# O que são os números p-ádicos e como fazer cálculo sobre eles

Enno Nagel *

Estas notas acompanham a minha palestra sobre "Os números p-ádicos e como fazer cálculo sobre eles" ministrada no dia 10 de maio de 2013 na Universidade Federal do Rio de Janeiro.

## Sumário



*Instituto de Matemática da Universidade Federal de Alagoas, Maceió

# 1 Números p-ádicos

## .. diretamente via a norma p-ádica

Uma *norma* sobre os números racionais $\mathbb{Q}$ é uma aplicação $\|\cdot\|\colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ tal que

(i) $\|x\| = 0 \iff x = 0$,

(ii) $\|xy\| = \|x\|\|y\|$, e

(iii) $\|x + y\| \leq \|x\| + \|y\|$.

**Teorema 1.1** (Ostrowsi). *Toda norma sobre $\mathbb{Q}$ é equivalente à norma usual $|\cdot|$ ou a uma norma p-ádica $|\cdot|_p$ para um número primo $p$.*

A seguir definimos $p$ por um número primo. Os números p-ádicos foram introduzidos há cerca de cem anos por Kurt Hensel. A invenção é relativamente recente em comparação aos números reais. Isto é devido à natureza contra-intuitiva da valorização $p$-ádica $|\cdot|_p$ que mede quantas vezes $p$ aparece na fatoração de um número inteiro (e contra-intuitivamente *diminui* quando a potência de $p$ *cresce*).

**Definição**. Seja $a \in \mathbb{Z}$. Pomos $|a|_p = 1/p^e$ se $a = a'p^e$ onde $p$ não divide $a'$.

*Nota.* A contra-intuição da norma p-ádica $|\cdot|_p$ é revelada pelo fato que ela é *não-arquimediana*, isto é $|1 + \cdots + 1| \leq 1$.

Esta norma estende-se multiplicativamente aos números racionais $\mathbb{Q}$. Conforme a $\mathbb{R}$, que consiste de todos os limites em $\mathbb{Q}$ com relação à valorização $|\cdot|$, declaramos analogamente:

**Definição**. Os *números p-ádicos* $\mathbb{Q}_p$ são o completamento de $\mathbb{Q}$ relativamente à norma $|\cdot|_p$.

## .. explicitamente via a expansão p-ádica

Analogamente à expansão decimal de um número real

$$a_0 + a_1 10^{-1} + a_2 10^{-2} + \cdots,$$

os números p-ádicos têm uma *expansão p-ádica.*

**Proposição 1.2.** *Os números p-ádicos se escrevem de maneira única*

$$\sum_{i \geq -\mathrm{N}} a_i p^i = a_{-\mathrm{N}} p^{-\mathrm{N}} + \cdots + a_0 + a_1 p^1 + a_2 p^2 + \cdots \quad \text{com } a_i \in \{0, \ldots, p-1\}.$$

Visto que as operações do corpo são contínuas com relação a topologia p-ádica, a multiplicação e adição são efetuadas naturalmente: O produto das expansões truncadas dos fatores converge ao produto das expansões inteiras.

**Exemplo**. (i) Tem-se $-1 = 111111\ldots$ em $\mathbb{Q}_2$. (Expansão binária.)

(ii) Tem-se $1/2 = 2^{-1}$ em $\mathbb{Q}_2$ e $1/2 = (p^n+1)/2 \to (0+1)/2 = 1/2$ em $\mathbb{Q}_p$ para $p > 2$.

*Nota.* Notamos duas diferenças com a expansão decimal dos números reais.

(i) Em todo número real há um sinal ± único. Observamos no exemplo acima que isto não vale para os números p-ádicos. Concluímos que $\mathbb{Q}_p$ não é ordenado.

(ii) Ao contrário, a expansão p-ádica é única. (Ao passo que $0,\bar{9} = 1$ em $\mathbb{R}$.)

A segunda observação é uma consequência da *desigualdade triangular forte* que enuncia $|x+y| \leq \max\{|x|, |y|\}$.

