Universidade Federal de Minas Gerais

Instituto de Ciências Exatas

Departamento de Matemática

Introdução aos números p-ádicos

Célio da Silva Cardoso

março de 2013

Agradeço aos meus filhos Felipe de 10 anos, Gabriela de 3 anos e à minha esposa que teve muita paciência nestes longos anos.
Gostaria de agradecer também a minha Professora Orientadora Cristina Marques, pela paciência e dedicação, pois sem seu apoio, esta monografia não terminaria.
Aos colegas Samantha Faasen ,Iã Faasen, Rana Faasen, Andréia, Decarte e Adailton que incentivaram a continuar os estudos.

1 Introdução

Nesta monografia faremos uma breve indrodução aos números p-ádicos. Veremos como eles surgiram e depois faremos sua definição formal. A idéia é indroduzir novas métricas no corpo dos racionais $\mathbb{Q}$ e de considerar seus completamentos. O mais interessante é que essa métrica está ligada a um número primo p e assim teremos informações aritméticas e topológicas.

Assim, toda a teoria de Cálculo pode ser apresentada nos corpos p-ádicos. O que muda aqui é como medimos nos racionais. Vários exemplos são apresentados na monografia.

Sumário

2 Como surgiram os números p-ádicos?

2.1 Um pouco de História

Os números p-ádicos foram introduzidos por Kurt Hensel, um matemático que nasceu na Prússia, na cidade que hoje tem o nome de Königsberg. Estudou matemática em Berlim e teve professores famosos como **Lipschitz, Weierstrass, Helmhotz** e especialmente **Kronecker**, o qual muito o influenciou. Seus trabalhos seguiram os mesmos caminhos de seu mestre, a saber desenvolvimento da arítmética no corpo dos números algébricos.

Em, 1897 utilizando o método de **Weierstrass** no desenvolvimento em séries de potências para funções algébricas descobriu que podia fazer uma analogia e daí surgiram números p-ádicos. Hensel fez uma analogia entre os irredutíveis de $\mathbb{C}[x]$ e os de $\mathbb{Z}$ dos inteiros, a saber $(x-a) \in \mathbb{C}[x]$ e os primos p inteiros.

Os números p-ádicos podem também ser considerados como completamento dos números racionais com uma métrica diferente do valor absoluto, a qual dá origem aos números reais.

A invenção de Hensel conduziu ao desenvolvimento de um campo pouco explorado pelos matemáticos da época e com grande repercussão. Os números p-ádicos são requisitados na obtenção de raízes de polinômios nos anéis mod$p$. Este é o famosso princípio local- global(veja [God] H. Godinho) , dado um polinômio com coeficientes em $\mathbb{Z}$ é bastante fácil obter raízes nos números p-ádicos e como este conjunto contém $\mathbb{Q}$, acabamos determinando as raízes do polinômio.

Em 1921, utilizando os números p-ádicos **Hasse e Minkowski** formulou o princípio local- global para formas quadráticas, dando um grande passo. Eles mostraram que para formas quadráticas, um polinômio

$$F(x_1, x_2, \ldots, x_n, \ldots)$$

homogeneo de grau dois apresenta soluções não triviais nos racionais se e somente se apresentar soluções nos números p-ádicos.

Hensel foi professor na Universidade de Marburg até a sua aposentadoria. Deste 1901 era diretor do jornal "Crelle"um famoso e prestígioso jornal da época.

Os números p-ádicos não se limitam a teoria dos números, hoje ele é empregado na física, química, geometria e recentemente na criptografia. Na física, os chamados vidros de spin, que apresentam partículas magnetizadas(veja [Dan] Daniel Barsky). Estas, por serem magnetizadas são desorganizadas estruturalmente e uma maneira de minimizar as interações magnéticas é ajustar e controlar as partículas em um ambiente controlado, na chamada "técnica das réplias"(copia das partículas). Esta técnica consiste em considerar n amostras idênticas, determinar a energia de interação magnética e anular os efeitos fazendo-os tender a zero. Tal técnica equivale a considerar uma série de números inteiros p-ádicos que tenda p-adicamente a zero, para todos os primos p do explorador de saída de quadriculação.

Também na física relativista, temos vários exemplos, e um dos mais notáveis consiste em utilizar os números p-ádicos na teoria de Plank. Os físicos teóricos investigam sobre a estrutura do espaço e tempo em pequena escala. Pelas leis da relatividade e da física quântica indicam que é impossível medir distâncias inferiores a chamada longitude de Plank, de ordem de 10^{-35} metros. A existência de uma distância mínima sugere possibilidade de que, a última estrutura do tempo e espaço pode ser descrita não em termos da estrutura dos números reais, mas nos termos da estrutura p-ádica.

2.2 Procurando zeros de polinômios

Suponha que queremos resolver equações do tipo

$$f(x) \equiv 0 \qquad \mod p^e \tag{1}$$

onde f é um polinômio com coeficientes inteiros e p um primo qualquer, isto é, queremos achar as raízes de f nos anéis $\frac{\mathbb{Z}}{p^e\mathbb{Z}}$ para todo natural e . Observe que toda solução da equação acima com $e > 1$ é

também solução para $e = 1$, mas a recíproca é falsa.

Uma classe mod p origina p classes mod p^2. Com efeito, seja $\overline{a} \in \frac{\mathbb{Z}}{p\mathbb{Z}}$; podemos escrevê-la na forma $\overline{a} = a + tp$ com $t \in \mathbb{Z}$ e $0 \leq a \leq p-1$. Aplicando o algoritmo de Euclides temos $t = qp + r$ com $o \leq r \leq p-1$ e as classes $\overline{\overline{a}} = a + (qp + r)p = a + rp + qp^2 = a + rp \mod p^2$ onde $o \leq r \leq p-1$.

Em $\frac{\mathbb{Z}}{3\mathbb{Z}}$, por exemplo, a classe $\overline{2} \in \frac{\mathbb{Z}}{3\mathbb{Z}}$ dá origem às classes $\overline{\overline{2}}, \overline{\overline{5}}$ e $\overline{\overline{8}}$ em $\frac{\mathbb{Z}}{9\mathbb{Z}}$.

Para fixarmos melhor as idéias, vamos tentar resolver a seguinte equação de congruência.

Exemplo 2.1.

$$x^2 \equiv 2 \mod 7^e \tag{2}$$

para todo número positivo e $\in \mathbb{N}$.

Começaremos encontrando as soluções mod 7, e depois as soluções mod 7^2 e assim sucessivamente. Por substituição direta, vemos que em $\frac{\mathbb{Z}}{7\mathbb{Z}}$, as classes 3 e $-3 \equiv 4$ são soluções de (2) $(mod\ 7)$.

Escrevendo $x_1 = 3 + 7t$ (o mesmo para $y_1 = -3 + 7t$) e substituindo em (2) temos:

$$\begin{array}{ccc} \overline{3}^2 & \equiv & 2 \quad em \frac{\mathbb{Z}}{7^2\mathbb{Z}} \\ (3+7t)^2 & \equiv & 2 \mod 7^2 \\ 3^2 + 2.3.7t & \equiv & 2 \mod 7^2 \\ 7 + 2.3.7t & \equiv & 0 \mod 7^2 \\ 7(1 + 2.3.t) & \equiv & 0 \mod 7^2 \\ 1 + 2.3.t & \equiv & 0 \mod 7 \\ 6t & \equiv & -1 \mod 7 \\ (-1)t & \equiv & -1 \mod 7 \\ t & \equiv & 1 \mod 7 \end{array}$$

Escrevendo $t = 1 + 7k$ e $x_2 = 3 + 7 \cdot (1 + 7k) = 3 + 7 \cdot 1 + 7^2 \cdot k$ temos que x_2 é uma solução (mod 7^2) de (2) onde $k \in \mathbb{Z}$. Analogamente, para $e = 3$, substituindo x_2 em (2) obtemos:

$$\begin{array}{ccc} x_2^2 & \equiv & 2 \mod 7^3 \\ (3 + 7.1 + 7^2.k)^2 & \equiv & 2 \mod 7^3 \\ 10^2 + 2.10.7^2.k & \equiv & 2 \mod 7^3 \\ 98 + 98.10k & \equiv & 0 \mod 7^3 \\ 2 + 20.k & \equiv & 0 \mod 7^1 \\ 6k & \equiv & -2 \mod 7 \\ -k & \equiv & -2 \mod 7 \\ k & \equiv & 2 \mod 7 \end{array}$$

Escrevendo $k = 2 + 7k_1$ teremos $x_3 = 3 + 7 \cdot 1 + 7^2(2 + 7 \cdot k_1) = 3 + 7 \cdot 1 + 7^2 \cdot 2 + 7^3 \cdot k_1$ é uma solução (mod 7^3) da equação (2).

Repetindo este raciocínio obtemos $x_4 = 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 7^4 \cdot k_2$ e assim obtendo algo do tipo:

$$\xi = 3 + 1 \cdot 7^1 + 2 \cdot 7^2 + 6 \cdot 7^3 + 6 \cdot 7^4 + ... \tag{3}$$

a qual é uma soma que parece infinita e é solução da equação (2) . E mais, esta solução foi surgindo através do aparecimento da sequência de inteiros

$$\{x_1, x_2, x_3, ...\}$$

que satisfaz:

$$\begin{cases} x_1 & \equiv & 3 & mod\ 7 \\ x_n & \equiv & x_{n-1} & mod\ 7^n \\ x_n^2 & \equiv & 2 & mod\ 7^{n+1} \end{cases}$$

Este ξ nos faz lembrar de dízimas periódicas e não periódicas que surgem quando procuramos solução da equação $x^2 = 2$ em $\mathbb{Q}$, a saber, para acharmos uma solucão de $x^2 = 2$ em $\mathbb{Q}$ nós vamos testando uma sequência de racionais, a saber:

$$1, \quad 1,4 \quad 1,41 \quad 1,414 \quad 1,4142, \quad \ldots$$

cujos quadrados são:

$$1, \quad 1,96 \quad 1,9881 \quad 1,999396 \quad 1,99996164, \ \ldots \tag{4}$$

Continuando nesse processo conseguimos obter números racionais cujos quadrados ficam tão próximos de 2 como quisermos (aqui próximo significa que a diferença entre eles tem valor absoluto praticamente nulo) e acabamos achando um decimal do tipo $1,41421356237309504880\ldots$. Essas considerações nos levaram a " estender $\mathbb{Q}$ "incluindo todos os decimais e não apenas os periódicos. E asim foi criado o conjunto dos números reais.

