Universidade Federal de Goiás
Instituto de Matemática e Estatística
Programa de Mestrado Profissional em
Matemática em Rede Nacional

Números p-Ádicos e Formas Quadráticas

Luiz Fernando Rodrigues Santana

Goiânia

2018

sistema de bibliotecas ufg

PRPG
PRÓ-REITORIA DE PÓS-GRADUAÇÃO

UFG

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TESES E DISSERTAÇÕES NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), regulamentada pela Resolução CEPEC nº 832/2007, sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou *download*, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: **[x] Dissertação** **[ ] Tese**

2. Identificação da Tese ou Dissertação:

Nome completo do autor: **Luiz Fernando Rodrigues Santana**

Título do trabalho: **Números *p*-Ádicos e Formas Quadráticas**

3. Informações de acesso ao documento:

Concorda com a liberação total do documento [**x**] SIM [ ] NÃO[1]

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF da tese ou dissertação.

Luiz Fernando Rodrigues Santana.

Assinatura do autor

Ciente e de acordo:

Assinatura do orientador

Data: **15 de Outubro de 2018**

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.
Casos de embargo:
- Solicitação de registro de patente;
- Submissão de artigo em revista científica;
- Publicação como capítulo de livro;
- Publicação da dissertação/tese em livro.

Luiz Fernando Rodrigues Santana

Números p-Ádicos e Formas Quadráticas

Trabalho de Conclusão de Curso apresentado ao Instituto de Matemática e Estatística da Universidade Federal de Goiás, como parte dos requisitos para obtenção do grau de Mestre em Matemática.
Área de Concentração:**Matemática do Ensino Básico.**
Orientador: **Prof. Dr. Paulo Henrique de Azevedo Rodrigues.**

Goiânia

2018

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Rodrigues S., Luiz Fernando
Números p-Ádicos e Formas Quadráticas [manuscrito] / Luiz Fernando Rodrigues S.. - 2018.
LIV, 54 f.

Orientador: Prof. Dr. Paulo Henrique de Azevedo Rodrigues.
Dissertação (Mestrado) - Universidade Federal de Goiás, Instituto de Matemática e Estatística (IME), PROFMAT - Programa de Pós graduação em Matemática em Rede Nacional - Sociedade Brasileira de Matemática (RG), Goiânia, 2018.
Bibliografia.

1. Números p-Ádicos. 2. Formas Quadráticas. 3. Princípio Local Global. 4. Teorema de Hasse. I. Rodrigues, Paulo Henrique de Azevedo, orient. II. Título.

CDU 511

Universidade Federal de Goiás - UFG
Instituto de Matemática e Estatística - IME
Mestrado Profissional em Matemática em Rede Nacional – PROFMAT/UFG
Campus Samambaia – Caixa Postal 131 – CEP: 74.001-970 – Goiânia-GO.
Fones: (62) 3521-1208 e 3521-1137 www.ime.ufg.br

Ata da reunião da banca examinadora da defesa de Trabalho de Conclusão de Curso do aluno Luiz Fernando Rodrigues Santana – Aos dez dias do mês de outubro do ano de dois mil e dezoito, às 14:00 horas, reuniram-se os componentes da Banca Examinadora: Prof. Dr. Paulo Henrique de Azevedo Rodrigues – Orientador, Prof. Dr. Ricardo Nunes de Oliveira e a Profª. Drª. Eunice Cândida Pereira Rodrigues, para, sob a presidência da primeiro, e em sessão pública realizada na sala do LEMAT do IME, procederem a avaliação da defesa intitulada **"Números p-Ádicos e Formas Quadráticas"**, em nível de mestrado, área de concentração Matemática do Ensino Básico, de autoria de Luiz Fernando Rodrigues Santana, discente do Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal de Goiás. A sessão foi aberta pela presidente da banca, Prof. Dr. Paulo Henrique de Azevedo Rodrigues, que fez a apresentação formal dos membros da banca. A seguir, a palavra foi concedida ao autor do TCC que, em 30 minutos, procedeu à apresentação de seu trabalho. Terminada a apresentação, cada membro da banca arguiu o examinando, tendo-se adotado o sistema de diálogo sequencial. Terminada a fase de arguição, procedeu-se à avaliação da defesa. Tendo em vista o que consta na Resolução nº. 1403/2016 do Conselho de Ensino, Pesquisa, Extensão e Cultura (CEPEC), que regulamenta os Programas de Pós-Graduação da UFG, e procedidas as correções recomendadas, o Trabalho foi **APROVADO** por unanimidade, considerando-se integralmente cumprido este requisito para fins de obtenção do título de **MESTRE EM MATEMÁTICA**, na área de concentração Matemática do Ensino Básico pela Universidade Federal de Goiás. A conclusão do curso dar-se-á quando da entrega, na secretaria do IME, da versão definitiva do trabalho, com as devidas correções supervisionadas e aprovadas pelo orientador. Cumpridas as formalidades de pauta, às 16:00 horas, a presidência da mesa encerrou a sessão e, para constar, eu, Sóstenes Soares Gomes, secretário do PROFMAT/UFG, lavrei a presente ata que, após lida e aprovada, segue assinada pelos membros da Banca Examinadora em duas vias de igual teor.

Prof. Dr. Paulo Henrique de Azevedo Rodrigues
Presidente – IME/UFG

Prof. Dr. Ricardo Nunes de Oliveira
Membro – IME/UFG

Profª. Drª. Eunice Cândida Pereira Rodrigues
Membro - UFMT

Luiz Fernando Rodrigues Santana graduou-se em Matemática pela Universidade Federal de Goiás, UFG. Licenciou-se nessa área do conhecimento no ano de 2014. Seu trabalho de conclusão de curso aborda resolução de problemas mediante as concepções de George Polya. Foi bolsista Capes durante o período do mestrado profissional. Atuou como professor do nível básico, médio e superior nos últimos onze anos. Atualmente é professor efetivo do Instituto Federal Goiano, Campus Iporá.

Dedico este trabalho a minha esposa, Vânia, e aos meus filhos, Pedro Raphael e Luiz Antônio.

A educação é o passaporte para o futuro, pois o amanhã pertence àqueles que o preparam hoje - Malcom X.

Agradecimentos

Esta parte me faz rememorar os programas da Xuxa, no início dos anos 90.
-Quero mandar um beijo para o Kleber, para minha mãe, para Karla, para meus irmãos, para minhas cunhadas, para minha esposa, para meus filhos e para meu cachorro. Não, espera, eu não tenho cachorro. Os beijos param nos meus filhos. Sempre quis escrever isso em um trabalho.

Agora, se propondo a escrever algo mais formal, mais acadêmico, mais culto, materializo meus agradecimentos.

Sou profundamente grato a Vânia Lauriano Gomes, minha esposa, minha amante, minha amiga, minha confidente, meu amor, por todo o carinho e compreensão estendidos a mim durante este processo.

Agradeço ao Luiz Antônio Rodrigues Gomes por me fazer, a cada sorriso inocente, a cada beijo sincero e a cada atitude sapeca, perceber o quanto a vida pode ser doce. Agradeço ao Pedro Raphael Inácio Gomes por aceitar ser meu filho e me permitir ser seu pai.

Agradeço a minha mãe, Edenir Tatiana Rodrigues, por tornar esse momento possível através de seu amor, seu trabalho e seu estímulo. Agradeço a Pedro Honorato Pinheiro, médico, amigo, filantropo, mas sobre tudo uma inspiração, uma referência, um tipo de ser humano na qual eu me espelho.

Agradeço ao meu orientador, professor e amigo, Paulo Henrique de Azevedo Rodrigues pela compreensão, sobretudo quanto ao tempo, pela motivação nos meus momentos de desânimo e por me fazer entender porque eu havia escolhido cursar matemática. Gratidão estendida ao coordenador do PROFMAT-UFG-Goiânia, professor Mário José

de Souza, pelo respeito a minha fé traduzido em ações que possibilitaram esse momento se concretizar.

Meu muito obrigado a André Lucas, Amanda, Isabela, Jéssica, João Carlos e Karla Karine. Um grande abraço de gratidão a todos os amigos envolvidos no processo, sintam-se representados nas pessoas de Eduardo Júnior, Renato Silva, Rogério da Silva Cavalcante e Selzimar.

Agradeço a Deus, na pessoa de Jesus Cristo, pelo dom da vida, pelo amor demonstrado na cruz, e pela capacidade a mim concedida para escrever este trabalho. Por fim, agradeço ao pessoal da CAPES pelo apoio financeiro, foram vinte e quatro meses recebendo aquela grana com muita alegria, foi uma pena ter acabado.

Resumo

Rodrigues S., L. F.. **Números p-Ádicos e Formas Quadráticas.** Goiânia, 2018. 54p. Dissertação de mestrado profissional, PROFMAT. Departamento de Matemática, Instituto de Matemática e Estatística, Universidade Federal de Goiás.

Este texto apresenta as propriedades e as definições de números p-ádicos atreladas à definição de formas quadráticas. O teorema de Hasse: "Toda forma quadrática, com 5 variáveis ou mais, possui zeros p-ádicos não triviais" exemplifica o Princípio Local Global, que por sua vez garante que se uma equação polinomial possui zeros racionais não triviais se, e somente se, possui zeros não triviais sobre $\mathbb{R}$ e sobre $\mathbb{Q}_p$, p primo.

Palavras-chave

Números p-Ádicos, Formas Quadráticas, Teorema de Hasse, Princípio Local Global.

Abstract

Rodrigues S., L. F.. **p-Adic Numbers and Quadratic Forms.** Goiânia, 2018. 54p. MSc Dissertation, PROFMAT. Department of Mathematics, Institute of Mathematics and Statistics, Federal University of Goiás.

This text presents the properties and definitions of p-adic numbers linked to the definition of quadratic forms. Hasse's theorem: "Every quadratic form, with 5 variables or more, has non-trivial p-adic zeros" exemplifies the Global Local principle, which in turn ensures that if a polynomial equation has non-trivial rational zeros if, and only if, It has non-trivial zeros over $\mathbb{R}$ and about $\mathbb{Q}_p$, p prime.

Keywords

p-Adic Number, Quadratic Forms, Hasse´s Theorem, Local-Global Principle.

