Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
PPGM - Departamento de Matemática
Mestrado Profissional em Matemática
em Rede Nacional PROFMAT

Números p-ádicos

por

Ítalo Moraes de Melo Gusmão

sob orientação do

Prof. Dr. Bruno Henrique Carvalho Ribeiro

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT-CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Agosto/2016
João Pessoa - PB

Números p-ádicos

por

Ítalo Moraes de Melo Gusmão

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: teoria dos números

Aprovada por:

Prof. Dr. Bruno H. C. Ribeiro - UFPB (Orientador)

Prof. Dr. Carlos Bocker Neto - UFPB

Prof. Dr. Rodrigo Genuíno Clemente - UFRPE

Agosto/2016

Agradecimentos

Agradeço a Deus, em sua bondade infinita, por permitir que este momento fizesse parte de minha jornada terrestre.

Aos meus pais, que foram responsáveis pelo meu desenvolvimento moral e intelectual através de todo apoio necessário para chegar onde cheguei, sem eles nada disto aconteceria.

Agradeço ao meu orientador, Doutor Bruno Ribeiro, participou comigo ao longo do desenvolvimento deste trabalho, dedicando seu conhecimento e tempo para me guiar à conclusão do mesmo.

A Suelen, por sua compreensão e apoio nos momentos mais estressantes, complicados e distantes que o andamento do curso provoca.

A Rafael, por todo companheirismo nos momentos de estudo, presença constante nesta andada em busca da conclusão deste mestrado.

À todos que estiveram presentes nesta longa caminhada. Aos colegas de PROFMAT, professores e alunos, que proporcionaram esta experiência única, poder compartilhar momentos de felicidades e dificuldades.

Dedicatória

A minha família. À Suelen. Àqueles que direta ou indiretamente estiveram presentes neste ciclo. A todos os que se alegram com o sucesso.

Resumo

Apresentamos e definimos os números inteiros p-ádicos como o resultado de uma busca por soluções, para um sistema de congruências, que parte de uma equação polinomial de uma variável, com coeficientes racionais. Constatamos que o conjunto dos inteiros p-ádicos é estritamente maior que os inteiros. Mostramos um critério para que um racional possua um correspondente num conjunto de inteiros p-ádicos. Buscamos a possibilidade de representarmos números irracionais e números complexos como inteiros p-ádicos. Algebricamente, o conjunto dos inteiros p-ádicos será um domínio de integridade e, partindo disto, buscamos a construção de um corpo de frações dos inteiros p-ádicos, que formarão, assim, o corpo dos racionais p-ádicos, de um ponto de vista puramente algébrico. Na segunda parte, vamos expor os fundamentos para a construção de uma norma diferente da habitual, estabelecendo assim uma nova métrica, no conjunto dos números racionais, e a construção de um corpo não-arquimediano.

Palavras-chave: teoria dos números; corpo não-arquimediano; números p-ádicos.

Abstract

We introduce and define the p-adics integer numbers as a search for solutions result, for a congruences system that derives from a variable polynomial equation with rational coefficients. We evidence that the p-adic integers set is strictly larger than the integers. We present a criterion so that a rational that holds a correspondent in a p-adic integers set. We search for the possibility to represent irrational and complex numbers as p-adics integers. Algebraically, the p-adic integers set will be an integral domain and, from this, we search for the construction of p-adic integers quotient field so that shall form the p-adic rationals field, from a purely algebraically point of view. In the second part, we will expose the bases for the construction of a norm that's different from the usual, establishing so a new metric in the rational numbers set and the construction of a non-archimedian field.

Key words: numbers theory; non-Archimedean field; p-adic numbers.

Sumário

Notações

Notações Gerais

- $\equiv \ (mod\ n)$ representará a congruência módulo n.
- (a, n) será o máximo divisor comum entre a e n.
- $\mathbb{Z}/n\mathbb{Z}$ é o anel de inteiros módulo n. Usaremos $\mathbb{Z}/p\mathbb{Z}$ quando n for primo.
- $\mathbb{Z}_p$ será o conjunto dos inteiros p-ádicos.
- $\mathbb{Q}_p$ será o conjunto dos racionais p-ádicos.
- $v_p(n)$ será a valorização p-ádica do racional n.
- $|\cdot|_p$ é a norma p-ádica.
- $\delta(x, y)$ é a métrica sobre $\mathbb{Q}$ com a norma p-ádica.

Introdução

A teoria dos números, partindo desde os mais simples conceitos como divisibilidade e fatoração em primos, aos mais sofisticados como a resolução do último teorema de Fermat, chama atenção pelas belas aplicações e implicações lógicas, além dos resultados que delas originam. O fascínio apresentado nos primeiros contatos com o tema impulsionaram a busca por conteúdos relacionados.

Buscamos trazer uma apresentação sucinta, à graduandos, graduados e mestrandos em matemática, que já tiveram contato com a teoria dos números em algum nível, um tema que não é tão comumente abordado em cursos de teoria dos números, como os apresentados nos cursos de graduação. Este foi o ponto de partida para o desenvolvimento de uma teoria concebida a pouco mais de 100 anos por Kurt Hensel, e que apresentou-se como uma bela ferramenta para o auxílio na resolução de vários problemas, entre eles um célebre, o último teorema de Fermat, que passou mais de 350 anos sem solução.

Após inúmeras buscas por referências que fundamentassem o conteúdo pretendido, percebemos que alguns pontos necessitavam de uma apresentação mais detalhada, talvez com uma visão diferenciada, servindo assim como um impulso inicial para a abordagem do conteúdo.

A ideia de abordar os números p-ádicos surgiu ao se buscar uma apresentação de uma aplicação da teoria dos números, que torna possível o desenvolvimento de toda uma estrutura de um corpo de frações diferente do habitual. Partindo do conjunto dos racionais sabemos que podemos construir, através de sequências de Cauchy, sua extensão, os números reais. Sabemos que no vasto campo da matemática, os números reais e seu fecho algébrico, os números complexos, desempenham um papel singular. Veremos que existe uma outra métrica, diferente da habitual, que nos dá um resultado similar.

O Trabalho está dividido em duas partes. A primeira parte busca apresentar os inteiros p-ádicos de maneira algébrica, partindo de uma abordagem não convencional para a resolução da equação

$$x = 1 + 2x.$$

Tal resolução, que é abordada de forma clara mais a frente, apresenta procedimentos coerentes, salvo o fato de uma série geométrica só convergir se a razão estiver entre zero e um.

Na seção 1.2 iniciamos nossa caminhada com os números p-ádicos, ainda com algumas definições que nos servirão de bases. Veremos também algumas particularidades da determinação de inteiros p-ádicos utilizando o que iremos definir como

sistema de congruências módulo p^n. Nas seções 1.2.2 e 1.2.3 são apresentados algoritmos para a adição e multiplicação, respectivamente, baseados em ideias apresentadas em [6].

Veremos que dado um $k \in \mathbb{Z}^+$, a representação p-ádica de $-k$ será infinita, e que é possível determinarmos um procedimento para indicar o inverso aditivo de um número p-ádico. Mostramos que os inteiros p-ádicos são um domínio de integridade. Através de exemplos, apresentamos um caminho para determinarmos os representantes p-ádicos de números racionais, evidenciando um critério para que um racional possua representação p-ádica para um dado p fixo. Também serão apresentados alguns irracionais algébricos como inteiros p-ádicos. Verificaremos que é possível representarmos um número complexo como um número p-ádico.

Partindo dos exemplos já vistos fica fácil de perceber que os inteiros p-ádicos é estritamente maior que os inteiros, para todo p primo e, além disso, veremos que o conjunto dos inteiros p-ádicos não é algebricamente fechado, o que podemos notar quando estamos tentando determinar o número áureo nos p-ádicos (exemplo 1.10), pois para $p = 2, 3, 5$ e 7 não é possível. A conclusão da primeira parte se dá com a construção do corpo de frações de $\mathbb{Z}_p$. Onde concluiremos apresentando uma relação entre os elementos de $Frac(\mathbb{Z}_p)$ e suas respectivas expansões em séries.

A segunda parte nos trás uma visão topológica dos inteiros p-ádicos, iniciando com algumas notas históricas na seção 2.1. Neste capítulo introduziremos a ideia de norma ou valor absoluto p-ádico, inicialmente observando minuciosamente as definições de valorização p-ádica, partindo da valorização de um inteiro, até chegarmos ao fato de que a valorização p-ádica de um racional independe do quociente de inteiros considerado, seja sua forma irredutível ou com representações equivalentes. Teremos introduzida a ideia de valor absoluto não-arquimediano e veremos que a norma p-ádica é um exemplo desta. Apresentaremos as ideias iniciais sobre a métrica no corpo dos racionais p-ádicos, além disso, a partir do momento que temos um valor absoluto bem definido, podemos descrever uma métrica sobre este corpo.

Será apresentado o conceito de desigualdade ultramétrica. Esta métrica induz uma topologia com características não comuns, entre elas faz com que todos os triângulos sejam isósceles e que, definidas as bolas "abertas" e "fechadas", respectivamente

$$B(c,t) = \{x \in \mathbb{K} : \ |x - c| < t\}$$

$$\overline{B(c,t)} = \{x \in \mathbb{K} : \ |x - c| \leq t\},$$

veremos que o conjunto $B(c,t)$ é aberto e fechado e o conjunto $\overline{B(c,t)}$ também é aberto e fechado.

Para um melhor embasamento as principais referências utilizadas foram [4], [2] e [6] referentes aos inteiros p-ádicos, além de um embasamento teórico sobre álgebra e teoria dos números com [3], [1], [5] e [8].

Capítulo 1

Números inteiros e racionais como inteiros p-ádicos

1.1 Motivação

Segundo [4], Kurt Hensel (1897) introduziu a ideia de número p-ádico para nos mostrar que é possível encontrarmos uma construção diferente da habitual para a métrica, e assim obtermos uma topologia sobre os racionais distinta da usual. Antes de apresentarmos a ideia de Hensel, vamos observar a seguinte situação:

Resolva a seguinte equação:[1]

$$x = 1 + 2x$$

Simplesmente poderíamos pensar numa resolução direta, encontrando $x = -1$ como solução. Mas um observador atento e um pouco mais criativo poderia pensar em tomar um meio iterativo e, como $x = 1 + 2x$, substituiria o x pelo seu valor, que num primeiro passo ficaria da seguinte forma:

$$x = 1 + 2(1 + 2x)$$

depois teríamos

$$x = 1 + 2(1 + 2(1 + 2x))$$

e

$$x = 1 + 2(1 + 2(1 + 2(1 + 2x))),$$

com este processo podendo se repetir várias vezes (de maneira infinita inclusive).

Observando tal fato, podemos pensar numa forma de construir uma sequência tal que

$$x_{n+1} = 1 + 2x_n.$$

[1] A resolução de fato será abordada no exemplo 1.3.

Neste ponto nos basta escolher um x_0, por exemplo partindo de um $x_0 = 1$, para podermos determinar, numa construção recorrente, uma sequência de modo que

$$\begin{aligned} x_0 &= 1 \\ x_1 &= 1 + 2x_0 = 1 + 2 \cdot 1 \\ x_2 &= 1 + 2x_1 = 1 + 2 \cdot (1 + 2 \cdot 1) \\ x_3 &= 1 + 2x_2 = 1 + 2 \cdot (1 + 2 \cdot (1 + 2 \cdot 1)) \\ &\vdots \end{aligned}$$

Realizando as operações em cada termo x_i da sequência temos que, neste caso, estamos somando potências de 2, observe:

$$\begin{aligned} x_0 &= 1 \\ x_1 &= 1 + 2 \\ x_2 &= 1 + 2 + 4 \\ x_3 &= 1 + 2 + 4 + 8 \\ &\vdots \end{aligned}$$

Que para n passos podemos representar como:

$$x_n = 1 + 2 + 2^2 + 2^3 + \ldots + 2^n$$

Vale ressaltar que, se tomarmos infinitos passos (n tendendo ao infinito), teremos uma soma infinita de potências. Assim sendo, também podemos escrever como uma soma de uma progressão geométrica, nesse caso com razão 2 e $a_0 = 1$, infinita.

$$S = \sum_{i=0}^{+\infty} 2^i$$

Neste ponto vale lembrar que uma soma infinita de uma progressão geométrica tem a seguinte forma:

$$1 + \alpha + \alpha^2 + \ldots = \frac{1}{1 - \alpha},$$

onde substituindo α por 2, obteremos -1. Apesar da substituição ser indevida, pois a soma de uma progressão geométrica infinita só converge se a razão estiver entre zero e um, isto nos apresenta um fato interessante, pois voltando para a equação original, ao resolvê-la de forma convencional, também obtemos o resultado -1. Tal fato aparentemente pode nos parecer um simples caso isolado, mas por outro lado podemos suspeitar deste processo e analisar mais a fundo as possibilidades para validar este caminho.

Notemos que seguimos um procedimento coerente, observando que podemos tratar a equação sugerida como uma série, até o fato de necessitarmos que a série seja convergente. Será possível que, através de alguma construção não convencional, podemos fazer uma série que aparentemente cresce indefinidamente, convergir?

Veremos que sim, é possível que isto aconteça. Mas antes precisaremos constatar toda a construção da estrutura matemática que nos proporcionará belos resultados acerca destas indagações.

1.2 Os inteiros p-ádicos.

A ideia de Hensel está ligada a resolução de sistemas de congruências módulo p^n. Este será o caminho que utilizaremos para determinarmos inteiros p-ádicos. Antes de considerarmos alguns exemplos, vamos relembrar algumas definições que nos serão úteis.

Definição 1.1 *Sejam a, b números inteiros e n um número natural. Diremos que a é congruente a b módulo n se a e b deixam o mesmo resto na divisão por n, em outras palavras, quando $(b-a)$ não deixa resto na divisão por n. Se isto acontece, escreve-se*

$$a \equiv b \ (mod \ n).$$

Por exemplo, $19 \equiv 3 \ (mod \ 8)$ e $21 \equiv 1 \ (mod \ 4)$, pois $19 - 3$ é divisível por 8, da mesma forma, $21 - 1$ é divisível por 4.

Note que, se tomarmos um número d natural, ele sempre será congruente módulo n ao seu resto na divisão euclidiana por n, sendo assim será congruente módulo n a algum dos números $0, 1, 2, 3, \ldots, n-1$. Por consequência, dois desses números não serão congruentes módulo n entre si.