Voltando ao nosso problema (1) e fazendo uma analogia com os números reais, queremos criar um ambiente onde nosso ξ faça sentido. Queremos " expandir $\mathbb{Q}$ "incluíndo os " números "da forma:

$$\xi = 3 + 7 \cdot 1 + 7^2 \cdot 2 + 7^3 \cdot 6 + \ldots$$

que apareceram na solução da equação $x^2 \equiv 2 \mod 7^n$. Observe que em $\mathbb{Q}$ tal equação não tem solução e que com o valor absoluto $|\ |$ normal de $\mathbb{Q}$ a série ξ não converge.

Considere agora um outro exemplo de equação de congruência que apresenta uma solução em $\mathbb{Q}$, como por exemplo:

Exemplo 2.2.

$$x^2 \equiv 81 \pmod{7^n}, \tag{5}$$

para todo natural n.

A equação acima nos racionais apresentam soluções 9 e -9 . Utilizando o mesmo processo anterior para resolver a equação de congruência (5), começaremos encontrando soluções $\mod 7$ depois $\mod 7^2$, $\mod 7^3$, e assim sucessivamente.

Percebemos que $x_0 = 9 \equiv 2$ e $y_0 = -9 = -2 \equiv 5$ são soluções da equação $x^2 \equiv 81 \pmod{7^n}$, para $n = 1$. Escrevendo $x_1 = x_0 + t_1.7$,(o mesmo para $y_1 = y_0 + t_1.7$) a fim de obter $\mod 7^2$ e substituindo na equação temos:

$$\begin{array}{ccccc} (x_0 + t_1.7)^2 & \equiv & 81 & \mod 7^2 \\ (2 + 7t_1)^2 & \equiv & 81 & \mod 7^2 \\ 2^2 + 2.2.7t_1 & \equiv & 81 & \mod 7^2 \\ -77 + 2.2.7t_1 & \equiv & 0 & \mod 7^2 \\ 7(-11 + 2.2.t_1) & \equiv & 0 & \mod 7^2 \\ -11 + 2.2.t_1 & \equiv & 0 & \mod 7 \\ 4t_1 & \equiv & 4 & \mod 7 \\ t_1 & \equiv & 1 & \mod 7 \end{array}$$

$x_1 = 2 + 1.7$ e $y_1 = 5 + 5.7$ são soluções da equação $x^2 \equiv 81 \pmod{7^2}$, para $n = 2$. De maneira análoga podemos fazer $x_2 = x_0 + x_1.7 + t_2.7^2$ e substituindo na equação temos:

$$\begin{array}{ccccc}
(x_0 + x_1.7 + t_2.7^2)^2 & \equiv & 81 & \mod 7^3 \\
(2 + 7.1 + t_2.7^2)^2 & \equiv & 81 & \mod 7^3 \\
(9 + t_2.7^2)^2 & \equiv & 81 & \mod 7^3 \\
9^2 + 2.9.7^2.t_2 & \equiv & 81 & \mod 7^2 \\
81 + 2.9.7^2.t_2 & \equiv & 81 & \mod 7^2 \\
7^2(2.9.t_2) & \equiv & 0 & \mod 7^2 \\
18.t_2 & \equiv & 0 & \mod 7 \\
4t_2 & \equiv & 0 & \mod 7 \\
t_2 & \equiv & 0 & \mod 7
\end{array}$$

Assim $x_2 = 2 + 1.7 + 0.7^2$ e $y_2 = 5 + 5.7 + 6.7^2$ são soluções da equação $x^2 \equiv 81 \pmod{7^n}$, para $n = 3$. Continuando encontramos duas sequências:

$$\begin{cases}
x_0 & = 9 = 2 \\
x_1 & = 2 + 1.7 = 9 \\
x_2 & = 2 + 1.7 + 0.7^2 = 9 \\
x_3 & = 2 + 1.7 + 0.7^2 + 0.7^3 = 9 \\
x_4 & = 2 + 1.7 + 0.7^2 + 0.7^3 + 0.7^4 = 9 \\
x_5 & = 2 + 1.7 + 0.7^2 + 0.7^3 + 0.7^4 = 9 \\
x_6 & = 2 + 1.7 + 0.7^2 + 0.7^3 + 0.7^4 + 0.7^5 = 9 \\
\cdots & \cdots \\
\cdots & \cdots \\
\cdots & \cdots
\end{cases}$$

e

$$\begin{cases}
y_0 & = -9 = -2 = 5 \\
y_1 & = 5 + 5.7 = 40 \\
y_2 & = 5 + 5.7 + 6.7^2 = 334 \\
y_3 & = 5 + 5.7 + 6.7^2 + 6.7^3 = 2392 \\
y_4 & = 5 + 5.7 + 6.7^2 + 6.7^3 + 6.7^4 = 16798 \\
y_5 & = 5 + 5.7 + 6.7^2 + 6.7^3 + 6.7^4 + 6.7^5 = 117640 \\
y_6 & = 5 + 5.7 + 6.7^2 + 6.7^3 + 6.7^4 + 6.7^5 + 6.7^6 = 823534 \\
\cdots & \cdots \\
\cdots & \cdots \\
\cdots & \cdots
\end{cases}$$

Concluímos que na solução da equação $x^2 \equiv 81 \pmod{7^n}$ aparecem as sequencias:

$$\begin{cases}
2 \quad 9 \quad 9 \quad 9 \quad 9 \quad 9 \quad \ldots \\
\\
5 \quad 40 \quad 334 \quad 2392 \quad 16789 \quad 117640 \quad \ldots
\end{cases}$$

Existem certas propriedades nas duas sequencias de soluções acima:

1. Os termos das soluções que aparecem são “coerentes ”, ou seja :

$$x_n \equiv x_{n-1} \pmod{7^n}$$

$$y_n \equiv y_{n-1} \pmod{7^n}$$

2. Os termos das sequências x_n e y_n satisfazem :

$$x_n < 7^{n+1} \qquad e \qquad y_n < 7^{n+1}$$

3. Cada x_n é a expansão 7-ádica da classe do número em $\frac{\mathbb{Z}}{7^{n+1}\mathbb{Z}}$

Note que as potências de p aparecem naturalmente nas duas soluções da equação acima e que toda equação do tipo:

$$f(x) \equiv 0 \qquad mod\ p^e \tag{6}$$

onde p é primo e com e natural apresentam os mesmos tipos de solução. Isto nos levará a criar um valor absoluto especial nos racionais, isto é, " um novo processo de medir "no conjunto dos racionais . Valor absoluto este, tal que, quanto maior potencia de p o número tiver, menor será o número. Os números p-ádicos surgirão assim.

2.3 Usando o Método de Newton

Por outro lado, podemos também resolver as equações do tipo (6) usando aproximações sucessivas através do **Método de Newton** .

Começaremos com uma solução de (6) com $e = 1$ e a refinamos para uma soluçao para $e = 2$, logo depois para $e = 3$, etc., fazendo com que cada solução seja obtida da anterior. Este método é usado em cálculo e consiste em determinar aproximações cada vez melhores para uma solução da equação $f(x) = 0$, dada alguma aproximação inicial. O método de Newton é iterativo permitindo encontrar soluções de equações de congruência usando o desenvolvimento em Taylor de $f(x)$, de modo que as soluções mod p^e sejam obtidas a partir das de mod p^{e-1}

No caso clássico, nós temos uma aproximação real para uma solução ξ da equação $f(x) = 0$, onde vamos supor por simplicidade que f apresenta uma expansão de Taylor ao redor do ponto x_0 e que $f^{'}(x_0) \neq 0$. Nós tentamos estimar $\xi - x_0 = h$ por um valor aproximado de h, e então repetindo o argumento começando com $x_1 = x_0 + h$, nós temos:

$$0 = f(\xi) = f(x_0 + h) = f(x_0) + f^{'}(x_0).h + \frac{1}{2}.f^{''}(x_0).h^2 + \ldots, \tag{7}$$

e supondo x_0 próximo de ξ , $|h|$ será pequeno e os termos envolvendo $h^2, h^3, h^4, \ldots$ serão desprezados. Descartando tais termos, nós tomamos h como o número que satisfaz:

$$f(x_0) + f^{'}(x_0).h = 0,$$

desenvolvendo em função de h , temos:

$$h = -\frac{f(x_0)}{f^{'}(x_0)}$$

substituindo h em $x_1 = x_0 + h$, obtemos :

$$x_1 = x_0 - \frac{f(x_0)}{f^{'}(x_0)}$$

a qual é a **forma standard de Newton.**

A expansão de Taylor de um polinômio reduz a uma identidade algébrica finita:

$$f(x_0 + h) = f(x_0) + f^{'}(x_0).h + \frac{1}{2}.f^{''}(x_0).h^2 + \ldots + \frac{1}{n!}f^n(x_0).h^n \tag{8}$$

onde $n = grf$ e a $f^{'}(x) = \left(\sum^n a_k x^k\right)^{'} = \sum^n k a_k x^{k-1}$

Observe que estamos usando a definição de derivada formalmente e a identidade de Taylor não depende dos processos de limites para polinômios. Agora, o termo $c_j.x^j$ em $f(x)$ nos leva ao termo correspondente

$$\frac{j.(j-1).\ldots.(j-k+1)}{k!}.c_j x^{j-k} = \binom{j}{k}.c_j x^{j-k}$$

em $\frac{f^k(x)}{k!}$ e assim os coeficientes $\frac{f^k(x_0)}{k!}$ são coeficientes inteiros se $x_0 \in \mathbb{Z}$ e $f(x) \in \mathbb{Z}[X]$

Suponha que já achamos todas as soluções x_0 de $f(x) = 0 \pmod{p^e}$; podemos usar x_0 para achar uma ou mais soluções de $f(x) = 0 \pmod{p^{e+1}}$ supondo que tais soluções são aproximações melhores de x_0. Agora x_0 é realmente uma classe mod p^e, assim $\overline{x_0}$ consiste de todos os números da forma $x_0 + tp^e$, $t \in \mathbb{Z}$, e esta classe origina p classses $(\text{mod } p^{e+1})$. Desse modo, a questão é: quais t podem ser escolhidos de modo que

$$f(x_0 + t.p^e) \equiv 0 \qquad (\text{mod } p^{e+1})? \tag{9}$$

Em **(8)** nós fazemos $h = t.p^e$ e observamos que todas as potências de h maiores que um são $(0 \mod p^{e+1})$ e nós obtemos

$$f(x_0 + t.p^e) \equiv f(x_0) + f^{'}(x_0).t.p^e \qquad (\text{mod } p^{e+1})$$

Para que **(9)** aconteça, temos que escolher t de modo que

$$t.p^e.f^{'}(x_0) \equiv -f(x_0) \qquad (\text{mod } p^{e+1})$$

ou

$$t.f^{'}(x_0) \equiv \frac{-f(x_0)}{p^e} \qquad (\text{mod} p)$$

Esta é uma congruencia linear em t, a qual tem o seguinte número de soluções :

$$\begin{cases} 0 & \text{se} \quad p \Big| f^{'}(x_0) & \text{mas} & p^{e+1} \not| f(x_0) \\ p & \text{se} \quad p \not| f^{'}(x_0) & \text{e} & p^{e+1} | f(x_0) \\ 1 & \text{se} \quad p \not| f^{'}(x_0) & & \end{cases}$$

Note que $a.t = b$ em $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ tem solução $t = \frac{b}{a}$ se $a \neq 0$ pois $\frac{\mathbb{Z}}{p\mathbb{Z}}$ é um corpo e não apresentará solução caso não exista a^{-1}. Se $a = 0$ e $b = 0, t$ pode ser qualquer em $\frac{\mathbb{Z}}{p\mathbb{Z}}$ e portanto apresentará p soluções.