Sumário

1 Introdução e Motivação

O ano era 2008. Estava o autor deste texto em seu segundo semestre da graduação em Matemática, mais precisamente licenciatura. Quiça um pouco perdido em seus primeiros dias universitários, nosso autor não pensava em desistir do curso, mas depois de seis meses na Universidade Federal de Goiás ainda não sabia responder o porquê havia escolhido cursar Matemática. Ele sabia que amava Matemática, entretanto naquele ambiente isso parecia pouco.

O mês era Agosto. Agora, novas disciplinas, mais precisamente Álgebra e Teoria dos Números. Álgebra tinha despertado tanto interesse quanto o semestre anterior, ou seja, nenhum. O autor ainda se questionava se havia feito a escolha correta para sua vida profissional. Ainda amava Matemática, contudo aquela paixão de ensino médio se tornara um namoro muito morno.

O período era o da tarde, talvez o segundo horário, não se tem certeza. Adentrara a sala um homem jovem, cabelos compridos presos, tatuagem ao braço, aparentando mais ou menos uns trinta anos. Em poucos segundos o homem se revelaria o professor. A aula foi de apresentação da disciplina, Teoria dos Números, mas diferentemente do habitual aquela aula se mostraria muito especial para o nosso autor.

O desafio era fascinante. No período final daquela aula, o professor propôs e seguinte problema; *"Um menino enterrou na praia 14 bolinha e anotou a quantidade em uma placa, deixando-a sobre o local. Um extraterrestre viu, foi até lá e riscou o número 14 e escrevendo no local os símbolos ††, sabendo-se que o ET tem dois braços e duas mãos com mesma quantidade de dedos em cada uma e seu sistema de numeração foi obtido da mesma forma que o nosso, quantos dedos ele tem nas mãos?"*

O encontro com a rainha. "*A Matemática é a rainha das Ciências, e a Teoria dos Números é a rainha da Matemática*", disse o grande C. F. Gauss. Assim como nos

fundamentos do xadrez, é preciso conhecer a dama, a rainha, e depois saber jogar com ela. Foi isso que aconteceu com nosso autor naquela tarde de Agosto do ano de 2008. Uma chama se ascendeu, ele entendera o quanto a Matemática era bela, todavia sobre o viés da Teoria dos Números a Matemática se tornara celestial.

A nova descoberta. Muitas ideias foram pensadas sobre o tema deste trabalho. Acatando uma sugestão de seu orientador, que não por acaso é o mesmo professor daquela disciplina em 2008, nosso autor teve o prazer de conhecer um pouco mais sobre a rainha da Matemática. Existe um outro tipo de completamento para os números racionais além dos números reais. O detalhamento de como se dá esse completamento será apresentado ao longo do nosso texto. Números p-ádicos é o nome dado a aquela descoberta.

O leitor. Você, amigo leitor, já iniciou essa jornada de descobertas. O presente texto foi construído de forma que a leitura possa ser acessível a qualquer pessoa que domine as propriedades básicas de Matemática. Será um enorme deleite conhecer os números p-ádicos e sua aplicação a formas quadráticas. No final de sua leitura, o estudante saberá o que são números p-ádicos, como aplicá-los a formas quadráticas e quantos dedos o ET tem nas mãos.

O texto. Este trabalho se propõem a entender o que são números p-ádicos e sua utilidade para resolução de formas quadráticas. Apresentamos uma caraterização de números inteiros p-ádicos via congruências módulo potências de um primo p, em seguida definimos o que são inteiros p-ádicos e, posteriormente, o que são números p-ádicos (racionais p-ádicos).

Consolidado o que são números p-ádicos, apresentamos os conceitos de anel, corpo, valor absoluto, métrica e sequência de Cauchy para propormos o Teorema de Ostrowski. Ostrowski garante que os únicos completamentos possíveis para o corpo dos racionais

são os números reais, via valor absoluto real, e os números p-ádicos, via valor absoluto p-ádico, para qualquer que seja p primo.

Concluímos nosso texto discorrendo sobre formas quadráticas. Mostramos que toda forma quadrática pode ser diagonalizada. Em seguida, apresentamos o Princípio Local Global munido de uma exemplificação: Hasse-Minkowski, que diz que o Princípio Local Global vale para formas quadráticas. Anunciamos a Conjectura de Artin, Terjanian, Ax-Kochen, Davenport-Lewis e o Teorema de Hasse, todas envolvendo zeros p-ádicos. Para provarmos Hasse, recorremos ao lema de Hensel e a Chevalley-Warning. Bons estudos!!!

2 Números p-Ádicos

2.1 Uma Maneira de identificar Um Inteiro p-Ádico

Os números p-ádicos foram descritos pela primeira vez por Kurt Hensel em 1897, contudo alguns dos trabalhos anteriores de Ernst Kummer podem ser considerados como uma utilização implícita de números p-ádicos. Os p-ádicos foram motivados principalmente por uma tentativa de trazer as ideias e técnicas de métodos de série de potência em teoria dos números. Sua influência agora se estende muito além disso. No campo da análise p-ádica, há uma forma alternativa de cálculo, mas isso é um tópico um pouco mais avançado.

Nós começamos este trabalho apresentando um exercício sobre congruência para entender uma maneira de determinar um inteiro p-ádico. É necessário saber o que é congruência logicamente, não é? Caso o leitor não domine os conceitos de congruência, uma leitura do livro ***Iniciação à Aritmética***, de Abramo Hefez, disponível gratuitamente em `http://www.obmep.org.br/docs/apostila1.pdf`, já vai ajudar bastante.

Vamos analisar congruências módulo potências de um número inteiro primo p. Começaremos com um exemplo. Considere a congruência

Exemplo 1. *Considere*

$$x^2 \equiv 2 \ (mod\ 7^n)$$

módulo uma potência do número primo 7. *Para* $n = 1$ *essa congruência possui duas soluções,*

$$x_0 \equiv \pm 3 \ (mod\ 7)$$

Agora, seja $n = 2$. *Temos*

$$x^2 \equiv 2 \ (mod \ 7^2)$$

isso implica que $x^2 \equiv 2 \ (mod \ 7)$, *e consequentemente a solução deve ser da forma* $x_0 + 7t_1$. *onde* x_0 *é o número que satisfaz a primeira equação. Procuramos, então, uma solução da forma* $x_1 = 3 + 7t_1$ *ou (* $x_1 = -3 + 7t_1$*). Substituindo* x_1 *nesta última equação, obtemos:*

$$(3 + 7t_1)^2 \equiv 2 \ (mod \ 7^2)$$

$$9 + 6.7t_1 + 7^2.t_1^2 \equiv 2 \ (mod \ 7^2)$$

$$7 + 6.7t_1 \equiv 0 \ (mod \ 7^2)$$

$$7 + 6.7t_1 \equiv 0 \ (mod \ 7)$$

$$1 + 6.t_1 \equiv 0 \ (mod \ 7)$$

$$t_1 \equiv 1 \ (mod \ 7)$$

Nós assim temos a solução $x_1 \equiv 3 + 7.1 \ (mod \ 7^2)$. *Analogamente, de maneira parecida, semelhantemente, etc, quando* $n = 3$ *nós temos* $x_2 = x_1 + 7^2.t_2$ *e da congruência*

$$(3 + 7 + 7^2.t_2)^2 \equiv 2 \ (mod \ 7^3)$$

nós encontramos $t_2 \equiv 2 \ (mod \ 7)$*; Isso é*

$$x_2 \equiv 3 + 7.1 + 7^2.2 \ (mod \ 7^3).$$

É fácil perceber que este processo pode seguir indefinidamente. Nós obteremos assim a sequência:

$$x_0, x_1, x_2, ..., x_n, ..., \tag{1}$$

Satisfazendo as condições:

1. $x_0 \equiv 3 \ (mod\ 7)$
2. $x_n \equiv x_{n-1} \ (mod\ 7^n)$
3. $x_n^2 \equiv 2 \ (mod\ 7^{n+1})$

O processo de construção da sequência (1) faz lembrar ao processo para encontrar a raiz quadrada de 2. De fato, o cálculo de $\sqrt{2}$ consiste em encontrar a sequência de números racionais $r_0, r_1, r_2, ..., r_n, ...,$, cujos quadrados convergem para 2, por exemplo:

$$|r_n^2 - 2| < \frac{1}{10^n}$$

Em nosso caso, nós construímos uma sequência de inteiros $x_0, x_1, x_2, ..., x_n, ...$, para o qual $x_n^2 - 2$ é divisível por 7^{n+1}. Esta analogia se torna mais precisa de dissermos que dois números inteiros são próximos (mais precisamente, p-próximos, onde p é algum primo), quando a diferença entre eles é divisível por alguma potência suficientemente grande de p. Com essa concepção de proximidade, nós podemos dizer que os quadrados dos números na sequência $x_0, x_1, x_2, ..., x_n, ...$, se tornam arbitrariamente 7-próximos a 2 a medida que n cresce.

A sequência r_n, acima, determina o número real $\sqrt{2}$. Podemos, assim, supor que a sequência $\{x_n\}$ também determina um número α, de um tipo diferente, tal que $\alpha^2 = 2$.

Notemos agora o seguinte fato. Se a sequência $\{r'_n\}$ de números racionais satisfaz $|r_n - r'_n| < \frac{1}{10^n}$ para todo n, então seu limite também é $\sqrt{2}$. Podemos então naturalmente assumir que a sequência $\{x'_n\}$, para o qual $x_n \equiv x'_n \ (mod\ 7^{n+1})$, deverá

determinar algum novo número α [a nova sequência $\{x'_n\}$, claramente, também satisfaz $x'_n \equiv x'_{n-1}\ (mod\ 7^n)$ e $x'^2_n \equiv 2\ (mod\ 7^{n+1})$]. Essa observação nos conduz a seguinte definição.

