27}$

- $|14|_3 = \dfrac{1}{3^{\text{ord}_3(14)}} = \dfrac{1}{3^{\text{ord}_3(2\cdot 7)}} = \dfrac{1}{3^0} = 1$
- $|68|_3 = \dfrac{1}{3^{\text{ord}_3(68)}} = \dfrac{1}{3^{\text{ord}_3(2^2\cdot 17)}} = \dfrac{1}{3^0} = 1$

de los anteriores cálculos y de la definiciones, observamos que

$$\text{ord}_p(p^n) = n$$

y como $\text{ord}_p(xy) = \text{ord}_p(x)\text{ord}_p(y)$, en virtud del teorema fundamental de la aritmética, si consideramos $n \in \mathbb{Z}$ y sea $n = p^a p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ la descomposición en factores primos de n, luego

$$\begin{aligned}\text{ord}_p(n) &= \text{ord}_p(p^a p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}) \\ &= \text{ord}_p(p^a)\text{ord}_p(p_1^{a_1})\text{ord}_p(p_2^{a_2}) \cdots \text{ord}_p(p_n^{a_n})\end{aligned}$$

como $p_1, p_2, \ldots, p_n$ son diferentes de p, tenemos que

$$\text{ord}_p(n) = a$$

donde a es la potencia de p que aparece en la descomposición prima de n. Por otro lado calculemos las normas 3-ádicas de los números racionales 1/3, 8/9, 27/5

- $|1/3|_3 = \dfrac{1}{3^{\text{ord}_3(1/3)}} = \dfrac{1}{3^{\text{ord}_3(1)-\text{ord}_3(3)}} = \dfrac{1}{3^{-1}} = 3$
- $|8/9|_3 = \dfrac{1}{3^{\text{ord}_3(8/9)}} = \dfrac{1}{3^{\text{ord}_3(8)-\text{ord}_3(9)}} = \dfrac{1}{3^{-2}} = 9$
- $|27/5|_3 = \dfrac{1}{3^{\text{ord}_3(27/5)}} = \dfrac{1}{3^{\text{ord}_3(27)-\text{ord}_3(5)}} = \dfrac{1}{3^3} = \dfrac{1}{27}$

Con el fin de hacer una teoría más general de aquí en adelante, consideremos una norma N sobre R,

Definición 1.4. La distancia entre $x, y \in R$ con respecto a N es

$$d_N(x, y) = N(x - y) \in \mathbb{R}^+$$

la anterior función satisface las siguientes propiedades:

1. $d_N(x, y) = 0$ si y sólo si $x = y$.
2. $d_N(x, y) = d_N(y - x)$.
3. $d_N(x, z) \leq d_N(x, z) + d_N(z, y)$ con $z \in R$.

Si N es no arquimediana.

$$d_N(x, y) \leq \text{máx}\{d_N(x, z), d_N(z, y)\}$$

con la igualdad si $d_N(x, z) \neq d_N(z, y)$ Sea (a_n) una sucesión de elementos de R,

Definición 1.5. La sucesión (a_n) tiende al limite $a \in R$ con respecto a N si:

$$\forall \epsilon > 0 \; \exists M \in \mathbb{N} \; : n > M \Longrightarrow d_N(a_n, a) < \epsilon$$

y usamos la notación $\lim\limits_{n\to\infty}{}^{(N)} a_n = a$

Definición 1.6. La sucesión (a_n) es de Cauchy con respecto a N si

$$\forall \epsilon > 0 \; \exists M \in \mathbb{N} \; : n, m > M \Longrightarrow d_N(a_n, a_m) < \epsilon$$

Teorema 1.3. Si $\lim\limits_{n\to\infty}{}^{(N)} a_n$ existe, entonces la sucesión es de Cauchy.

Demostración:
Sea $a = \lim\limits_{n\to\infty}{}^{(N)} a_n$, entonces podemos encontrar M_1 tal que

$$n > M_1 \Longrightarrow d_N(a_n, a) < \frac{\epsilon}{2}$$

si $m, n > M_1$ entonces $d_N(a_m, a) < \frac{\epsilon}{2}$ luego

$$\begin{aligned} d_N(a_m, a_n) &\leq d_N(a_m, a) + d_N(a_n, a) \\ &< \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon \end{aligned}$$ □