No primeiro caso, a solução x_0 no nível p^e não dará origem a soluções no nível p^{e+1}. No segundo caso, x_0 já era uma solução no nível p^{e+1} e todas as outras p que ele origina também serão. Nestes dois casos, caracterizados pelo fato de que $p \Big| f^{'}(x_0)$, x_0 é chamado de solução singular de (1). Uma solução x_0 é não singular de (1) quando $p \not| f^{'}(x_0)$ e esta originará a uma única solução x_1 de $f(x) \equiv 0 \pmod{p^{e+1}}$ dada por:

$$x_1 \equiv x_0 - \frac{f(x_0)}{f^{'}(x_0)} \qquad \text{mod } p^{e+1}$$

a qual é a analogia completa da **fórmula de Newton.**

O procedimento para resolver (1) com $e > 1$ deverá agora estar claro, se nós soubermos as soluções para $e = 1$. Cada uma dessas soluções iniciais gera 0,1 ou p soluções no nível p^2, cada uma dos quais por sua vez origina 0 , 1 ou p soluções no nível p^3 , e assim sucessivamente e todas as soluçoes podem ser achados resolvendo congruências linear $(\text{mod}p)$. Este é o caminho que embora pareça complicado, não é: se reduz a resolver (6) para $e = 1$.

Exemplo 2.3. *Queremos resolver a equação*

$$f(x) = x^3 - 4.x^2 + 5.x - 6 \equiv 0 \qquad (\text{mod } 3^e)$$

Com uma computação simples verificamos que $f(0) \equiv 0 \pmod 3$ e $x_0 = 0$ é a única solução da equação em $\frac{\mathbb{Z}}{3\mathbb{Z}}$. Tomando $x_1 = 0 + 3.t_1$ tentaremos encontrar soluções (mod p^2), ou seja, queremos determinar $t_1 \in \mathbb{Z}$ tal que:

$$f(0 + 3.t_1) \equiv 0 \qquad (\text{mod } 3^2)$$

Pelo algoritmo de Newton temos que encontrar as soluções da equação linear

$$\begin{array}{rcll} f^{'}(0).t_1 & \equiv & -\frac{f(0)}{3} & (\text{mod } 3^1) \\ (x^3 - 4.x^2 + 5.x - 6)^{'}(0)t_1 & \equiv & -\frac{-6}{3} & (\text{mod } 3^1) \\ 5.t_1 & \equiv & 2 & (\text{mod } 3^1) \\ t_1 & \equiv & 1 & (\text{mod } 3^1) \end{array}$$

Colocando $t_1 = 1 + 3.t_2$, obtemos $x_1 = 3 + 9.t_2$, e queremos obter $t_2 \in \mathbb{Z}$ de modo que:

$$f(3) + 9.t_2.f^{'}(3) \equiv 0 \qquad (\text{mod } 3^3)$$

ou melhor, resolver

$$f^{'}(3).t_2 \equiv -\frac{f(3)}{3^2} \qquad (\text{mod} 3)$$

desenvovendo obtemos:

$$2.t_2 \equiv 0 \qquad (\text{mod} 3)$$

obtemos então :

$$t_2 \equiv 0 \qquad (\text{mod} 3)$$

Continuando com o processo obtemos uma solução do tipo :

$$\begin{array}{rcl} x_0 & = & 0 \\ x_1 & = & 0 + 1.3^1 \\ x_2 & = & 0 + 1.3^1 + 0.3^2 \\ x_3 & = & 0 + 1.3^1 + 0.3^2 + 0.3^3 \\ x_4 & = & 0 + 1.3^1 + 0.3^2 + 0.3^3 + 0.3^4 \\ x_5 & = & 0 + 1.3^1 + 0.3^2 + 0.3^3 + 0.3^4 + 0.3^5 \end{array}$$

Exemplo 2.4. *Resolver a equação*

$$f(x) = 3x^5 - 10x^4 + 3x^3 - 2x - 1 \equiv 0 \qquad (\text{mod } 7^e)$$

Verificamos que $f(0) \equiv -1 \pmod 7$ e $x_0 = 1$ é a única solução da equação em $\frac{\mathbb{Z}}{7\mathbb{Z}}$. Tomando $x_1 = 1 + 7.t_1$ tentaremos encontrar soluções (mod 7^2), ou seja, queremos determinar $t_1 \in \mathbb{Z}$ tal que:

$$f(1 + 7.t_1) \equiv 0 \qquad (\text{mod } 7^2)$$

pelo algoritmo de Newton temos que encontrar as soluções da equação linear

$$\begin{array}{rcll} f^{'}(1).t_1 & \equiv & -\frac{f(1)}{3} & (\text{mod } 7^1) \\ (3x^5 - 10x^4 + 3x^3 - 2x - 1)^{'}(0)t_1 & \equiv & -\frac{-7}{7} & (\text{mod } 7^1) \\ 3.t_1 & \equiv & 2 & (\text{mod } 7^1) \\ t_1 & \equiv & 5 & (\text{mod } 7^1) \end{array}$$

Colocando $t_1 = 5 + 7.t_2$, obtemos $x_1 = 1 + 5.7 + 7^2.t_2$, e queremos obter $t_2 \in \mathbb{Z}$ de modo que:

$$f(36) + 7^2.t_2.f^{'}(36) \equiv 0 \qquad (\text{mod } 7^3)$$

ou melhor, resolver

$$f^{'}(36).t_2 \equiv -\frac{f(36)}{7^2} \qquad (\text{mod}7)$$

obtemos então :

$$t_2 \equiv 5 \qquad (\text{mod}7)$$

Prosseguindo com o processo alcançamos uma solução do tipo :

$$\begin{array}{lcl} x_0 & = & 0 \\ x_1 & = & 1 + 5.7^1 \\ x_2 & = & 1 + 5.7^1 + 2.7^2 \\ x_3 & = & 1 + 5.7^1 + 2.7^2 + 4.7^3 \\ x_4 & = & 1 + 5.7^1 + 2.7^2 + 4.3^3 + 5.7^4 \\ x_5 & = & 1 + 5.7^1 + 2.7^2 + 4.3^3 + 5.7^4 + 0.7^5 + ... \end{array}$$

Novamente chegamos em sequências bem parecidas com as iniciais usando o Método de Newton.

Com esta introdução surge a necessidade da criação de novos números, os quais deverão estender o conjunto dos racionais e servirão para resolver equações diofantinas mod p^e.

Para isto definiremos um novo valor absoluto em $\mathbb{Q}$ e com este valor absoluto nossas séries ξ convergirão para os **números p-ádicos** .

3 Definindo os números p-ádicos

Vimos no parágrafo anterior a necessidade da criação de um novo conjunto numérico que inclua os **" números "da forma:**

$$\xi = 3 + 1.7 + \ 2.7^2 \ + 6.7^3 + \ldots .$$

Eles apareceram na solução da equação $x^2 \equiv 2 \pmod{7^n}$.

Surge assim a pergunta: - Como definir tais números?

Sabemos que todo número natural $f \in \mathbb{N}$ se escreve de modo único na forma

$$f = a_0 + a_1 p + a_2 p^2 + ... + a_n p^n$$

onde $a_i \in \{ \ 0, 1, 2, 3, ...p-1 \ }$ chamada de expansão p-ádica de f. Ela pode ser achada dividindo f repetidamente por p, usando o algoritmo

$$\begin{array}{ccccc} f & = & a_0 & + & pf_1 \\ f_1 & = & a_1 & + & pf_2 \\ f_2 & = & a_2 & + & pf_3 \\ \ldots & = & \ldots & & \\ \ldots & = & \ldots & & \\ \ldots & = & \ldots & & \\ f_{n-1} & = & a_{n-1} & + & pf_n \\ f_n & = & a_n. & & \end{array}$$

Assim usando a notação do parágrafo anterior, a solução da equação

$$x \ = \ f \quad \bmod p^e \tag{10}$$

para todo $e \geq 1$ é a série:

$$\sum_{i=0}^{\infty} a_i p^i \tag{11}$$

cujas somas parciais formam a sequência

$$\begin{array}{lcllllll} x_1 & = & a_0 & & \equiv & f & \bmod p^1 \\ x_2 & = & a_0 + a_1 p & & \equiv & f & \bmod p^2 \\ x_3 & = & a_0 + a_1 p + a_2 p^2 & & \equiv & f & \bmod p^3 \\ . & & & & & & & \\ . & & & & & & & \\ . & & & & & & & \\ x_n & = & a_0 + a_1 p + \ldots + a_{n-1} p^{n-1} & & \equiv & f & \bmod p^n \\ x_{n+1} & = & a_0 + a_1 p + \ldots + a_n p^n & & \equiv & f & \bmod p^{n+1} \\ x_{n+2} & = & a_0 + a_1 p + \ldots + a_n p^n + 0 p^{n+1} & = \ f & \equiv & f & \bmod p^{n+2} \\ x_{n+3} & = & & f & \equiv & f & \bmod p^{n+3} \\ x_{n+4} & = & & f & \equiv & f & \bmod p^{n+4} \\ . & & & & & & & \\ . & & . & & & & & \\ . & & & . & & & & \end{array}$$

As somas parciais formam a sequência

$$a_0, \quad a_0 + a_1.p, \quad a_0 + a_1.p + a_2 p^2, \quad \ldots \quad , a_0 + \ldots + a_n p^n, \quad f, \quad f, \quad f$$

isto é, as somas parciais x_i são as classes de f no anel $\mathbb{Z}_{p^i}$ e quando p^i for maior do que f começarão a repetir e serão iguais a f.

Exemplo 3.1. Se $f = 5$ e $p = 3$ teremos:

$$\begin{array}{lcll} x_1 & = & 2 & \equiv 5 \quad \text{mod}3 \\ x_2 & = & 2 + 1.3 & \equiv 5 \quad \text{mod}3^2 \\ x_3 & = & 2 + 1.3 + 0.3^2 = 5 & \equiv 5 \quad \text{mod}3^3 \end{array}$$

Assim , as somas parciais formam a sequência:

$$2 \qquad 5 \qquad 5 \qquad 5 \qquad 5 \qquad 5 \qquad 5$$

E os inteiros negativos ? Como achar sua expansão p-ádica?