Aqui deixamos ao leitor a fácil verificação de que se mantém as propriedades de reflexividade, simetria, transitividade, compatibilidade com a soma e a diferença, compatibilidade com o produto e com a regra do cancelamento. O leitor pode verificar estes resultados em [8] e obter um estudo mais detalhado sobre congruências em [5].

Portanto, temos que a relação $\equiv \ (mod \ n)$ (ser equivalente ao resto da divisão por n) tem um comportamento muito parecido com a relação de igualdade usual, com um pouco mais de atenção, vemos que, tanto a relação de congruência como a igualdade, são relações de equivalências envolvendo números inteiros.

Em geral, temos uma relação de equivalência $\sim$ sobre um conjunto genérico X quando:

(1) For reflexiva: $x \sim x \ \forall \ x \in X$.

(2) For simétrica: $x \sim y \Longrightarrow y \sim x$.

(3) For transitiva: $x \sim y$ e $y \sim z \Longrightarrow x \sim z$.

Não é foco deste trabalho apresentar de forma minuciosa as particularidades da construção desta relação de equivalência resultante da relação de congruência. Ficando a cargo do leitor, caso queira familiarizar-se melhor ou simplesmente relembrar, ver [8], para um estudo mais completo, consultar [1].

Definição 1.2 *Um inteiro p-ádico é definido como uma sequência da forma*

$$[\ldots, a_n, a_{n-1}, \ldots, a_2, a_1]_p \tag{1.1}$$

onde $0 \leqslant a_i \leqslant p-1$ *e* p *um número primo.*

Definição 1.3 *Dado um* p *primo, fixo, o conjunto formado por todos os inteiros p-ádicos será representado por* $\mathbb{Z}_p$.

Definição 1.4 *Chamaremos de anel de inteiros módulo* n *o quociente de* $\mathbb{Z}$ *pela relação* $\equiv\ (mod\ n)$. *Denotaremos*[2] *tal anel por* $\mathbb{Z}/n\mathbb{Z}$.

Por exemplo, para $n = 2$, teremos o anel $\mathbb{Z}/2\mathbb{Z}$. Formado pelas classes de equivalência correspondentes a congruência módulo 2, isto é, os elementos congruentes ao 0 e os elementos congruentes ao 1, que denotaremos por $\bar{0}$ e $\bar{1}$ respectivamente. Em [3] o leitor pode aprofundar-se ou apenas relembrar as propriedades e resultados acerca dos anéis quocientes.

Para resolvermos as congruências, consideraremos os anéis $\mathbb{Z}/p^n\mathbb{Z}$, com n número natural e p um número primo, ou seja, serão os anéis gerados pelas potências de um número primo.

1.2.1 Resolvendo congruências módulo p^n.

O caminho que buscaremos para determinar um número p-ádico passa pela sequência de soluções de um sistema de congruências. Portanto, tornam-se necessárias as definições que seguem.

Definição 1.5 *O conjunto de equações da forma*

$$X - a \equiv 0\ (mod\ p^i)$$

com $1 \leq i \leq n$, *será denominado sistema de congruências módulo* p^n, *e denotado da forma:*

$$X - a \equiv 0\ (mod\ p^n).$$

Utilizaremos os sistemas de congruências módulo p^n para encontrarmos inteiros p-ádicos. Nosso objetivo não é generalizar de alguma forma a resolução de um sistema de congruências desse tipo. Vamos seguir através de exemplos que nos apresente as particularidades da determinação de inteiros p-ádicos.

Ao resolvermos um sistema de congruências, encontraremos uma sequência de resultados que definiremos como segue.

Definição 1.6 *A sequência* $(x_i)_{1\leq i\leq n}$ *das soluções de* $X - a \equiv 0\ (mod\ p^n)$ *será dita coerente se*

$$x_{i+1} \equiv x_i\ (mod\ p^i)$$

para todo i, $1 \leq i < n$.

[2]Por convenção neste trabalho, deixaremos a notação $\mathbb{Z}_p$, que apresenta-se mais natural para os anéis quocientes em outras situações, destinada a representar os números inteiros p-ádicos.

Portanto, quando estamos resolvendo um sistema de congruências módulo p^n, estamos buscando uma sequência de soluções coerentes.

Outro fato importante de se perceber é que cada x_i pode ser escrito como uma série de potências de tal forma que temos

$$x_1 = a_1 \cdot p^0$$
$$x_2 = a_1 \cdot p^0 + a_2 \cdot p$$
$$x_3 = a_1 \cdot p^0 + a_2 \cdot p + a_3 \cdot p^2$$
$$x_4 = a_1 \cdot p^0 + a_2 \cdot p + a_3 \cdot p^2 + a_4 \cdot p^3$$
$$\vdots$$
$$x_n = a_1 \cdot p^0 + a_2 \cdot p + a_3 \cdot p^2 + a_4 \cdot p^3 + \cdots + a_n \cdot p^n.$$

Para escrevermos nosso inteiro p-ádico, consideraremos os coeficientes

$$a_1, a_2, a_3, \ldots$$

da série de potências encontrada.

Exemplo 1.1 *Determinar um inteiro 2-ádico solução para a equação* $x - 3 = 0$.

Solução: Resolvendo a congruência $x - 3 \equiv 0 \ (mod\ 2^n)$ temos,
para $n = 1$:

$$x_1 - 3 \equiv 0 \ (mod\ 2) \Longrightarrow$$
$$x_1 \equiv 3 \ (mod\ 2) \Longrightarrow$$
$$x_1 \equiv 1 \ (mod\ 2).$$

Temos nossa primeira solução, para $n = 1$, $x_1 = 1$.

Para $n = 2$, ficamos com:

$$x_2 - 3 \equiv 0 \ (mod\ 2^2)$$
$$x_2 \equiv 3 \ (mod\ 2^2)$$

Observe que a partir do x_2, as soluções se repetem, pois $3 < 2^n$ a partir de $n = 2$, logo, teremos como conjunto solução

$$s = (1, 3),$$

que é uma sequência coerente. O representante 2-ádico solução desta equação pode ser determinado observando-se a soma de potências e tomando apenas os coeficientes de cada termo, neste caso ficamos com:

$$x_2 = 1 \cdot 2^0 + 1 \cdot 2^1.$$

Assim, encontramos

$$[1, 1]_2.$$

■

Vejamos que $x - 3 = 0$ possui solução nos inteiros, a saber $x = 3$ e, não por coincidência, o representante 2-ádico da solução da equação é o correspondente binário do 3.

Encontrar representantes 2-ádicos de números inteiros positivos é buscar o representante binário deste número. A única diferença será a representação.

Exemplo 1.2 *Determinar o representante 5-ádico do 436.*

Solução: Podemos buscar uma equação tal que sua solução seja o 436. Mas como vimos no exemplo anterior que para números inteiros positivos o processo é idêntico ao método utilizado para mudança de base, vamos buscar escrever o 436 como uma soma de potências. O representante do 436 nos 5-ádicos será $[3, 1, 2, 1]_5$, pois temos que 436 pode ser escrito como uma soma de potências de base 5 da seguinte forma:

$$436 = 1 \cdot 5^0 + 2 \cdot 5^1 + 1 \cdot 5^2 + 3 \cdot 5^3.$$

■

Veremos mais a frente, que para um número natural o processo sempre será finito.

Exemplo 1.3 *Utilizando congruências, determinar uma solução para a equação proposta no início deste capítulo ($x = 1 + 2x$), para $p = 2$.*

Solução: Tomemos o sistema de soluções positivas para a congruência

$$x \equiv 1 + 2x \ (mod\ 2^n).$$

Inicialmente podemos escrever, após simples manipulações:

$$x_n \equiv -1 \ (mod\ 2^n),$$

que, para melhor visualização do resultado, vamos analisar alguns passos. Para $n = 1$, teremos:

$$x_1 \equiv -1 \ (mod\ 2) \Longrightarrow x_1 \equiv 1 \ (mod\ 2),$$

para $n = 2$:

$$x_2 \equiv -1 \ (mod\ 2^2) \Longrightarrow x_2 \equiv 3 \ (mod\ 4),$$

$n = 3$:

$$x_3 \equiv -1 \ (mod\ 2^3) \Longrightarrow x_3 \equiv 7 \ (mod\ 8).$$

Teremos como solução, a sequência:

$$(1, 3, 7, 15, 31, 63, \dots)$$

Observe que cada termo, exceto o primeiro, é coerente com seu antecessor. Além disso, cada x_i pode ser escrito como uma soma de potências de 2.

$$x_1 = 1 = 1 \cdot 2^0$$

$$x_2 = 3 = 1 \cdot 2^0 + 1 \cdot 2^1$$
$$x_3 = 7 = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2$$

Realizando este processo n vezes, teremos

$$x_n = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + \cdots + 1 \cdot 2^n$$

Portanto, o inteiro 2-ádico solução da equação $x = 1 + 2x$ será:

$$[\ldots, 1, 1, 1, 1, 1]_2$$

■

Podemos ver que a equação resolvida anteriormente possui o -1 como solução e mais a frente veremos que o resultado encontrado é o representante p-ádico do -1. Veremos também, após a definição da adição e da multiplicação nos inteiros p-ádicos, que para todo inteiro negativo, sua representação p-ádica será infinita.

1.2.2 Adição em $\mathbb{Z}_p$.

Sejam a e b dois inteiros p-ádicos para um dado p primo fixo. Vimos que para construirmos um representante p-ádico necessariamente teremos uma soma de potências de p. Portanto, para cada p-ádico distinto, teremos uma série de potências associada. Consideremos estas séries associadas. Sejam:

$$a = \sum_{i>0} a_i p^{i-1} \quad \text{e} \quad b = \sum_{i>0} b_i p^{i-1}$$

A adição $a + b$ será um novo inteiro p-ádico c,

$$c = \sum_{i>0} c_i p^{i-1}$$

tal que $c_k = a_k + b_k$ se $a_k + b_k \leq p - 1$, caso contrário, $c_k = a_k + b_k - p$ e "transportamos" $+1$ para o próximo coeficiente, no caso a_{k+1}. Assim prosseguimos até o $a_n + b_n$. Fazendo uma analogia com o algoritmo da soma que utilizamos usualmente e considerando a representação p-ádica dos números, observemos o seguinte exemplo.

Exemplo 1.4 *Determinar a soma de* $[2, 0, 1, 1, 2, 0]_3 + [1, 0, 1, 0, 0, 2]_3$.

Solução: Podemos resolver a soma $[2, 0, 1, 1, 2, 0]_3 + [1, 0, 1, 0, 0, 2]_3$ da seguinte forma:

$$\begin{array}{rcccccccc} & 1 & & & & & & & \\ & & [2, & 0, & 1, & 1, & 2, & 0]_3 \\ + & & [1, & 0, & 1, & 0, & 0, & 2]_3 \\ \hline & [1, & 0, & 0, & 2, & 1, & 2, & 2]_3 \end{array}$$

Obtendo como resultado $[1, 0, 0, 2, 1, 2, 2]_3$.
Observemos que

$$528 = [2, 0, 1, 1, 2, 0]_3 \quad \text{e} \quad 272 = [1, 0, 1, 0, 0, 2]_3$$

e que $[1, 0, 0, 2, 1, 2, 2]_3 = 800$, que é a soma $528 + 272$.

■

Voltemos ao exemplo 1.3. Nele determinamos $[\ldots, 1, 1, 1, 1, 1]_2$ como solução 2-ádica de $x = 1 + 2x$. Sabemos também que nos inteiros p-ádicos, para qualquer p, o 1 é $[1]_p$. Tomemos o $[1]_2$. Veja que podemos representar o $[1]_2$ por $[\ldots, 0, 0, 0, 1]_2$.

$$\begin{array}{rccccc} & 1 & 1 & 1 & 1 & \\ & [\ldots, & 1, & 1, & 1, & 1, & 1]_2 \\ + & [\ldots, & 0, & 0, & 0, & 0, & 1]_2 \\ \hline & [\ldots, & 0, & 0, & 0, & 0, & 0]_2 \end{array}$$

Encontramos o $[0]_2$. A representação 2-ádica para o zero. Mas estamos somando 1 com algum valor que nos dá o zero como resultado, então tal número tem que ser a representação p-ádica do -1. Corroborando com o que já observamos sobre representação p-ádica de inteiros negativos.

1.2.3 Multiplicação em $\mathbb{Z}_p$.

Tal como a soma, é possível construir para o produto um processo análogo ao realizado com os números naturais. Neste fato, quando a multiplicação de dois coeficientes é maior que $p - 1$, procederemos de forma similar como com a adição. Sejam a e b dois números p-ádicos, com a_i e b_j dígitos desses números. Consideremos também q_{ij} como o quociente de $a_i \cdot b_j$ por p e r_{ij} como o resto desta mesma divisão. Quando multiplicarmos dois dígitos desses números, caso o produto seja menor que p, continuaremos a multiplicação normalmente. Caso seja igual ou maior que p, dividiremos o resultado por p, somando-se o quociente ao próximo dígito a esquerda, "descendo" o resto da divisão. Observe os exemplos que seguem:

Exemplo 1.5 *Consideremos $n_1 = 27$, $n_2 = 8$ e $p = 5$. Calcular $n_1 \cdot n_2$.*

Solução: Temos que $27 = [1, 0, 2]_5$ e $8 = [1, 3]_5$. O algoritmo para o produto $[1, 0, 2]_5 \cdot [1, 3]_5$ seria o seguinte:

$$\begin{array}{rcccc} & & & 1 & \\ & & 1 & 0 & 2 \\ \times & & & 1 & 3 \\ \hline & & 3 & 1 & 1 \\ + & 1 & 0 & 2 & \\ \hline & 1 & 3 & 3 & 1 \end{array}$$

Com o algoritmo temos que $[1, 0, 2]_5 \cdot [1, 3]_5 = [1, 3, 3, 1]_5 = 216 = 27 \cdot 8$.