Ejemplo 1.1. Sea $R = \mathbb{Q}$, $N = |\;|_p$, $a_n = 1 + p + \cdots + p^{n-1}$, luego

$$\begin{aligned} |a_{n+k} - a_n|_p &= |p^n + p^{n+1} + \cdots + p^{n+k-1}|_p \\ &= |p^n(1 + p + \cdots + p^{k-1})|_p \\ &= \frac{1}{p^n} \end{aligned}$$

entonces para cada $\epsilon > 0$, tomamos M talque $p^M \geq 1/\epsilon$. Así $n > M$ tenemos que

$$|a_m - a_n|_p < \frac{1}{p^M} \leq \epsilon.$$

Consideremos $a = 1/(p-1) \in \mathbb{Q}$, entonces $a_n = (p^n - 1)/(p-1)$, luego

$$|a_n - a|_p = \left| \frac{p^n}{1-p} \right|_p = \frac{1}{p^n}$$

así para $\epsilon > 0$, tenemos

$$|a_n - a|_p < \epsilon$$

usando nuestra notación.

$$\lim_{n\to\infty}{}^{(p)} 1 + p + \cdots + p^{n-1} = \frac{1}{p-1}$$

Definición 1.7. Una sucesión (a_n) es llamada sucesión nula si

$$\lim_{n\to\infty}{}^{(N)} a_n = 0$$

Veamos que $\lim\limits_{n\to\infty}{}^{(N)} a_n = 0$ es equivalente a $\lim\limits_{n\to\infty} N(a_n) = 0$

$$\forall \epsilon > 0\ \exists M \in \mathbb{N}\ : n > M \Longrightarrow d_N(a_n, 0) = N(a_n) < \epsilon$$
$$\forall \epsilon > 0\ \exists N \in \mathbb{N}\ : n > N \Longrightarrow |N(a_n)| < \epsilon$$

Como $|N(a_n)| = N(a_n)$ porque $N(a_n) \geq 0$, entonces tenemos la equivalencia.
Definamos los siguientes conjuntos:

$$CS(R, N) = \text{ El conjunto de las sucesiones de Cauchy}$$
$$Null(R, N) = \text{ El conjunto de las sucesiones nulas}$$

Por el teorema 3, $Null(R, N) \subseteq CS(R, N)$. Podemos dotar de estructura de anillo a $CS(R, N)$ definiendo

$$(a_n) + (b_n) = (a_n + b_n)$$
$$(a_n) \times (b_n) = (a_n \times b_n)$$

Los elementos $0_{CS} = (0)$ y $1_{CS} = (1)$ son los elementos neutro para la suma y el producto de $CS(R, N)$.

Teorema 1.4. $Null(R, N)$ es un ideal a derecha e izquierda de $CS(R, N)$

Demostración:
Sean $(a_n) \in CS(R, N)$ y $(b_n) \in Null(R, N)$. Luego $\lim\limits_{n\to\infty}{}^{(N)} b_n = 0$
Como (a_n) es de Cauchy entonces existen $k > 0$ y M' tales que para $n > M'$, $N(a_n) < k$. Tomemos M'' tal que $N(b_n) < \frac{\epsilon}{k}$. Sea $M = \text{máx}\{M', M''\}$. Luego

$$N(a_n b_n) = N(a_n)N(b_n) < kN(b_n) < k\tfrac{\epsilon}{k} = \epsilon$$

Por tanto $\lim\limits_{n\to\infty}{}^{(N)} a_n b_n = 0$, es decir $a_n b_n \in Null(R, N)$ □

Definición 1.8. El anillo cociente $CS(R, N)/Null(R, N) = \widehat{R}_N$ es llamado la completación de R respecto a la norma N y notamos $\{a_n\}$ la clase de equivalencia de la sucesión (a_n)

Teorema 1.5. $|N(x) - N(y)| \leq N(x - y)$

Demostración:
Tenemos

$$N(x) = N((x - y) + y) \leq N(x - y) + N(y)$$
$$N(x) - N(y) \leq N(x - y)$$

De manera análoga

$$N(y) - N(x) \leq N(x - y)$$

Luego

$$|N(x) - N(y)| \leq N(x - y) \qquad \square$$

Teorema 1.6. El anillo $\widehat{R}_N$ con la suma + y el producto × dados por

$$\{a_n\} + \{b_n\} = \{a_n + b_n\},\ \ \{a_n\} \times \{b_n\} = \{a_n \times b_n\}$$

tiene una norma $\widehat{N}$ tal que $\widehat{N}(\{a\}) = N(a)$ para todas las sucesiones de Cauchy constantes, $(a_n) = a$, con $a \in R$, esta norma definida por:

$$\widehat{N}(\{c_n\}) = \lim_{n\to\infty} N(c_n)$$

Finalmente $\widehat{N}$ es no arquimediana si y sólo si N lo es.