Definição 1. *Seja p um número primo qualquer. A sequência de números inteiros $\{x_n\} = \{x_0, x_1, x_2, ..., x_n, ...\}$ satisfazendo*

$$x_n \equiv x_{n-1}\ (mod\ p^n)$$

para todo $n \geq 1$, determina um objeto chamado ***número inteiro p-ádico****.(O conjunto de todos os números inteiros p-ádicos é representado por $\mathbb{Z}_p$).*

Perceba que essa "construção" de números inteiros p-ádicos é uma analogia a "construção" do $\sqrt{2}$ como já foi mencionado. No caso do $\sqrt{2}$, nossa sequência seria : $\{3; 3,1; 3,14; 3,141; 3,1415; 3,14159; ...\}$. (Construção, aqui, é sinônimo de existência.)

Uma consequência direta dessa definição é a forma que se segue de representar ***números inteiros p-ádicos***, semelhante a representação decimal de números inteiros.

$$[..., a_n, a_{n-1}, ..., a_2, a_1, a_0]_p$$

onde $0 \leq a_i \leq p-1$ e p é um número primo.

Essa notação é convencional em aritmética. Para representar um número n em uma base p, agrupamos os seus dígitos em uma sequência da seguinte forma:

$$..., a_i, a_{i-1}, ..., a_2, a_1, a_0$$

onde é evidente que a partir de um certo ponto, todos os a_i são zero. Observe o exemplo abaixo.

Exemplo 2. *1. Seja $p = 2$, $n = [110111001]_2$ é um número inteiro 2-ádico.*

2. *Seja* $p = 3$, $n = [021120202]_3$ *é um número inteiro 3-ádico.*

3. *Seja* $p = 5$, $n = [324314021]_5$ *é um número inteiro 5-ádico.*

4. *Seja* $p = 7$, $n = [325614021]_7$ *é um número inteiro 7-ádico.*

Observação: *Com base nessa definição 1, e nessa consequente representação dos números inteiros p-ádicos, podemos propor uma representação para número inteiro p-ádicos utilizando somatório. Esse conceito de somatório é aprendido, ainda, nas séries iniciais. O número* 862 *nada mais é do que o somatória de oito centenas, seis dezenas e duas unidades. Observe a seguinte representação referente a números inteiros p-ádicos.*

Um número inteiro n p-ádico pode ser representado por uma soma de potências de um número primo p, logo é um número representado por

$$n = a_0 + a_1p + a_2p^2 + a_3p^3 + ... = \sum_{i=0}^{\infty} a_ip^i$$

onde $0 \leq a_i \leq p - 1$.

Considere o seguinte caso: Seja $k = 10$, claro que $10 = 2.5$ não é primo. Tendo $n = [59732]_{10}$, podemos escrever na base decimal $n = 5.10^4+9.10^3+7.10^2+3.10^1+2.10^0$. Que é um somatório de potência de base 10. Perceba também que $0 \leq a_i \leq 9$. Caso como esse são trabalhados no estudo de matemática desde de as séries iniciais. Agora, com essa analogia em mente, observe o próximo exemplo para valores primos.

Exemplo 3. *1. Seja* $p = 7$, 7 *é primo. Tendo* $n = [4632]_7$, *podemos escrever na base* 7, $n = 4.7^3 + 6.7^2 + 3.7^1 + 2.7^0$. *Que é um somatório de potência de base 7. Perceba também que* $0 \leq a_i \leq 6$.

2. *Seja* $p = 5$, 5 *é primo. Tendo* $n = [243]_5$, *podemos escrever na base* 5, $n = 2.5^2 + 4.5^1 + 3.7^0$. *Que é um somatório de potência de base 5. Perceba também que* $0 \leq a_i \leq 4$.

3. *Seja* $p = 3$, 3 *é primo. Tendo* $n = [2101]_3$, *podemos escrever na base* 3, $n = 2.3^3 + 1.3^2 + 0.3^1 + 1.3^0$. *Que é um somatório de potência de base 3. Perceba também que* $0 \leq a_i \leq 2$.

Os números n′s apresentados no exemplo 3, *itens* $2, 3$ *e* 4 *são números inteiros, respectivamente,* 7*-ádicos,* 5*-ádicos e* 3*-ádicos.*

Nós sabemos que depois de estudarmos o conjunto números inteiros segue o estudo do conjunto dos números racionais, as frações, também chamados, informalmente, de números com vírgula. Podemos, então, estender esse raciocínio para os números p-ádicos, questionando se é possível que os números p-ádicos possam ser racionais, representados em forma de fração e/ou ter vírgula? E aí, caro leitor? Você está curioso para saber a resposta? É provável que você tenha suposto uma resposta afirmativa. Continuemos a leitura, responderemos essas perguntas na próxima seção.

2.2 Números p-Ádicos

Com base no que foi apresentado até aqui, podemos por extensão, supor uma representação de um número p-ádico qualquer, que chamaremos de racionais p-ádicos. Temos assim nossa próxima definição que responderá as perguntas do parágrafo anterior. Segue abaixo a definição de números racionais p-ádicos.

Definição 2. *Um número n se diz racional p-ádico quando é determinado por uma soma de potências de um número primo p da seguinte forma*

$$n = a_{-r}p^{-r} + a_{-r+1}p^{-r+1} + ... + a_0 + a_1p^1 + a_2p^2 + a_3p^3 + ...$$

onde $0 \leq a_i \leq p - 1$ *e* $r \in \mathbb{N}$. *(O conjunto de todos os números racionais p-ádicos é*

representado por $\mathbb{Q}_p$.)

Nesse momento, nós estamos bem próximos de responder a pergunta que foi feita a linhas atrás, a saber: *Números p-ádicos podem possuir vírgula?* E a resposta é sim!!! Contudo, após uma breve análise da definição 2, já é possível perceber isso. Tomemos alguns exemplos.

Exemplo 4. *1. Seja $p = 7$, 7 é primo. Tendo $n = [124, 562]_7$, podemos escrever na base 7, $n = 1.7^2 + 2.7^1 + 4.7^0 + 5.7^{-1} + 6.7^{-2} + 2.7^{-3}$. Que é um somatório de potências de base 7. Perceba também que $0 \leq a_i \leq 6$.*

2. Seja $p = 5$, 5 é primo. Tendo $n = [243, 32]_5$, podemos escrever na base 5, $n = 2.5^2 + 4.5^1 + 3.7^0 + 3.5^{-1} + 2.5^{-2}$. Que é um somatório de potências de base 5. Perceba também que $0 \leq a_i \leq 4$.

3. Seja $p = 3$, 3 é primo. Tendo $n = [2101, 22]_3$, podemos escrever na base 3, $n = 2.3^3 + 1.3^2 + 0.3^1 + 1.3^0 + 2.3^{-1} + 2.3^{-2}$. Que é um somatório de potências de base 3. Perceba também que $0 \leq a_i \leq 2$.

Se, eventualmente, o leitor ainda não tenha conseguido visualizar essa ideia, faça uma observação deste número na base 10: $n = 397, 54$. Este número decimal pode ser escrito assim $n = 3.10^2 + 9.10^1 + 7.10^0 + 5.10^{-1} + 4.10^{-2}$, viu como ficou fácil!

Observação: *O conceito de valor absoluto p-ádico, proposição 2, só será discutido no próximo capítulo, porém utilizaremos aqui essa proposição para justificar a definição 2. Seja α algum número p-ádico. Afirmamos que se $|\alpha|_p \leq 1$, então $\alpha \in \mathbb{Z}_p$. Agora, se $|\alpha|_p > 1$, suponha que $|\alpha|_p = p^k$ com $k > 0$. Considere $\beta = p^k\alpha$, como $|\beta|_p = 1$, temos que*

$$\beta = \beta_0 + \beta_1.p + \beta_2.p^2 + ...$$

então

$$\alpha = \frac{\beta_0}{p^k} + \frac{\beta_1}{p^{k-1}} + ... + \frac{\beta_{k-1}}{p} + \beta_k + \beta_{k+1}p + ... + \beta_{k+r}p^r + ...$$

com $0 \leq \beta \leq (p-1)$ *para cada n. Essa discussão estabelece a definição anterior.*

As operações de adição e multiplicação se dão da mesma forma que a tradicional. No entanto, destacamos que o conjunto dos números p-ádicos não é ordenado, logo não há de se falar em $a > b$, a e $b \in \mathbb{Q}_p$. Embora o conceito de positivo e negativo exista, sua utilidade dependerá da conveniência. Por outro lado o conceito de oposto continua existente. Veremos exemplos disso a seguir.

Faremos, aqui, mais uma indicação de leitura, os números [2] e [4] das referências. Ambos trazem alguns exemplos sobre as operações matemáticas básicas envolvendo números racionais p-ádicos. Nós nos abstemos que apresentar exemplos neste trabalho. Entretanto, uma simples leitura dos textos citados é suficiente para compreensão das operações elementares no conjuntos dos números racionais p-ádicos. Almejamos que o leitor, caso ache necessário, desfrute do prazer da procura e da descoberta.

Além do mais, nesses exemplos você, caro leitor, verá curiosidades sobre os números p-ádicos deste tipo:

1. Embora exista número p-ádico negativo, sua representação pode ser positiva. Considere o conjunto 5-ádico, temos

$$\begin{array}{rr} & ...444444 \\ + & \underline{...000001} \\ & ...000000 \end{array}$$

Assim sendo, podemos afirmar que no conjunto 5-ádico $...444444 = -1$. Portanto,

a utilização de um número p-ádico ora positivo, ora negativo, vai depender da situação, como já dissemos.

2. Números p-ádicos podem se estender infinitamente para a esquerda. Consequência da definição de inteiros p-ádicos. Caso o número já finito, basta completar os demais dígitos com zeros.

3. Números p-ádicos não podem se estender infinitamente para a direita. Via observação acima.

4. Todos números racionais são p-ádicos. (Proposições 4 e 5, do capítulo 3).

5. Nem todos números reais são números p-ádicos. (Veja teorema 1) .

Na próxima seção apresentaremos uma caracterização um pouco diferente dos números p-ádicos. Falaremos sobre valor absoluto, corpos e anéis. Todavia, não tem nada a ver com "casamento", "namoro" ou "compromisso". Tenha sempre em mente que estamos diante de conceitos matemáticos. Obviamente, toda analogia é bem-vinda. Abuse de sua imaginação para internalizar esses conceitos. Vamos explicar todos essas definições no próximo capítulo.