Vamos achar por exemplo a expansão p-ádica de -1, isto é, queremos resolver a equação

$$x + 1 = 0 \pmod{p^e}$$

para todo $e \geq 1$.

A classe de -1 em $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ é $p - 1$

em $\dfrac{\mathbb{Z}}{p^2\mathbb{Z}}$ é $p^2 - 1 \equiv p - 1 + (p-1)p \pmod{p^2}$

e sucessivamente temos que em $\dfrac{\mathbb{Z}}{p^n\mathbb{Z}}$ a classe de -1 é

$p^n - 1 \equiv p - 1 + (p-1)p + (p-1)p^2 + ... + (p-1)p^{n-1} \pmod{p^n}$.
Assim:

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + (p-1)p^3 + ... = \sum_{\nu=0}^{\infty}(p-1)p^{\nu}.$$

Observe que a série $x = -1 = \sum_{\nu=0}^{\infty}(p-1)p^{\nu}$ significa que p^e divide $x + 1$ para todo $e \geq 1$. Com efeito,

$$\begin{array}{rcll} -1 + 1 & = & 1 + (p-1) + (p-1)p + (p-1)p^2 + (p-1)p^3 + \ldots & \\ & = & p + (p-1)p + (p-1)p^2 + (p-1)p^3 + \ldots & \\ & = & p^2 + (p-1)p^2 + (p-1)p^3 + \ldots & \\ & = & p^3 + (p-1)p^3 + (p-1)p^4 + \ldots & \\ & = & p^4 + (p-1)p^4 + (p-1)p^5 + \ldots & \\ & = & p^5 + (p-1)p^5 + (p-1)p^6 + \ldots & = \ldots \end{array}$$

Interessante, não?

Temos assim séries infinitas como foi na seção anterior no caso de -2 . Em geral, se n for negativo , basta achar uma potência p^k maior que n e assim, $n + p^k$ vai ser um inteiro positivo e ache a expansão p-ádica de $n + p^k$:

$$n + p^k = \sum_{\nu=0}^{k-1} a_{\nu}p^{\nu}.$$

$$n = \sum_{\nu=0}^{k-1} a_{\nu}p^{\nu} - p^k.$$

$$n = \sum_{\nu=0}^{k-1} a_{\nu}p^{\nu} + (-1)p^k.$$

$$n = \sum_{\nu=0}^{k-1} a_\nu p^\nu + (\sum_{\nu=0}^{\infty}(p-1)p^\nu)p^k.$$

$$n = \sum_{\nu=0}^{k-1} a_\nu p^\nu + \sum_{\nu=0}^{\infty}(p-1)p^{\nu+k}$$

Assim vimos que todos os inteiros $n \in \mathbb{Z}$ podem ser escritos de modo único na forma:

$$n = \sum_{\nu=0}^{\infty} a_\nu p^\nu.$$

onde $p-1 \geq a_\nu \geq 0$. Esta é a chamada de **expansão p-ádica de n.**

Exemplo 3.2. Determinar a expansão 3-ádica de -10.
É fácil ver que

$$-10 + 3^3 = 17 = 2 + 2.3^1 + 1.3^2.$$

Desenvolvendo temos:

$$-10 = 2 + 2.3^1 + 1.3^2 - 3^3$$

$$-10 = 2 + 2.3^1 + 1.3^2 + (-1)\,3^3$$

$$-10 = 2 + 2.3^1 + 1.3^2 + 2.3^3 + 2.3^4 + \ldots + 2.3^n + \ldots$$

E os racionais não inteiros? - Como achar sua expansão p-ádica?

Todo inteiro f e mais geralmente todo racional pode ser escrito da forma $f = g/h$ onde $p \nmid h$.

Como p não divide h, então a classe de h tem inverso em qualquer anel $\frac{\mathbb{Z}}{p^i\mathbb{Z}}$,assim basta escrever a classe residual de $h^{-1} \in \frac{\mathbb{Z}}{p^i\mathbb{Z}}$ e depois multiplicar por g e assim acharmos a expansão p-ádica de $\frac{g}{h} = g.h^{-1}$.
Ou seja:

$$\begin{array}{lcl}
\overline{x_0} & = & a_0 \qquad\qquad\qquad\qquad\quad (\text{mod }\ ) \\
\overline{x_1} & = & a_0 + a_1 p \qquad\qquad\quad (\text{mod } p^2) \\
\overline{x_2} & = & a_0 + a_1 p + a_2 p^2 \qquad (\text{mod } p^3) \\
\vdots & & \\
\end{array}$$

Exemplo 3.3.

Vamos achar a expansão 5-ádica de $\frac{2}{3}$:

$$\begin{array}{lllllll}
\frac{2}{3} & = & 2.3^{-1} & = & 2.2 \pmod{5^1} & \equiv & 4 \pmod{5^1} \\
\\
\frac{2}{3} & = & 2.3^{-1} & = & 2.17 \pmod{5^2} = 34 & \equiv & 9 = 4 + 1.5 \pmod{5^2} \\
\\
\frac{2}{3} & = & 2.3^{-1} & = & 2.42 \pmod{5^3} = 84 & \equiv & 84 = 4 + 1.5 + 3.5^2 \pmod{5^3} \\
\\
\frac{2}{3} & = & 2.3^{-1} & = & 2.417 \pmod{5^4} = 834 & \equiv & 209 = 4 + 1.5 + 3.5^2 + 1.5^3 \pmod{5^4} \\
. & . & . & . & . & . & . \\
. & . & . & . & . & . & . \\
. & . & . & . & . & . & .
\end{array}$$

Ou seja, vemos assim que tais racionais são inteiros p-ádicos.

Geralmente, todo racional da forma $f = p^{-m}.\frac{g}{h}$ onde $mdc(gh, p) = 1$, e $m \in \mathbb{Z}$ e se

$$a_0 + a_1 p + a_2 p^2 + a_3 p^3 + ...$$

é a expansão p-ádica de g/h então

$$a_0 p^{-m} + a_1 p^{-m+1} + a_2 p^{-m+2} + ... + a_m + a_{m+1} p + ... \in \mathbb{Z}_p$$

é a expansão p-ádica de f.

Inicialmente isto tem um sentido formal, isto é, $\sum_{\nu=-m}^{\infty} a_\nu p^\nu$ significa a sequencia de somas parciais

$$s_n = \sum_{\nu=-m}^{n-1} a_\nu p^\nu \tag{12}$$

está será a nossa primeira definição de números p-ádicos.

Definição 3.1. *Seja p um número primo fixo. Um* **número p-ádico** *é uma série formal infinita*

$$a_{-m} p^{-m} + ... + a_{-1} p^{-1} + a_0 + a_1 p^1 + a_2 p^2 + ... ,$$

na qual $a_i \in \{ 0, 1, 2, 3, ...p - 1 \}$ e $m \in \mathbb{Z}$

Definição 3.2. *Os* **inteiros p-ádicos** *são os números p-ádicos onde $m = 0$, isto é, são as séries:*

$$a_0 + a_1 p^1 + a_2 p^2 + ... ,$$

O conjunto de todos os **números p-ádicos** será denotado por $\mathbb{Q}_p$ e o dos **inteiros p-ádicos** por $\mathbb{Z}_p$

Exemplo 3.4. *Existem racionais não inteiros que são inteiros p-ádicos.*

Por exemplo, já vimos que a expansão de

$$\frac{2}{3} \text{ é } 4 + 1.5 + 3.5^2 + 1.5^3 + \ldots \quad \text{e assim} \quad \frac{2}{3} \in \mathbb{Z}_5.$$

Podemos também provar que

$$1 + 3 + 3^2 + 3^3 + \ldots$$

é a extensão 3-ádica de $\dfrac{-1}{2}$.

Exemplo 3.5. *Determinar a expansão* 5*-ádica de* $\dfrac{33}{25}$

$$\frac{33}{25} = 5^{-2}.33 = 5^{-2}.(3 + 1.5^1 + 1.5^2)$$

$$\frac{33}{25} = 5^{-2}.33 = (3.5^{-2} + 1.5^{-1} + 1)$$

Exemplo 3.6. *Determinar a expansão* 5*-ádica de* $\dfrac{137}{25}$

$$\frac{137}{25} = 5^{-2}.137 = 5^{-2}.(2 + 2.5^1 + 0.5^2 + 1.5^3)$$

$$\frac{137}{25} = 5^{-2}.137 = (2.5^{-2} + 2.5^{-1} + 0.5^2 + 1.5^1)$$

Tudo que fizermos anteriormente para achar a expansão p-ádica de um número racional qualquer resulta do seguinte teorema que surge quando achamos as classes no anel quociente $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$:

Teorema 3.1. *As classes* $a \pmod{p^n}$ *em* $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$ *são expressas unicamente na forma:*

$$a \equiv a_0 + a_1p^1 + a_2p^2 + ... + a_{n-1}p^{n-1} \pmod{p^n}$$

onde $0 \leq a_i < p$ para $i = 1, 2, ..., n-1$.

Demonstração:

Usaremos indução em n. Se $n = 1$, o teorema é obviamente verdadeiro. supondo que a afirmativa é válida para $n-1$, temos a única representação

$$a = a_0 + a_1p + a_2p^2 + ... + ...a_{n-2}p^{n-2} + gp^{n-1}$$

onde $g \in \mathbb{Z}$. Como $g = a_{n-1} \pmod{p}$,com $0 \leq a_{n-1} < p$ e a_{n-1} é unicamente definido, o teorema está provado.

Exemplo 3.7. *Mais geralmente podemos provar que a expansão p-ádica de* $\frac{1}{1-p}$ *é :*

$$\frac{1}{1-p} = 1 + p + p^2 + p^3 + \ldots.$$

Com efeito, através de verificação direta nós temos que

$$1 = (1 + p + p^2 + p^3 + ... + p^{n-1})(1 - p) + p^n \ ,$$

logo

$$\frac{1}{1-p} = 1 \ + \ p \ + \ p^2 \ + \ p^3 \ + \ ... \, p^{n-1} \qquad (\text{mod } p^n).$$

Pelo Teorema 3.1., segue o resultado.

Exemplo 3.8.

O exemplo acima pode ser determinado também achando as soluções das equações de congruência

$$x = 1 + p.x \qquad \text{em} \quad \mathbb{Z}_{p^e}.$$

Elas são o inverso de $1 - p \pmod{p^e}$. Vamos resolvê-la usando recorrência para **qualquer** p primo.

$$\begin{array}{lcccc} x_o & = & 1 & & \\ x_1 & = & 1 + p.t_0 & = & 1 + p \\ x_2 & = & 1 + p.t_1 & = & 1 + p + p^2 \\ x_3 & = & 1 + p.t_2 & = & 1 + p + p^2 + p^3 \\ & & \dots & & \\ x_n & = & 1 + p + p^2 + p^3 + \ldots + p^n & & \end{array}$$

Assim, temos que:

1. $1 \ + \ 3 \ + \ 3^2 \ + 3^3 \ + v \ldots = \quad \dfrac{-1}{2} \mod 3^e$

   A expansão p-ádica 3-ádica de $\dfrac{-1}{2}$.