Demostración:
Como (a_n) es de Cauchy con respecto a N entonces $(N(a_n))$ es de Cauchy respecto a $|\ |$, porque

$$|N(a_n) - N(a_m)| \leq N(a_n - a_m) < \epsilon$$

como $\mathbb{R}$ es completo respecto a $|\ |$ entonces existe l tal que

$$\lim_{n\to\infty} N(a_n) = l$$

luego hay un M' tal que para $n > M'$ tenemos que $|l - N(a_n)| < \epsilon$. Veamos que $\widehat{N}$ es una norma

$$\begin{aligned}\widehat{N}(\{a_n\}) = 0 &\iff \lim_{n\to\infty} N(a_n) = 0\\ &\iff (a_n) \text{ es una sucesión nula}\\ &\iff \{a_n\} = 0\end{aligned}$$

dadas $\{a_n\}$, $\{b_n\}$ tenemos

$$\begin{aligned}\widehat{N}(\{a_n\}\{b_n\}) = \widehat{N}(\{a_n b_n\}) &= \lim_{n\to\infty} N(a_n b_n)\\ &= \lim_{n\to\infty} N(a_n)N(b_n)\\ &= \lim_{n\to\infty} N(a_n) \lim_{n\to\infty} N(b_n)\\ &= \widehat{N}(\{a_n\})\widehat{N}(\{b_n\})\end{aligned}$$

finalmente

$$\begin{aligned}\widehat{N}(\{a_n\} + \{b_n\}) &= \lim_{n\to\infty} N(a_n + b_n)\\ &\leq \lim_{n\to\infty} N(a_n) + N(b_n)\\ &= \lim_{n\to\infty} N(a_n) + \lim_{n\to\infty} N(b_n)\\ &= \widehat{N}(\{a_n\}) + \widehat{N}(\{b_n\}),\end{aligned}$$

luego $\widehat{N}$ es una norma. □

Teorema 1.7. Sea R un anillo con norma no arquimediana N, suponga que (a_n) es una sucesión de Cauchy y $b \in R$ es tal que $b \neq \lim\limits_{n\to\infty}{}^{(N)} a_n$. Entonces existe un M tal que $m, n > M$

$$N(a_n - b) = N(a_m - b)$$

Demostración:
Notemos que como (a_n) es de Cauchy con respecto a N

$$|N(a_m - b) - N(a_n - b)| \leq N(a_n - a_m) < \epsilon$$

luego $(N(a_n - b))$ es de Cauchy en $\mathbb{R}$. Sea $l = \lim_{n\to\infty} N(a_n - b)$. Luego existe M_1 tal que para $n > M_1$ se tiene que

$$N(a_n - b) > \frac{l}{2}$$

también existe un M_2 tal que para $m, n > M_2$ se tiene

$$N(a_m - a_n) < \frac{l}{2}$$

Tomemos $M = \text{máx}\{M_1, M_2\}$ y consideremos $m, n > M$. Entonces

$$\begin{aligned} N(a_m - b) &= N((a_n - b) + (a_m - a_n)) \\ &= \text{máx}\{N(a_n - b), N(a_m - a_n)\} \\ &= N(a_n - b) \end{aligned}$$

Porque $N(a_m - a_n) < \frac{l}{2} < N(a_n - b)$. □

Si (a_n) no es una sucesión nula, entonces la sucesión $(N(a_n))$ es constante.

Este teorema muestra que desde cierto M, $\widehat{N}(\{a_n\}) = N(a_n)$, es eventualmente constante. Volviendo al teorema 6. Tomemos $\{a_n\}$ y $\{b_n\}$ tales que

$$\widehat{N}(\{a_n\}) \neq \widehat{N}(\{b_n\});$$

si tomamos $b = 0$ en el teorema anterior podemos encontrar enteros M', M'' tales que

$$n > M' \Longleftrightarrow N(a_n) = \widehat{N}(\{a_n\})$$

y

$$n > M'' \Longleftrightarrow N(b_n) = \widehat{N}(\{b_n\})$$

Para $n > \text{máx}\{M', M''\}$ tenemos

$$\begin{aligned} N(a_n + b_n) &= \text{máx}\, N(a_n), N(b_n) \\ &= \text{máx}\, \widehat{N}(\{a_n\}), \widehat{N}(\{b_n\}) \end{aligned}$$

En este punto, podemos desarrollar este procedimiento con cualquier anillo conmutativo con unidad, en particular con un campo, en el presente articulo desarrollaremos la teoría anteriormente expuesta para el campo de numeros racionales $\mathbb{Q}$

2. Campo de los números p-ádicos

Consideremos la completación de $\mathbb{Q}$ respecto a la norma $||_p$, luego a $\widehat{\mathbb{Q}}$ se le denomina el campo de los números p-ádicos y los notaremos como $\mathbb{Q}_p$, como consecuencia de la completación tenemos una copia de $\mathbb{Q}$ en $\mathbb{Q}_p$.