■

Exemplo 1.6 *Vamos considerar os representantes 7-ádicos para os números* 741 *e* 369*. Calcular o produto destes representantes, nos 7-ádicos.*

Solução: Inicialmente observemos que $369 = [1,0,3,5]_7$ e $741 = [2,1,0,6]_7$. Construindo, passo a passo, teremos um algoritmo da seguinte forma:

$$\begin{array}{cccccc} & & & {\scriptstyle 3} & {\scriptstyle 4} & \\ & & 1 & 0 & 3 & 5 \\ \times & & 2 & 1 & 0 & 6 \\ \hline & & 6 & 3 & 1 & 2 \\ & 0 & 0 & 0 & 0 & \end{array}$$

Vale observar neste ponto que: ao multiplicarmos o 6 por 5, que nos dá 30 como resultado, dividimos por 7, o 2 que é seu resto, "desce" e o 4, que é o quociente, "sobe" sobre o próximo termo da esquerda. Continuando, temos

$$\begin{array}{cccccccc} & & & & & {\scriptstyle 1} & & \\ & & & & {\scriptstyle \not 3} & {\scriptstyle \not 4} & & \\ & & & 1 & 0 & 3 & 5 & \\ & \times & & 2 & 1 & 0 & 6 & \\ \hline & & & 6 & 3 & 1 & 2 & \\ & & 0 & 0 & 0 & 0 & & \\ & 1 & 0 & 3 & 5 & & & \\ + & 2 & 1 & 0 & 3 & & & \\ \hline & 2 & 2 & 1 & 6 & 1 & 1 & 2 \end{array}$$

Encontramos assim o número $[2,2,1,6,1,1,2]_7$ que é o representante p-ádico para 273429 (resultado do produto de 369 por 741).

■

1.2.4 Representantes p-ádicos de inteiros negativos.

Chegamos a conclusão anteriormente que o representante p-ádico do -1 possuía representação infinita.[3] Agora que temos definido os conceitos de adição e multiplicação de inteiros p-ádicos, poderemos afirmar que a representação p-ádica de um número negativo será sempre infinita.

Proposição 1.1 *Seja $k \in \mathbb{Z}^+$, então a representação p-ádica de $-k$ é infinita.*

Demonstração: Já vimos que a multiplicação está definida nos inteiros p-ádicos e que para determinarmos o inverso aditivo de qualquer número basta multiplicarmos ele por -1. Se a representação p-ádica do -1 for infinita para todo p primo, temos que a representação p-ádica de qualquer inteiro negativo será infinita.
Portanto, queremos mostrar que -1 possui representação p-ádica infinita para qualquer p primo. Para isso, buscaremos o representante p-ádico para a solução da equação $x + 1 = 0$, considerando o sistema de congruências $x + 1 \equiv 0 \ (mod\ p^n)$.

[3] Fato observado na seção 1.2.2.

Teremos

$$\begin{aligned} x_1 &\equiv -1 \ (mod\ p) \rightarrow x_1 = p-1 \\ x_2 &\equiv -1 \ (mod\ p^2) \rightarrow x_2 = p^2-1 \\ x_3 &\equiv -1 \ (mod\ p^3) \rightarrow x_3 = p^3-1 \\ x_4 &\equiv -1 \ (mod\ p^4) \rightarrow x_4 = p^4-1 \\ &\vdots \end{aligned}$$

Formando uma sequência de soluções

$$(p-1, p^2-1, p^3-1, p^4-1, \dots).$$

É simples perceber que tal sequência de soluções é coerente, pois cada termo x_i é congruente a x_{i-1} módulo p^{i-1}. Podemos assim, escrever como uma série de potências da forma:

$$\alpha = (p-1)\cdot p^0 + (p-1)\cdot p^1 + (p-1)\cdot p^2 + (p-1)\cdot p^3 + \cdots .$$

Chegando assim ao representante p-ádico do -1, que terá a seguinte estrutura:

$$[\dots, (p-1), (p-1), (p-1), (p-1)]_p, \ \forall\ p \ \text{ primo.} \tag{1.2}$$

Sempre que $k \in \mathbb{Z}^+$, para determinarmos a representação p-ádica do $-k$, basta multiplicarmos a representação p-ádica do k pela representação p-ádica do -1, que será sempre da forma 1.2.
Seja $k = [a_n, a_{n-1}, \dots, a_2, a_1]_p$, faremos

$$-k = [\dots, (p-1), (p-1), (p-1), (p-1)]_p \cdot [a_n, a_{n-1}, \dots, a_2, a_1]_p.$$

A representação do $-k$ será sempre infinita, pois a representação do -1 sempre será infinita.

■

Portanto podemos nos fazer a seguinte pergunta: Qual a estrutura algébrica de $\mathbb{Z}_p$? As implicações seguintes nos darão uma visão mais ampla para respondermos esta pergunta.

1.2.5 $(\mathbb{Z}_p, +)$ é um Grupo Abeliano.

Por analogia com os números reais, é evidente que a adição de inteiros p-ádicos é fechada, associativa e comutativa, e que o elemento aditivo neutro é apenas a série com todos os coeficientes iguais a zero. Mas o que sabemos sobre os inversos aditivos? Aqui queremos decidir o seguinte: dado um α inteiro p-ádico, que forma terá o $-\alpha$?

Notemos que qualquer inteiro positivo tem representação p-ádica finita, pois para cada x número inteiro é possível tomarmos um n suficientemente grande para termos

$p^n > x$. Tornando-o, por construção, finito.

Seja $[1]_p$ a unidade. Sejam também

$$\alpha = [\ldots, 0, 0, 0, a_n, a_{n-1}, \ldots, a_3, a_2, a_1]_p$$

um p-ádico finito, e

$$-\alpha = [\ldots, b_{n+3}, b_{n+2}, b_{n+1}, b_n, b_{n-1}, b_{n-2}, \ldots, b_3, b_2, b_1]_p$$

o seu inverso aditivo.

Observe que temos $\alpha + (-\alpha) = 0$, assim ao somarmos termo a termo encontraremos o número p-ádico $\beta = [\cdots, 0, 0, 0, \cdots, 0, 0, 0]$, observe que para isso acontecer basta que a soma dos termos seja igual a p, pois $p = 0$ em $\mathbb{Z}_p$.

Assim, temos:

$$b_1 + a_1 = p \Rightarrow b_1 = p - a_1 \Rightarrow b_1 = (p-1) - a_1 + [1]_p$$

Observe que, assim como na base 10, quando a soma entre dois termos for igual ou maior, no caso a p, deve-se acrescentar uma (ou mais) unidade(s) a soma dos termos seguintes, ou seja,

$$b_2 + a_2 + 1 = p \Rightarrow b_2 = (p-1) - a_2$$

$$b_3 + a_3 + 1 = p \Rightarrow b_3 = (p-1) - a_3$$

Generalizando esse processo chegamos ao seguinte resultado:

$$b_n + a_n + 1 = p \Rightarrow b_n = (p-1) - a_n$$

Veja também que:

$$b_{n+1} + 0 + 1 = p \Rightarrow b_{n+1} = p - 1$$

$$b_{n+2} + 0 + 1 = p \Rightarrow b_{n+2} = p - 1$$

Logo, temos que

$$b_{n+k} + 0 + 1 = p \Rightarrow b_{n+k} = p - 1$$

para todo $k \geq 1$.

Assim, podemos criar um método rápido e direto para encontrar o simétrico de um número na forma p-ádica.

$$-\alpha = [\cdots, p-1, p-1, \cdots, (p-1)-\alpha_n, (p-1)-\alpha_{n-1}, \cdots, (p-1)-\alpha_2, (p-1)-\alpha_1] + [1]_p$$

Agora, se temos qualquer inteiro p-ádico $\alpha = \sum_{i>0} \alpha_i p^{i-1}$ podemos definir seu inverso aditivo. Tomemos um γ tal que

$$\gamma = \sum_{i>0} (p-1-\alpha_i) p^{i-1}. \tag{1.3}$$

Este número é bem definido como um inteiro p-ádico desde que $0 \leq \alpha_i \leq p-1 \Longrightarrow 0 \leq p-1-\alpha_i \leq p-1$. Pelo argumento de que $\alpha+\gamma+1 = 0$ temos que para qualquer $\alpha \in \mathbb{Z}$ temos um inverso aditivo, notadamente $\gamma+1$. Uma vez que os inteiros p-ádicos possuem inverso aditivo, $\mathbb{Z}_p$ junto com a adição formam um grupo abeliano. Como consequência, agora podemos representar os inteiros negativos como um número p-ádico. Em outras palavras, temos $\mathbb{Z} \subset \mathbb{Z}_p$.

Exemplo 1.7 *Determinar o inverso aditivo do inteiro 5-ádico* $\alpha = [1, 2, 0, 3]_5$.

Solução: Utilizando 1.3, podemos determinar γ. Teremos

$$\gamma = [\ldots, 4, 4, 4, 3, 2, 4, 1]_5.$$

Agora nos basta somar a unidade. Encontrando

$$-\alpha = [\ldots, 4, 4, 4, 3, 2, 4, 2]_5.$$

■

1.2.6 $(\mathbb{Z}_p, +, \cdot)$ é um Anel.

Tal qual acontece com a adição, a multiplicação nos inteiros p-ádicos é fechada, associativa e comutativa, por analogia com os números reais. A identidade da multiplicação é justamente o 1, pois $1 = 1 + 0 \cdot p + 0 \cdot p^2 + 0 \cdot p^3 + \ldots$ para todo primo $p \in \mathbb{Z}$.

1.2.7 $(\mathbb{Z}_p, +, \cdot)$ é um Domínio de Integridade.

Como já temos um anel comutativo, nos basta mostrar que $\mathbb{Z}_p$ não possui divisores de zero.

Proposição 1.2 *Para todo* a *e* $b \in \mathbb{Z}_p$,

$$a \cdot b = 0 \Longleftrightarrow a = 0 \text{ ou } b = 0.$$

Demonstração: *Seja* $a = \sum_{i>0} a_i p^{i-1}$, $b = \sum_{i>0} b_i p^{i-1} \in \mathbb{Z}$. *Vamos supor que* $a \cdot b = c = \sum_{i>0} c_i p^{i-1}$. *Se* a *e* b *são ambos diferentes de zero, cada um deles tem*

um coeficiente diferente de zero, por exemplo a_n para a e b_m para b. Pela definição da multiplicação p-ádica, temos

$$c_{n+m} = a_n b_m \ mod\ p.$$

Desde que p não divida a_n ou b_m, este não divide $a_n \cdot b_m \Longrightarrow c_{n+m} \neq 0$ então $c \neq 0$ e assim

$$a \cdot b = 0 \Longleftrightarrow a = 0 \ ou\ b = 0.$$

■

1.2.8 Racionais como inteiros p-ádicos.

Nesta seção, nosso objetivo é apresentar o procedimento para obtenção do representante p-ádico de um número racional. Além disso, ver que nem sempre é possível determinarmos um representante p-ádico para um número racional dado um p fixo.

Exemplo 1.8 *Determinar uma solução para $2x - 3 = 0$ no conjunto dos 5-ádicos.*

Solução: Analisaremos as soluções para a congruência $2x - 3 \equiv 0\ (mod\ p^n)$ com n tendendo ao infinito. Ficamos com:

$$\begin{gathered}
2x \equiv 3\ (mod\ 5) \Longrightarrow x_1 \equiv 4\ (mod\ 5) \\
2x \equiv 3\ (mod\ 5^2) \Longrightarrow x_2 \equiv 14\ (mod\ 5^2) \\
2x \equiv 3\ (mod\ 5^3) \Longrightarrow x_3 \equiv 64\ (mod\ 5^3) \\
2x \equiv 3\ (mod\ 5^4) \Longrightarrow x_4 \equiv 314\ (mod\ 5^4) \\
2x \equiv 3\ (mod\ 5^5) \Longrightarrow x_5 \equiv 1564\ (mod\ 5^5) \\
\vdots
\end{gathered}$$

Ficamos com uma sequência coerente de soluções

$$x = (4, 14, 64, 314, 1564, \dots)$$

Note ainda que podemos escrever cada x_i como uma soma de potências, ficando com:

$$\begin{gathered}
x_1 = 4 = 4 \cdot 5^0 \\
x_2 = 14 = 4 \cdot 5^0 + 2 \cdot 5^1 \\
x_3 = 64 = 4 \cdot 5^0 + 2 \cdot 5^1 + 2 \cdot 5^2 \\
x_4 = 314 = 4 \cdot 5^0 + 2 \cdot 5^1 + 2 \cdot 5^2 + 2 \cdot 5^3 \\
x_5 = 1564 = 4 \cdot 5^0 + 2 \cdot 5^1 + 2 \cdot 5^2 + 2 \cdot 5^3 + 2 \cdot 5^4
\end{gathered}$$

Fazendo n tender ao infinito, teremos

$$x_n = 4 \cdot 5^0 + 2 \cdot 5^1 + 2 \cdot 5^2 + 2 \cdot 5^3 + 2 \cdot 5^4 + \dots$$

Portanto o inteiro 5-ádico, solução da equação $2x - 3 = 0$ será:

$$[\dots, 2, 2, 2, 2, 4]_5.$$

■

Tomemos o resultado deste exemplo, $[\ldots, 2, 2, 2, 2, 4]_5$. Vamos multiplicar ele por $[2]_5$, que é o inteiro p-ádico correspondente ao número inteiro 2. Vejamos:

$$\begin{array}{rcccccc} & & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & \\ & [\ldots & 2, & 2, & 2, & 2, & 4]_5 \\ \times & [\ldots & 0, & 0, & 0, & 0, & 2]_5 \\ \hline & [\ldots & 0, & 0, & 0, & 0, & 3]_5 \end{array}$$

Encontramos o $[3]_5$ como resultado. Observe que o $[3]_5$ é o correspondente 5-ádico do 3. Multiplicamos um número por 2 e encontramos o 3, este número só pode ser o $\frac{3}{2}$, o que coincide com a solução da equação $2x - 3 = 0$ nos racionais.

Proposição 1.3 *Seja* $\frac{a}{b}$, $a, b \in \mathbb{Z}$, $b \neq 0$ *e* $(a, b) = 1$. *A fração* $\frac{a}{b}$ *possui representação p-ádica se e somente se* $(b, p) = 1$.

Demonstração: Para encontrarmos o representante p-ádico de $\frac{a}{b}$ consideremos a equação linear $bx - a = 0$, além disto, esta equação tem que possuir soluções no sistema de congruências

$$bx - a \equiv 0 \ (mod\ p^n).$$

Mas observe que este sistema de congruências só possui solução se a primeira equação tiver solução. No caso,

$$bx_1 \equiv a \ (mod\ p).$$

E esta equação só possui solução quando b possui inverso multiplicativo em $\mathbb{Z}/p\mathbb{Z}$. Isto acontece se e somente se $(b, p) = 1$. Portanto, fica claro que para termos um representante p-ádico para $\frac{a}{b}$ necessitamos que $(b, p) = 1$.

■

Observando a proposição anterior fica fácil perceber que o denominador da fração, na sua forma irredutível, não pode ser múltiplo de p, visto que o p é fixo.

1.2.9 Irracionais algébricos como inteiros p-ádicos.

Números irracionais algébricos também podem ser representados como inteiros p-ádicos. Para isto ser possível é necessário alguns fatos. Inicialmente definiremos o que vem a ser um resíduo quadrático.

