Universidade Federal do Rio Grande do Sul

Instituto de Matemática

Programa de Pós-Graduação em Matemática

NÚMEROS p-ÁDICOS TRANSCENDENTES E SÉRIES DE RACIONAIS QUE CONVERGEM EM QUALQUER COMPLETAMENTO DE $\mathbf{Q}$

por

GERTRUDES REGINA TODESCHINI HOFFMANN

Porto Alegre, dezembro de 2000

Dissertação submetida por GERTRUDES REGINA TODESCHINI HOFFMANN como requisito parcial para a obtenção do grau de Mestre em Matemática pelo Programa de Pós-Graduação em Matemática do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.

Professor Orientador:
Dra. Cydara Cavedon Ripoll

Banca Examinadora:
Dra. Ada Maria de Souza Doering
Dr. Alveri Alves Sant'Ana
Dr. Yves Albert Emile Lequain

Data de Defesa: 11 de dezembro de 2000.

Agradecimentos

À Universidade Federal do Rio Grande do Sul e toda a equipe de professores do Programa de Pós Graduação pelo incentivo, dedicação e competência.

À Cydara, uma verdadeira professora, agradeço de modo muito especial pelo incentivo e entusiasmo demonstrados tanto no início do curso como na etapa final de orientação para este trabalho.

A todos os colegas, pela amizade, apoio e ajuda nos momentos difíceis durante os anos de curso.

Ao meu marido, Clovis, pelo companheirismo, estímulo e compreensão.

Por fim, agradeço às minhas filhas Anelise e Leticia e a toda minha família, que entenderam as minhas ausências. A eles dedico este trabalho.

ABSTRACT

When we consider the completion of $\mathbb{Q}$ with respect to the usual absolute value we obtain the field of the real numbers $\mathbb{R}$. But if we do the same with respect to any other absolute value of $\mathbb{Q}$ we obtain the field of the p-adic numbers $\mathbb{Q}_p$, where p is a prime. In this work we consider the convergence of series in $\mathbb{Q}_p$ and in $\mathbb{R}$ and construct series of racional numbers with amazing convergence properties.

We also prove that it is possible to obtain a series of rational numbers that converges in all completions of $\mathbb{Q}$ even if we prescribe its sum in each completion.

RESUMO

Quando tomamos o valor absoluto usual e o completamento de $\mathbb{Q}$ em relação à métrica induzida por ele, o resultado é o corpo $\mathbb{R}$ dos números reais; fazendo o mesmo processo com qualquer outro valor absoluto definido em $\mathbb{Q}$, obtemos um dos corpos p-ádicos $\mathbb{Q}_p$. O propósito deste trabalho é explorar a convergência de séries em $\mathbb{Q}_p$ e em $\mathbb{R}$, construindo algumas séries de números racionais com propriedades de convergência surpreendentes. Provamos também que é possível construir uma série de números racionais que converge em qualquer completamento de $\mathbb{Q}$ para um valor pré-fixado de $\mathbb{Q}_p$ e de $\mathbb{R}$.

Índice

Introdução: 1

Capítulo 1: 3

1.1 *Valores absolutos em um corpo*: 3
1.2 *Os valores absolutos em* $\mathbb{Q}$. *O corpo dos números* p *–ádicos*: 4
1.3 *Exemplos*: 8
1.4 *Uma estimativa para* $|n!|_p$: 12

Capítulo 2: *Números Transcendentes e o Teorema de Liouville nas versões real e p-ádica* 16

2.1 *Números Reais Transcendentes e o Teorema de Liouville real* 16
2.2 *Prolongamentos de um valor absoluto de* $\mathbb{Q}$ *a uma extensão finita de* $\mathbb{Q}$. 21
2.3 *Números* p-ádicos *Transcendentes* 25
2.4 *Séries que convergem para um* p *–ádico transcendente, com* $p \in V_{\mathbb{Q}}$ 31

Capítulo 3: *Séries que convergem para números* p *–ádicos prescritos, com* $p \in V_{\mathbb{Q}}$: 38

3.1 *Enunciado e demonstração do resultado* 38
3.2 *Algorítmo para a construção da série* 47
3.3 *Exemplos* 48

Referências Bibliográficas 68

INTRODUÇÃO

Sabemos que, se $|\ \ |$ denota o valor absoluto usual em $\mathbb{Q}$, então $\mathbb{R}$ é o completamento topológico de $\mathbb{Q}$ em relação à métrica induzida por $|\ \ |$, ou seja, $\mathbb{R}$ é o menor corpo que contém $\mathbb{Q}$ e no qual toda seqüência de Cauchy de racionais converge. Assim, a noção de convergência depende fortemente do valor absoluto usual $|\ \ |$ em $\mathbb{Q}$.