Definición 2.1. El disco unitario alrededor de $0 \in \mathbb{Q}_p$ es el conjunto de enteros p-ádicos

$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a|_p \leq 1\}$$

Teorema 2.1. $\mathbb{Z}_p$ es un subanillo de $\mathbb{Q}_p$, además $\text{Fr}(\mathbb{Z}_p) = \mathbb{Q}_p$

Teorema 2.2. Si $x \in \mathbb{Z}_p$, existe una sucesión $a_0, a_1, \ldots, a_n, \ldots \in \mathbb{Z}$, $0 \leq a_n \leq p - 1$ tal que

$$x = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + \cdots$$

Tomemos $a \in \mathbb{Q}_p$, entonces si $|a|_p \leq 1$ por definición $a \in \mathbb{Z}_p$, por otro lado si $|a|_p > 1$ podemos suponer que $|a|_p = p^k$ con $k > 0$, y consideremos $b = p^k a$, de este modo $|b|_p = 1$ así por la proposición anterior

$$b = b_0 + b_1 p + b_2 p^2 + \cdots + b_k p^k + \cdots$$

de lo que concluimos que

$$a = \frac{b_0}{p^k} + \frac{b_1}{p^{k-1}} + \cdots + \frac{b_{k-1}}{p} + b_k + b_{k+1} p + \cdots$$

Teorema 2.3. Cada número p-ádico $a \in \mathbb{Q}_p$ tiene una expansión única

$$a = \frac{a_{-r}}{p^r} + \frac{a_{1-r}}{p^{r-1}} + \cdots + \frac{a_{-1}}{p} + a_0 + a_1 p + \cdots$$

con $a_n \in \mathbb{Z}$ y $0 \leq a_n \leq (p-1)$, además $a \in \mathbb{Z}_p$ si y sólo si $a_{-r} = 0$ para $r > 0$.

Estas última expansión es conocida como el desarrollo de Hensel de a, además, es importante determinar r en la expansión p-ádica de un número arbitrario, esto se consigue con la desigualdad ultramétrica.

3. Aritmética p-ádica

Usaremos la siguiente notación para no utilizar el desarrollo de Hensel en las operaciones de suma y multiplicación.

$$a_{n_0} \ldots, a_0 a_1 a_2 a_3 \quad \text{para} \quad \sum_{i=n_0}^{\infty} a_i p^i$$

3.1. suma de dos números p-ádicos

La suma $x + y = \sum_{n=n_0}^{\infty} c_n p^n$ de los números

$$\sum_{n=n_0}^{\infty} a_n p^n \quad \text{y} \quad \sum_{n=n_1}^{\infty} b_n p^n$$

se define recursivamente por:

$$\epsilon_n = 0 \quad \text{para } n \leq n_0$$

y para los demás valores de n

$$\epsilon_n + a_n + b_n = c_n + e_{n+1} \cdot p.$$

En esta definición ϵ_n es la cantidad que se lleva por cada potencia de p y la anterior expresión se puede entender como tomar clase residual módulo p y llevar el multiplo de p a su siguiente potencia

3.2. Multiplicación

La multiplicación se define como

$$\sum_{n=n_0}^{\infty} a_n p^n \cdot \sum_{k=n_1}^{\infty} b_k p^k = \sum_{j=n_1+n_0}^{\infty} c_j p^j$$

donde $c_j = \sum_{i=n_0}^{j-n_1} a_i b_{j-i}$ y $c_j = 0$ para $j < n_0 + n_1$.
La diferencia con las operaciones definidas en los racionales y las anteriores es que se hacen de izquierda a derecha, no de derecha a izquierda, pese a que un número p-ádico es una serie de Laurent, podemos obtener aproximaciones de sus sumas y multiplicaciones.