Definição 1.7 *Sempre que uma equação da forma*

$$X^2 \equiv d \ (mod\ p)$$

possuir solução (isto é, se d for um "quadrado perfeito" em $\mathbb{Z}/p\mathbb{Z}$*) diremos que d é um resíduo quadrático módulo p.*

Exemplo 1.9 *Determinar os representantes 11-ádicos das soluções de* $x^2 - 3 = 0$.

Solução: Sabidamente, $x^2 - 3 = 0$ não possui solução em $\mathbb{Z}$. Utilizaremos um método semelhante ao utilizado anteriormente para encontrarmos ao menos uma expansão p-ádica para as soluções desta equação. Temos $p = 11$. Queremos encontrar uma expansão 11-ádica para possíveis soluções da equação dada. Portanto queremos analisar o sistema de congruências

$$x^2 \equiv 3 \ (mod\ 11^n).$$

Para o caso $n = 1$, temos que

$$x_1^2 \equiv 3 \ (mod\ 11) \Rightarrow x_1 \equiv \pm 5 \ (mod\ 11)$$
$$x_1 \equiv 5 \ (mod\ 11) \text{ ou } x_1 \equiv 6 \ (mod\ 11)$$

Para $n = 2$, fazemos $x = 5 + 11k$ ou $x = 6 + 11k$ e resolvemos:

$$(5 + 11k)^2 \equiv 3 \ (mod\ 11^2)$$
$$25 + 110k + 121k^2 - 3 \equiv 0 \ (mod\ 121)$$
$$22 + 110k \equiv 0 \ (mod\ 121)$$
$$2 + 10k \equiv 0 \ (mod\ 11)$$
$$10k \equiv 9 \ (mod\ 11)$$
$$k \equiv 2 \ (mod\ 11)$$

Então, chegamos à

$$x = 5 + 11 \cdot 2$$
$$x = 27 \Rightarrow X \equiv 27 \ (mod\ 121)$$

Com as soluções sendo

$$x_2 \equiv \pm 27 \ (mod\ 121)$$
$$x_2 \equiv 27 \ (mod\ 121) \text{ ou } x_2 \equiv 94 \ (mod\ 121)$$

Para $n = 3$, procederemos de maneira análoga a anterior, portanto consideremos $x = 27 + 121j$ ou $x = 94 + 121j$ e, substituindo, determinamos:

$$(27 + 121j)^2 \equiv 3 \ (mod\ 1331)$$
$$27^2 + 54 \cdot 121j + 11^4 j^2 - 3 \equiv 0 \ (mod\ 1331)$$
$$726 + 54 \cdot 121j \equiv 0 \ (mod\ 1331)$$
$$6 + 54j \equiv 0 \ (mod\ 11)$$

$$54j \equiv 5 \ (mod\ 11)$$
$$j \equiv 6 \ (mod\ 11)$$

Assim teremos,

$$x = 27 + 121 \cdot 6$$
$$x = 753 \Rightarrow x \equiv 753 \ (mod\ 1331)$$

Com soluções

$$x_3 \equiv \pm 753 \ (mod\ 1331)$$
$$x_3 \equiv 753 \ (mod\ 1331) \text{ ou } x_3 \equiv 578 \ (mod\ 1331)$$

Como este processo acontece indefinidamente, podemos observar duas sequências coerentes de soluções, sendo elas

$$\alpha_1 = (5, 27, 753, \ldots)$$

e

$$\alpha_2 = (6, 94, 578, \ldots) = (-5, -27, -753, \ldots) = -\alpha_1$$

que nos apresenta duas séries de potências:

$$\alpha_1 = 5 \cdot 11^0 + 2 \cdot 11 + 6 \cdot 11^2 + \ldots$$

e

$$\alpha_2 = 6 \cdot 11^0 + 8 \cdot 11^1 + 4 \cdot 11^2 + \ldots$$

Os representantes 11-ádicos de α_1 e α_2 serão

$$\alpha_1 = [\ldots, 4, 8, 6]_{11}$$
$$\alpha_2 = [\ldots, 6, 2, 5]_{11}$$

Esses, números, α_1 e α_2 são de fato soluções para a equação $x^2 = 3$ no conjunto dos inteiros 11-ádicos.

■

No exemplo anterior, determinamos os representantes 11-ádicos que são solução da equação $x^2 - 3 = 0$. Se tomarmos o α_1 por exemplo, e multiplicarmos por ele mesmo, teremos:

$$\alpha_1 \cdot \alpha_1 = [\ldots, 4, 8, 6]_{11} \cdot [\ldots, 4, 8, 6]_{11} = [\ldots, 0, 0, 3]_{11} = [3]_{11},$$

e o $[3]_{11}$ é a representação 11-ádica do 3. O mesmo vale para o α_2. Sendo assim podemos admitir que α_1 e α_2 são as representações 11-ádicas de $\pm\sqrt{3}$.

Exemplo 1.10 *Determinar as soluções da equação $x^2 - x - 1 = 0$ no conjunto dos inteiros p-ádicos.*

Solução: Estamos querendo determinar soluções para o sistema de congruências

$$x^2 - x - 1 \equiv 0 \ (mod\ p^n). \tag{1.4}$$

De maneira geral, estamos querendo resolver a congruência

$$ax^2 + bx + c \equiv 0 \ (mod\ n),$$

que é o mesmo que, completando quadrados, resolvermos a seguinte congruência:

$$(2ax + b)^2 \equiv b^2 - 4ac \ (mod\ n).$$

Assim teremos em nosso exemplo que resolver a congruência 1.4, que será o mesmo que resolvermos o sistema de congruências

$$(2x - 1)^2 \equiv 1 + 4 \ (mod\ p^n) \Longrightarrow (2x - 1)^2 \equiv 5 \ (mod\ p^n).$$

Escrevendo $2x - 1 = \alpha$ ficamos com:

$$\alpha^2 \equiv 5 \ (mod\ p^n).$$

Notemos aqui que precisamos de um p primo tal que o 5 seja um resíduo quadrático módulo p (definição 1.7), para resolvermos o caso $n = 1$. Como vamos determinar uma sequência coerente de soluções, se o caso $n = 1$ não possuir solução, nosso problema não tem solução.[4] O primeiro primo que possui 5 como resíduo quadrático é o 11, vamos utilizá-lo. Para $n = 1$ ficaremos com

$$\alpha_1^2 \equiv 5 \ (mod\ 11) \Longrightarrow \alpha_1 \equiv \pm 4 \ (mod\ 11).$$

Podemos dividir em dois casos:

$$\alpha_1' \equiv 4 \ (mod\ 11) \Longrightarrow (2x_1' - 1) \equiv 4 \ (mod\ 11)$$
$$2x_1' \equiv 5 \ (mod\ 11)$$
$$x_1' \equiv 8 \ (mod\ 11)$$

e

$$\alpha_1'' \equiv -4 \ (mod\ 11) \Longrightarrow (2x_1'' - 1) \equiv 7 \ (mod\ 11)$$
$$2x_1'' \equiv 8 \ (mod\ 11)$$
$$x_1'' \equiv 4 \ (mod\ 11).$$

Repetiremos o processo, agora para o caso $n = 2$. Ficaremos com

$$\alpha_2^2 \equiv 5 \ (mod\ 11^2) \Longrightarrow \alpha_2 \equiv \pm 48 \ (mod\ 11^2).$$

Separando em dois casos,

$$\alpha_2' \equiv 48 \ (mod\ 11^2) \Longrightarrow (2x_2' - 1) \equiv 48 \ (mod\ 11^2)$$

[4] Ver [8] e [9] para relembrar ou aprofundar-se sobre os resíduos quadráticos.

$$2x_2' \equiv 49 \ (mod\ 11^2)$$
$$x_2' \equiv 85 \ (mod\ 11^2)$$

e

$$\alpha_2'' \equiv -48 \ (mod\ 11^2) \Longrightarrow (2x_2'' - 1) \equiv 73 \ (mod\ 11^2)$$
$$2x_2'' \equiv 74 \ (mod\ 11^2)$$
$$x_2'' \equiv 37 \ (mod\ 11^2)$$

Para uma melhor visualização do nosso problema, vamos seguir por mais duas vezes estes passos, considerando $n = 3$ e $n = 4$. Para $n = 3$:

$$\alpha_3^2 \equiv 5 \ (mod\ 11^3) \Longrightarrow \alpha_3 \equiv \pm 73 \ (mod\ 11^3).$$
$$\Downarrow$$
$$\alpha_3' \equiv 73 \ (mod\ 11^3) \Longrightarrow (2x_3' - 1) \equiv 73 \ (mod\ 11^3)$$
$$2x_3' \equiv 74 \ (mod\ 11^3)$$
$$x_3' \equiv 37 \ (mod\ 11^3)$$

e

$$\alpha_3'' \equiv -73 \ (mod\ 11^3) \Longrightarrow (2x_3'' - 1) \equiv 1258 \ (mod\ 11^3)$$
$$2x_3'' \equiv 1259 \ (mod\ 11^3)$$
$$x_3'' \equiv 1295 \ (mod\ 11^3)$$

Para $n = 4$:

$$\alpha_4^2 \equiv 5 \ (mod\ 11^4) \Longrightarrow \alpha_4 \equiv \pm 6582 \ (mod\ 11^4).$$
$$\Downarrow$$
$$\alpha_4' \equiv 6582 \ (mod\ 11^4) \Longrightarrow (2x_4' - 1) \equiv 6582 \ (mod\ 11^4)$$
$$2x_4' \equiv 6583 \ (mod\ 11^4)$$
$$x_4' \equiv 10612 \ (mod\ 11^4)$$

e

$$\alpha_4'' \equiv -6582 \ (mod\ 11^4) \Longrightarrow (2x_4'' - 1) \equiv 8059 \ (mod\ 11^4)$$
$$2x_4'' \equiv 8060 \ (mod\ 11^4)$$
$$x_4'' \equiv 4030 \ (mod\ 11^4)$$

Perceba que podemos construir duas sequências coerentes x_a e x_b com os resultados obtidos. São elas:

$$x_a = (8, 85, 1295, 10612, \dots)$$

e

$$x_b = (4, 37, 37, 4030, \dots).$$

Um sistema coerente de soluções nos permite escrever x_a e x_b como soma de potências de base $p = 11$. Ficaremos com o seguinte:

$$x_a = 8 \cdot 11^0 + 7 \cdot 11 + 10 \cdot 11^2 + 7 \cdot 11^3 + \cdots$$

$$x_b = 4 \cdot 11^0 + 3 \cdot 11 + 0 \cdot 11^2 + 3 \cdot 11^3 + \cdots$$

Finalmente, escrevendo o representante p-ádico de cada uma das raízes anteriores, temos:

$$x_a = [\dots, 7, 10, 7, 8]_{11}$$

$$x_b = [\dots, 3, 0, 3, 4]_{11}$$

Estes são os números que representam a proporção áurea, no conjunto dos 11-ádicos.

■

1.2.10 Complexos como inteiros p-ádicos.

Ainda utilizando congruências quadráticas, podemos ir um pouco mais além. O que acontecerá se construirmos um sistema de congruências partindo de uma equação polinomial, que possua apenas raízes complexas? Vejamos o exemplo que segue.

Exemplo 1.11 *Determinar se a equação $x^2+1 = 0$ possui solução no conjunto dos inteiros 5-ádicos.*

Solução: O proposto para resolvermos este problema será considerarmos o sistema de congruências

$$x^2 + 1 \equiv 0 \ (mod\ 5^n).$$

Como já visto, para cada n encontraremos ao menos duas soluções possíveis, portanto, será possível determinar duas sequências de soluções coerentes, implicando assim dois representantes 5-ádicos. Para $n = 1$, temos

$$x_1^2 + 1 \equiv 0 \ (mod\ 5) \Longrightarrow x_1^2 \equiv -1 \ (mod\ 5)$$

$$\Longrightarrow x_1^2 \equiv 4 \ (mod\ 5)$$

$$\Longrightarrow x_1 \equiv \pm 2 \ (mod\ 5)$$

$$x_1' = 2 \quad \text{ou} \quad x_1'' = 3.$$

Com $n = 2$,

$$x_2^2 + 1 \equiv 0 \ (mod\ 5^2) \Longrightarrow x_2^2 \equiv -1 \ (mod\ 5^2)$$

$$\Longrightarrow x_2^2 \equiv 24 \ (mod\ 5^2)$$

$$\Longrightarrow x_2 \equiv \pm 7 \ (mod\ 5^2)$$
$$x_2' = 7 \ \text{ ou } \ x_2'' = 18.$$

$n = 3$:

$$x_3^2 + 1 \equiv 0 \ (mod\ 5^3) \Longrightarrow x_3^2 \equiv -1 \ (mod\ 5^3)$$
$$\Longrightarrow x_3^2 \equiv 124 \ (mod\ 5^3)$$
$$\Longrightarrow x_3 \equiv \pm 57 \ (mod\ 5^3)$$
$$x_3' = 57 \ \text{ ou } \ x_3'' = 68.$$

$n = 4$:

$$x_4^2 + 1 \equiv 0 \ (mod\ 5^4) \Longrightarrow x_4^2 \equiv -1 \ (mod\ 5^4)$$
$$\Longrightarrow x_4^2 \equiv 624 \ (mod\ 5^4)$$
$$\Longrightarrow x_4 \equiv \pm 182 \ (mod\ 5^4)$$
$$x_4' = 182 \ \text{ ou } \ x_4'' = 443$$

$n = 5$:

$$x_5^2 + 1 \equiv 0 \ (mod\ 5^5) \Longrightarrow x_5^2 \equiv -1 \ (mod\ 5^5)$$
$$\Longrightarrow x_5^2 \equiv 3124 \ (mod\ 5^5)$$
$$\Longrightarrow x_5 \equiv \pm 1068 \ (mod\ 5^5)$$
$$x_5' = 1068 \ \text{ ou } \ x_5'' = 2057$$

$n = 6$:

$$x_6^2 + 1 \equiv 0 \ (mod\ 5^6) \Longrightarrow x_6^2 \equiv -1 \ (mod\ 5^6)$$
$$\Longrightarrow x_6^2 \equiv 15624 \ (mod\ 5^6)$$
$$\Longrightarrow x_6 \equiv \pm 1068 \ (mod\ 5^6)$$
$$x_6' = 1068 \ \text{ ou } \ x_6'' = 14557$$

Este processo, aparentemente, se dará de forma que para cada n que considerarmos, sempre teremos um par de soluções. Até o momento, temos duas sequências de soluções coerentes, que são

$$\alpha_1 = (2, 7, 57, 182, 2057, 14557, \dots)$$
$$\alpha_2 = (3, 18, 68, 443, 1068, 1068, \dots).$$

Que, escrevendo como uma série de potências, chegamos a:

$$\alpha_1 = 2 \cdot 5^0 + 1 \cdot 5^1 + 2 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + 4 \cdot 5^5 + 2 \cdot 5^6 + \dots$$
$$\alpha_2 = 3 \cdot 5^0 + 3 \cdot 5^1 + 2 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + 0 \cdot 5^5 + 2 \cdot 5^6 + \dots$$

Chegando as representações 5-ádicas:

$$\alpha_1 = [\ldots, 2, 4, 3, 1, 2, 1, 2]_5$$
$$\alpha_2 = [\ldots, 2, 0, 1, 3, 2, 3, 3]_5$$

Com o objetivo de verificarmos se há algum tipo de periodicidade na representação, buscamos auxílio a um método computacional para continuarmos encontrando algumas soluções.