2. $1 \ + \ 5 \ + \ 5^2 \ + v5^3 \ + v \ldots = \quad \frac{-1}{4} \mod 5^e$

   A expansão p-ádica 5-ádica de $\dfrac{-1}{4}$.

3. $1 \ + \ 7 \ + \ 7^2 \ + \ 7^3 \ + \ \ldots = \quad \dfrac{-1}{6} \mod 7^e$

   A expansão p-ádica 7-ádica de $\dfrac{-1}{6}$.

4. $1 \ + \ 2 \ + \ 2^2 \ + \ 2^3 \ + \ \ldots = \quad \dfrac{-1}{1} = -1 \mod 2^e$

   A expansão p-ádica 2-ádica de $\dfrac{-1}{1} = -1$.

Resumindo como todo racional pode ser escrito da forma $f = p^{-m}\dfrac{g}{h}$ onde $mdc(gh, p) = 1 \, , m \in \mathbb{N}$ e se

$$a_0 + a_1 p + a_2 p^2 + a_3 p^3 + ...$$

é a expansão p-ádica de g/h então

$$a_0 p^{-m} + a_1 p^{-m+1} + a_2 p^{-m+2} + ... + a_m + a_{m+1} p + ... \in \mathbb{Q}_p$$

é a expansão p-ádica de f.

Temos assim a aplicação:

$$\begin{array}{ccc} \mathbb{Q} & \hookrightarrow & \mathbb{Q}_p \\ f & \hookrightarrow & \sum_{\imath=0}^{\infty} a^i p^i \end{array}$$

a qual é injetiva pela unicidade do Teorema 3.1.
Podemos identificar $\mathbb{Q}$ com sua imagem em $\mathbb{Q}_p$ e assim $\mathbb{Q} \subset \mathbb{Q}_p$ e $\mathbb{Z} \subset \mathbb{Z}_p$,como já vimos. Assim, a todo número racional f associamos a série

$$\sum_{\nu=-m}^{\infty} a_\nu p^\nu$$

a qual é a sua expansão p-ádica. Podemos assim dizer que a expansão p-ádica de um número racional é a sua série de Laurent e estamos analizando o número racional localmente perto do primo p.

A expansão p-ádica de um $f \in \mathbb{Q}$ vai mostrar se $p|f$ e qual é a maior potência de p que divide p. Isto é, num certo sentido estamos considerando os números como funções. As séries de Laurent são usadas para analizar funções complexas $f(z)$ próximas de um ponto onde $\alpha \in \mathbb{C}$ e existe algum problema (não são definidos, não possuem derivadas) em α e não próximo de α. A série de Laurent de f é da forma:

$$f(z) = \sum_{\imath=n_0}^{\infty} a_p (z-\alpha)^i$$

e $n_0 > 0$ dizer que α é zero então f de ordem n_0,
e se $n_0 < 0$ dizer que α é um pólo de f de ordem $-n_0$.

Observe que temos uma analogia entre $\mathbb{Z}$ e $\mathbb{C}[z]$, ambos são domínios de ideais principais, seus elementos irredutíveis são os primos p e $(z-\alpha)$ com $\alpha \in \mathbb{Z}$, respectivamente e seus corpos de frações se $\mathbb{Q}$ e $\mathbb{C}[z]$ respectivamente Hensel criou os números p-ádicos para completar a analogia entre $\mathbb{Z}$ e $\mathbb{C}[z]$ e as séries de Laurent tem seu análogo nas expansões p-ádicas.

Os termos dessa sequencia estão em diferentes anéis $\dfrac{\mathbb{Z}}{p^n\mathbb{Z}}$, os quais estão relacionados através das projeções:

$$\frac{\mathbb{Z}}{p\mathbb{Z}} \xleftarrow{\lambda_1} \frac{\mathbb{Z}}{p^2\mathbb{Z}} \xleftarrow{\lambda_2} \frac{\mathbb{Z}}{p^3\mathbb{Z}} \xleftarrow{\lambda_3} \ldots$$

e a relação $\lambda_n(\overline{s}_{n+1}) = \overline{s_n}$. .
.
.

Exemplo 3.9. *Como achar a expansão 5-ádica de* $\dfrac{3}{8}$ *?*

Como $8^{-1} = 2 \bmod 5$, $8^{-1} = 22 \bmod 5^2, 8^{-1} = 32 \bmod 5^3$,

então:

$$\frac{3}{8} = 3.(2 \bmod 5) = (1 \bmod 5) \Rightarrow s_0 = 1 \bmod 5$$

$$\frac{3}{8} = 3.(22 \bmod 5^2) = (16 \bmod 5^2) \Rightarrow s_1 = 1 + 3 \cdot 5 \bmod 5^2$$

$$\frac{3}{8} = 3.(47 \bmod 5^3) = (141 \bmod 5^3) \Rightarrow s_2 = 1 + 3 \cdot 5 + 0 \cdot 5^2 \bmod 5^3$$

.
.
.

4 Valor absoluto p-ádico

Aqui vamos tentar repetir a criação dos números reais. A primeira coisa que temos de fazer será criar um valor absoluto interessante para nossos objetivos, para termos o conceito de estar próximo. Como em $\mathbb{R}$, os números p-ádicos serão os limites de sequencias de racionais do tipo ξ.

Relembrando que uma seqüência $\{ x_i \}$ de números racionais é chamada **seqüência de Cauchy** se dado qualquer $\epsilon > 0$, existe $N \in \mathbb{N}$ (que pode depender de ϵ) tal que

$$|x_i - x_s| < \epsilon; \qquad \forall\, i, s > N.$$

No caso presente, a série ξ em (7) na seção 1 tem a seqüencia de somas parciais da forma

$$x_k = b_0 + b_1 \cdot 7^1 + \ldots + b_k \cdot 7^k$$

e

$$x_m = b_0 + b_1 \cdot 7^1 + \ldots + b_m \cdot 7^m$$

com $0 \geq b_i < 7$. Então, supondo $m > k$:

$$\begin{aligned} x_m - x_k &= b_m \cdot 7^m + b_{m+1} \cdot 7^{m+1} + \ldots + b_{k-1} \cdot 7^{k-1} \\ &= 7^{k-1}(b_{k-1} + b_k \cdot 7^1 + \ldots + b_m \cdot 7^{m-k+1}) \end{aligned}$$

e a diferença entre x_k e x_m é caracterizada pelo fato do número ser divisível por uma potência alta de 7 se k e m são ambos grandes.

Isto nos sugere a seguinte definição de **valor absoluto p-ádico**$|\ |_p$:

Seja $a = \frac{b}{c} \in \mathbb{Q}$ um número racional não nulo com b e $c \in \mathbb{Z}$. Nós dividimos b e c pelo primo p tantas vezes quanto possível tal que

$$a = \frac{p^m b_1}{c_1}, \qquad (b_1 c_1, p) = 1,$$

e definimos

$$| \ a \ |_p = \frac{1}{p^m}.$$

valor absoluto p-ádico tem a propriedade de ser pequeno quando a for divisível por uma alta potência do primo p. Em particular, as somas parciais associadas com a série p-ádica $a_0 + a_1 p + a_2 p^2 + ...$ forma uma seqüencia convergente com respeito ao valor absoluto $|\ |_p$.

O valor absoluto p-ádico $|\ |_p$ satisfaz as mesmas propriedades do valor absoluto usual:

1. $|\ |_p$ é uma aplicação de $\mathbb{Q}^*$ em $\mathbb{Z}^*$

2. $|\ |_p \geq 0 \quad e \qquad |x|_p = 0 \quad \Leftrightarrow x = 0$

3. $|-x|_p = |x|_p$, ou seja o valor absoluto p-ádico de um número racional negativo é igual ao seu simétrico.

4. $|xy|_p = |x|_p \cdot |y|_p$

O valor absoluto definido nos reais é dito arquimediano pois satisfaz a seguinte propriedade, também chamada de desigualdade triangular:

$$|x + y| \leq |x| + |y|.$$

Numa valorização p-ádica existe uma relação mais forte do que a dos reais, chamada também de **distância ultra métrica**:

$$|x+y|_p \leq max\{|x|_p, |y|_p\}$$

com iqualdade quando $|x|_p \neq |y|_p$. Com efeito suponha que

$$\begin{array}{ccc} p^t \mid x & \text{e} & p^{t+1} \nmid x \text{ e} \\ p^u \mid y & \text{e} & p^{u+1} \nmid x \end{array}$$

isto é, $x = \dfrac{p^t x_1}{x_2}$ e $mdc(x_1 x_2, p) = 1$ e analogamente com y . temos que

$$p^{min(t,u)} \mid (x+y) \qquad |x+y|_p \quad \leq max \quad \{|x|_p, |y|_p\}.$$

Exemplo 4.1.

1. $|60|_3 = \dfrac{1}{3^1} = \dfrac{1}{3}$
2. $|27|_3 = \dfrac{1}{3^3} = \dfrac{1}{27}$
3. $|25|_5 = \dfrac{1}{5^2} = \dfrac{1}{25}$
4. $|27|_5 = \dfrac{1}{5^0} = 1$
5. $|\dfrac{1}{25}|_5 = \dfrac{1}{\frac{1}{5^2}} = 25$

O fato central agora é que as propriedades acima são as únicas propriedades do valor absoluto p-ádico $|\ |_p$ usado na construção do completamento topológico de $\mathbb{R}$ através de $\mathbb{Q}$ usando as sequências de Cauchy, e portanto repetir todos os passos da construção de $\mathbb{R}$ a partir do valor absoluto definido em $\mathbb{Q}$.

Existem diferenças entre a métrica p-ádica e a métrica Euclidiana(a definida pelo valor absoluto usual). Enquanto que na norma Euclidiana existem triângulos escalenos, isósceles e equiláteros, no valor absoluto p-ádico todos os triângulos são isósceles. De acordo com a desiguladade ultra-métrica:

$$|x+y|_p \quad \leq \ max\{|x|_p, |y|_p\}$$

temos

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

de fato

$$d(x,y) = |x-y|_p$$

$$d(x,y) = |x-z+z-y|_p \ \leq \ max\{|x-z|_p, |y-z|_p\}$$

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

Ou seja $d(x,y)$ é igual a $d(x,z)$ caso $d(x,z) > d(y,z)$, ou $d(x,y) = d(y,z)$ caso $d(y,z) > d(x,z)$, de qualquer modo teremos um triângulo isósceles.