### .. topologicamente via o limite inverso

De fato, se expandirmos $a = \sum_{i \geq \mathrm{I}} a_i p^i$ e $b = \sum_{j \geq \mathrm{J}} b_j p^j$, então

$$|a-b|_p = p^{-\mathrm{K}} \text{ com K = primeiro índice } k \text{ onde } a \text{ e } b \text{ diferem.}$$

**Proposição**. *A bola de unidade*

$$\mathbb{Z}_p = \mathrm{B}_{\leq 1}(0) = \{x \in \mathbb{Q}_p : |x|_p \leq 1\} = \{\sum_{i \geq 0} a_i p^i : a_i \in \{0, \ldots, p-1\}\}$$

*em $\mathbb{Q}_p$ é um anel.*

*Demonstração:* Se $|x|, |y| \leq 1$, então $|x+y| \leq 1$ pela desigualdade triangular forte, isto é $\mathbb{Z}_p$ e fechado sob adição e então um anel. □

Segue um desenho da imagem da árvore binária de $\mathbb{Z}_2$. Descrição dos números binários, da norma e da distância e das bolas sobre eles. Esta descrição figurativa se manifesta na terceira descrição dos números p-ádicos, que torna suas propriedades topológicas mais claras.

**Proposição 1.3.** *Tem-se* $\mathbb{Z}_p = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$.

Vemos que duas bolas contêm-se ou são disjuntas, isto é $\mathbb{Q}_p$ é totalmente o. Todas estas diferenças, a desigualdade triangular forte e a topologia desconexa são uma consequência da propriedade de $|\cdot|$ sendo não-arquimediana. Chamamos um corpo completo $\mathbf{K}$ tal que a sua norma $|\cdot|$ é não-arquimediana de um *corpo não-arquimediano.*

## Notas algébricas

Como $\mathbb{Q}_p$ é completo as propriedades algébricas são de um ponto de vista da Teoria dos Números mais fáceis. Observamos que pela definição $\mathbb{Q} \subseteq \mathbb{Q}_p$ é denso e então $\mathrm{Aut}(\bar{\mathbb{Q}}_p) = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Notamos que ao contrário de $\mathbb{R} =$ completamento de $\mathbb{Q}$ por $|\cdot|$, onde $\#\,\mathrm{Gal}(\bar{\mathbb{R}}/\mathbb{R}) = \#\,\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = 2$, o grupo $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ é infinito.

Hasse popularizou esses números mostrando que algumas propriedades podem ser verificadas *localmente*, isto é se uma propriedade aritmética de um número $x \in \mathbb{Q}$ vale em todos os $\mathbb{Q}_p$ para $p$ qualquer, então vale em $\mathbb{Q}$ também.

Dado um polinômio $\mathrm{P} \in \mathbb{Z}[\mathrm{X}_1,\ldots,\mathrm{X}_d]$, o objetivo é, em vez de procurar soluções $\mathrm{P}(x) = 0$ nos números inteiros diretamente, procurá-las módulo $p^n$ para todos os números primos $p$ e $n \in \mathbb{N}$. Esta resolubilidade para todos $n \in \mathbb{N}$, é concisamente reformulada pelos números p-ádicos.

**Teorema 1.4.** *A congruência* $\mathrm{P}(x) \equiv 0 \bmod p^n$ *é resolúvel para todos* $n \in \mathbb{N}$ *se e tão-somente se* $\mathrm{P}(x) \equiv 0$ *é resolúvel em* $\mathbb{Z}_p$.

Agora resta a questão quando a resolubilidade *local*, isto é, em todos os $\mathbb{Q}_p$ para todos $p$ primos é suficiente para resolubilidade *global*, isto é em $\mathbb{Q}$. Isto não basta em geral, mas se valer, facilita a vida bastante. Tem-se o seguinte exemplo.

**Teorema** (Hasse-Minkowski). *Uma forma quadrática há um zero em* $\mathbb{Q}$ *se e tão-somente se há um zero em* $\mathbb{Q}_p$ *para todo* $p$ *assim como em* $\mathbb{R}$.

As propriedades algébricas mais fáceis de $\mathbb{Q}_p$ nos permitem a provar o teorema seguinte.

**Proposição**. *Uma forma quadrática de posto* $n \geq 5$ *sempre há um zero em* $\mathbb{Q}_p$.

**Corolário**. *Uma forma quadrática de posto* $n \geq 5$ *há um zero em* $\mathbb{Q}$ *se e tão-somente se ela tem um zero em* $\mathbb{R}$.

*Nota.* O teorema de Hasse-Minkowsi estende-se à classificação de formas quadráticas sobre $\mathbb{Q}$. Ou seja, duas formas $f$ e $g$ são equivalentes sobre $\mathbb{Q}$ se e tão-somente se eles são equivalentes sobre $\mathbb{Q}_p$ para todo $p$ assim como sobre $\mathbb{R}$.

Agora estas formas sobre estes corpos completos permitem uma parametrização concisa.