$n = 7$

$$x_7^2 + 1 \equiv 0 \ (mod\ 5^7) \Longrightarrow x_7^2 \equiv -1 \ (mod\ 5^7)$$
$$\Longrightarrow x_7^2 \equiv 78124 \ (mod\ 5^7)$$
$$\Longrightarrow x_7 \equiv \pm 32318 \ (mod\ 5^7)$$
$$x_7' = 32318 \ \text{ ou } \ x_7'' = 45807$$

$n = 8$:

$$x_8^2 + 1 \equiv 0 \ (mod\ 5^8) \Longrightarrow x_8^2 \equiv -1 \ (mod\ 5^8)$$
$$\Longrightarrow x_8^2 \equiv 390624 \ (mod\ 5^8)$$
$$\Longrightarrow x_8 \equiv \pm 110443 \ (mod\ 5^6)$$
$$x_8' = 110443 \ \text{ ou } \ x_8'' = 280182$$

Seguindo este mesmo processo, encontramos

$$x_9' = 280182 \ \text{ ou } \ x_9'' = 1672943$$
$$x_{10}' = 3626068 \ \text{ ou } \ x_{10}'' = 6139557$$
$$x_{11}' = 23157318 \ \text{ ou } \ x_{11}'' = 25670807$$

Até o x_{11}, havíamos encontrado duas soluções para cada equação. A partir do x_{12} passamos a encontrar mais que duas soluções para a equação. Para o x_{12} foram encontradas 11337 raízes. Sendo que apenas um par destas 11337 são coerentes com as soluções encontradas para o x_{11}. Mais uma vez com auxilio computacional, foi possível determinarmos qual destas raízes nos seriam úteis. são elas:

$$x_{12}' = 123327057 \ \text{ e } \ x_{12}'' = 120813568$$

Para o x_{13} encontramos 14940 raízes. Novamente, um único par é coerente com a solução anterior, sendo ele:

$$x_{13}' = 123327057 \ \text{ e } \ x_{13}'' = 1097376068$$

Para o x_{14} encontramos 81325 raízes. O único par coerente foi:

$$x'_{14} = 5003169557 \quad \text{e} \quad x''_{14} = 1097376068$$

Para o x_{15} encontramos 171083 raízes. Com o seguinte par coerente:

$$x'_{15} = 11109655182 \quad \text{e} \quad x''_{15} = 19407922943$$

Completando as sequências coerentes que encontramos inicialmente ficaremos com

$$\alpha_1 = (2, 7, 57, 182, 2057, 14557, 45807, 280182, 280182, 6139557, 25670807, 123327057, 123327057, 5006139557, 11109655182 \dots)$$

$$\alpha_2 = (3, 18, 68, 443, 1068, 1068, 32318, 110443, 1672943, 3626068, 23157318, 120813568, 1097376068, 1097376068, 19407922943, \dots).$$

Encontraremos mais uma vez, dois representantes p-ádicos, que serão:

$$\alpha_1 = [\dots, 1, 4, 0, 2, 2, 3, 0, 3, 2, 4, 3, 1, 2, 1, 2]_5$$
$$\alpha_2 = [\dots, 3, 0, 4, 2, 2, 1, 4, 1, 2, 0, 1, 3, 2, 3, 3]_5$$

■

Podemos observar no exemplo anterior que é possível determinarmos inteiros p-ádicos correspondentes aos números complexos $\pm i$ $(\pm\sqrt{-1})$. Vimos que, ao menos até o 15º dígito, não há repetições de períodos, nos induzindo a supor que tal inteiro p-ádico é não-periódico.

Percebemos que a partir da congruência $x^2 \equiv -1 \ (mod\ 5^n)$, para $12 \leq n \leq 15$ encontramos várias soluções para cada uma das equações, porém, para cada uma delas haviam apenas um par de soluções coerentes com as soluções anteriores. Restando assim, apenas um par de solução para cada equação, como era de se esperar.

Além disso, cabe observar que este par de soluções também são simétricas entre si, como nos outros exemplos já vistos. Podemos verificar tal acontecimento considerando uma das soluções e utilizando o fato já visto anteriormente que diz que dado um inteiro p-ádico φ, seu inverso aditivo será dado por $\gamma + 1$ e γ definido pela equação 1.3. Neste ponto, temos um detalhe interessante, sabemos que se somarmos dois valores simétricos entre si, resultará 0, no caso estudado, $[0]_5$. O que só faz sentido se estivermos nos inteiros p-ádicos. Portanto, temos aqui duas representações, uma para o $+i$ e outra para o $-i$.

Agora temos dois fatos a estudar. Primeiro veremos que $\mathbb{Z}_p$ será sempre estritamente maior que $\mathbb{Z}$ e $\mathbb{Z}_p$ nunca será algebricamente fechado.

Proposição 1.4 *$\mathbb{Z}_p$ é estritamente maior que $\mathbb{Z}$, para todo p primo.*

Demonstração: Seja $\vartheta : \mathbb{Z} \longmapsto \mathbb{Z}_p$ uma função que relaciona um inteiro a seu representante p-ádico. É fácil observar que ϑ é injetora, pois cada elemento de $\mathbb{Z}$ possui seu representante p-ádico. Mas ϑ não é sobrejetora, pois sempre podemos tomar um $x \in \mathbb{Z}_p$ raiz de uma equação da forma $X^2 = m$ com $m \in \mathbb{N}$, tal que não possua raiz em $\mathbb{Z}$. Portanto, $\mathbb{Z}_p$ é estritamente maior que $\mathbb{Z}$.

■

Teorema 1.1 *$\mathbb{Z}_p$ não é algebricamente fechado.*

Demonstração: Para o caso $p = 2$, iniciemos a solução do sistema de congruências,

$$X^2 \equiv 3 \ (mod\ 2^n).$$

Observe que, para $n = 1$, temos:

$$X^2 \equiv 1 \ (mod\ 2) \Rightarrow X \equiv \pm 1 \ (mod\ 2).$$

Agora seja $x' = -1 + 2k$ e $x" = 1 + 2k$ soluções de $X^2 \equiv 3 \ (mod\ 2^2)$. Note que,

$$(-1 + 2k)^2 \equiv 3 \ (mod\ 4) \ \Rightarrow \ 1 \equiv 3 \ (mod\ 4)$$

que é uma contradição, pois $1 \equiv 1 \ (mod\ 4)$. Portanto, para $p = 2$, conseguimos ao menos um polinômio de uma variável e grau maior ou igual a 1, com coeficientes em $\mathbb{Z}/p\mathbb{Z}$ q ue não possui raiz em $\mathbb{Z}_p$. Falta mostrar para p primo ímpar.

Para $p \neq 2$, basta tomarmos um m tal que

$$X^2 \equiv m \ (mod\ p)$$

não possua solução, isto quer dizer: m não é um resíduo quadrático módulo p. Sabemos que, se $X^2 \equiv m \ (mod\ p^n)$ admite uma sequência de soluções, então $X^2 \equiv m \ (mod\ p)$ possui solução. Então m tem que ser resíduo quadrático módulo p. Porém $\mathbb{Z}/p\mathbb{Z}$ possui exatamente $\dfrac{p+1}{2}$ resíduos quadráticos, a saber

$$0^2, 1^2, 2^2, 3^2, \cdots, \left(\frac{p-1}{2}\right)^2 \quad (mod\ p)$$

já que todo $a \in \mathbb{Z}$ é congruente a $\pm\, b \ (mod\, p)$ para algum b tal que $0 \leq b \leq (p-1)/2$, de modo que X^2 é congruente a um dos elementos da lista acima. Sendo assim, temos $\dfrac{p+1}{2}$ resíduos, mas podemos construir p polinômios distintos de uma variável e grau igual a 2, com coeficientes em $\mathbb{Z}/p\mathbb{Z}$, consequentemente, pelo principio das casas dos pombos, sempre haverá polinômios de uma variável e grau igual a 2 que não possuirão raízes em $\mathbb{Z}_p$. Concluindo assim que $\mathbb{Z}_p$ não é algebricamente fechado.

■

1.2.11 Os racionais p-ádicos como corpo de fração de $\mathbb{Z}_p$.

Mostramos que $\mathbb{Z}_p$ é um domínio de integridade, portanto é comum nos questionarmos: "Será que os números inteiros p-ádicos formam um corpo?" Infelizmente a resposta é não. Como se verifica, a maioria dos inteiros p-ádicos diferentes de zero, especificamente aqueles em que seu primeiro coeficiente é igual a zero, não possui inverso. Antes de provar este fato, precisamos de uma nova definição.

Definição 1.8 *Vamos definir o que chamaremos de redução módulo p a função $\varepsilon : \mathbb{Z}_p \longmapsto \mathbb{Z}/p\mathbb{Z}$ tal que, dado*

$$a = \sum_{i>0} a_i p^{i-1} \mapsto a_1 \ mod \ p.$$

Pode-se perceber facilmente que ε é um homomorfismo de anel sobrejetor.

Definição 1.9 *Denotaremos por $\mathbb{Z}_p^{\times}$ o conjunto formado por todos os elementos de $\mathbb{Z}_p$ que são invertíveis.*

Proposição 1.5 *Um inteiro p-ádico $a = \sum_{i>0} a_i p^{i-1}$ é invertível se e somente se $a_1 \neq 0$. Em outras palavras*

$$\mathbb{Z}_p^{\times} = \left\{ a = \sum_{i>0} a_i p^{i-1} \ \in \ \mathbb{Z}_p : a_1 \neq 0 \right\}.$$

Demonstração: Seja ε um homomorfismo. Sabemos que se um inteiro p-ádico possui um inverso, sua redução módulo p também deverá ter um inverso. Partindo da função ε podemos obter o conjunto dos inteiros p-ádicos com primeiros coeficientes iguais a zero, assim devemos ter

$$\mathbb{Z}_p^{\times} \subset \left\{ \sum_{i>0} a_i p^{i-1} : a_1 \neq 0 \right\}.$$

Agora nos basta mostrar a igualdade. Claramente, dado um $a \in \mathbb{Z}_p$ com $a_1 \neq 0$, $\varepsilon(a)$ é não nula e, seja um p primo, temos um inverso b_1 satisfazendo $0 < b_1 < p$ e $a_1 b_1 \equiv 1 \ mod \ p$. Podemos expressar esta congruência como $a_1 b_1 = 1 + kp$. Se fizermos $a = a_1 + p\alpha$, teremos

$$ab_1 = (a_1 + p\alpha)b_1 = a_1 b_1 + p\alpha b_1 = 1 + tp$$

fazendo $t = \alpha b_0$, $t \in \mathbb{Z}_p$. Se pudermos mostrar que $1 + tp$ é invertível, então teremos um inverso para a, que poderemos escrever

$$ab_1(1 + tp)^{-1} = 1, \ a^{-1} = b_1(1 + tp)^{-1}.$$

Nós mostramos que, se pudermos encontrar um inverso para inteiros p-ádicos da forma $a = 1 + tp$, então podemos encontrar um inverso para qualquer inteiro p-ádico cujo primeiro coeficiente é diferente de zero. Mas perceba que

$$(1 + tp) \cdot (1 - tp + t^2p^2 - t^3p^3 + t^4p^4 - \dots) =$$
$$(1 - tp + t^2p^2 - t^3p^3 + t^4p^4 - \dots) \cdot (tp - t^2p^2 + t^3p^3 - t^4p^4 + \dots) = 1.$$

Quando realizamos a soma, as parcelas vão se cancelando, restando apenas o 1. Então teríamos um candidato a inverso de $(1+tp)$, que seria o $(1 - tp + t^2p^2 - t^3p^3 +$

$t^4p^4 - \dots)$. Mas precisamos garantir que $(1 - tp + t^2p^2 - t^3p^3 + t^4p^4 - \dots)$ ainda é um inteiro p-ádico. Consideremos (α_k) uma sequência de inteiros p-ádicos. De fato cada $\alpha_i p^{i-1} \in \mathbb{Z}_p$, e além disso teremos

$$[\dots, \alpha_1^3, \alpha_1^2, \alpha_1^1, \alpha_1^0]_p = \alpha_1$$
$$[\dots, \alpha_2^3, \alpha_2^2, \alpha_2^1, 0]_p = \alpha_2 p^1$$
$$[\dots, \alpha_3^3, \alpha_3^2, 0, 0]_p = \alpha_3 p^2$$
$$\vdots$$

Vamos mostrar que o somatório infinito $\sum_{i>0}^{\infty} \alpha_i p^{i-1}$ é ainda um inteiro p-ádico. Agora, usando a adição (como definida em 1.2.2), cada termo será somado um número finito de vezes, portanto $\sum \alpha_i p^{i-1}$ continuará sendo um inteiro p-ádico. Conseguimos assim um inverso para $1 + tp$.

$$(1 + tp)^{-1} = 1 - tp + (tp)^2 - \dots = 1 + c_1p^0 + c_2p^1 + c_3p^2 + \dots$$

com todos os coeficientes c_i satisfazendo $0 \leq c_i \leq p - 1$.

Agora que encontramos um inverso para $1+tp$, sabemos que podemos determinar um inverso para qualquer p-ádico inteiro com primeiro coeficiente não nulo, assim provando a igualdade dos conjuntos.

■

Até o momento temos que $(\mathbb{Z}_p, +, \cdot)$ é um domínio de integridade. Vimos também que $(\mathbb{Z}_p, +, \cdot)$ não é um corpo. Nosso objetivo é construir agora um corpo de frações de $\mathbb{Z}_p$.

