Pequeñísima introducción a los números p-ádicos...

María Ximena Loarca Hass

Universidad del Valle de Guatemala
Teoría de números

Noviembre 2024

Introducción

En 1897 Kurt Hensel exploraba una analogía entre el anillo de los enteros $\mathbb{Z}$, con su cuerpo de fracciones $\mathbb{Q}$ y el anillo de polinomios con coeficientes complejos $\mathbb{C}[x]$ junto con su cuerpo de fracciones $\mathbb{C}(x)$.

Antes de definiciones, un poco de historia:

- La motivación principal era llevar ideas y técnicas de las series de potencias a la teoría de números.
- Creados para resolver problemas de divisibilidad, ecuaciones modulares y ecuaciones diofánticas.
- Se encuentran en el análisis, geometría, física y criptología.

Números reales

Recordemos la construcción de los números reales:

- Anillo de enteros $\mathbb{Z}$.
- Números racionales como el campo de fracciones de los enteros $\mathbb{Q}$.
- La norma usual es $|x|$ para $x \in \mathbb{Q}$.
- La distancia entre dos números x y $y \in \mathbb{Q}$ se define como $|x - y|$.
- Completación de $\mathbb{Q}$ utilizando sucesiones de Cauchy.
- Extender $\mathbb{Q}$ con los límites faltantes de las sucesiones, los irracionales $\mathbb{I}$, para crear $\mathbb{R}$.

Números p-ádicos

Ahora pensando en este método de completación respecto a una norma, consideremos al espacio métrico $(\mathbb{Q}, |\cdot|_p)$, el cual no es completo.

Definición 1. El campo de los números p-ádicos $\mathbb{Q}_p$ extiende al campo de los números racionales $\mathbb{Q}$ respecto a la norma p-ádica $|\cdot|_p$.

Tenemos una nueva manera de comprender a los "números".

Valuación p-ádica

Sea p un número primo fijo. Sabemos por el Teorema Fundamental de la Aritmetica que para cada $a \in \mathbb{Z}$, existe un único $n \in \mathbb{Z}_{\geq 0}$ tal que $a = p^n r$, con $(r, p) = 1$. Tal que podemos hacer las siguientes definiciones:

Definición 2.
Se define a la **valuación p-ádica** de un número racional como:

- $v_p(x) = max\{n \in \mathbb{Z} : p^n | x\} \geq 0$, si $x \in \mathbb{Z} \setminus \{0\}$.
- $v_p(q) = v_p(a) - v_p(b,)$ si $q = a/b \in \mathbb{Q}$.

Proposición 1.
Sean $x, y \in \mathbb{Q}$. Entonces se cumplen:

(a) $v_p(x) = \infty \iff x = 0$

(b) $v_p(xy) = v_p(x) + v_p(y)$

(c) $v_p(x + y) \geq min\{v_p(x), v_p(y)\}$, y si $v_p(x) \neq v_p(y)$ se da la igualdad.

Nuestro primo 3

Seleccionemos un número primo p=3 para poder observar como funcionan los números 3-ádicos.

Entonces la valuación 3-ádica de los números racionales es

$$v_3(x) = max\{n \in \mathbb{Z} : 3^n | x\} \geq 0, \quad \text{si } x \in \mathbb{Z} \setminus \{0\}.$$

Por ejemplo:

- $v_3(18) = 2$ ya que podemos escribir $18 = 3^2 \cdot 2$.
- $v_3(27) = 3$ ya que podemos escribir $27 = 3^3$.
- $v_3(5) = 0$ ya que podemos escribir $5 = 3^0 \cdot 5$.
- $v_3(\frac{1}{3}) = -1$ ya que podemos escribir $\frac{1}{3} = 3^{-1}$.

Norma p-ádica

Esta valuación nos permite definir la norma p-ádica:

Definición 3.
Si p es un número primo fijo, se define en $\mathbb{Q}$ la **norma p-ádica** como $|x|_p = p^{-v_p(x)}$.

Definimos $|0|_p = 0$. Y notemos que $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$.

Proposición 2.
Si $x \in \mathbb{Q}$, entonces:

(a) $|x|_p = 0 \iff x = 0$

(b) $|xy|_p = |x|_p|y|_p$

(c) $|x+y|_p \leq max\{|x|_p, |y|_p\}$, y si $|x|_p \neq |y|_p$ se da la igualdad. (Desigualdad ultramétrica)

Entonces es un valor absoluto no arquimediano.

Métrica p-ádica

Toda norma en un espacio induce una distancia, entonces sea la siguiente definición:

Proposición 4.
Se define en $\mathbb{Q}$ la **métrica p-ádica** , como $d_p(x, y) = |x - y|_p$.

Y recordemos la **definición 1.**

Definición 1. El campo de los números p-ádicos $\mathbb{Q}_p$ extiende al campo de los números racionales $\mathbb{Q}$ respecto a la norma p-ádica $|\cdot|_p$

Nuestro primo 3

Observemos como se ven estas definiciones utilizando nuestro primo 3.

La **norma 3-ádica** se define como $|x|_3 = 3^{-v_3(x)}$.