Ejemplo 3.1. Sean $x = 111,21210\ldots$ y $y = 22,00101\ldots$ elementos de $\mathbb{Q}_3$, luego su suma es

$$\begin{array}{cccccccccc} & 1 & 1 & 1 & , & 2 & 1 & 2 & 1 & 0 \\ + & & 2 & 2_1 & , & 0_1 & 0_1 & 1 & 0_1 & 1_1 \\ \hline & 1 & 0 & 1 & , & 0 & 2 & 0 & 2 & 1 \end{array}$$

esto se debe a que el desarrollo de Hensel más largo es el de x, entonces llamemos a $x + y = c_{-3}c_{-2}c_{-1}, c_0c_1c_2c_3c_4c_5$, así $c_{-3} = 1$, $c_{-2} = 1 + 2 \equiv 1 \cdot 3 \mod 3$ y llevamos una potencia de 3, $c_{-1} = 1 + 2 + 1 \equiv 1 + 1 \cdot 3 \mod 3$ y así el proceso continua, hasta obtener la aproximación deseada, en la tabla se escriben en subindice las cantidades que se llevan
La multiplicación es de forma analoga, por ejemplo $x = 1,212\ldots$ y $y = 2,22\ldots$

$$\begin{array}{cccccccccccc} & 1 & , & 2 & 1 & 2 & \ldots & \cdot & 2 & , & 2 & 2\ldots \\ \hline 2 & 4 & , & 2 & 4 & \ldots & & & & & & \\ & 2 & , & 4 & 2 & \ldots & & & & & & \\ & 0 & , & 2 & 4 & \ldots & & & & & & \\ & 0 & , & 0_2 & 2_3 & \ldots & & & & & & \\ \hline 2 & 0 & , & 1 & 0 & \ldots & & & & & & \end{array}$$

Ahora busquemos desarrollos de Hensel de numeros conocidos, por ejemplo de -1 y de $1/6$, como $1 - 1 = 0$ dado que $\mathbb{Z} \subseteq \mathbb{Z}_p$ tenemos que si

$$-1 = a_0 + a_1 \cdot 3 + a_2 \cdot 3^2 + a_3 \cdot 3^3 + \cdots$$

es su desarrollo de Hensel

$$\begin{array}{ccccccccccc} & 1 & & & & & & & & & \\ + & a_0 & + & a_1 \cdot 3 & + & a_2 \cdot 3^2 & + & a_3 \cdot 3^3 & + \cdots & & \\ \hline & 0 & & 0 & & 0 & & 0 & & 0 \end{array}$$

por tanto $a_0 + 1 \equiv 0 \mod 3$, es decir, $a_0 = 2$ y se lleva una potencia de 3, por otro lado $a_1 + 1 + 1 \equiv 0 \mod 3$ de este modo $a_1 = 1$ y siguiendo este procedimiento llegamos a que.

$$-1 = 2 + 1 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + \cdots$$

en un caso más general si $a \in \mathbb{Q}_p$, por lo visto anteriormente

$$\frac{a_{-m}}{p^m} + \frac{a_{1-m}}{p^{m-1}} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots$$

entonces $-a$ es igual a

$$\frac{p - a_{-m}}{p^m} + \frac{(p + 1 - a_{1-m})}{p^{m-1}} + \cdots + (p - 1 - a_0) + (p - 1 - a_1)p + \cdots .$$

Siguiendo con los ejemplos, hallemos el desarrollo de Hensel de $1/6$ en $\mathbb{Q}_3$, lo primero que se observa es que $|1/6|_3 = 3$, luego $1/6 \notin \mathbb{Z}_p$, debemos determinar en que potencia de 3 comienza

su desarrollo de Hensel, por la desigualdad ultramética vemos que la potencia es -1. Así supongamos que

$$\frac{1}{6} = \frac{a_{-1}}{3} + a_0 + a_1 \cdot 3 + a_2 \cdot 3^2 + \cdots$$

como $6 \cdot 1/6 = 1$ y como $6 = 2 \cdot 3$,

$$1 = 6 \cdot \frac{1}{6} = 2a_{-1} + 2a_0 \cdot 3 + 2a_1 \cdot 3^2 + 2a_2 \cdot 3^3 + \cdots$$

entonces $2a_{-1} \equiv 1 \mod 3$ por tanto $a_1 = 1$ y se lleva una potencia de 3, pasando al siguiente coeficiente $2a_0 + 1 \equiv 0 \mod 3$ luego $a_0 = 1$ y siguiendo este razonamiento vemos que