Seja $\mathbb{Z}_p^* = \mathbb{Z}_p - \{[0]_p\}$ para todo p primo. Vamos definir uma relação de equivalência no conjunto

$$\mathbb{X} = \{(a, b) : a \in \mathbb{Z}_p, b \in \mathbb{Z}_p^*\}.$$

Seja $(a, b), (c, d) \in \mathbb{X}$ então teremos

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Esta relação é uma relação de equivalência, visto que:

i) $\forall\ (a, b)\ \in\ \mathbb{X} \Rightarrow (a, b) \sim (a, b)$;

ii) $\forall\ (a, b)$ e $(c, d) : (a, b) \sim (c, d)\ \Leftrightarrow (c, d) \sim (a, b)$;

iii) Dados (a, b), (c, d) e (e, f) temos

$$(a, b) \sim (c, d) \wedge (c, d) \sim (e, f) \Rightarrow (a, b) \sim (e, f).$$

Vamos denotar por $\frac{a}{b}$ (em vez de $\overline{(a,b)}$) a seguinte classe de equivalência:

$$\frac{a}{b} = \{(y,z) \in \mathbb{X} : yb = za\}.$$

Assim,

$$\frac{a}{b} = \frac{y}{z} \text{ em } \mathbb{X}/_\sim \iff by = az \text{ em } \mathbb{Z}_p.$$

Precisamos agora, definir as operações $+$ e $\cdot$ no conjunto quociente

$$\mathbb{X}/_\sim = \left\{\frac{a}{b} : a \in \mathbb{Z}_p, b \in \mathbb{Z}_p^*\right\} = \mathbb{K}.$$

Sejam (a,b) e $(c,d) \in \mathbb{Z}_p \times \mathbb{Z}_p^*$. Então definiremos a soma como:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

e o produto como:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

Como $\mathbb{Z}_p$ é domínio de integridade, se $b, d \in \mathbb{Z}_p^*$ teremos $bd \in \mathbb{Z}_p^*$.

Proposição 1.6 *As operações $+$ e $\cdot$ estão bem definidas em $\mathbb{K}$.*

Demonstração: Consideremos $\frac{a}{b} = \frac{a'}{b'}$ e $\frac{c}{d} = \frac{c'}{d'}$ então,

1) $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$;

2) $\frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}$.

De $\frac{a}{b} = \frac{a'}{b'}$ e $\frac{c}{d} = \frac{c'}{d'}$ segue que $ab' = ba'$ e $cd' = dc'$ em $\mathbb{Z}_p$.

Agora,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{a'd' + b'c'}{b'd'} = \frac{a'}{b'} + \frac{c'}{d'} \Leftrightarrow$$

$$(ad+bc)b'd' = (a'd' + b'c')bd \text{ em } \mathbb{Z}_p \Leftrightarrow$$

$$(ab')(dd') + (cd')(bb') = (a'b)(dd') + (c'd)(bb') \text{ em } \mathbb{Z}_p.$$

Disto, 1) segue das igualdades $ab' = ba'$ e $cd' = c'd$.

Para mostrar 2) basta observarmos que em $\mathbb{Z}_p$ temos:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'} \Leftrightarrow (ab')(cd') = (a'b)(c'd)$$

e o resultado segue pelas igualdades $ab' = a'b$ e $cd' = c'd$.

■

Denotaremos por $a^{\#} = \frac{a}{1}$ onde $a \in \mathbb{Z}_p$ e 1 é a unidade de $\mathbb{Z}_p$ ($[1]_p$), e denotaremos

$$\mathbb{Z}_p^{\#} = \left\{ a^{\#} = \frac{a}{1} : a \in \mathbb{Z}_p \right\} \subset \mathbb{K} = \left\{ \frac{a}{b} : a \in \mathbb{Z}_p, b \in \mathbb{Z}_p^* \right\}.$$

É fácil provar que $\mathbb{Z}_p^{\#}$ é um domínio de integridade com unidade $1^{\#} \in \mathbb{Z}_p^{\#}$. Aliás $1^{\#}$ é tal que,

$$\forall\ \frac{a}{b} \Rightarrow \frac{a}{b} \cdot 1^{\#} = 1^{\#} \cdot \frac{a}{b} = \frac{a}{b},$$

e mais ainda,

$$\forall\ \frac{a}{b} \in \mathbb{K} \ \text{ temos } \ \frac{a}{b} + 0^{\#} = 0^{\#} + \frac{a}{b} = \frac{a}{b}.$$

Consideremos a seguinte função:

$$\begin{aligned} \phi \ : \ \mathbb{Z}_p &\longrightarrow \mathbb{Z}_p^{\#} \\ a &\longmapsto a^{\#} \end{aligned}$$

É de imediata verificação que:

a) $Im\phi = \mathbb{Z}_p^{\#}$;

b) $N(\phi) = \{a \in \mathbb{Z}_p : a^{\#} = 0^{\#}\} = \{0\}$;

c) $\phi(a+b) = (a+b)^{\#} = a^{\#} + b^{\#} = \phi(a) + \phi(b) \ \ \forall\ a, b \in \mathbb{Z}_p$;

d) $\phi(a \cdot b) = (a \cdot b)^{\#} = a^{\#} \cdot b^{\#} = \phi(a) \cdot \phi(b) \ \ \forall\ a, b \in \mathbb{Z}_p$.

Portanto,

$$\mathbb{Z}_p \simeq \mathbb{Z}_p^{\#} \subset \mathbb{K}.$$

Observe também que, se $\frac{a}{b} \neq 0^{\#}$ em $\mathbb{K}$, isto é, $a \neq 0$ em $\mathbb{Z}_p$, então $\frac{b}{a} \in \mathbb{K}$ e mais, $\frac{a}{b} \cdot \frac{b}{a} = 1^{\#}$.

Partimos de um $(\mathbb{Z}_p, +, \cdot)$ domínio de integridade e construímos $\mathbb{K}$. Além disso, $\mathbb{Z}_p \simeq \mathbb{Z}_p^{\#} \subset \mathbb{K}$. O conjunto $\mathbb{K}$ possui todas as propriedades de $\mathbb{Z}_p$, além disso, dado $\frac{a}{b} \in \mathbb{K}$, $a, b \in \mathbb{Z}_p^*$ existe um $\frac{b}{a}$ tal que $\frac{a}{b} \cdot \frac{b}{a} = 1^{\#}$.

Concluímos que $\mathbb{K}$ é um corpo. E da forma que foi definido, $\mathbb{K}$ será o corpo de frações de $\mathbb{Z}_p$, introduzindo assim este corpo de uma maneira puramente algébrica.

Definição 1.10 *O corpo dos racionais p-ádicos será o conjunto* $\mathbb{Q}_p = Frac(\mathbb{Z}_p)$, *juntamente com as operações* $+$ *e* $\cdot$ *como são definidas para um corpo quociente qualquer.*

Desta forma como definimos $\mathbb{Q}_p$, teremos que $\mathbb{Z}_p \subset \mathbb{Q}_p$, e como $\mathbb{Z} \subset \mathbb{Z}_p$, teremos que $\mathbb{Q} \subset \mathbb{Q}_p$. Podemos esperar que, da mesma forma que há uma relação entre os inteiros p-ádicos e suas respectivas expansões em séries, exista uma relação entre os elementos de $Frac(\mathbb{Z}_p)$ e suas respectivas expansões em séries. Para chegarmos a tal resultado, necessitaremos de alguns fatos.

Definição 1.11 *Seja* $a \in \mathbb{Z}_p$. *Seja* a_k *o primeiro termo da representação p-ádica de a tal que* $a_k \neq 0$. *Fica definido que a ordem de a será k e será denotado da forma*

$$ord(a) = k.$$

Lema 1.1 *Seja* $a \in \mathbb{Z}_p$ *e* $ord(a) = k$. *Se* $a = p^k u \Rightarrow u \in \mathbb{Z}_p^\times$.

Demonstração: Observe que, quando $ord(a) = 0$, temos $a_0 \neq 0$, o que implica $a \in \mathbb{Z}_p^\times$. Se $ord(a) = k$, $k \neq 0$, o primeiro elemento não nulo de a será o a_k, com $a_0, a_1, a_2, \ldots, a_{k-1} = 0$. Seja u um inteiro p-ádico tal que $u_i = a_{k+i}$, com $i \geq 0$, $i \in \mathbb{N}$. Perceba que $a = p^k u$ (estamos deslocando cada termo de u k vezes para a esquerda). Com esta nossa construção, $u_0 = a_k$, como a_k é não nulo, $u \in \mathbb{Z}_p^\times$.

■

Lema 1.2 *Dados* $a, b \in \mathbb{Z}_p$ *teremos que* $ord(ab) = ord(a) + ord(b)$.

Demonstração: Observe que

$$a = \sum_{i>0} a_i p^{i-1} \quad \text{e} \quad b = \sum_{j>0} b_j p^{j-1}.$$

Se $ord(a) = k_1$ e $ord(b) = k_2$ a menor potência de p no produto ab será $p^{k_1+k_2}$. O que nos faz ver que

$$ord(ab) = ord(a) + ord(b).$$

■

Proposição 1.7 *Qualquer* $x \in \mathbb{Q}_p$ *pode ser representado como uma série da forma*

$$\sum_{i \geq m}^{\infty} a_i p^{i-1} = a_m p^{m-1} + a_{m+1} p^m + \cdots + a_1 + a_2 p + \cdots$$

onde $m \in \mathbb{Z}$ *e* $0 \leq a_i \leq p-1$.

Demonstração: O objetivo é mostrar que

$$\left\{\sum_{i\geq m} a_i p^{i-1} : m, a_i \in \mathbb{Z}, 0 \leq a_i \leq p-1\right\} = Frac(\mathbb{Z}_p).$$

Consideremos que exista uma série desta forma, e mais especificamente, uma para $m < 0$ (isto é, não formará um inteiro p-ádico). Vamos reescrever esta série como uma soma de vários termos:

$$a_m p^{m-1} + a_{m+1}p^m + \cdots + a_1 + a_2 p + \cdots = a_m \frac{1}{p^{-m+1}} + a_{m+1}\frac{1}{p^{-m}} + \cdots + \sum_{i>0} a_i p^{i-1}$$

onde cada $a_i \in \mathbb{Z}$ e $p^{-k} \in \mathbb{Z}_p$ se $k < 0$. Observe que a parte finita da soma forma um termo do tipo $\frac{a}{b}$, $a, b \in \mathbb{Z}_p$ e a parte infinita é um inteiro p-ádico. Como $\mathbb{Z}_p \subset Frac(\mathbb{Z}_p)$, temos uma soma de elementos de $Frac(\mathbb{Z}_p)$, veja também que se $m \geq 0$ temos justamente um inteiro p-ádico. Visto isso, podemos dizer que

$$\left\{\sum_{i\geq m} a_i p^{i-1} \ : \ m, a_i \in \mathbb{Z}, \ 0 \leq a_i \leq p-1\right\} \subset Frac(\mathbb{Z}_p).$$

Tomemos agora um a inteiro p-ádico de ordem k. Pelo lema 1.1, podemos escrever $a = p^k u$, com $u \in \mathbb{Z}_p^\times$. Perceba que, se pegarmos $\frac{a}{b} \in Frac(\mathbb{Z}_p)$ com $ord(a) = n$ e $ord(b) = m$, podemos escrever

$$\frac{a}{b} = \frac{cp^n}{dp^m} = cp^n \cdot (dp^m)^{-1} = (cd^{-1}) \cdot p^{n-m}.$$

Como $ord(a) = n$, $c \in \mathbb{Z}_p^\times$ (Lema 1.1). Deste fato, é direto perceber que $ord(c) = 0$. O mesmo argumento pode ser utilizado para ver que $ord(d) = 0$. Como $ord(d) = 0$, fica claro que $d \in \mathbb{Z}_p^\times$, e além disso $ord(d^{-1}) = 0$. Mas pelo lema 1.2, $ord(cd^{-1}) = ord(c) + ord(d^{-1})$, o que nos dá $ord(cd^{-1}) = 0$. Portanto cd^{-1} é unidade (isto é, inversível em $\mathbb{Z}_p$). Assim o produto $cd^{-1} \cdot p^{n-m}$ pode ser expresso pela série

$$\sum_{i\geq n-m} a_i p^{i-1}$$

que é idêntica a série correspondente ao representante p-ádico de cd^{-1}, deslocando o início da série para o índice $n-m$. Se $n < m$, a série iniciará com índice negativo e potências de expoentes negativos, e teremos

$$\left\{\sum_{i\geq m} a_i p^{i-1} \ : \ m, a_i \in \mathbb{Z}, \ 0 \leq a_i \leq p-1\right\} \supset Frac(\mathbb{Z}_p),$$

concluindo assim a igualdade.

■

Capítulo 2

Uma visão topológica dos inteiros p-ádicos

Será necessário, partindo do que já vimos, apresentarmos algumas definições, proposições e resultados em geral que tornarão nosso estudo mais amplo. A proposta deste capítulo é apresentar os rudimentos substanciais para um estudo um pouco mais aprofundado sobre os p-ádicos.

2.1 Notas históricas

Voltemos por um instante ao final do século XIX, na região de Kalinigrad, Rússia (naquela época: Königsberg, Prússia). Em 29 de dezembro de 1861 nascera Kurt Hensel, filho de Sebastian Hensel e Julie von Adelson, que pertencia a uma família de artistas, músicos e cientistas.

Hensel foi educado em casa até os 9 anos de idade e, após mudar-se para Berlim, passou a frequentar o Fridrich-Wilhelm Gymnasium. Lá encontrou sua inspiração para estudar matemática: K H Schellbach. Nesta época, estudantes alemães não escolhem uma única universidade para estudar, mas frequentam várias instituições com a finalidade de provar os cursos. Os estudos de Hensel estavam entre Berlim e Bonn. Entre seus professores estavam Lipschitz, Weierstrass, Borchardt, Kirchhoff, Helmholtz e Kronecker. Kronecker, que foi a maior influência sobre Hensel, supervisionou seus estudos de doutoramento na universidade de Berlim. Hensel apresentou sua tese "*Arithmetische Untersuchungen über Diskriminaten und ihre ausserwesentlichen teiler*" (Sobre estudos aritméticos não essenciais e seus discriminantes) à Berlim, em 1884. Continuou seus trabalhos na universidade de Berlim até apresentar sua tese de habilitação, tornando-se um conferencista externo em 1886.

Hensel foi nomeado para uma cátedra na universidade de Marburg em 1901, passando o resto de sua carreira lá, aposentando-se em 1930, mas permanecendo em Marburg.