Por ejemplo:

- $|18|_3 = 3^{-v_3(18)} = 3^{-2} = \frac{1}{9}$.
- $|27|_3 = 3^{-v_3(27)} = 3^{-3} = \frac{1}{27}$.
- $|5|_3 = 3^{-v_3(5)} = 3^{-0} = 1$.
- $|\frac{1}{3}|_3 = 3^{-v_3(\frac{1}{3})} = 3^{-(-1)} = 3$.

La **métrica 3-ádica** , se define como $d_3(x, y) = |x - y|_3$.

Por ejemplo:

- $d_3(27 - 18) = |27 - 18|_3 = |9|_3 = 3^{-v_3(9)} = 3^{-2} = \frac{1}{9}$.

Lema 1.
El campo de los racionales $\mathbb{Q}$ no es completo respecto a ningún valor absoluto no trivial.

Definición 4.
Sea $|\cdot|_p$ un valor absoluto no arquimediano sobre $\mathbb{Q}$. Entonces sea $\mathcal{C}$ el conjunto de todas las sucesiones de Cauchy en $\mathbb{Q}$ con respecto a $|\cdot|_p$.

Definamos...

Definición 5.
Una sucesión (x_n) en un espacio métrico (X, d_p) es de Cauchy si:

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N} \text{ tal que } \forall m, n > N,\ d_p(x_n, x_m) < \varepsilon.$$

Proposición 5.
$\mathcal{C}$ es un anillo conmutativo unitario.

Proposición 6.
El conjunto

$$\mathcal{N} := \{(x_n) \in \mathcal{C} : \lim_{n\to\infty} |x_n|_p = 0\}$$

es un ideal maximal de $\mathcal{C}$.

Definición 6.
Definimos al campo de los números p-ádicos como el cociente del anillo $\mathcal{C}$ con el ideal maximal $\mathcal{N}$, es decir, $\mathbb{Q}_p = \mathcal{C}/\mathcal{N}$.

Teorema 1.
Para cada primo p, existe un campo $\mathbb{Q}_p$ con un valor absoluto no arquimediano $|\cdot|_p$ tal que:

(i) Existe una inclusión $\mathbb{Q} \to \mathbb{Q}_p$ y el valor absoluto inducido por $|\cdot|_p$ sobre $\mathbb{Q}$ por la inclusión coincide con el valor absoluto p-ádico;

(ii) La imagen de $\mathbb{Q}$ bajo la inclusión es densa en $\mathbb{Q}_p$ con respecto al valor absoluto $|\cdot|_p$;

(iii) $\mathbb{Q}_p$ es completo con respecto al valor absoluto $|\cdot|_p$.

El campo $\mathbb{Q}_p$ satisfaciendo (i), (ii) y (iii) es el único salvo isomorfismo que preserva los valores absolutos.

Enteros p-ádicos

Ahora exploremos al campo $\mathbb{Q}_p$...

Lema 2.
Para cada $x \in \mathbb{Q}_p \setminus \{0\}$ existe un entero $v_p(x) = n$ tal que $|x|_p = p^{-n}$.
Es decir, la valuación p-ádica v_p se extiende a $\mathbb{Q}_p$.

Definición 7.
El anillo de los enteros p-ádicos esta definido como:

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

Proposición 7.
El anillo de los enteros p-ádicos $\mathbb{Z}_p$ es un anillo local cuyo ideal maximal es $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}$. Además:

(i) $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \in \mathbb{Q} : p \text{ no divide a } b \right\}$.

(ii) La imagen de la inclusión $\mathbb{Z} \to \mathbb{Z}_p$ es densa.

(iii) Para cualquier $x \in \mathbb{Z}_p$ existe una sucesión de Cauchy (α_n) que converge a x y que verifica las siguientes propiedades:

a) $\alpha_n \in \mathbb{Z}$ satisface $0 \leq \alpha_n \leq p^n - 1$;

b) para todo $n \geq 2$ tenemos $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$.

Bajando al nivel de los elementos

Bajemos al nivel de los elementos, para el campo $\mathbb{Q}_p$ y el anillo de enteros $\mathbb{Z}_p$.

Corolario 1.
Todo $x \in \mathbb{Z}_p$ puede expresarse como

$$x = b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots ,$$

donde $0 \leq b_i \leq p-1$ y esta representación es única.

Corolario 2.
Todo $x \in \mathbb{Q}_p$ puede expresarse de la forma

$$x = b_{-m} p^{-m} + \cdots + b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots = \sum_{n=-m}^{\infty} b_n p^n,$$

donde $0 \leq b_i \leq p-1$ y $-m = v_p(x)$. Además, esta representación es única.

Nuestro primo 3

Observemos la representación 3-ádica de los números con los que hemos trabajado.