## 2 Cálculo

Recordemo-nos de que por causa da desigualdade triangular forte $\mathbb{Q}_p$ é topologicamente desconexo. Estudemos este fenômeno mais geralmente. Seja doravante $\mathbf{K}$ um tal corpo completo *não-Arquimediano.*

Por causa da topologia totalmente desconexa, haverá *nenhum* equivalente do Teorema do Valor Intermediário e portanto nem

- do Teorema do Valor Médio (TVM), e nem
- do Teorema Fundamental do Cálculo.

Estes dois teoremas estão no centro da Teoria de Cálculo. Duas consequências:

- TVM $\implies$ Diferenciabilidade parcial contínua implica Diferenciabilidade total
- Teorema Fundamental do Cálculo $\implies$ O espaço das funções diferençáveis é completo respeito à norma natural.

Observe abaixo em detalhes como contornar a falta do TVM no parágrafo seguinte.

### Funções diferençáveis sobre os números reais

Vejamos primeiro a situação clássica sobre $\mathbb{R}$. Seja $X \subseteq \mathbb{R}$ um intervalo aberto e $f : X \to \mathbb{R}$.

**Definição**. Uma função $f$ é $\mathscr{C}^1$ no ponto $x_0 \in X$ se

$$f'(x_0) = \lim_{x \to x_0} \frac{f(x) - f(x_0)}{x - x_0}$$

exista. Declaramos que $f$ é $\mathscr{C}^1$ se $f$ é $\mathscr{C}^1$ em todos os pontos $x_0 \in X$ e é contínua.

**Proposição 2.1.** *Seja* X *compacto. O espaço* $\mathscr{C}^1(\mathrm{X},\mathbb{R})$ *com a norma*

$$\|f\|_{\mathscr{C}^1} = \max\{\|f\|_{\sup}, \|f'\|_{\sup}\}$$

*é completo.*

*Demonstração:* A prova habitual usa o teorema fundamental do cálculo. □

Se $\mathbb{R}$ é substituído por um corpo **K** não-arquimediano, então esta proposição é incorreta. Por isso vamos mudar a definição de derivabilidade para este enuncio ficar correto. Portanto darei uma demonstração diferente da Proposição 2.1 acima que indica como podemos proceder neste caso.

**Proposição 2.2.** *A função* $f \in \mathscr{C}^1(\mathrm{X},\mathbb{R})$ *se e tão-somente se a função*

$$f^{]1[}(x,y) = \frac{f(x) - f(y)}{x - y},$$

*definida para todos* $x, y \in \mathrm{X}$ *desiguais, estende-se a uma função* $f^{[1]} \colon \mathrm{X} \times \mathrm{X} \to \mathbb{R}$ *contínua.*

*Demonstração:* A direção $\Longleftarrow$ é fácil. Na outra direção, se $(x,y) \to (a,a) \in \mathrm{X}\times\mathrm{X}$. Então

$$f^{]1[}(x,y) = f'(\xi) \to f'(a) = f^{[1]}(a,a) \quad \text{com } \xi \in [x,y]$$

onde a primeira igualdade provém do Teorema do Valor Médio e a segunda da continuidade de $f'$. Logo $f^{[1]}$ é contínua em todos os pontos, pois $f^{]1[}(\{(x,y) \in \mathrm{X} \times \mathrm{X} : x \neq y)$ é denso em $f^{[1]}(\mathrm{X} \times \mathrm{X})$. □

**Corolário.** *Seja* X *compacto. O espaço* $\mathscr{C}^1(\mathrm{X},\mathbb{R})$ *é completo.*

*Demonstração:* Como visto acima pelo Teorema do valor médio, a norma $\|f\| = \max\{\|f\|_{\sup}, \|f^{[1]}\|_{\sup}\}$ é igual a norma

$$\|f\|_{\mathscr{C}^1} = \max\{\|f\|_{\sup}, \|f'\|_{\sup}\}.$$

Então, quanto à primeira norma, esta proposição é evidente. □

## Funções $r$-vezes diferençáveis sobre espaços $p$-ádicos vetoriais

### Definição da diferenciabilidade de grau 1.

Visto que não há o teorema do valor intermediário com todas suas consequências, em particular o teorema do valor médio usado na prova da Proposição 2.2 acima, propõe-se a definição seguinte para obter um equivalente da Proposição 2.1:

**Definição** (para compensar o Teorema do Valor Médio ausente). Sejam $\mathrm{X} \subseteq \mathbf{K}$ aberto e $f\colon \mathrm{X} \to \mathbf{K}$. Então $f$ é $\mathscr{C}^1$ no ponto $a \in \mathrm{X}$ se o limite

$$\lim_{(x,y)\to(a,a)} f^{]1[}(x,y) \quad \text{com } f^{]1[} = \frac{f(x)-f(y)}{x-y} \quad \text{para } x,y \text{ diferentes}$$

existe. Então $f$ é $\mathscr{C}^1$ se $f$ é $\mathscr{C}^1$ em todos os pontos $a \in \mathrm{X}$ ou igualmente se $f^{]1[}$ estende a uma função $f^{[1]}$ contínua.