Dedicou muitos anos para a edição de obras completas de Kronecker. Na verdade, ele publicou cinco volumes das obras de Kronecker entre os anos de 1895 e 1930. Curiosamente, essas datas abrangem a carreira de Hensel quase que exatamente, com o primeiro volume aparecendo no ano entre o seu doutoramento e sua habilitação, e o último volume que aparece no ano que se aposentou. Notadamente, o trabalho

de Hensel seguiu o de seu orientador de doutorado, Kronecker, no desenvolvimento da aritmética em corpos de números algébricos.

Em 1897, o método de Weierstrass do desenvolvimento de séries de potências para funções algébricas levou a invenção dos números p-ádicos. Hensel estava interessado na exata potência de um primo que divide o discriminante de um corpo de números algébricos. Os números p-ádicos podem ser considerados como um preenchimento dos números racionais de um modo diferente a partir da conclusão habitual que nos leva aos números reais. Segundo [11], Hensel iniciou uma investigação sobre números p-ádicos na última década do século XIX, motivado por algumas analogias apresentadas entre números primos pertencentes a um corpo e fatores lineares presentes em corpos de funções, desempenhando papéis semelhantes nestas teorias. Estes fatos já haviam sido apresentados em artigos de Kronecker e de Dedekind e Heinrich Weber, baseados num manuscrito, até então inédito, de Kronecker, datado de 1858.

A invenção de Hensel levou ao desenvolvimento do conceito de um corpo com valorização que teve uma grande influência sobre posteriores temas na matemática. Ele foi capaz de utilizar seus métodos para provar muitos resultados na teoria das formas quadráticas e teoria dos números. Entre alguns artigos que ele publicou incluem-se: *Veränderlichen und Abelschen Integrale* (Variáveis e as Integrais Abelianas), 1901; *Über die Entwickelung der algebraischen Zahlen em Potenzreihen* (Sobre o desenvolvimento de inteiros algébricos em série de potências), 1901; *Eine neue Theorie der algebraischen Zahlen* (Uma nova teoria de inteiros algébricos), 1918; *Neue Begründung der arithmetischen theorie der algebraischen funktionen einer variablen* (Nova justificativa da teoria aritmética das funções algébricas de uma variável), 1919. Informações mais detalhadas podem ser obtidas em [10], como os desenvolvimentos matemáticos contemporâneos e os respectivos responsáveis.

2.2 Norma ou valor absoluto

2.2.1 Norma em um corpo qualquer

Apresentaremos inicialmente algumas definições mais gerais para apoiarmos nossa evolução para definições que nos serão bastantes úteis. Começaremos pela que segue.

Definição 2.1 *Norma, ou valor absoluto, num corpo $\mathbb{K}$ qualquer é uma função*

$$|\ |: \mathbb{K} \longrightarrow \mathbb{R}_+$$

que satisfaz as seguintes condições:

i) $|x| = 0 \leftrightarrow x = 0$;
ii) $|xy| = |x||y| \quad \forall \quad x, y, \in \mathbb{K}$;
iii) $|x + y| \leq |x| + |y| \ \forall \ x, y \in \mathbb{K}$.

E quando satisfaz adicionalmente a condição

iv) $|x + y| \leq max\{|x|, |y|\} \ \forall \ x, y \in \mathbb{K}$;

o valor absoluto se diz não-arquimediano, caso contrário, se diz arquimediano.

Podemos observar que a condição (iv) implica a (iii), pois

$$max\{|x|, |y|\} \ \leq \ |x| + |y| \ \forall \ x, y \in \mathbb{K}.$$

No valor absoluto usual, quando $\mathbb{K} = \mathbb{Q}$, é fácil verificar que ele é um valor absoluto em $\mathbb{Q}$. E, tomando $x = 1$ e $y = 1$, em (iv), podemos perceber que é um valor absoluto arquimediano, visto que $|1 + 1| \geq max\{|1|, |1|\}$, contradizendo (iv).

O valor absoluto trivial é definido da seguinte forma:

- $|x| = x$ se $x \geq 0$;
- $|x| = -x$ se $x < 0$.

No estudo dos p-ádicos nos será útil uma outra definição de norma, e a partir de agora veremos algumas bases necessárias para a introdução deste novo conceito.

2.2.2 Valorização p-ádica

Definição 2.2 *Seja $n \in \mathbb{Z}$, $n \neq 0$ e p um número primo, vamos definir a função $v_p(n)$, $\mathbb{Z} \longrightarrow \mathbb{Z}$, que chamaremos de valorização p-ádica, estabelecida pela condição*

$$n = p^{v_p(n)} \cdot n' \qquad com \quad p \nmid n'.$$

Em outras palavras, dado um p primo, $v_p(n)$ é o maior expoente de p na decomposição de n em fatores primos.

Por exemplo, para $n = 42$ e $p = 3$ temos

$$42 = 3^1 \cdot (2 \cdot 7) \ \text{ e } \ 3 \nmid 2 \cdot 7$$

Portanto,

$$v_3(42) = 1.$$

Até o momento temos a valorização p-ádica definida para os inteiros, é fácil perceber que se $n = ab$, então

$$v_p(n) = v_p(ab) = v_p(a) + v_p(b)$$

pois as decomposições de a e b em fatores primos são únicas, tornando a decomposição de ab também única. Caso p não seja fator primo de a, $v_p(a) = 0$, o mesmo vale para b. Caso contrário, seja p^{α_1} a maior potência de p em a, disto $v_p(a) = \alpha_1$, analogamente p^{α_2} a maior potência de p em b, $v_p(b) = \alpha_2$. Teremos que a maior potência de p no produto $a \cdot b$ será $p^{\alpha_1 + \alpha_2}$ que implica em

$$v_p(ab) = \alpha_1 + \alpha_2 = v_p(a) + v_p(b).$$

Definição 2.3 *Se* $x = \frac{a}{b} \in \mathbb{Q}$ *e* p *é um número primo, a valorização p-ádica é definida da seguinte forma:*

$$v_p(x) = v_p(a) - v_p(b)$$

Para $n = 0$, $v_p(0) = +\infty$.

Proposição 2.1 *A definição de valorização p-ádica de um número racional apresentada anteriormente é independente da representação do quociente de inteiros utilizada, seja na sua forma irredutível ou com representações equivalentes.*

Demonstração: Seja $a,\ b,\ c$, e $d \in \mathbb{Z}^*$, mostremos que

$$\frac{a}{b} = \frac{c}{d} \Rightarrow v_p\left(\frac{a}{b}\right) = v_p\left(\frac{c}{d}\right)$$

Se $\frac{a}{b} = \frac{c}{d}$, então $ad = bc$. Como $ad = bc = x$, $x \in \mathbb{Z}$, $x \neq 0$, temos

$$v_p(ad) = v_p(bc) \Rightarrow v_p(a) + v_p(d) = v_p(b) + v_p(c)$$

$$\Rightarrow v_p(a) - v_p(b) = v_p(c) - v_p(d)$$

Pela definição 2.3, temos

$$v_p\left(\frac{a}{b}\right) = v_p\left(\frac{c}{d}\right)$$

■

Proposição 2.2 *A valorização p-ádica de um* $x \in \mathbb{Q}$ *é regida pela condição*

$$x = p^{v_p(x)} \cdot \frac{a}{b}$$

com p *primo e* $p \nmid ab$.

Demonstração: De fato é verdade, dado p primo, seja $x = \frac{c}{d}$, se p não é fator primo nem de c nem de d, então, $v_p(x) = 0$ e

$$x = p^0 \cdot \frac{a}{b} \Rightarrow \frac{c}{d} = \frac{a}{b}$$

Seja p^{α_1} a maior potência de p na decomposição de c em fatores primos e p^{α_2} a maior potência de p em d. De fato, podemos escrever

$$c = p^{\alpha_1} \cdot a \ \text{ e } \ d = p^{\alpha_2} \cdot b$$

Então

$$x = \frac{c}{d} = \frac{p^{\alpha_1} \cdot a}{p^{\alpha_2} \cdot b} = \frac{p^{\alpha_1}}{p^{\alpha_2}} \cdot \frac{a}{b} = p^{\alpha_1 - \alpha_2} \cdot \frac{a}{b}$$

Como $\alpha_1 - \alpha_2 = v_p(\frac{c}{d}) = v_p(x)$,

$$x = p^{v_p(x)} \cdot \frac{a}{b}$$

O fato de p^{α_1} e p^{α_2} serem as maiores potências de p respectivamente a c e d, nos garante que $p \nmid a \cdot b$.

■

Lema 2.1 *Para todo $x, y \in \mathbb{Q}$ temos*

i) $v_p(xy) = v_p(x) + v_p(y)$;
ii) $v_p(x+y) \geq min\{v_p(x), v_p(y)\}$.

Com as convenções óbvias em relação a $v_p(0) = +\infty$.

Demonstração: (i) Seja a, b, c e $d \in \mathbb{Z}^*$, podemos escrever $x = \dfrac{a}{b}$ e $y = \dfrac{c}{d}$.

Portanto,

$$v_p(xy) = v_p\left(\frac{a}{b} \cdot \frac{c}{d}\right).$$

Pela definição 2.3,

$$v_p\left(\frac{ac}{bd}\right) = v_p(ac) - v_p(bd).$$

Como

$$v_p(ac) = v_p(a) + v_p(c)$$

e

$$v_p(bd) = v_p(b) + v_p(d)$$

Temos

$$v_p(ac) - v_p(bd) = v_p(a) + v_p(c) - (v_p(b) + v_p(d))$$
$$v_p(ac) - v_p(bd) = v_p(a) + v_p(c) - v_p(b) - v_p(d)$$
$$v_p(ac) - v_p(bd) = v_p(a) - v_p(b) + v_p(c) - v_p(d)$$

Disto, podemos escrever

$$v_p(ac) - v_p(bd) = v_p\left(\frac{a}{b}\right) + v_p\left(\frac{c}{d}\right).$$

Como $v_p(xy) = v_p(ac) - v_p(bd)$ e $v_p(ac) - v_p(bd) = v_p\left(\dfrac{a}{b}\right) + v_p\left(\dfrac{c}{d}\right)$ e ainda, $x = \dfrac{a}{b}$ e $y = \dfrac{c}{d}$ então teremos

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

(ii) Seja $a = p^n\frac{x_1}{y_1}$ e $b = p^m\frac{x_2}{y_2}$ onde $p \nmid x_1 \cdot y_1$ e $p \nmid x_2 \cdot y_2$. Assim teremos:

$$v_p(x+y) = v_p\left(p^n\frac{x_1}{y_1} + p^m\frac{x_2}{y_2}\right).$$

Sem perda de generalidade, podemos considerar $m \geq n$. Colocando o p^n em evidência, ficamos com

$$v_p\left[p^n\left(\frac{x_1}{y_1} + p^{m-n}\frac{x_2}{y_2}\right)\right] \overset{por(i)}{=} v_p(p^n) + v_p\left(\frac{x_1}{y_1} + p^{m-n}\frac{x_2}{y_2}\right).$$

Sabemos que $v_p(p^n) = n$, portanto nos basta analisar a parte que falta. Observemos que

$$v_p\left(\frac{x_1}{y_1} + p^{m-n}\frac{x_2}{y_2}\right) = v_p\left(\frac{x_1y_2 + p^{m-n}x_2y_1}{y_1y_2}\right).$$

Como $p \nmid y_1 \cdot y_2 \Longrightarrow v_p(y_1y_2) = 0$, aplicando a regra para a razão, temos

$$v_p(x_1y_2 + p^{m-n}x_2y_1) - v_p(y_1y_2) = v_p(x_1y_2 + p^{m-n}x_2y_1)$$

Se $m = n$,

$$x_1y_2 + p^{m-n}x_2y_1 = x_1y_2 + x_2y_1,$$

daí

$$v_p(x_1y_2 + x_2y_1) \geq 0.$$

Se $m \neq n$ teremos

$$p \nmid (x_1y_2 + p^{m-n}x_2y_1),$$

pois

$$p \mid (p^{m-n}x_2y_1) \text{ e } p \nmid x_1y_2,$$

portanto

$$v_p(x_1y_2 + p^{m-n}x_2y_1) = 0.$$

Teremos então,

$$v_p(x+y) = v_p(p^n) + v_p\left(\frac{x_1y_2 + p^{m-n}x_2y_1}{y_1y_2}\right) = n + k \geq min\{v_p(x), v_p(y)\}$$

com $k \geq 0$.

■

Definição 2.4 *Para qualquer $x \in \mathbb{Q}$ e p primo, definimos o valor absoluto p-ádico de x por*

$$| \ |_p = p^{-v_p(x)}$$

com a convenção natural no caso em que $x = 0$, de modo que $|0|_p = 0$.

Teorema 2.1 *A função $| \ |_p$ é um valor absoluto não-arquimediano em $\mathbb{Q}$.*

Demonstração: Para mostrar que esta função é um valor absoluto não arquimediano, temos que mostrar três itens, que são:

(i) $|x|_p = 0 \Leftrightarrow x = 0$.

(ii) $|xy|_p = |x|_p|y|_p \ \forall \ x, y \ \in \ \mathbb{K}$.

(iii) $|x + y|_p \leq max\{|x|_p, |y|_p\} \ \forall \ x, y \in \mathbb{K}$.

(i) A demonstração é direta.