- 18: La representación 3-ádica es $\ldots 00200_3$.

$$18 = 2 \cdot 3^2 = \cdots + 0 \cdot 3^3 + 2 \cdot 3^2 + 0 \cdot 3^1 + 0 \cdot 3^0$$

- 27: La representación 3-ádica es $\ldots 001000_3$.

$$27 = 3^3 = \cdots + 0 \cdot 3^4 + 1 \cdot 3^3 + 0 \cdot 3^2 + 0 \cdot 3^1 + 0 \cdot 3^0$$

- 5: La representación 3-ádica es $\ldots 00012_3$.

$$5 = 1 \cdot 3^1 + 2 \cdot 3^0 = \cdots + 0 \cdot 3^3 + 0 \cdot 3^2 + 1 \cdot 3^1 + 2 \cdot 3^0$$

Donde estos son enteros 3-ádicos, pues cumplen con la definición de no contener potencias negativas de 3.

Nuestro primo 3

Ahora observemos la representación de un número no entero 3-ádico.

- $\frac{1}{3}$: La representación 3-ádica es $\ldots 000.1_3$.

$$\frac{1}{3} = 1 \cdot 3^{-1} = \cdots + 0 \cdot 3^1 + 0 \cdot 3^0 + 1 \cdot 3^{-1}$$

Pequeña y rápida visualización

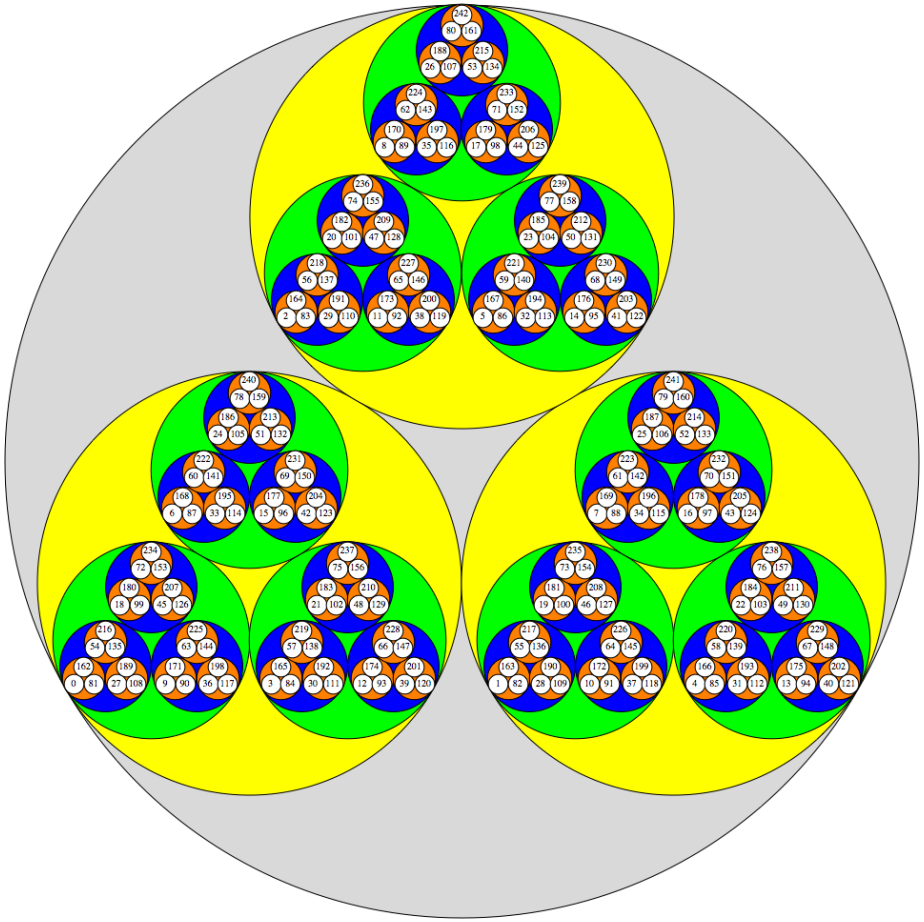

Figure: Números 3-ádicos

Algunos resultados

Por último, veamos algunas propiedades y resultados de $\mathbb{Q}_p$ y $\mathbb{Z}_p$:

- $\mathbb{Z}$ es denso en $\mathbb{Z}_p$.
- $\mathbb{Q}_p$ se define como el cuerpo de cocientes del anillo $\mathbb{Z}_p$. Es decir $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$.
- $\mathbb{Q}_p$ es un espacio topológico de Hausdorff localmente compacto y totalmente disconexo.
- Las unidades de $\mathbb{Z}_p$ son:
$$\mathbb{Z}_p^\times := \{x \in \mathbb{Z}_p : |x|_p = 1\}$$
- Tanto $\mathbb{Z}_p$ como $\mathbb{Q}_p$ son no numerables y poseen la cardinalidad del continuo.

Referencias

- Hubbard. C. M. (2023). Introducción a los números p-ádicos. Repositorio institucional de la Universidad de La Laguna.

- Beshenov, A. (2018). Introducción a los números p-ádicos. CADADR. Números p-ádicos.

- Lafuenre, R. (2008). Los números p-ádicos y el Teorema de Hasse-Minkowski. Universidad Nacional de La Plata. Números p-ádicos.

¿Preguntas?

¡Gracias por su atención!