3 O Corpo dos Números p-Ádicos

No texto adiante, nós vamos apresentar como se dá a construção dos números p-ádicos. Antes, porém, vamos relembrar o que é valor absoluto, e depois vamos perceber as implicações de valor absoluto na construção dos números p-ádicos. Neste instante vamos requerer de você um pouco mais de abstração, todavia ao final deste estudo você não será mais o mesmo. Este capítulo está fundamentado em [6], [9] e [12] de nossa bibliografia.

3.1 Valor Absoluto

Definição 3. *Seja C um corpo. A função $|\cdot| : C \to \mathbb{R}_+$ é chamada de* ***Valor Absoluto*** *de C se as seguintes propriedades estão satisfeitas para qualquer x e $y \in C$.*

1. $|x| = 0 \iff x = 0$
2. $|x.y| = |x|.|y|$
3. $|x + y| \leq |x| + |y|$

3.2 Corpo

Tendo em mãos a definição de valor absoluto, cabe, agora, definir o que é corpo. Não, não estamos falando do "corpo humano" ou "corpo de bombeiros". Neste contexto, o contexto matemático, até podemos fazer uma analogia com essas ideias já concebidas de corpo.

Entretanto, em matemática, corpo é uma estrutura onde as operações básicas, adição e multiplicação, funcionam direitinho. Quando se adiciona dois elementos de um corpo, a soma destes elementos continua pertencente ao corpo. Quando se multiplica

dois elementos do corpo, o produto destes elementos continua pertence ao corpo. Mais formalmente temos:

Definição 4. ***Corpo*** *é um anel comutativo, com unidade, em que todo elemento diferente de zero possui inverso multiplicativo.*

Parece que não ajudou muito, né? Neste momento, você está se perguntado o que é anel? O que é comutativo? O que é unidade do anel? O que é inverso multiplicativo? As respostas a essas perguntas estão contidas na definição de anel que se seguem abaixo.

3.3 Anel

Definição 5. ***Anel*** *é um conjunto A com duas operações binárias $(+)$ e $(\cdot)$, chamadas respectivamente de adição e multiplicação, que satisfaz as seguintes condições para quaisquer elementos a, b e $c \in A$:*

1. *Associatividade aditiva: para $\forall$ a, b, $c \in A$, temos $(a + b) + c = a + (b + c)$.*
2. *Existência do elemento neutro aditivo: para $\forall$ $a \in A$, temos $a + 0 = 0 + a = a$.*
3. *Existência de simétrico aditivo: para $\forall$ $a \in A$ $\exists$ $b \in A$ tal que $a + b = 0$.*
4. *Comutatividade aditiva: para $\forall$ a, $b \in A$, temos $a + b = b + a$*
5. *Associatividade multiplicativa: para $\forall$ a, b, $c \in A$, temos $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*
6. *Distributividade multiplicativa em relação a adição (à esquerda e à direita): para $\forall$ a, b, $c \in A$, temos $a \cdot (b+c) = a \cdot b + a \cdot c$; temos também $(a+b) \cdot c = a \cdot c + b \cdot c$*
7. *Existência de elemento neutro multiplicativo: $\exists$ $1 \in A$, $1 \neq 0$, tal que $\forall$ $a \in A$, $1 \cdot a = a \cdot 1 = a$.*

Assim, percebemos que para se ter um anel, é preciso gozar de algumas propriedades. Sabemos portanto, pela definição de anel, o que é um anel, o que é a comutatividade do anel, o que são os elementos neutros do anel, aditivo e multiplicativo. No entanto, ainda não sabemos o que é o inverso multiplicativo. Quando os anéis satisfazem todas as propriedades anteriores e, também, próxima condição, ele se torna um corpo. Segue:

8. Existência de elemento inverso multiplicativo: para $\forall\ a \in A$, $\exists\ b \in A$, *tal que* $a \cdot b = b \cdot a = 1$.

Aqui já entendemos o é valor absoluto, anel e corpo. Um pouco mais elucidados sobre esses conceitos, caminhamos para a seguinte proposição:

3.4 Valor Absoluto Real

Proposição 1. *Seja* $|\cdot|_\infty : \mathbb{Q} \to \mathbb{R}_+$, *definida como*

$$|x|_\infty = \begin{cases} x, & se \quad x \geq 0, \\ -x, & se \quad x < 0. \end{cases}$$

$|\cdot|_\infty$ *é o valor absoluto de* $\mathbb{Q}$, *e será chamado de Valor Absoluto Real.*

O símbolo ∞ é uma mera notação para diferenciá-lo de outros valores absolutos.

Caro leitor, podemos neste momento definir um outro tipo de valor absoluto. É possível fazer isso? Sim. Mas, valor absoluto não é definido de maneira única? Não. Podemos, então, definir valor absoluto de uma forma que envolva números p-ádicos, afinal *Números p-ádicos e Formas Quadráticas* é o tema central de nosso texto? Sim, sim, sim!!! Se bem que até agora nós não falamos nada sobre formas quadráticas, mas tenha calma, chegaremos lá. No momento temos uma proposição muito importante para apresentar. Segue que:

3.5 Valor Absoluto p-Ádico

Proposição 2. *Seja* $|\cdot|_p\ \mathbb{Q} \to \mathbb{R}$, *onde* p *é um número primo. Note que qualquer* $x \in \mathbb{Q}$ *não nulo pode ser escrito na forma* $p^n\frac{a}{b}$ *onde* n *é um número inteiro, com* a *e* b, *também, pertencentes aos inteiros,* $b \neq 0$, $p \nmid ab$. *A função* $|\cdot|_p$, *definida por*

$$|x|_p = \begin{cases} p^{-n}, & se \quad x = p^n\frac{a}{b} \neq 0, \\ 0, & se \quad x = 0. \end{cases}$$

é um valor absoluto de $\mathbb{Q}$, *e é chamado de valor absoluto p-ádico satisfazendo.*

1. $|x|_p = 0 \Leftrightarrow x = 0$
2. $|x.y|_p = |x|_p.|y|_p$
3. $|x + y|_p \leq max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$

Demonstração *Sejam* $x,\ y \in \mathbb{Q}$

1. $|x|_p = 0 \Leftrightarrow x = 0$, pois $p^{-n} > 0$.
2. Se $x = 0$ ou $y = 0$, então $|x \cdot y|_p = 0$ e $|x|_p \cdot |y|_p = 0$, logo, vale a propriedade. Se $x \neq 0$ e $y \neq 0$, podemos escrever $x = p^n\frac{a}{b}$ e $y = p^m\frac{c}{d}$ onde $p \nmid abcd$. Então, $|x \cdot y|_p = |p^{n+m}\frac{ac}{bd}|_p = p^{-n-m} = p^{-n} \cdot p^{-m} = |x|_p \cdot |y|_p$.
3. Se $x = 0$ ou $y = 0$, então $|x + y|_p = |x|_p + |y|_p$.

   Se $x + y = 0$, então $|x + y|_p = |0|_p = 0 \leq |x|_p + |y|_p$, pois $|\cdot|_p$ é sempre maior ou igual a zero.

   Se $x \neq 0$, $y \neq 0$ e $x + y \neq 0$; podemos escrever $x = p^n\frac{a}{b}$ e $y = p^m\frac{c}{d}$ onde $p \nmid abcd$. Suponha $n \leq m$. Assim, $|x|_p \geq |y|_p$. Além disso, $|x + y|_p = |p^n\frac{a}{b} + p^m\frac{c}{d}|_p = |p^n\frac{(a\cdot d + p^{m-n}b\cdot c)}{b\cdot d}|_p \leq p^{-n} = |x|_p$. De maneira semelhante $m \leq n \Rightarrow |y|_p \geq |x|_p$. Logo, $|x + y|_p \leq max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$. ■

3.6 Métrica

Os valores absolutos estão intimamente ligados ao conceito de distância. Toma-se uma medida como referência chamada de unidade, e a partir desta unidade medida deduz-se todas as demais: dobro da unidade, triplo da unidade, metade da unidade, um terço da unidade, etc. Vamos entender melhor isso através do conceito de métrica.

Definição 6. *Seja C um conjunto. A função d: $C \times C \to \mathbb{R}_+$ é chamada de* ***métrica*** *de C se possuir as seguintes propriedades para quaisquer x, y e $z \in C$:*

1. $d(x, y) = 0 \Leftrightarrow x = y$.

2. $d(x, y) = d(y, x)$.

3. $d(x, z) \leq d(x, y) + d(y, z)$.

Temos ainda que (C, d) é chamado de **espaço métrico**.

Vamos, agora, casar os conceitos de valor absoluto e métrica, para tanto utilizaremos mais uma proposição. Esta, por sua vez, apresenta que uma métrica pode ser induzida por uma valor absoluto. Observe.

Proposição 3. *Seja C um corpo e $|\cdot|$ um valor absoluto de C. Então a função d: $C \times C \to \mathbb{R}_+$ definida por $d(x, y) = |x - y|$ é uma métrica de C.*

Demonstração: *Sejam x, y e $z \in C$*

1. $d(x, y) = 0 \Leftrightarrow |x - y| = 0 \Leftrightarrow x - y = 0 \Leftrightarrow x = y$.

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

3. $d(x, z) = |x - z| = |x - y + y - z| \leq |x - y| + |y - z| = d(x, y) + d(y, z)$. ■

Portanto, se utilizarmos o conceito *valor absoluto* estaremos utilizando o conceito de *métrica* e vice-versa. Isso é muito bom, porque vai deixar nosso trabalho mais prazeroso, mais palatável. Então, continuemos firmes, fortes e felizes.

Neste momento, vamos fazer a caracterização do corpo dos números p-ádicos de uma maneira formal. Não se assuste, você vai perceber que um pouquinho de imaginação é suficiente para entender tudo.

3.7 Sequência de Cauchy

Em Matemática, uma sequência (a_n) é dita de *Cauchy* se a distância entre os termos vai se aproximando de zero. Nossa intuição nos leva a perceber que os termos (a_n) vão ficando cada vez um mais próximo do outro a medida que n cresce. Um exemplo clássico é $a_n = \frac{1}{n}$. Pense um pouco no motivo dessa sequência ser de *Cauchy*. Com tudo isso que apresentamos, podemos fazer uma definição de gala para uma sequência de *Cauchy*.