(ii)Pela definição 2.4 temos que $|xy|_p = p^{-v_p(xy)}$ e $v_p(xy) = v_p(x) + v_p(y)$ temos:

$$p^{-v_p(xy)} = p^{(-1)v_p(xy)} = \left(\frac{1}{p}\right)^{v_p(xy)} = \left(\frac{1}{p}\right)^{v_p(x)+v_p(y)}$$

$$= \left(\frac{1}{p}\right)^{v_p(x)} \cdot \left(\frac{1}{p}\right)^{v_p(y)} = p^{-v_p(x)} \cdot p^{-v_p(y)} = |x|_p \cdot |y|_p.$$

(iii) Queremos mostrar que

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

Sabemos que $|x|_p = p^{-v_p(x)}$, então,

$$|x + y|_p = p^{-v_p(x+y)}.$$

Do lema 2.1, segue que $v_p(x + y) \geq min\{v_p(x), v_p(y)\}$. Disto,

$$p^{-v_p(x+y)} \leq p^{-(min\{v_p(x),v_p(y)\})}.$$

Sem perda de generalidade consideremos $min\{v_p(x), v_p(y)\} = v_p(x)$, então

$$|x+y|_p = p^{-v_p(x+y)} \leq p^{-v_p(x)} = |x|_p \leq max\{|x|_p, |y|_p\}.$$

■

Corolário 2.1 *Se p_1 e p_2 forem primos distintos, então $|\ |_{p_1} \neq |\ |_{p_2}$.*

Demonstração: Fixemos um $x \in \mathbb{Q}$, p_1 e p_2 primos distintos. Seja x da forma $\frac{a}{b}$, com $a \in \mathbb{Z}$ e $b \in \mathbb{Z}^*$. Se $p_1 \nmid x$ e $p_2 \nmid x$, temos que

$$|x|_{p_1} = |x|_{p_2} = \frac{1}{p_1^0} = \frac{1}{p_2^0} = 1.$$

Se $p_1 \mid x$ ou $p_2 \mid x$ teremos que

$$|x|_{p_1} = \frac{1}{p_1^m} \text{ ou } |x|_{p_2} = \frac{1}{p_2^n}.$$

Como $p_1 \neq p_2$, então $\frac{1}{p_1^m} \neq \frac{1}{p_2^n}$. Último ponto a observarmos, caso aconteça que p_1 e p_2 ambos dividam x, teremos:

$$x = p_1^m \cdot p_2^n \cdot \frac{c}{d},$$

que, por definição da norma p-ádica nos dá:

$$|x|_{p_1} = \frac{1}{p_1^m} \text{ e } |x|_{p_2} = \frac{1}{p_2^n}.$$

Como $p_1 \neq p_2$,

$$|x|_{p_1} \neq |x|_{p_2}.$$

Portanto, vale a afirmação $|\ |_{p_1} \neq |\ |_{p_2}$.

■

Corolário 2.2 *Se $x \in \mathbb{Q}$ e $|x|_p \leq 1$ para todo p primo, então $x \in \mathbb{Z}$.*

Demonstração: Como $x \in \mathbb{Q}$, x é da forma $\frac{a}{b}$, com $a, b \in \mathbb{Z}$ e $b \neq 0$. Seja p um número primo que divida x (caso não exista p primo que divida x, teremos então $x = 1$). Então

$$x = p^m \cdot \frac{c}{d},\ c, d \in \mathbb{Z},\ d \neq 0 \text{ e } m > 0.$$

Mas $m > 0$ somente se $p \mid c$ e $p \nmid d$ ou a potência de p que divide c for maior que a potência de p que divide d. Teríamos:

$$\frac{a}{b} = \frac{p^u \cdot c}{p^v \cdot d} \text{ onde } u > v \text{ e } u - v = m.$$

Observe que para $b \neq 1$, sempre existirá um p primo tal que $p^k \mid b$ para algum $k > 0$, $k \in \mathbb{N}$. Nas ocasiões onde $k > u$ teremos $|x|_p > 1$. Portanto, temos que ter $b = 1$, que faz x ser da forma $\frac{a}{1}$, com $a \in \mathbb{Z}$. Concluindo assim que $x \in \mathbb{Z}$.

■

Neste ponto temos definida uma norma (ou valor absoluto), a qual chamamos de norma p-ádica, estabelecida sobre o conjunto dos racionais. Da teoria de espaços métricos, se temos estabelecido sobre um corpo, uma norma, esta induz uma métrica. Além disso todo corpo, quando munido de uma métrica, pode ser completado (para mais detalhes ver [7]). Poderíamos chamar este completamento de racionais p-ádicos (uma construção detalhada pode ser vista em [2]), porém esta concepção é bem diferente da construída ao final do capítulo 1. Nele, construímos os racionais p-ádicos como corpo de frações dos inteiros p-ádicos. Podemos nos indagar a cerca destas construções, buscando saber o quanto estas estruturas aparentemente distintas, possuem em comum.

De fato estas construções são equivalentes, pois é possível que a norma p-ádica seja estendida aos racionais p-ádicos como corpo de frações dos inteiros p-ádicos. Ainda, os racionais p-ádicos definidos como corpo de frações, em conjunto com esta norma p-ádica, é completo e por isso coincide com o completamento dos racionais com a norma p-ádica. Estes não são resultados simples de serem apresentados e fogem ao escopo deste trabalho expor tais conclusões com todos seus detalhes.

2.3 Métrica e Topologia

A partir do momento que temos bem definido um valor absoluto num determinado corpo, podemos construir uma métrica e esta induzir uma topologia sobre o corpo em questão. Veremos nesta seção algumas implicações em torno desta construção.

Definição 2.5 *Seja K um corpo e $|\ |$ um valor absoluto em K. Definimos uma métrica em K da seguinte forma:*

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

Partindo desta definição, podemos nos restringir aos p-ádicos da seguinte forma:

Definição 2.6 *Seja $|\ |_p$ o valor absoluto em $\mathbb{Q}$. Analogamente à definição 2.5 podemos definir uma métrica sobre $\mathbb{Q}$ utilizando o valor absoluto $|\ |_p$ da seguinte forma:*

$$\delta(x, y) = |x - y|_p.$$

Por estarmos nos direcionando a um valor absoluto não-arquimediano (Teorema 2.1), temos o lema que segue.

Lema 2.2 *Como nosso valor absoluto é não-arquimediano temos que*

$$\delta(x,y) = |x-y|_p \;\Rightarrow\; \delta(x,y) \;\leq\; max\{\delta(x,z),\delta(z,y)\} \;\; \forall\; x,y,z \;\in \mathbb{Q}.$$

Demonstração: Temos que $x \in \mathbb{Q}$. Vimos que x pode ser escrito da forma

$$x = p^m \cdot \frac{a}{b},$$

com p primo, m,a,$b \in \mathbb{Z}$, $b \neq 0$ e $p \nmid a \cdot b$. Podemos então escrever $-x$ da forma:

$$-x = p^m \cdot (-\frac{a}{b}).$$

Ficando claro assim, que $v_p(x) = m = v_p(-x)$. Teremos então $|x|_p = |-x|_p = p^{-m}$.

Outro fato é que

$$|x+y|_p \leq max\{|x|_p, |y|_p\} \;\forall\; x,y \in \mathbb{Q}.$$

Observe que $|x-y|_p = |x+z-z-y|_p = |(x-z)+(z-y)|_p$. Portanto,

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

Como $|x-y|_p = \delta(x,y)$ podemos concluir que $\delta(x,y) \leq max\{\delta(x,z),\delta(z,y)\}$.

■

Esta desigualdade é conhecida como "desigualdade ultramétrica". Se temos um espaço onde esta desigualdade é satisfeita, chamamos de "espaço ultramétrico". Uma métrica deste tipo induz uma topologia com uma sucessão de características especiais. Observemos algumas.

Proposição 2.3 *Seja $\mathbb{K}$ um corpo e $|\;|$ um valor absoluto não-arquimediano em $\mathbb{K}$. Se $x,y \in \mathbb{K}$ e $|x| \neq |y|$ então*

$$|x+y| = max\;\{|x|,|y|\}.$$

Demonstração: Sem perda de generalidade, podemos supor que $|x| > |y|$. Então temos que $|x+y| \leq |x| = max\;\{|x|,|y|\}$. Por outro lado, $x = (x+y)-y$, onde

$$|x| \leq max\;\{|x+y|,|y|\}.$$

Como $|x| > |y|$, esta desigualdade só pode valer se $max\;\{|x+y|,|y|\} = |x+y|$; logo $|x| \leq |x+y|$, daí $|x| = |x+y|$.

■

Corolário 2.3 *Em um espaço ultramétrico, todos os triângulos são isósceles.*

Demonstração: Podemos tomar como exemplo os valores absolutos p-ádicos sobre $\mathbb{Q}$. Disto teremos que $|x|$ será dada por $|x|_p$ anteriormente definido como $|x|_p = p^{-v_p(x)}$. Num primeiro caso, consideremos $x, y \in \mathbb{Z}$. Consideremos $v_p(x) = m$ e $v_p(y) = n$, então

$$x = p^m a \qquad y = p^n b \qquad p \nmid ab.$$

Ou, representando como valores absolutos p-ádicos, temos

$$|x|_p = p^{-m} \qquad |y|_p = p^{-n}$$

Teremos $|x| > |y|$ quando $n < m$; digamos que $m = n + \varphi$. Então

$$x + y = p^n x' + p^{n+\varphi} y' = p^n (x' + p^\varphi y').$$

Como $p \nmid x'$ temos $p \nmid (x' + p^\varphi y')$, chegamos a $v_p(x+y) = n$ e $|x+y|_p = p^{-n} = |x|_p$, confirmando a proposição.

Por outro lado, se $|x|_p = |y|_p$, isto é, $n = m$, temos

$$x + y = p^n (x' + y')$$

onde $p \nmid x'y'$, mas pode acontecer que $p \mid (x' + y')$. Portanto, o máximo que podemos concluir é que $v_p(x + y) \geq n = min\{v_p(x), v_p(y)\}$, desta forma

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

Vale observar que $|x|_p$, $|y|_p$ e $|x + y|_p$ são, em qualquer caso, dois a dois, iguais.

Esta propriedade é característica de espaços ultramétricos, induzindo sobremaneira sua topologia. A seguir, veremos como a topologia de um corpo influi sobre como ele se comporta.

■

Definição 2.7 *Seja $\mathbb{K}$ um corpo provido de um valor absoluto $|\ |$, $c \in \mathbb{K}$ e $t \in \mathbb{R}_+$. Definiremos as bolas "aberta" e "fechada" de centro c e raio t por*

$$B(c,t) = \{x \in \mathbb{K} : \ |x - c| < t\}$$

$$\overline{B(c,t)} = \{x \in \mathbb{K} : \ |x - c| \leq t\}$$

Porém, se observarmos o caso não-arquimediano, teremos um fato interessante.

Proposição 2.4 *Seja $\mathbb{K}$ um corpo provido de um valor absoluto não-arquimediano. Então:*

i) se $a \in B(c,t)$, então $B(c,t) = B(a,t)$;

ii) se $a \in \overline{B(c,t)}$, então $\overline{B(c,t)} = \overline{B(a,t)}$;

iii) o conjunto $B(c,t)$ é aberto e fechado na topologia induzida por $|\ |$;

iv) se $t \neq 0$, o conjunto $\overline{B(c,t)}$ é aberto e fechado na topologia induzida por $|\ |$;

v) se c, $d \in \mathbb{K}$ e t, $s \in \mathbb{R}_+^\times$, temos que $B(c,t) \cap B(d,s) \neq \emptyset \iff B(c,t) \subset B(d,s)$ ou $B(c,t) \supset B(d,s)$;

vi) se c, $d \in \mathbb{K}$ e t, $u \in \mathbb{R}_+^\times$, temos que $\overline{B(c,t)} \cap \overline{B(d,u)} \neq \emptyset \iff \overline{B(c,t)} \subset \overline{B(d,u)}$ ou $\overline{B(c,t)} \supset \overline{B(d,u)}$.

Demonstração: *i) Observe que b pertence a $B(c,t)$ se e somente se $|b-c| < t$. Agora, seja um x pertencente a $B(c,t)$, se $|x-c| < t$, teremos*

$$|x-a| \leq max\{|x-c|, |a-c|\} < t,$$

onde chegaremos a $B(c,t) \subset B(a,t)$. Trocando a e c, chegamos a $B(a,t) \subset B(c,t)$, concluindo que $B(c,t) = B(a,t)$.

ii) Basta alterarmos o argumento em i), de $<$ para $\leq$, que a demonstração ocorre da mesma forma.

iii) Em qualquer espaço métrico, $B(c,t)$ é um aberto. Para ver que neste caso $B(c,t)$ é também um fechado, basta notar que um x pertence a $B(c,t)$ se e somente se toda bola aberta em torno de x intercepta $B(c,t)$. Escolha $s \leq t$, isto implica que $B(c,t) \cap B(x,s) \neq \emptyset$, então existe

$$a \in B(c,t) \cap B(x,s).$$

Mas então $|a-c| < t$ e $|a-x| < s \leq t$, onde teremos

$$|x-c| < max\{|x-a|, |a-c|\} < t$$

de modo que $x \in B(c,t)$.

iv) Análogo a (iii) trocando-se $<$ por $\leq$.

v) Podemos supor que $t \leq s$. Se existe $d \in B(c,t) \cap B(a,s)$, temos, por iii), que $B(c,t) = B(d,t)$ e $B(a,s) = B(d,s)$. Logo

$$B(c,t) = B(d,t) \subset B(d,s) = B(a,s)$$

como queríamos.

vi) Idêntico ao anterior, usando (iv).

■

Referências Bibliográficas

[1] Burton, David M. *Elementary number theory*, Boston, Allyn and Bacon, 1976. 390 p. ISBN 0-205-06978-9.

[2] Bachman, George. *Introduction to p-Adic Numbers and Valuation Theory*, New York. Academic Press, 1964. 172 p.

[3] Gonçalves, Adilson. *Introdução a Álgebra*, 5 ed. Rio de Janeiro: IMPA, 2008. 194 p. (Projeto Euclides) ISBN 978-85-244-0108-4.

[4] Gouvêa, Fernando Quadros. *Primeiros passos p-ádicos*. Rio de janeiro: IMPA. ISBN 85-244-0042-0.

[5] Hefez, Abramo. *Elementos de Aritmética*, 2 ed. Rio de Janeiro: SBM, 2011. 176 p. (Coleção do Professor de Matemática; 2) ISBN 978-85-85818-25-8.

[6] Koblitz, Neal. *p-Adic Numbers, p-Adic Analysis, and Zeta Functions*, second edition, New York: Spring-Verlag, 1984. 147 p. ISBN 0-387-96017-1.

[7] Lima, E. L.. *Espaços Métricos*, 2 ed. Rio de Janeiro: IMPA, 2015. 299 p. ISBN 978-85-244-0158-9.

[8] Martínez, Fábio Brochero; et al., *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro*, 2 ed. Rio de Janeiro : IMPA, 2013. 481 p. (Projeto Euclides) ISBN 978-85-244-0312-5.

[9] Serre, J. -P.. *A Course in Arithmetic*, New York: Spring-Verlag, 1973. 115 p. (Graduates texts in mathematics, 7.) ISBN 0-387-90040-3.

[10] Turnbull wwww Server. *Kurt Hensel*. Disponível em: <http://www-groups.dcs.st-and.ac.uk/∼history/Biographies/Hensel.html>. Acessado em: 9 de junho de 2016.

[11] Ullrich, P. *The genesis of Hensel's p-adic numbers, in Charlemagne and his heritage. 1200 years of civilization and science in Europe, Aachen, 1995*, p. 163-178. Brepols: Turnhout, 1998.