Um outro fato interessante do valor absoluto p-ádico é o fato de que todo ponto interior ao círculo diferente do centro também é centro da circunferência, com efeito,:

Considere um círculo de raio r e centro a, $C(a,r)$. O lugar geométrico dos pontos interiores ao circulo é $IntC(a,r) = \{x \in C(a,r) \| \ d(a,x) \ < \ r\}$.

Teorema 4.1. *Se $b \in IntC(a,r)$ então $C(a,r) = C(b,r)$.*

Demonstração:

seja $x \in IntC(a,r)$ então $d(a,x) < r$ e $d(b,a) \leq d(a,r)$ e

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

ou seja:

$$x \in C(b,r) \quad \Rightarrow \quad C(a,r) \quad \subset \quad C(b,r)$$

Analogamente temos

$$C(b,r) \quad \subset \quad C(a,r)$$

Implica em

$$C(a,r) = C(b,r)$$

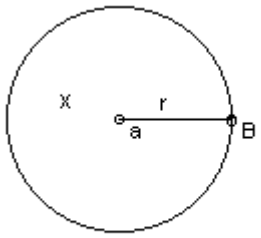

Figura 1: Propriedades da distância Ultra Métrica

Na análise real, utilizando a norma Euclidiana os únicos conjuntos abertos e fechados ao mesmo tempo são os reais $\mathbb{R}$ e o conjunto vazio $\not\emptyset$.

Utilizando a norma p-ádica, verificamos que os conjuntos representados por bolas

$$C(a,r) = |x-a|_p > r, \forall x,$$

são simultaneamente abertos e fechados . A saber:

Considere $C(a,r)$ uma bola de centro a e raio r. Suponha que c é um ponto de aderância de $C(a,r)$ ou seja, dado $\epsilon > 0$, temos:

$$C(a,r) \cap C(c,\epsilon) \neq 0,$$

de modo que ϵ representa o raio da bola C. Deste modo $C(c,\epsilon)$ contêm pontos de $C(a,r)$. Seja $x \in C(a,r) ex \in C(c,\epsilon)$.Para $\epsilon \leq r$, temos

$$C(c,\epsilon) = C(x,\epsilon) \subset C(x,r) = C(a,r).$$

Logo $\overline{C(a,r)} = C(a,r)$, ou seja $C(a,r)$ é fechado e aberto ao mesmo tempo. Utilizando o item

anterior, podemos mostrar que a fronteira de uma bola aberta é um conjunto vazio. Ou seja, a interseccção da bola com com o seu complementar é vazio .Na norma Euclidiana, o espaço geomérico delimitado pela fronteira de uma bola de centro a e raio r é a circunferência. Este mesmo conceito é extendido para a

norma p-ádica. A saber:

Seja $C(a,r)$ uma bola de centro a e raio r. Como $C(a,r) = \overline{C(a,r)}$, pois, o conjunto é aberto e fechado ao mesmo tempo, logo o complemetar de $C(a,r)$ também é fechado, Como a intersecção de $C(a,r)$ e o seu complementar é tudo, concluímos que a fronteira é vazia.

Em todos os exemplos descritos mudando a métrica estaremos criando outro corpos, que podem ser úteis na solução de problemas algébricos ou geométricos. Um ramo de pesquisa matemática é a utilidade desses novos corpos.

5 A sequência de inteiros p-ádicos

5.1 O conjunto Ω_p

Uma das maneiras de apresentar os números p-ádicos é por meio de sequências de potências de números primos. A partir desse capítulo formalizaremos o conceito de números p-ádicos.

Seja Ω_p o conjunto formado por todas as sequências de inteiros da forma :

$$\{x_n\} = \{x_0,\ x_0 + x_1 \cdot p,\ x_0 + x_1 \cdot p + x_2 \cdot p^2,\ \ldots\},$$

que satisfazem a propriedade :

$$\begin{cases} x_1 \equiv x_0 \pmod{p} \\ x_n \equiv x_{n-1} \pmod{p^n} \quad \text{para todo} \quad n \in \mathbb{N}. \end{cases}$$

Em Ω_p definimos a relação :

$$\{x_n\} \sim \{y_n\} \Leftrightarrow x_n \equiv y_n \pmod{p^{n+1}} \quad \text{para todo} \quad n \in \mathbb{N}.$$

É fácil demonstrar que :

Lema 5.1. $(\Omega_p, \sim)$ *é uma relação de equivalência.*

Definição 5.1. *Chamaremos de* **inteiro p-ádico** *as classes de equivalência das sequências originadas da relação de equivalência* $\sim$*.O conjunto dos inteiros p-ádicos será representado por* Z_p*. Usaremos ainda a notação* $\{x_n\}$ *para as classes de equivalência.*

Em $\mathbb{Z}_p$ definimos as operações:

$$\begin{array}{rccccc} \textbf{Soma}: & \mathbb{Z}_p & + & \mathbb{Z}_p & \Rightarrow & \mathbb{Z}_p \\ & \{x_n\} & + & \{y_n\} & \Rightarrow & \{x_n + y_n\} \\ \textbf{Produto}: & \mathbb{Z}_p & \times & \mathbb{Z}_p & \Rightarrow & \mathbb{Z}_p \\ & \{x_n\} & \cdot & \{y_n\} & \Rightarrow & \{x_n \cdot y_n\} \end{array}$$

É fácil ver, que a soma e a multiplicação em $\mathbb{Z}_p$ estão bem definidas, isto é independem da escolha do representante da classe. Também a soma em $\mathbb{Z}_p$ é comutativa, associativa e possui elemento neutro $0 = \{0, 0, 0, 0, 0, \}$. O simétrico de $\{a_n\}$ é a classe $\{-a_n\}$. A multiplicação em $\mathbb{Z}_p$ é comutativa, possui o elemento neutro $1 = \{1, 1, 1, 1, 1, ...\}$ e é distribuitiva em relação a soma. Logo $\mathbb{Z}_p$ **é um anel comutativo com unidade.**

Observação :

Podemos considerar que $\mathbb{Z}$ "está contido" em $\mathbb{Z}_p$, para cada $k \in \mathbb{Z}$, consideramos a sequencia constante

$$\{k\} = \{k, k, ..., k\} \in \mathbb{Z}_p$$

Formalmente isto significa :

Lema 5.2. *Existe um isomorfismo injetivo de* $\mathbb{Z}$ *em* $\mathbb{Z}_p$

Demonstração:

Defina a função:

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & \mathbb{Z}_p \\ & k & \longmapsto & \{k,k,k,k,,...\} \end{array}$$

É fácil verificar que f é um homomorfismo de anéis e é injetivo.

$$k \longrightarrow \{k,k,k,k...\} \qquad \text{entre} \qquad \mathbb{Z} \quad \text{e} \quad \mathbb{Z}_p.$$

5.2 $\mathbb{Z}_p$ é um domínio de integridade

Veremos agora que $\mathbb{Z}_p$ não possui divisores de zero (0) a ssim $\mathbb{Z}_p$ será um dominio de integridade como passaremos a demonstrar agora.

Teorema 5.3. $\mathbb{Z}_p$ *é um domínio de integridade.*

Demonstração:

Dados α e $\beta \in \mathbb{Z}_p$ temos que provar que se $\alpha \cdot \beta = 0$, então $\alpha = 0$ ou $\beta = 0$. Para provarmos isto é necessário a demonstração dos lemas a seguir:

Lema 5.4. $\alpha \in \mathbb{Z}_p$, α *é uma unidade p-ádica se, e somente se,* $x_0 \not\equiv 0 \pmod{p}$.

Demonstração :
Seja α uma unidade **p-ádica em** $\mathbb{Z}_p$, pela definição de unidade existe um $\beta \in \mathbb{Z}_p$ tal que $\alpha.\beta = 1$. Considere $\{x_n\}$ e $\{y_n\}$ as sequências em Ω_p que representam α e β. Logo

$$\alpha.\beta = \{x_n.y_n\} = \{x_0.y_0, x_1.y_1, ..., x_n.y_n, ...\} \sim \{1,1,...,1,...\}$$

temos $x_i.y_i \equiv 1 \pmod{p^i}$ para todo $i \in \{0,1,2,...,n,...\}$

implica que

$$x_0 \not\equiv 0 \qquad (\mathrm{mod} p^i) \qquad i \in \mathbb{N}.$$

Vamos provar agora a recíproca.

Seja $\alpha \in \mathbb{Z}_p$ e $\{x_n\}$ a sua respectiva sequência em Ω_P que o represente de modo que $x_0 \not\equiv 0$. Pela definição de número p-ádico temos que $x_n \equiv x_{n-1}$ para qualquer valor de $n \in \mathbb{N}$, logo podemos escrever que

$$x_n \equiv x_{n-1} \equiv x_{n-2} \equiv x_{n-3} \equiv ...x_2 \equiv x_1 \equiv x_o \qquad (\mathrm{mod} p)$$

Como $x_0 \not\equiv 0$ por hipótese temos que $x_i \not\equiv 0$ para todo $i \in \mathbb{N}$. Logo

$$mdc(x_i, p) = 1$$

,então

$$mdc(x_i, p^i) = 1 \quad i \in \mathbb{N}.$$

Pela definição de equação de congruência a equação

$$\{y_n \,.\, x_n\} \equiv 1 \qquad \mod p^i$$

sempre apresenta solução para $y_n \in \mathbb{N}^*$, podemos supor que existe uma sequência y_n tal que $x_n.y_n \equiv 1 \quad n \in \mathbb{N}$. Devemos mostrar que a sequência construida pertence a Ω_p, para isso :

$$\begin{array}{ccccc} x_n \,.\, y_n & \equiv & 1 & (\mathrm{mod} p^n) & n \in \mathbb{N} \quad (1) \\ (x_n & \equiv & x_{n-1} & (\mathrm{mod} p^n) & n \in \mathbb{N} \quad (3) \\ x_0 & \not\equiv & 0 & & \end{array}$$

Multiplicando (3) por y_n temos:

$$\begin{array}{ccccc} y_n \,.\, x_n & \equiv & y_n \,.\, x_{n-1} & (\mathrm{mod} p^n) & n \in \mathbb{N} \\ 1 & \equiv & y_n \,.\, x_{n-1} & (\mathrm{mod} p^n) & n \in \mathbb{N} \\ 1 \,.\, (y_{n-1}) & \equiv & y_n \,.\, (x_{n-1}).(y_{n-1}) & (\mathrm{mod} p^n) & n \in \mathbb{N} \\ 1 \,.\, (y_{n-1}) & \equiv & y_n \,.\, 1 & (\mathrm{mod} p^n) & n \in \mathbb{N} \\ y_{n-1} & \equiv & y_n & (\mathrm{mod} p^n) & n \in \mathbb{N} \end{array}$$

Percebemos que $\{y_n\}$ satisfaz as propriedades em Ω_p, logo.

$$\{x_n\} \,.\, \{y_n\} \qquad \equiv \quad 1 \quad (\mathrm{mod} p^n) \quad n \in \mathbb{N}$$

Consideremos β o número pádico que representa a sequencia $\{y_n\}$, logo

$$\alpha \,.\, \beta \quad \equiv \qquad 1$$

Como $\beta \not\equiv 0$ por construção, temos que α representa uma unidade em $\mathbb{Z}_p$.