Definição 7. *Seja C um corpo com um valor absoluto $|\cdot|$. Seja $(a_n)_{n\in\mathbb{N}}$ uma sequência de C. A sequência (a_n) é dita* ***sequência de Cauchy*** *se, dado $\varepsilon > 0$, $\exists\ n_0\ \in \mathbb{N}$ tal que $\forall\ i, j \in \mathbb{N}$ onde $i > j > n_0$ então $|a_i - a_j| < \varepsilon$.*

É importante perceber que as sequências de Cauchy são definidas em espaços métricos. Contudo sabemos que o valor absoluto induz uma métrica, assim sendo podemos defini-la em termos de valores absolutos. Isso vai ser bem útil já, já. Aguarde!

Temos agora duas definições muito importantes para o conclusão deste trabalho. São elas:

Definição 8. *Um corpo C é dito* ***completo*** *se toda sequência de Cauchy de C, usando valor absoluto $|\cdot|$, converge*[1].

[1]qualidade ou disposição do que é convergente; direção para um ponto comum. Ex: $a_n = \frac{1}{n}$

Definição 9. *O conjunto $\overline{C}$ é dito* ***completamento de um corpo*** *C pelo valor absoluto $|\cdot|$ se as seguintes condições forem satisfeitas:*

1. *$\overline{C}$ é completo.*
2. *Existe uma isometria $d : C \to \overline{C}$. O valor absoluto estendido para $\overline{C}$, denotado $|\cdot|_{\overline{C}}$, é tal que $|d(x)|_{\overline{C}} = |x|$, para todo $x \in C$.*
3. *Para todo $x \in \overline{C}$ existe $(a_n)_{n\in\mathbb{N}}$, uma sequência de Cauchy de C, tal que $x = \lim_{n\to\infty} a_n$.*

Proposição 4. *O completamento dos números racionais $\mathbb{Q}$ usando o valor absoluto real, forma um corpo, denominado corpo do números reais, e denotado $\mathbb{R}$.*

Não vamos nos aprofundar nessa proposição. Para uma análise completa sobre esse assunto recomendamos a leitura de [7]. Lá tem tudo e mais um pouco que o leitor possa querer saber sobre a construção dos números reais, seja pela construção de Cantor ou pelos cortes de Dedekind. Sigamos em frente sem desanimar.

Proposição 5. *O completamento dos números racionais $\mathbb{Q}$ usando o valor absoluto p-ádico, para algum p primo, forma um corpo, denominado corpo p-ádico, e denotado $\mathbb{Q}_p$.*

3.8 Teorema de Ostrowski

Algumas afirmações importantes: Todo corpo que possui uma métrica pode ser completado. Para mais profundidade, verificar em [9]. Como afirmado acima, o completamento dos $\mathbb{Q}$ via valor absoluto p-ádico implica nos $\mathbb{Q}_p$, uma demonstração completa pode ser localizada em [8]. Para a leitura de alguns comentários objetivos, e com simplicidade única, recomendamos [2].

converge para zero a medida que os valores de n vão aumentando, $n \in \mathbb{N}^*$

No próximo teorema, temos a afirmação de que todo completamento de $\mathbb{Q}$ ou é o valor absoluto real ou o valor absoluto p-ádico. Vamos mostrar que a métrica apresentada é equivalente a métrica real ou é equivalente a métrica p-ádica. Isso pode ser afirmado pois teremos métricas equivalentes. Lembre-se: *Duas normas* $|\cdot|_1$ *e* $|\cdot|_2$*, definidas num espaço vetorial* V[2]*, são equivalentes se existem* $a > 0$ *e* $b > 0$ *satisfazendo* $a|v|_1 \leq |v|_2 \leq b|v|_1$ *para todo* $v \in V$.

A demonstração desse teorema é um pouco mais abstrata do que tudo que tratamos até aqui. Entretanto você, amigo leitor, vai se sair bem. Temos mais uma oportunidade de se apropriar de conhecimentos novos, não desanime, o saber é sempre transformador.

Teorema 1. ***Ostrowski:*** *Toda métrica (valor absoluto) sobre* $\mathbb{Q}$ *é equivalente ao valor absoluto real* $|\cdot|$ *ou ao valor absoluto p-ádico* $|\cdot|_p$ *para um número primo p.*

Demonstração Seja φ uma métrica arbitrária não trivial de $\mathbb{Q}$. Dois casos são possíveis: ou existe algum número natural $a > 1$, tal que $\varphi(a) > 1$, ou então $\varphi(n) \leq 1$ para todo número natural n. Considere o primeiro caso. Como

$$\varphi(n) = \varphi(1 + 1 + ... + 1) \leq \varphi(1) + ... + \varphi(1) = n$$

podemos definir

$$\varphi(a) = a^{\alpha},$$

onde α é um número real que satisfaz $0 < \alpha < 1$.

Tomando um número natural arbitrário N, decompondo-o em potência de a, temos:

$$N = x_0 + x_1 a + x_2 a^2 + ... + x_{k-1} a^{k-1},$$

[2]Veja [12] em nossa referência.

onde $0 \leq x_i \leq a-1, (\ 0 \leq i \leq k-1),\ x_{k-1} \geq 1$. Assim N satisfaz a inequação

$$a^{k-1} \leq N < a^k.$$

pela propriedades métricas, e pela definição $\varphi(n)$ e $\varphi(a)$, segue

$$\varphi(N) \leq \varphi(x_0) + \varphi(x_1).\varphi(a) + ... + \varphi(x_{k-1}).\varphi(a^{k-1})$$

$$\leq (a-1)(1 + a^2 + ... + a^{(k-1)\alpha})$$

$$= (a-1)\frac{a^{k\alpha}-1}{a^\alpha - 1}$$

$$< (a-1)\frac{a^{k\alpha}}{a^\alpha - 1} = \frac{(a-1)a^\alpha}{a^\alpha - 1}a^{(k-1)\alpha}$$

$$\leq \frac{(a-1)a^\alpha}{a^\alpha - 1}N^\alpha = CN^\alpha;$$

isto é

$$\varphi(N) < CN^\alpha$$

onde C é uma constante independente de N. trocando N por N^m na inequação, com m um número natural, nós obtemos:

$$\varphi(N)^m = \varphi(N^m) < CN^{m\alpha},$$

daí

$$\varphi(N) < \sqrt[m]{C}N^\alpha$$

se m tende ao infinito, nós chegamos em

$$\varphi(N) \leq N^\alpha.$$

agora, sendo $N = a^k - b$, onde $0 < b \leq a^k - a^{k-1}$, nós obtemos

$$\varphi(N) \geq \varphi(a^k) - \varphi(b) = a^{\alpha k} - \varphi(b).$$

Mas já sabemos que

$$\varphi(b) \leq b^\alpha \leq (a^k - a^{k-1})^\alpha,$$

e assim

$$\varphi(N) \geq a^{\alpha k} - (a^k - a^{k-1})^\alpha = \left[1 - \left(1 - \frac{1}{a}\right)^\alpha\right] a^{\alpha k} = C_1 a^{\alpha k} > C_1 N^\alpha,$$

onde a constante C_1 não depende de N. Seja m, novamente, um número natural arbitrário. Se N é trocado por N^m na inequação anterior, então

$$\varphi(N)^m = \varphi(N^m) > C_1 N^{\alpha m},$$

disso

$$\varphi(N) > \sqrt[m]{C_1} N^\alpha$$

e quando $m \to \infty$ isso implica

$$\varphi(N) \geq N^\alpha.$$

Comparando as desigualdades acima, vemos que $\varphi(N) = N^\alpha$ para qualquer número natural N. Agora, seja $x = \pm N_1/N_2$ um número racional arbitrário, diferente de zero (N_1 e N_2 são número naturais). Então

$$\varphi(x) = \varphi\left(\frac{N_1}{N_2}\right) = \frac{\varphi(N_1)}{\varphi(N_2)} = \frac{N_1^\alpha}{N_2^\alpha} = |x|^\alpha$$

Nós temos que se $\varphi(a) > 1$ para pelo menos um número natural a, então a métrica φ é da forma dada acima.

Agora, nos direcionamos para o caso

$$\varphi(n) \leq 1$$

para todo número natural n. Se para cada número primo p, temos $\varphi(p) = 1$, então pela condição (3), nós também temos $\varphi(n) = 1$ para todo número natural n, e assim $\varphi(x) = 1$ para todo racional $x \neq 0$. Mas isso deveria contradizer a suposição de que φ é não trivial. Assim, para algum primo p, nós temos $\varphi(p) < 1$. Assumindo que para algum outro primo q, $q \neq p$, nós também temos $\varphi(q) < 1$. Tomando os expoentes k e l tais que

$$\varphi(p)^k < \frac{1}{2}, \quad \varphi(q)^l < \frac{1}{2}.$$

como p^k e q^l são primos entre si, então existem inteiros u e v tal que $up^k + vq^l = 1$. Por (2.7), $\varphi(u) \leq 1$ e $\varphi(v) \leq 1$, de modo que

$$1 = \varphi(1) = \varphi(up^k + vq^l) \leq \varphi(u)\varphi(p)^k + \varphi(v)\varphi(q)^l < \frac{1}{2} + \frac{1}{2}.$$

Esta contradição demonstra que existe um único primo p tal que

$$\varphi(p) = \rho < 1.$$

Como $\varphi(q) = 1$ para qualquer outro número primo, $\varphi(a) = 1$ para cada inteiro a que é primo relativo com p. Seja $x = p^m(a/b)$ um número racional não negativo (a e b

inteiros, relativamente primos com p). Então

$$\varphi(x) = \varphi(p^m)\frac{\varphi(a)}{\varphi(b)} = \varphi(p^m) = \rho^m.$$

Concluímos, então, a demonstração do teorema. ■

Neste momento, nós encerramos nossa explanação sobre números p-ádicos. Vamos nos direcionarmos para o estudo de forma quadráticas. É, isso aí! Até que enfim. Discorreremos sobre a segunda parte referente ao título do nosso texto. Você está empolgado? Sim? Muito bom. Então vamos nessa! Nos vemos na próxima seção. Até lá.