Ora fica a questão de como iterar a noção de diferenciabilidade: Como definir uma função *duas* vezes diferençável? Observemos que ora $f^{[1]}$ é uma função em duas variáveis (ao contrário da função $f'$ no caso real!) assim que não podemos iterar esta definição diretamente.

Logo, é necessário tratar o caso de múltiplas variáveis para definir a diferenciação iterada de uma função já de uma variável só: Recordemo-nos da definição de uma função derivável sobre espaços vetoriais normados:

**Definição**. Sejam V e $\mathbf{E}$ espaços vetoriais, $\mathrm{X} \subseteq \mathrm{V}$ aberto e $f\colon \mathrm{X} \to \mathbf{E}$. Então $f$ é $\mathscr{C}^1$ no ponto $a \in \mathrm{X}$ se existe uma aplicação linear contínua A tal que para todos $\varepsilon > 0$ existe $\mathrm{U} \ni a$ aberto em X tal que

$$f(x+h) - f(x) = \mathrm{A}\cdot h + \mathrm{R}(x+h,x)$$

onde o resto satisfaz $\|\mathrm{R}(x+h,x)\| \leq \varepsilon\|h\|$ para todos $x+h, x \in \mathrm{U}$.

### Diferenciabilidade iterada.

Esta definição não rende diretamente uma definição de diferenciabilidade geral, mas indica como proceder em geral:

**Definição** (da Diferenciabilidade Parcial Simultânea). Sejam $\mathrm{V}, \mathbf{E}, \mathrm{X} \subseteq \mathrm{V}$ e $f\colon \mathrm{X} \to \mathbf{E}$ como acima e tenha V coordenadas, isto é, $\mathrm{V} = \mathbf{K}^d$ com $e_1, \ldots, e_d$ a base natural. Então $f$ é $\mathscr{C}^1$ se para todos $x+h, x \in \mathrm{X}$ com $h \in \mathbf{K}^{*d}$ a função $f^{]1[}(x+h,x)$ definida por

$$(x+h,x) \mapsto \mathrm{A} \in \mathrm{Hom}_{\mathbf{K}}(\mathrm{V},\mathbf{E})$$

com

$$\mathrm{A}\cdot h_k e_k = f(x + h_1e_1 + \cdots + h_{k-1}e_{k-1} + h_ke_k) - f(x + h_1e_1 + \cdots + h_{k-1}e_{k-1})$$

estende-se a uma função contínua $f^{[1]}\colon \mathrm{X}\times\mathrm{X} \to \mathrm{Hom}_{\mathbf{K}}(\mathrm{V},\mathbf{E})$.

Notemos que $\mathrm{X}\times\mathrm{X} \subseteq \mathrm{V}\times\mathrm{V}$ é novamente um espaço vetorial com coordenados naturais e $\mathrm{im}\, f \subseteq \mathrm{Hom}_{\mathbf{K}}(\mathrm{V},\mathbf{E})$ também é novamente um espaço vetorial de dimensão finita.

**Definição**. Dizemos que $f\colon \mathrm{X} \to \mathbf{E}$ é $\mathscr{C}^2$ se $f$ é $\mathscr{C}^1$ e $f^{[1]}\colon \mathrm{X}\times\mathrm{X} \to \mathrm{Hom}_{\mathbf{K}}(\mathrm{V},\mathbf{E})$ é $\mathscr{C}^1$. Geralmente, $f$ é $\mathscr{C}^n$ se $f$ é $\mathscr{C}^{n-1}$ e $f^{[n-1]}$ é $\mathscr{C}^1$.

Com esta definição concluída podemos compreender melhor as propriedades destas funções. Pois esta definição é complicada e não tínhamos até este momento muita teoria sobre a diferenciabilidade, mesmo a verificação das propriedades naturais exige muita atenção.