$$\frac{1}{6} = \frac{2}{3} + 1 + 1 \cdot 3 + 1 \cdot 3^2 + \cdots$$

por otro lado podemos estar interesados en obtener la raíz cuadra de un número entero por ejemplo $\sqrt{5} \in \mathbb{Q}_3$, supongamos en principio que $x = \sqrt{5} \in \mathbb{Z}_3$. Sea

$$x = a_0 + a_1 \cdot 3 + a_2 \cdot 3^2 + a_3 \cdot 3^3 + \cdots,$$

como $x^2 = 5$,

$$a_0^2 + 2a_0(a_1 \cdot 3 + a_2 \cdot 3^2 + a_3 \cdot 3^3 + \cdots) + (a_1 \cdot 3 + a_2 \cdot 3^2 + a_3 \cdot 3^3 + \cdots)^2 = 5$$

si consideramos la anterior ecuación en $\mathbb{Z}/\not\Vdash Z$ (los enteros módulo 3), obtenemos

$$a_0^2 \equiv 1 \mod 3$$

luego a_0 es 1 o 2, si lo consideramos como 1 así tenemos la relación

$$1 + 2(a_1 \cdot 3 + a_2 \cdot 3^2 + a_3 \cdot 3^3 + \cdots) + (a_1 \cdot 3 + a_2 \cdot 3^2 + a_3 \cdot 3^3 + \cdots)^2 = 5$$

si volvemos a considerar ésta ecuación en $\mathbb{Z}/\nrightarrow Z$ tenemos que

$$1 + 2a_1 \cdot 3 \equiv 5 \mod 3$$

resolviendo esta congruencia

$$\begin{aligned} 6 + 2a_1 \cdot 3 &\equiv 0 \mod 9 \\ 3(2 + 2a_1) &\equiv 0 \mod 9 \\ 2 + 2a_1 &\equiv 0 \mod 3 \end{aligned}$$

obtenemos que $a_1 = 2$ y así consecutivamente logramos el desarrollo de Hensel de $\sqrt{5}$ en $\mathbb{Q}_3$

4. Existencia de raices cuadradas

Consideremos $\sqrt{p}$, si $\sqrt{p} \in \mathbb{Q}$, entonces $|(\sqrt{p})^2|_p = |p|_p = 1/p$, eso significa que $|\sqrt{p}|_p = \sqrt{\frac{1}{p}}$ como $|\mathbb{Q}_p| = p^{\mathbb{Z}}$ por tanto $\sqrt{p}$ no esta en $\mathbb{Q}_p$

Teorema 4.1 (lema de Hensel). Sea $F(x) = c_0 + c_1x + \cdots + c_nx^n$ un polinomio cuyos coeficientes son enteros p-ádicos. Sea $F'(x) = c_1 + 2c_2x + 3c_3x^2 + \cdots + nx^{n-1}$ la derivada formal de F. Sea a_0 un entero p-ádico tal que $F(a) \equiv 0 \mod p$ y $F'(a) \not\equiv 0 \mod p$. Entonces existe un único entero p-ádico tal que

$$F(a) = 0 \quad 1 \quad a \equiv a_0 \mod p$$

Por tanto si consideramos $\mathbb{Q}_3$ y los siguientes polinomios

- $f(x) = x^2 + 2$,
- $g(x) = x^2 - 2$,
- $h(x) = x^3 \pm 1$.

Luego por el lema de Hensel;

- Como $f(1) = 1^2 + 2 \equiv 3 \mod 3$ y $f'(x) = 2x|_{x=1} = 2 \not\equiv 3 \mod 3$ entonces tiene una raiz en $\mathbb{Q}_3$, es decir, $\sqrt{-2} \in \mathbb{Q}_3$
- Como no existe entero a_0 tal que $g(a_0) \equiv 0 \mod 3$, dado que $g(1) \equiv 2 \mod 3$ y $g(2) \equiv 2 \mod 3$ entonces no existe un entero p-ádico a tal que $g(a) = 0$, por tanto $\sqrt{2} \notin \mathbb{Q}_3$.
- Calculando la derivada tenemos $h'(x) = (3)x^2 \equiv 0 \mod 3$, luego no existen raíces cubicas de la unidad.

Bibliografía

[1] Baker, A.J., *An introduction to p-adic numbers and p-adic analysis*. Departement of Mathematics, Glasgow university, 2005.

[2] Koblitz, Neal, *p-adic numbers, p-adic analysis, and zeta-functions*. Springer-Verlag, New York, 1977.

[3] Mathiak, K., *Bewertungstheorie*. Institut für Algebra und Zahlentheorie, Braunshwieg, 1977.