4 Formas Quadráticas sobre $\mathbb{Q}_p$

4.1 Formas Quadráticas

Depois de todas essa jornada, chegamos a parte final de nosso trabalho. Estudamos os números p-ádicos, a seguir veremos sua aplicação a formas quadráticas. Faremos a diante algumas afirmações, conjecturas e/ou definições sobre formas quadráticas e números p-ádicos, em seguida, encadearemos de maneira mais harmônica e coesa possível esses conceitos. Culminaremos o trabalho com a demonstração do teorema de Hasse-Minkowski, a parte mais importante do trabalho, que você amigo leitor conhecerá já, já. Vamos em primeiro lugar definir formas quadráticas. Ansioso? Então vamos em frente.

Definição 10 (***Forma Quadrática***). *Função polinomial, $F : C^n \to C$, de grau n , cuja expressão tem apenas termos de grau 2, é dita de* ***forma quadrática*** *e dada por:*

$$F(x_1, x_2, ..., x_n) = \alpha_1 x_1^2 + \beta_{1,2} x_1 x_2 + ... + \beta_{1,n} x_1 x_n + \alpha_2 x_2^2 + ... + \beta_{2,n} x_2 x_n + ... + \alpha_n x_n^2$$

com α_i *e* $\beta_{j,k} \in \mathbb{R}, 1 \leq i \leq n, 1 \leq j \leq k \leq n$.

Um conceito que se segue a esta definição é o fato que a expressão da forma quadrática de uma função polinomial pode ser escrita na forma matricial como o produto de x, matriz linha de n elementos, por M_F, matriz quadrada de ordem n e por x^T, matriz coluna de n elementos, nessa ordem. Temos

$F : C^n \to C$

$F(x_1, x_2, ..., x_n) = \alpha_1 x_1^2 + \beta_{1,2} x_1 x_2 + ... + \beta_{1,n} x_1 x_n + \alpha_2 x_2^2 + ... + \beta_{2,n} x_2 x_n + ... + \alpha_n x_n^2$

$$F(x_1, x_2, ..., x_n) = \begin{bmatrix} x_1 & x_2 & \dots & x_n \end{bmatrix} \begin{bmatrix} \alpha_1 & \frac{\beta_{1,2}}{2} & \dots & \frac{\beta_{1,n}}{2} \\ \frac{\beta_{1,2}}{2} & \alpha_2 & \dots & \frac{\beta_{2,n}}{2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\beta_{1,n}}{2} & \frac{\beta_{2,n}}{2} & \dots & \alpha_n \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

Exemplo 5. $F : \mathbb{R}^3 \to \mathbb{R}$

$F(x_1, x_2, x_3) = x_1^2 + 2x_1x_2 + 3x_2^2 - x_2x_3 - x_3^2$

$$xM_Fx^T = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 1 & 3 & -\frac{1}{3} \\ 0 & -\frac{1}{2} & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = x_1^2 + 2x_1x_2 + 3x_2^2 - x_2x_3 - x_3^2$$

$xM_Fx^T = F(x_1, x_2, x_3)$

O que aconteceria caso a matriz M_F pudesse ser diagonalizada? A álgebra linear propõem que uma matriz quadrada M_F pode ser diagonalizável se for possível apresentar uma matriz D diagonal semelhante à matriz M_F, portanto, se há uma matriz inversível P tal que $P^{-1}M_FP$ é igual a matriz diagonal D. Considere o próximo exemplo.

Exemplo 6. *Sejam* $F : \mathbb{R}^2 \to \mathbb{R}$

$F(x_1, x_2) = x_1^2 + 5x_1x_2 + 2x_2^2$

$$F(x_1, x_2) = xM_Fx^T = \begin{bmatrix} x_1 & x_2 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

Agora,

$$PM_FP^{-1} = \begin{bmatrix} -3 & 1 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} -\frac{1}{5} & \frac{1}{5} \\ \frac{2}{5} & \frac{3}{5} \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 4 \end{bmatrix} = D$$

Assim sendo, temos uma nova matriz com novas variáveis, devido a mudança de coordenadas[3]*. Matriz essa, semelhante a primeira, que não alterar o resultado do sistema.*

$$F(y_1, y_2) = yDy^T = \begin{bmatrix} y_1 & y_2 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 4 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$$

$F(y_1, y_2) = -y_1^2 + 4y_2^2$

Esse processo, a diagonalização, torna a resolução destas formas quadráticas muito mais fácil. Uma boa notícia para você, amigo leitor:"*toda matriz simétrica é diagonalizável*". Para mais detalhes, leitura [12] de nossa bibliografia. Pautados nessas informações apresentadas nos parágrafos anteriores, afirmamos "*Toda matriz simétrica é equivalente a uma forma diagonal* do tipo:"

$$F(x_1, ..., x_n) = a_1x_1^2 + ... + a_nx_n^2$$

Perceba que trabalhar com a forma diagonal é muito mais cômodo. Temos um polinômio homogêneo de grau 2 diagonalizado, o que torna o caminho para resolução de formas quadráticas muito mais deleitoso.

[3]Veja [12].

4.2 Princípio Local Global

Sabemos que uma função polinomial de grau 2 pode ser escrita na forma diagonalizada. O princípio local global, definido adiante, afirma que uma função possui raízes racionais não triviais se, e somente se, possui raízes em $\mathbb{R}$ e em $\mathbb{Q}_p$, para qualquer primo p. O princípio local global vale para algumas funções polinomiais, entretanto estamos particularmente interessados nas funções polinomiais homogêneas de grau 2, as formas quadráticas.

Uma pergunta que poderia ser feita é: *Será que o Princípio Local Global vale para formas quadráticas?* A resposta a essa pergunta e o, próprio, Princípio local Global são ferramentas fundamentais para o conclusão deste trabalho. Temos:

Princípio Local Global *Uma equação polinomial possui zeros racionais não triviais se, e somente se, possui zeros não triviais sobre* $\mathbb{R}$ *e sobre* $\mathbb{Q}_p$*, primo* p*.*

Portanto, se uma função polinomial possui raízes em $\mathbb{R}$ e em $\mathbb{Q}_p$, qualquer que seja p primo, então a função polinomial possui raízes em $\mathbb{Q}$. Se uma função polinomial possui raízes em $\mathbb{Q}$, então esta função possui raízes em $\mathbb{R}$ e em $\mathbb{Q}_p$, para qualquer primo p.

Sabemos que $\mathbb{Q}$ é um subconjunto de $\mathbb{R}$, e sabemos também que $\mathbb{Q}$ é um subconjunto de $\mathbb{Q}_p$, para qualquer p primo,como vimos na capítulo anterior, pelo teorema 1. Isso garante a ida, ou seja, se tivermos raízes racionais, obviamente, teremos raízes reais e raízes p-ádicas. Entretanto, e a volta? *Como garantir a existência de raízes reais e raízes p-ádicas para se apresentar as raízes racionais?* É exatamente isso que iremos mostrar nessa parte final do trabalho, em especial para formas quadráticas.

Uma afirmação que vem como consequência do princípio local global é a que se segue: "*O Princípio Local-Global vale para formas quadráticas*". Por meio desta asser-

tiva, nomeada de *Hasse-Minkowski*, encaixamos os conceitos de formas quadráticas e o princípio local global. Algebrizando o princípio local global atrelando-o as formas quadráticas temos:

4.3 Hasse-Minkowski (1923)

Hasse-Minkowski (1923) *Seja* $f(x_1, ..., x_n) = a_1x_1^2 + ... + a_nx_n^2$ *uma forma quadrática com coeficientes em* $\mathbb{Q}$. *Então* $f(x_1, ..., x_n) = 0$ *tem solução não trivial em* $\mathbb{Q}$ *se, e somente se,* $f(x_1, ..., x_n) = 0$ *tem solução não trivial em* $\mathbb{R}$ *e em* $\mathbb{Q}_p$ *para cada primo p.*

Temos então aqui um exemplo de função polinomial, a forma quadrática, que satisfaz o Princípio Local Global, respondendo assim a pergunta deixada acima: *Será que o Princípio Local Global vale para formas quadráticas? SIM!*

Nutrimos, como já mencionado, interesse nesse caso. Temos aqui a parte mais importante de nosso trabalho. Se este texto fosse o céu, certamente esta parte, Hasse-Minkowski, seria o sol, supondo que esteja de dia, e este dia não esteja nublado. Se este texto fosse o planeta terra, Hasse-Minkowski seria o núcleo. Se este texto fosse o corpo humano, Hasse-Minkowski seria o coração e o cérebro. Deu para perceber que essa pate é importante para nosso trabalho, não é?

A seguir apresentamos uma conjectura atribuída a Emil Artin, que a propôs para Helmut Hasse, no dia 27 de setembro de 1927, de acordo com o diário de Hasse.

4.4 Conjectura de Artin

Conjectura de Artin (1935): *Todo polinômio homogêneo de grau k em pelo menos* $k^2 + 1$ *variáveis possui zeros p-ádicos não triviais.*

Nós estamos interessados, naturalmente, quando $k = 2$. Nosso objeto de desejo são as formas quadráticas, como você amigo leitor sabe bem, logo direcionaremos nossas atenções ao único par primo, a saber o número dois. Podemos então conjecturar que todo polinômio homogêneo de grau 2 em pelo menos $2^2 + 1 = 5$ variáveis possui zeros p-ádicos não triviais.