Lema 5.5. *Todo inteiro p-ádico $\alpha \in \mathbb{Z}_p$ pode ser escrito de maneira única na forma $\alpha = p^m \,.\, \xi$, onde $m \in \mathbb{N}$ e ξ uma unidade p-ádica.*

Demonstração:
Suponha que α não seja uma unidade p-ádica e considere $\{x_n\}$ a sequência que o represente. Então pelo lema anterior devemos ter $x_0 \equiv 0 \,(\mod p)$. Seja m o menor inteiro positivo tal que $x_m \not\equiv 0 \quad (\mod p^{m+1})$. Além disso para todo $s \in \mathbb{N}$ temos que:

$$x_{m+s} \equiv x_{m+s-1} \equiv \ldots x_{m+s-(s-1)} \equiv x_m \equiv x_{m-1} \equiv 0 \quad (\mathrm{mod} p^m).$$

Deste modo podemos definir $y_s = \frac{x_{m+s}}{p^m} \in \mathbb{Z}$ e por hipótese $y_0 \not\equiv 0 \quad (\mathrm{mod} p)$. Não é difícil verificar que $\{y_n\} \in \Omega_p$ e $\{y_s\}$ representa uma unidade.

$$\alpha = p^n \,.\, \mu \qquad e \qquad \beta = p^m \,.\, \xi \qquad n, m \in \mathbb{N}.$$

logo

$$\begin{array}{ll} \alpha \,.\, \beta & = 0 \quad = p^n \,.\, \mu \,.\, p^m \,.\, \xi \\ \alpha \,.\, \beta & = 0 \quad = p^{n+m} \,.\mu \,.\, \xi \end{array}$$

Como μ e ξ são unidades, então $p^{n+m} = 0$, absurdo, logo

$$\alpha = 0 \quad \text{ou} \quad \beta = 0.$$

Como Z_p é um domínio de integridade ele admite um corpo de frações. Chamaremos o corpo de frações de $\mathbb{Z}_p$ de corpo p-ádico e o representaremos por $\mathbb{Q}_p$

6 Sequências p-ádicas

Seja $\{x_n\} = \{x_0, x_1, \ldots, x_n, \ldots\}$ uma sequência p-ádica, isto é, $x_n \in \mathbb{Q}_p$ para todo $n \in \mathbb{N}$.

Dizemos que a sequência $\{x_n\}$ converge para $a \in \mathbb{Q}_p$ que representaremos por $\lim_{n\to\infty} x_n = a$ se, e somente se,

$$\lim_{n\to\infty} |x_n - a|_p = 0$$

Observamos que na relação acima $|x_n - a|_p$ representa um número real.

Exemplo 6.1.

A sequência $\{5^n\} = \{5^0, 5^1, 5^2, \ldots, 5^n, \ldots\}$ para $n \to \infty$ no corpo $\mathbb{Q}_5$ converge a zero. De fato:

$$\lim_{n\to\infty} |5^n - 0|_5 = \lim_{n\to\infty} 5^{-v_5(5^n)} = \lim_{n\to\infty} 5^{-n} = 0$$

Exemplo 6.2.

Considerando a mesma sequência $\{5^n\} = \{5^0, 5^1, 5^2, \ldots, 5^n, \ldots\}$ para $n \to \infty$ no corpo $\mathbb{Q}_p$ com $p \neq 5$ o limite não é zero. De fato,

Suponha que $\lim_{n\to\infty} 5^n = 0 \qquad (p \neq 5)$, logo,

$$\lim_{n\to\infty} |5^n - 0|_p = \lim_{n\to\infty} p^{-v_5(5^n)}$$

Como $(p, 5^n) = 1$ para todo $n \in \mathbb{N}$ pois p e 5 são primos entre si, então 5^n é uma unidade p-ádica em $\mathbb{Q}_p$ com $(p \neq 5)$. Com isso,

$$\lim_{n\to\infty} |5^n - a|_p = \lim_{n\to\infty} p^0 = 1$$

Os exemplos citados mostram-nos que quando usamos uma métrica diferente, os critérios de convergência também mudam. No 1º exemplo a sequência conhecida $\{5^n\}$ tende para ∞ para n grande. E em $\mathbb{Q}_p$ com $p \neq 5$ ela converge para zero. Nos reais tal sequência é a famosa série geométrica divergente de razão 5.

Mas o fato mais interessante que o estudo feito em análise real pode ser estendido para uma análise p-ádica. Existem algumas características comuns no corpo dos reais e no corpo dos números p-ádicos.

De modo análogo uma sequência p-ádica não pode possuir dois limites distintos.

Considere uma sequência p-ádica $\{x_n\} = \{x_o, x_1, \ldots, x_n, \ldots\}$.

Teorema 6.1. *Se* $\lim_{n\to\infty} x_n = a$ *e* $\lim_{n\to\infty} x_n = b$, *com* a *e* $b \in \mathbb{Q}_p$ *então* $a = b$.

Demonstração:

$\lim_{n\to\infty} x_n = a \Rightarrow \lim_{n\to\infty} |x_n - a|_p = 0.$

e

$\lim_{n\to\infty} x_n = b \Rightarrow \lim_{n\to\infty} |x_n - b|_p = 0.$

Usando as propriedades de valor absoluto p-ádico

$$|a - b|_p = 0 \leq max\{|a - x_n|_p, |x_n - b|_p\}$$

Tomando o limite de ambos os lados temos:

$\lim_{n\to\infty} |(x_n - b) - (a - b)|_p = 0 \leq max\{\lim_{n\to\infty} |(x_n - b) - c|_p, \lim_{n\to\infty} |c - (a - b)|_p\}.$

Ou seja:

$$\lim_{n\to\infty} |a - b|_p = 0 \quad \Rightarrow \quad \lim_{n\to\infty} a = b \quad e \quad \lim_{n\to\infty} b = a \quad \Rightarrow \quad a = b$$

Definição 6.1. *Uma sequência $\{x_n\}$ em $\mathbb{Q}_p$ é dita limitada, quando a sequência $|x_n|_p$ (em $\mathbb{R}$) for limitada. Ou seja existe $M > 0 \in \mathbb{Q}_P$ tal que $|x_n|_p \leq M$ para todo $n \in \mathbb{N}$.*

Lema 6.2. *Toda sequência p-ádica convergente é limitada.*

Considere $\{x_n\}$ uma sequência p-ádica convergente e seja $a = \lim_{n\to\infty}\{x_n\}$ com $a \in \mathbb{Q}_p$ e $n \in \mathbb{N}$. Tomando $\epsilon = 1$, vemos que existe $n_0 \in \mathbb{N}$ tal que para todo $n \geq n_0$ teremos $|x_n - a|_p \leq 1$.
Por outro lado utilizando as propriedades da norma p-ádica temos:

$$\begin{array}{lcll} |a_n - 0|_p & \leq & max & \{|a_n - a|_p, |a - 0|_p\} \\ |a_n - 0|_p & \leq & max & \{|a_n - a|_p, |a|_p\} \quad \leq \quad |a_n - a|_p \quad + \quad |a|_p \\ |a_n - a|_p & \geq & |a_n|_p - |a|_p & \end{array}$$

Com isso temos que:

$$|a_n|_p \leq |a_n - a|_p + |a|_p,$$

Então para todo $n \geq n_0$ teremos $|a_n|_p \leq 1 + |a|_p$. Fazendo

$$M = max\{|a_0|_p, |a_1, \ldots, |a_{n0}|_p, 1 + |a|_p\}$$

teremos $|a_n|_p \leq M$ para todo $\mathbb{N}$ provando assim que a sequencia é limitada.

Teorema 6.3. *Sejam $\{a_n\}$ e $\{b_n\}$ duas sequencias p-ádicas*

1. Se $a_n = a \in \mathbb{Q}_p$ para todo $n \in \mathbb{N}$, então $\lim_p |a_n|_p = a$.
2. Se $\lim_{n\to\infty} a_n = a\, e\, \lim_{n\to\infty} b_n = b$, então :

   (a) $\lim_{n\to\infty} a_n + b_n = a + b$.

   (b) $\lim_{n\to\infty} a_n.b_n = a.b$.

Demonstração análoga aos reais.

Teorema 6.4. *Seja $\{x_n\} = \{x_o, x_1, \ldots, x_n, \ldots\}$ uma sequencia p-ádica. Dizemos que a sequência $\{x_n\}$ é convergente, se e somente se,*

$$\lim_{n,m\to\infty} |x_m - x_n|_p = 0 \qquad n, m \in \mathbb{N}.$$

Demonstração:

$$(\Rightarrow)$$

Considere a $= \lim_{n\to\infty} |x_m|_p = 0$, com $a \in \mathbb{Q}_p$. Utilizando a propriedade ultra- métrica temos:

$$|x_m - x_n|_p \leq max\{|a - x_m|_p, |x_n - a|_p\},$$

tomando limites de ambos os lados:

$$\lim_{n,m\to\infty} |x_m - x_n|_p \leq max\{\lim_{n,m\to\infty} |a - x_m|_p, \lim_{n,m\to\infty} |x_n - a|_p\}$$

logo,

$$\lim_{n,m\to\infty} |x_m - x_n|_p = 0$$

$(\Leftarrow)$

Suponhamos que $\lim_{n,m\to\infty} |x_m - x_n|_p = 0$. Então existe $n_0 \in \mathbb{N}$ tal que para $n, m \geq n_0 \Rightarrow |x_m - x_{n_0}|_p < 1$.
Em particular, para $m \geq n_0$ teremos:

$$|x_m - x_{n_0}|_p < 1.$$

Mas como,

$$|x_m|_p = |x_m - x_{n_0} + x_{n_0}|_p \leq max\{|x_m - x_{n_0}|_p, |x_{n_0}|_p\}$$

Ou seja,

$$|x_m|_p \leq max\{1, |x_{n_0}|_p\}$$

Se considerarmos

$$M = \{max\{|x_0|_p, |x_1|_p, \ldots, |x_{n_0}|_p, 1\},$$

t9eremos: $|x_n| \leq M$ para todo $n \in \mathbb{N}$. Logo a sequência $\{x_n\}$ é limitada.