Generalizei esta definição a $\mathscr{C}^r$-funções, funções $r$-vezes diferençáveis para $r \in \mathbb{R}_{\geq 0}$ em [Nag11] e verifiquei que elas satisfazem, como esperado, muitas propriedades naturais. Mostrei igualmente que esta definição complicada permite uma descrição muito mais direta em vários casos.

## 3 A base de Mahler

Seja $\mathbf{E}$ um corpo completo não-arquimediano e $\mathbf{o}_{\mathbf{E}} = \{x \in \mathbf{E} \mid |x| \leq 1\}$ o seu anel de inteiros. Denotem

$$\mathscr{C}^0(\mathbb{Z}_p) = \{ \text{ todas as funções contínuas } f\colon \mathbb{Z}_p \to \mathbf{E}\},$$

e

$$\mathscr{D}^0 = \{ \text{ todas as formas lineares contínuas } \int\colon \mathscr{C}^0(\mathbb{Z}_p) \to \mathbf{E}\}.$$

Como $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, segue de um fato geral que $\mathscr{D}(\mathbb{Z}_p) = \mathbf{E}\otimes_{\mathbf{o}_{\mathbf{E}}}\varprojlim \mathbf{o}_{\mathbf{E}}[\mathbb{Z}/p^n\mathbb{Z}]$. Então observamos que

$$\bigcup_{n\in\mathbb{N}} \mathbf{E}[\mathbb{Z}/p^n\mathbb{Z}] = \{ \text{ as funções localmente constantes } \}$$

são densas em $\mathscr{C}^0(\mathbb{Z}_p)$. Por conseguinte obtemos dualmente, lembrando que uma forma linear sendo contínua se e tão-somente se é limitada, que

$$\mathscr{D}^0(\mathbb{Z}_p) = \mathbf{E} \otimes_{\mathbf{o}_{\mathbf{E}}} \varprojlim \mathbf{o}_{\mathbf{E}}[\mathbb{Z}/p^n\mathbb{Z}] =: \mathbf{E} \otimes_{\mathbf{o}_{\mathbf{E}}} \mathbf{o}_{\mathbf{E}}[[\mathbb{Z}_p]].$$

Visto que $\mathbb{Z}_p$ é topologicamente cíclico, gerado pelo elemento $\mathbf{1}$ por exemplo, obtemos o *isomorfismo de Iwasawa*

$$\begin{aligned} \mathbf{o}_{\mathbf{E}}[[\mathbb{Z}_p]] &\xrightarrow{\sim} \mathbf{o}_{\mathbf{E}}[[\mathrm{X}]] \\ \mathbf{1} &\mapsto \mathrm{X} - 1. \end{aligned}$$

Concluímos

$$\mathbf{E} \otimes \mathbf{o}_{\mathbf{E}}[[\mathrm{X}]] \xrightarrow{\sim} \mathscr{D}(\mathbb{Z}_p).$$

Pela dualidade de Schikhof,

$$\begin{aligned} c_0(\mathbb{N}) &\xrightarrow{\sim} \mathscr{C}^0(\mathbb{Z}_p) \\ e_n &\mapsto \binom{x}{n}, \end{aligned}$$

onde $c_0(\mathbb{N})$ denote as sequências que convergem a zero, $e_n$ a seqüência cuja única coordenada não-nula é 1 na posição $n$, e onde $\binom{x}{n} = x(x-1)\cdots(x-n)/n!$ é o coeficiente binomial como função sobre $\mathbb{Z}_p$. Sob este isomorfismo natural, a imagem de $\mathscr{C}^r(\mathbb{Z}_p) \subseteq \mathscr{C}^0(\mathbb{Z}_p)$ permite a descrição concisa seguinte:

**Teorema 3.1.** *Tem-se o isomorfismo*

$$c_r(\mathbb{N}) = \{(a_n) \colon |a_n| n^r \to 0\} \xrightarrow{\sim} \mathscr{C}^r(\mathbb{Z}_p).$$

*Isto é, uma função $f : \mathbb{Z}_p \to \mathbf{E}$ é $r$-vezes diferençável se e tão-somente se $f(x) = \sum a_n \binom{x}{n}$ com $|a_n| n^r \to 0$.*

## Referências


[Nag11] E. Nagel, *Fractional non-Archimedean differentiability*, Univ. Münster, Mathematisch-Naturwissenschaftliche Fakultät (Diss.), 2011. zbMATH 1223.26011. Confer http://nbn-resolving.de/urn:nbn:de:hbz:6-75409405856.