4.5 Terjanian (1966)

Mesmo com importante avanço realizado, a conjectura de Artin permanece sem solução, é uma conjectura como o nome já diz. De fato, não há um único caso para o qual a conjectura de Artin é demonstrada. Isso é tão verdade que Guy Terjanian, matemático francês, apresentou, em 1966, um contra-exemplo para a conjectura de Artin. Ele apresentou um polinômio homogêneo de grau 4 com 18 variáveis que não possuía solução não triviais. Contudo, isso, segundo a Conjectura de Artin, não deveria ocorrer, pois $18 > 4^2 + 1 = 17$. Formalizando-se, segue:

Terjanian (1966): *Apresentou o primeiro contra-exemplo à Conjectura de Artin, exibindo um polinômio homogêneo de grau 4 sobre* $\mathbb{Q}_2$ *em 18* $(> 4^2 + 1 = 17)$ *variáveis que não possui zeros não triviais.*

Terjanian observou que a forma

$G(x) = G(x_1, x_2, x_3) = x_1^4 + x_2^4 + x_3^4 - x_1^2x_2^2 - x_1^2x_3^2 - x_2^2x_3^2 - x_1x_2x_3(x_1 + x_2 + x_3)$

é tal que

$$G(x) \equiv \begin{cases} 1 \ (mod\ 4), & \text{se algum } x_i \text{ é ímpar.} \\ 0 \ (mod\ 16), & \text{se todos } x_i\text{'s são pares.} \end{cases}$$

pois $x^2 \equiv x^4 \equiv 1(mod\ 4)$ se x é ímpar. Tome agora

$$H(x) = H(x_1, ..., x_9) = G(x_1, x_2, x_3) + G(x_4, x_5, x_6) + G(x_7, x_8, x_9)$$

logo

$$H(x)\begin{cases} \not\equiv 1 \ (mod\ 4), & \text{se} \quad \text{algum } x_i \text{ é ímpar.} \\ \equiv 0 \ (mod\ 16), & \text{se} \quad \text{todos } x_i\text{'s são pares.} \end{cases}$$

finalmente seja

$$F(x) = F(x_1, ..., x_{18}) = H(x_1, ..., x_9) + 4H(x_{10}, ..., x_{18}).$$

Vamos supor que exista $\beta \in \mathbb{Z}_2^{18}$ tal que $F(\beta) = 0$. Sem perda de generalidade podemos assumir que β é um zero primitivo (possui uma unidade 2- ádica em alguma de suas coordenadas), logo

$$F(\beta) = H(\beta_1, ..., \beta_9) + 4H(\beta_{10}, ..., \beta_{18}) = 0.$$

Se a unidade 2-ádica está entre as primeiras nove coordenadas, teremos

$$0 \equiv F(\beta) = H(\beta_1, ..., \beta_9) \ (mod\ 4)$$

que contradiz $H(x)$. Logo a unidade deve estar entre as nove últimas coordenadas, mas então

$$0 \equiv F(\beta) = 4H(\beta_{10}, ..., \beta_{18}) \ (mod\ 16)$$

o que também contradiz $H(x)$.

Isso nos mostra que F não tem zeros 2-ádicos apesar de ter 18 variáveis, contrariando a Conjectura de Artin. ■

4.6 Ax - Kochen (1965)

O amigo leitor pode estar se perguntando: A Conjectura de Artin vale ou não vale? Artin conjecturou que é possível encontrar zeros p-ádicos em um polinômio homogêneo de grau k em k^2+1 variáveis, porém Terjanian contra-argumentou que existe pelo menos um caso contrário. E agora? Agora surgem mais duas personagens nesse debate: James Axe e Simon B. Kochen. Estes homens apresentam um teorema que diz que para cada inteiro positivo n existe um conjunto finito $A(n)$ formado por números primos, tal que se p é qualquer primo que não está em $A(n)$ então todo polinômio homogêneo de grau k sobre os números p-ádicos em k^2+1 variáveis possui zeros p-ádicos não triviais. Segue:

Teorema 2. ***(Ax - Kochen (1965))*** *Para todo inteiro $n \geq 1$, o conjunto $A(n)$ dos primos para os quais $\mathbb{Q}_p$ não satisfaz a Conjectura de Artin é finito.*

Resolvemos assim nosso problema. Artin afirmou que "Todo polinômio homogêneo de grau k em k^2+1 variáveis possui zeros p-ádicos não triviais". Terjanian afirmou que nem sempre "Todo polinômio homogêneo de grau k em k^2+1 variáveis possui zeros p-ádicos não triviais". Ax-Kochen resolveram esse debate afirmando que se não for possível que "Todo polinômio homogêneo de grau k em pelo menos k^2+1 variáveis possui zeros p-ádicos não triviais", então este conjunto de primos p que não satisfaça a Conjectura de Artin é finito, ou seja, se não é possível, não é possível em um conjunto finito.

O conjunto de número primos é infinito. De fato, a quantidade de primos é finita. Sejam então, $p_1, p_2, ..., p_n$ a lista de todos os primos existentes. Tomemos $R = p_1 \cdot p_2 \cdot ... \cdot p_n + 1$. É óbvio que R não é divisível por nenhum dos p_i ´s de nossa lista, por outro lado R é maior do que qualquerp_i. Sabemos também que todo inteiro maior do que 1 pode ser representado de maneira única, a menos da ordem, como um produto de fatores primos. Dessa forma, R é um número primo ou possui algum fator primo e isto

implica na existência de um número primo que não está em nossa lista. Portanto o sequência de números primos é infinita. Com isso em mente, podemos afirmar que há infinitas soluções que satisfazem a Conjectura de Artin.

4.7 Davenport-Lewis

Para encerrar esse debate, apresentamos mais duas pessoas: H. Davenport e D. J. Lewis. Este dois matemáticos apresentaram o seguinte teorema, que recebe seus nomes:

Teorema 3. ***(Davenport-Lewis)*** *Todo polinômio diagonal de grau k em $n \geq k^2 + 1$ variáveis sempre possui zeros p-ádicos não triviais.*

Para mais detalhes, indicamos a leitura de [11] em nosso bibliografia. Artin afirmou que "Todo polinômio homogêneo de grau k em pelo menos $k^2 + 1$ variáveis possui zeros p-ádicos não triviais", afirmação esta que já repetimos algumas vezes em nosso texto. Terjanian apresentou um contra-exemplo a esta afirmação. Ax e Kochen resolveram esse debate afirmando que o conjuntos de números primos que não satisfaz a Conjectura de Artin é finito. Davenport e Lewis foram mais além, eles afirmam que a Conjectura de Artin vale, não apenas em $k^2 + 1$ variáveis, mas também em n variáveis, salvo $n \geq k^2 + 1$.

4.8 Teorema de Hasse

Com todas essas informações em mãos, podemos agora sintetizar todas elas no teorema a seguir. Perceba, então, que o teorema a abaixo ilustra um caso particular, que nos interessa, para o teorema de Hasse-Minkowski, que por sua vez apresenta a validade do Princípio Local Global para formas quadrática, a saber uma forma quadrática em

pelo menos 5 variáveis, com coeficientes racionais, terá zero racional se, e somente se, tiver zero real e zeros p-ádicos.

Consequentemente, se afirmamos que Hasse-Minkowski é o ápice do trabalho, seu núcleo, a parte mais importante, então o teorema de Hasse é a bandeira fincada no topo da montanha, a cereja do bolo, a exemplificação desejada. Segue:

Teorema 4. ***(Teorema de Hasse)*** *Toda forma quadrática em pelo menos 5 variáveis possui zeros p-ádicos não triviais.*

Observe que como a forma do polinômio homogêneo é quadrática, então o grau do polinômio é 2, o que acarreta 5 variáveis pela Conjectura de Artin. Davenport-lewis garante que são pelo menos 5 variáveis, pode haver mais variáveis. Ax-Kochen garante que pode não haver solução para alguns conjuntos de números primos, como apresentou Terjanian, porém esses conjuntos desses números primos que não satisfazem a Conjectura de Artin são finitos. Assim sendo, há infinitas solução p-ádicas não triviais para toda forma quadrática em pelo menos 5 variáveis.

Essa afirmação é muito forte, portanto precisa ser provada, e é o que faremos a diante, para tanto carecemos de mais um resultado, mais precisamente um lema. Segue:

4.9 Lema de Hensel

Considere uma função polinomial diagonalizada de grau k com n variáveis. Se essa função polinomial for congruente a zero módulo potências de algum p primo, então a função polinomial possui raízes em $\mathbb{Q}_p$. Formalizando isso, temos:

Lema 1. ***(Lema de Hensel)*** *Considere a forma diagonal* $f(x_1, ..., x_n) = a_1x_1^k + ... + a_nx_n^k$ *com* $a_i \in \mathbb{Z}$. *Seja* p *um primo e escreva* $k = p^\tau k_0$. *Defina*

$$\gamma = \begin{cases} 1, & se \quad \tau = 0; \\ \tau + 1, & se \quad \tau > 0 \quad e \quad p > 2; \\ \tau + 2, & se \quad \tau > 0 \quad e \quad p = 2. \end{cases}$$

Se a congruência

$$f(x_1, ..., x_n) \equiv \ 0 \ (mod \ p^{\gamma})$$

tem solução não singular módulo p, então

$$f(x_1, ..., x_n) = 0$$

tem solução em $\mathbb{Q}_p$.

4.10 Demonstração do Teorema de Hasse

O que acontece com os coeficientes ao considerarmos $f(x_1, ..., x_n)$ *módulo p?*
No conjunto de todas as formas quadráticas com coeficientes inteiros considere as seguintes mudanças de variáveis:

(i). $f'(x_1, ..., x_n) = f(p^{r_1}x_1, ..., p^{r_n}x_n)$, com $r_i \in \mathbb{Z}$;

(ii). $f''(x_1, ..., x_n) = \frac{a}{b} f(x_1, ..., x_n)$, com $\frac{a}{b} \neq 0$.

Diremos que f e g são equivalentes se uma pode ser obtida da outra por uma combinação de (i) e (ii). Isto define uma relação de equivalência.

Reescreva

$f(x_1, ..., x_n) = f_0(x_1, ..., x_{m_0}) + pf_1(x_{m_0+1}, ..., x_n)$ *Onde os coeficientes de* f_0 *e de* f_1 *não são divisíveis por p. Utilizando as mudanças (i) e (ii), podemos supor que* $m_0 \geq 3$. *De fato, se* $m_0 \leq 2$, *então o número de variáveis em* f_1 *é maior ou igual a 3, pois* $n \geq 5$. *Faça então a mudança*

$$f'(x_1, ..., x_n) = pf(x_1, ..., x_{m_0}, p^{-1}x_{m_0+1}, ..., p^{-1}x_n)$$

Considerando p um primo ímpar, logo $p > 2$, pelo Lema de Hensel, basta encontrarmos soluções não singulares módulo p para a congruência

$$a_1x_1^2 + ... + a_{m_0}x_{m_0}^2 \equiv 0 \ (mod\ p)$$

A existência de solução para essa congruência é garantida pelo próximo teorema. Perceba que temos uma demonstração dentro da demonstração, fato que não compromete em nada seu silogismo, sua lógica, seu encadeamento de ideia, amigo leitor.