Construiremos uma subsequencia convergente.
Dado qualquer $\epsilon > 0$, existe, por hipótese $n_1 \in \mathbb{N}$, tal que

$$m, n \geq n_1 \Rightarrow |x_m - x_n|_p < \epsilon.$$

De maneira analoga existe $n_2 \in \mathbb{N}$ tal que

$$n_j \geq n_2 \Rightarrow |x_{n_j} - a|_p < \epsilon.$$

Tomando $N = max\{n_1, n_2\}$ e escolhendo $m, n_j \geq N$, teremos

$$|x_m - x_{n_j}|_p < \epsilon \quad e \quad |x_{n_j} - a|_p < \in,$$

então

$$\begin{array}{rcll} |x_m - a|_p & = & |x_m - x_{n_j} + x_{n_j} - a|_p & \leq \\ & & \leq max\{|x_m - x_{n_j}|_p, |x_{n_j - a}|_p\} & \leq \epsilon \end{array}$$

Ou seja,

$$\lim_{n\to\infty} |x_n - a|_p = 0$$

e assim ,

$$\lim_{n,\to\infty} |x_n|_p = a$$

No corpo dos $\mathbb{Q}_p$, queremos falar sobre sequencias de Cauchy e conceito de convergencia. Utilizando a norma p-ádica e lembrando-se que para uma sequencia ser de Cauchy se dado $\epsilon > 0$, então existe n_0 tal que para $n, m > n_0$ teremos:

$$|x_n - x_m|_p < \epsilon$$

que é justamente o teorema anterior. De modo que pra um corpo ser completo é necessário de todas as sequencias de Cauchy apresentam limites neste corpo.

Ao considerarmos conjunto do corpo de $\mathbb{Q}_p$, com sua norma p-ádica e o conjunto formado por todos os limites das sequencias de Cauchy, obteremos um corpo estritamente maior que $\mathbb{Q}_p$. Este corpo maior foi construido pela mesma maneira de Dedekind construiu os reais, a partir dos racionais, pelo processo que chamamos de completamento.

$$\{\mathbb{Q}_p\,, |\,|_p\,, \text{ sequências de Cauchy}\} = \text{ corpo completo}$$

6.1 Lema de Hensel

Um dos resultados mais importantes da utilização dos números p-ádicos recai no famoso Lema de Hensel.

O Lema de Hensel nos dão uma condição importante e necessária que polinômios com coeficientes inteiros p-ádicos apresentem raíz em $\mathbb{Z}_p$

Lema 6.5. *Lema de Hensel*

Seja $F(x) = a_0 + a_1X + a_0X^2 + \ldots + a_nX^n$ polinômio com coeficientes inteiros p-ádicos. Suponha que exista um inteiro p-ádico x_1 tal que:

$$F(x_1) \equiv 0 \qquad (\text{mod } p)$$

Caso $F'(x_1) \not\equiv 0 \pmod{p}$, então existe um inteiro p-ádico x com $x \equiv x_1 \pmod{p}$ e $F(x) = 0$.

Demonstração:

Para provarmos que tal x existe construiremos uma sequência de Cauchy $a_0, a_1, a_2, \ldots + a_n$, satisfazendo

necessariamente:

$$\begin{array}{lll} i) & F(a_n) \equiv 0 & (\text{mod } p^{n+1}) \\ & & //ii) \qquad a_n \\ & \equiv a_{n-1} & (\text{mod } p^n) \end{array}$$

Para tal, utilizaremos como ferramenta um método já discutido anteriormente,as aproximações sucessivas de Newton para encontrar raízes de polinômios. Pela hipótese já existe um termo a_0 e pela condição imposta existe $a_1 \in \mathbb{Z}_p$ tal que:

$$a_1 = a_0 + b_1p$$

para algum $b_1 \in \mathbb{Z}$.

Escrevendo o polinômio $F(x)$ na forma de Taylor, teremos:

$$F(a_1) = F(a_0 + b_1p) = F(a_0) + (F'a_0)b_1p + \ldots + F^n(a_0)b_1^np^n \equiv 0 \qquad (\text{mod } p)$$

ou seja:

$$F(a_1) = F(a_0 + b_1p) = F(a_0) + (F'a_0)b_1p \equiv 0 \qquad (\text{mod } p)$$

pondo $F(a_0) = px$, com $x \in \mathbb{Z}$ de modo que:

$$\begin{array}{lll} px + F'(a_0)b_1p & \equiv 0 & (\text{mod } p^2) \\ p(F(a_0) + F'(a_0)b_1) & \equiv 0 & (\text{mod } p^2) \\ x + (F'a_0)b_1 & \equiv 0 & (\text{mod } p) \end{array}$$

ou seja:

$$b_1 = \frac{-x}{F'(a_0)} \equiv 0 \qquad (\text{mod } p)$$

mas,por hipótese $p \not| F'(a_0)$. Sendo assim podemos dizer que $F'(a_0)$ representa uma unidade p-ádica e como tal invertível.

Escolhendo adequadamente $b_1 \in \{0, 1, 2, \ldots, p-1\}$ obtemos:

$$a_1 = a_0 + b_1p$$

De maneira idêntica dado $a_{n-1} \in Z_p$ tal que $F(a_{n-1}) \equiv 0 \pmod{p}$, podemos encontrar um $a_n \in \mathbb{Z}_p$ tal que:

$$a_n = a_{n-1} + b_{n-1}p$$

com $b_{n-1} \in \mathbb{Z}p$. Com isso construimos uma sequência de termos inteiros p-ádicos

$$\{a_0, a_1, \ldots, a_n, \ldots,\}$$

que satisfazem as condições $i)$ e $ii)$

É fácil perceber que tal sequência acima é de Cauchy e que se x for seu limite então :

$$F(x) = 0 \qquad \text{e} \qquad x \equiv a_0$$

Direto do Lema de Hensel, podemos determinar raízes de funções quadráticas pelo corolário abaixo.

Corolário 6.6. *Seja p um primo ímpar e suponha b um inteiro p-ádico não nulo e que seja quadrado* (mod p). *Então b é um quadrado de um número p-ádico.*

O Corolário pode ser provado usando o mesmo método para provar que -1 é um inteiro 5-ádico quadrado. O resultado também pode ser obtido utilizando o Lema de Hensel. Defina $f(x) = x^2 - b$ e seja $x_1^2 \equiv b \pmod{p}$. então $f(x_1) \equiv 0 \pmod{p}$ e $f'(x_1) = 2x_1 \not\equiv 0 \pmod{p}$, como p é primo e $x_1 \not\equiv 0 \pmod{p}$ por hipótese o Lema de Hensel mostra que existe um inteiro p-ádico x com $F(x) = 0$. Mostrando que $x^2 = b$ como queríamos.

Para $p = 2$ o corolário é falso. Por exemplo, 5 é um quadrado (mod 2), mas não é um quadrado (mod 2^3) e portanto não é quadrado $2-$ádico. Entretando, o procedimento intuitivo fornece o seguinte :

Se ϵ é um inteiro $2-$ádico tal que $\epsilon \equiv 1 \pmod{2^3}$, então é um inteiro $2-$ádico ao quadrado se, e somente se $\epsilon \equiv 1 \pmod{2^3}$.

Como todo inteiro pádico é congruente a um inteiro (mod p^m). Então existe um $a \in \mathbb{Z}_p$ tal que $\epsilon \equiv a \pmod{2^3}$

Mas como ϵ é um quadrado existe $\eta \in Z_p$ tal que $\epsilon = \eta \pmod{2^3}$. Utilizando do mesmo argumento existe $b \in \mathbb{Z}p$ de forma que $\eta \equiv b^2 \pmod{2^3}$ Assim $a \equiv b^2 \pmod{2}^3$. Como a é impar, pois representa uma unidade p-ádica, obtemos $a \equiv 1 \pmod{2^3}$ e lembrando que 3, 5 e 7 não representam resíduos quadráticos (mod 2^3). Concluimos que $\in = 1$.

Hasse-Minkowski Uma consequencia direta do Lema de Hensel, é aplicado a formas quadráticas no teorema de **Hasse-Minkowski**.

Teorema 6.7. *Seja*

$$F(x_1, x_2, \ldots, x_n, \ldots) \in Q(x_1, x_2, \ldots, x_n, \ldots)$$

polinômio homogênio de grau dois. A equação

$$F(x_1, x_2, \ldots, x_n, \ldots) = 0$$

apresenta soluções não triviais em $\mathbb{Q}$ se, e somente se, apresentar soluções não triviais em $\mathbb{Q}_p$ para todo p primo e em $\mathbb{R}$.

A demonstração desse teorema é ardua e cansativa, fugindo dos propósitos dessa indrodução. Aqueles que por curiosidade quiserem aprofuncar poderão consultar[Ser] e [Bosh].

6.2 Conclusão

Vale ressaltar que os números p-ádicos são construidos de modo análogo a construção dos números reais, a única diferença é como calcularmos a norma em p-ádico. Ao mudarmos esta maneira de medir distâncias de números , encontramos um leque de oportunidades para um novo corpo. No conjunto dos números reais existem vários Critérios de Convergência, porém nenhum deles é 100 % eficaz e em certas ocasiões é dificil saber qual o melhor critério, mas na norma p-ádica temos apenas um único crítério de convergência. Assim os números p-ádicos são escritos como sequências de potências primas e quanto maior

a potência, menor o número, então numa sequência de termos infinitos ao percebermos que a potência fica cada vez maior, o limite da sequência tenderá a zero para n muito grande.

Voltando a questão original, encontrar soluções de funcões $f(x) \equiv 0 \bmod p^n$, podemos ter nenhuma solução caso : $p \Big| f^{'}(x_0)$ mas $p^{e+1} \not| f(x_0)$, p soluções se : $p \not| f^{'}(x_0)$ e $p^{e+1} | f(x_0)$ ou uma solução se: $p \not| f^{'}(x_0)$. Caso a equação caia nos dois últimos casos podemos encontrar as soluções utilizando o método de Newton, uma ferramenta bastante útil no cálculo. Os valores $x_1, x_2, x_3, ...$, serão obtidos apartir dos termos anteriores.

Referências

[1] [Bosh] S.Bosch, U.Güntzer, and R.Remmert. *Non-Archimedian Analysis*. Sprinter-Verlag, 1994.

[2] [Ser] J.P.Serre. *A Course in Aritmetric.* Springer Verlag. New York, 1973.

[3] [God] H. Godinho. *O teorema de Hasse- Minkowski e a geometria de Artin.* Tese de mestrado, Universidade de Brasilia, 1996.

[4] [Sho] H. Godinho, S. Shokranian e Marcus Soares. *Teoria dos Números.* Brasilia, 2ª ed., 1999.

[5] [Fer] Fernado Gouvea. *P-adic Numbers* . EUA , 1995.

[6] [Dan] Daniel Barsky e Gilles Christol. *Los Números p-ádicos.* Editora Mundo Científico(nº161,vol 15)