Teorema 5. ***(Teorema de Chevalley-Warning)*** *Sejam p um primo e $f(x_1, ..., x_n)$ um polinômio com coeficientes inteiros e grau k. Se $n > k$, então o número de soluções da congruência $f(x_1, ..., x_n) \equiv 0 \ (mod\ p)$ é divisível por p. Em particular, se o polinômio não possui termo constante, existe solução não trivial*

Demonstração: Suponhamos que a congruência tenha s soluções $A_i = (a_1^{(i)}, ..., a_n^{(i)})$, $1 \leq i \leq s$. Seja $g(x_1, ..., x_n) = 1 - f(x_1, ..., x_n)^{p-1}$, então g satisfaz:

$$g(x_1, ..., x_n) = \begin{cases} 1, & \text{quando} \quad (x_1, ..., x_n) \equiv A_i \ (mod\ p); \\ 0, & \text{caso contrário;} \end{cases}$$

Para qualquer $A = (a_1, ..., a_n)$, defina

$$D_A(x_1, ..., x_n) = \prod_{j=1}^{n}(1 - (x_j - a_j)^{p-1}).$$

É fácil ver que

$$D_A(x_1,...,x_n) = \begin{cases} 1, & \text{quando} \quad (x_1,...,x_n) \equiv A \ (mod\ p); \\ 0, & \text{caso contrário;} \end{cases}$$

Seja $g^*(x_1,...,x_n) = D_{A_1}(x_1,...,x_n) + ... + D_{A_s}(x_1,...,x_n)$.

Da equação acima, resulta que g^* tem as mesmas soluções que g, para quaisquer que sejam $x_1,...,x_n$. Mais que isso, $g^*(x_1,...,x_n) \equiv (x_1,...,x_n)$ ($mod\ p$), qualquer que seja $(x_1,...,x_n)$. Assim, para cada monômio, os coeficientes de g^* e g são congruentes módulo p. Como em cada D_{A_i} existe um termo de grau $n(p-1)$, a saber, o termo $(-1)^n(x_1.....x_n)^{p-1}$. O coeficiente de $(x_1.....x_n)^{p-1}$ em g^* é $s(-1)^n$. Contudo, o coeficiente de $(x_1.....x_n)^{p-1}$ em g é 0, pois o grau de g é menor que $n(p-1)$, o que implica que $s(-1)^n \equiv 0\ (mod\ p)$ portanto $p|s$.■

De fato, caso $p > 2$, pelo Lema de Hensel, temos $\gamma = 1$. Assim sendo $f_0 + pf_1 \equiv 0\ (mod\ p)$ implica em $f_0 \equiv 0\ (mod\ p)$. Mais precisamente, queremos que

$$a_1x_1^2 + ... + a_{m_0}x_{m_0}^2 \equiv 0\ (mod\ p)$$

tenha solução. Supomos $m_0 \geq 3$, aqui temos também $k = 2$. Explicitamente, $m_0 > k$, por Chevalley-Warning, garantimos a existência de soluções.

Agora, caso $p = 2$, no Lema de Hensel, teremos $\gamma = 3$, ou seja, a existência de solução 2-ádica é garantida pela existência de solução de

$$a_1x_1^2 + ... + a_{m_0}x_{m_0}^2 + 2(a_{m_0+1}x_{m_0+1}^2 + ... + a_nx_n^2) \equiv 0\ (mod\ 8)$$

com x_i ímpar, para algum $1 \leq i \leq m_0$. Lembre que $m_0 \geq 3$.

No caso $3 \leq m_0 < n$:

Considere a forma parcial

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + 2a_nx_n^2$$

Como $a_1 + a_2 = 2b$ temos:

$$a_1 + a_2 + 2a_nb^2 \equiv 2b + 2b^2 \ (mod\ 4)$$

$$a_1 + a_2 + 2a_nb^2 \equiv 2b(1 + b) \ (mod\ 4)$$

$$a_1 + a_2 + 2a_nb^2 \equiv 0 \ (mod\ 4)$$

Ou seja,

$$a_1 + a_2 + 2a_nb^2 = 4c$$

Faça agora $x_1 = x_2 = 1;\ x_3 = 2c$ e $x_n = b$. Assim,

$$a_1^2 + a_2^2 + a_3(2c)^2 + 2a_nb^2 \equiv 4a_3c^2 + 4c \ (mod\ 8)$$

$$a_1^2 + a_2^2 + a_3(2c)^2 + 2a_nb^2 \equiv 4c^2 + 4c \ (mod\ 8)$$

$$a_1^2 + a_2^2 + a_3(2c)^2 + 2a_nb^2 \equiv 4c(c + 1) \ (mod\ 8)$$

$$a_1^2 + a_2^2 + a_3(2c)^2 + 2a_nb^2 \equiv 0 \ (mod\ 8)$$

Já no caso $m_0 = n$, considere a forma parcial

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2$$

Se $a_1 + a_2 \equiv a_3 + a_4 \ (mod\ 4)$, faça $x_1 = x_2 = x_3 = x_4 = 1$.

Se $a_1 + a_2 \equiv 0 (mod\ 4)$, faça $x_1 = x_2 = 1$ e $x_3 = x_4 = 0$.

Em qualquer caso, teremos $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 = 4b$.

Faça assim $x_5 = 2b$ e então

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2 \equiv 4b + 4a_5b^2 (mod\ 8)$$

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2 \equiv 4b + 4b^2 (mod\ 8)$$

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2 \equiv 0 \ (mod\ 8) \blacksquare$$

Diante de tudo isso discorremos durante este capítulo, conseguimos assim garantir que existem raízes p-ádicas para formas quadráticas. Todavia, se retomarmos o Princípio Local Global temos: "Uma equação polinomial possui zeros racionais não triviais se, e somente se, possui zeros não triviais sobre $\mathbb{R}$ *e sobre* $\mathbb{Q}_p$*, primo* p". Garantimos o $\mathbb{Q}_p$. Apresentamos as soluções p-ádicas. Mas e quanto a $\mathbb{R}$? E as soluções reais?

Para termos $F(x_1, ..., x_n) = a_1x_1^2 + ... + a_nx_n^2 = 0$ no corpo dos números reais, basta tomarmos $a_i = -a_j$ com $1 \leq i < j \leq n$, e considerarmos todos os demais coeficientes $a_k = 0$ com $1 \leq k \leq n$, $a_k \neq a_i$ e $a_k \neq a_j$. Com isso garantimos a existência de soluções reais, o que finaliza esta discussão. Simples, não é mesmo?!

Neste capítulo, primeiramente, definimos o que é uma forma quadrática. Em seguida, afirmamos que toda forma quadrática pode ser escrita na forma diagonal. A partir daí, explanamos o Princípio Local-Global, ilustrado-o com Hasse-Minkowsk, que garante que o Princípio Local-Global vale para formas quadráticas. As proposições de Artin, Terjanian, Ax-Kochen, Davenport-Lewis, Hasse, Hensel e Chevalley-Warning deram dinâmica e validade a tudo que nós apresentamos. Todos estas afirmações correlacionaram os números p-ádicos e as formas quadráticas, tendo por objetivo assegurar

a existência de soluções racionais para formas quadráticas se garantíssemos a existência de soluções p-ádicas e reais, como foi feito.

antes de nos despedirmos, para você, amigo leitor, que perseverou até aqui, o nosso presente é a resolução do problemas/desafio apresentado no início deste trabalho. Veja só!

Solução: *O número* 14 *é representado pelo ET por* $\dagger\dagger$. *Considerando que a base de numeração do ET é* b, *podemos escrever:*

$$14 = \dagger.b^1 + \dagger.b^0 \implies$$

$$14 = \dagger(b+1) \implies$$

$$2.7 = \dagger(b+1) \implies$$

com b *é par, então* $b+1$ *é impar. Assim sendo:*

$$b + 1 = 7$$

$$b = 6$$

Portanto o ET possui 6 dedos, três em cada mão.

Este problema nos fez entender o quanto a Matemática, sobre tudo a Teoria dos Números, é maravilhosa. Fez ascender em nós uma alegria imensurável. Nos respondeu o porque de termos escolhidos a Matemática como profissão. Que você amigo leitor possa conseguir visualizar isso também. Que através deste breve estudo sobre números p-ádicos e formas quadráticas, você possa ter sentido, pelo menos um pouco, desta emoção indescritível que a Teoria dos Números no proporciona. Forte abraço. Até uma próxima.

Referências

[1] Borevich, z.i.; Shafarevich, i.r., *Number Theory*, Academic Press Inc.(1966).

[2] Gusmão,í.m.m., *Números p-ádicos*, João Pessoa.(2016).

[3] Hefez,a., *Iniciação à Aritmética*, Rio de Janeiro, IMPA.(2015).

[4] Fazio,V.S., *Introdução à Teoria de Galois: Corpos p-ádicos*, Florianópolis.(2016).

[5] Amorim,É., *Números p-ádicos e Teorema de Monsky*, New Jersey.(2015).

[6] Artin, m., *Algebra*, New Jersey.(1991).

[7] Aguilar , i. Dias, m. , *A Construção dos Números Reais e suas Extensões*, 4º Colóquio da Região Centro-Oeste .(2015).

[8] Bachman, g., *Introduction to p-Adic Number and Valuation Theory*, New York.(1964).

[9] Lima, e.l., *Espaços Métricos*, Rio de Janeiro.(2015).

[10] Ferreira, m.a., *Resolvendo Equações em Corpos p-Ádicos*,VII Bienal da SBM. Alagoas.(2014).

[11] Godinho, h., *Polinômios Homogêneos sobre Números p-Ádicos*,Lisboa. (1999).

[12] Boldrini, j.l., *Álgebra Linear*. (1980).

[13] Veras, d.s., *Solubilidade de sistemas de equações aditivas sobre o corpo dos números p-ádicos com uma restrição sobre p*. (2013).