A noção de valor absoluto pode ser generalizada a um corpo qualquer, (veja cap 1) e a partir de um valor absoluto sobre um corpo K pode-se definir uma métrica sobre K e portanto um novo completamento de K pode ser construido.

Em $\mathbb{Q}$ pode-se definir outros valores absolutos, os valores absolutos p-ádicos $|\ \ |_p$, onde p é um primo qualquer, e a métrica induzida por este novo valor absoluto dará origem a um correspondente completamento que chamamos de **Corpo dos números p-ádicos $\mathbb{Q}_p$**.

Ostrowski, em 1935, provou que todo valor absoluto não trivial em $\mathbb{Q}$ é equivalente a um dos valores absolutos p-ádicos $|\ \ |_p$ ou ao valor absoluto usual $|\ \ |$. Além disso, todos estes valores absolutos $|\ \ |$ e $|\ \ |_p$ são não equivalentes.

A nossa proposta é explorar o tema "convergência de séries de racionais em qualquer completamento de $\mathbb{Q}$".

Inicialmente veremos, no capítulo 2, que, fixado $p \in V_{\mathbb{Q}} = \{ p \in \mathbb{N}, p$ primo $\} \cup \{\infty\}$, é possível construir uma série de números racionais que converge em $\mathbb{Q}_p$. Em particular, é possível decidir se a soma da série é um número algébrico ou é um número transcendente em $\mathbb{Q}_p$. A seguir, construiremos uma série de racionais que é convergente em cada $\mathbb{Q}_p$ e cuja soma é transcendente sobre $\mathbb{Q}$. Para tal demonstraremos os Teoremas de Liouville real e p-ádico.

Finalmente, no capítulo 3 veremos também que é possível construir uma seqüência de números racionais não nulos tal que para cada $p \in V_{\mathbb{Q}}$ a série por eles formada converge em $\mathbb{Q}_p$ para pré-fixado $\alpha_p \in \mathbb{Q}_p$(veja Teorema 4.1, onde obtemos até um algoritmo para a construção de tal série). Em particular, podemos exigir que a soma da série seja sempre um mesmo número racional, respondendo assim uma questão colocada por Koblitz [K,p.85] (Koblitz questionava até se isto seria possível - veja [K], pag 142).

A referência para este trabalho é [B-S].

Convenções:

* "primo " significará sempre primo positivo.

* Ao considerarmos um número racional x, escreveremos $x = \frac{a}{b}$ com b sempre positivo.

* Às vezes denotaremos o valor absoluto usual em $\mathbb{Q}$ ou em $\mathbb{R}$ simplesmente por $|\ \ |$, mas outras vezes ele será denotado por $|\ \ |_\infty$.

Notações:

$V_{\mathbb{Q}} = \{p/\ p\ é\ primo\} \cup \{\infty\}$

$\mathbb{R}_+ = (0, \infty)$

CAPÍTULO 1

Salientamos aqui apenas alguns resultados sobre números p-ádicos que estarão sendo utilizados com mais freqüência neste trabalho.

Os detalhes podem ser encontrados nos vários títulos indicados na Bibliografia.

1.1 Valores absolutos em um corpo

Definição: Um **valor absoluto** num corpo K qualquer é uma função $|\ |: K \to \mathbb{R}_+$ que satisfaz as sequintes condições:

(i) $\forall\ x \in K,\ |x| = 0 \Leftrightarrow x = 0$

(ii) $\forall\ x,\ y \in K, |xy| = |x||y|$

(iii) $\forall\ x,\ y \in K, |x+y| \leq |x| + |y|$,

sendo esta última chamada **desigualdade triangular**.

Se tivermos ainda satisfeita a condição:

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

chamada **desigualdade triangular forte**, teremos um **ultra valor absoluto**.

Definição: Um valor absoluto $|\ |$ num corpo K é dito **arquimediano** se $|m.1| > |1|$, para algum $m \in \mathbb{N}$, onde por $m.1$ representamos a soma de m parcelas iguais à unidade de K.

*Proposição*1.1: As seguintes condições são equivalentes, com respeito a um valor absoluto $|\ |$ definido num corpo K :

(i) $|\ |$ é não arquimediano

(ii) $\forall n \in \mathbb{N}^*,\ \forall x_1,...,x_n \in K,\ |x_1 + ... + x_n| \leq \max_{1 \leq i \leq n}\{|x_i|\}$

Prova: Veja [E], pag 5 □

Definição: Dois valores absolutos $|\ |_1$ e $|\ |_2$ definidos em um corpo K se dizem **equivalentes** se induzem a mesma topologia em K.

Teorema 1.2: Dois valores absolutos $|\ |_1$ e $|\ |_2$ em um corpo K são equivalentes se, e somente se, existe um número real positivo α tal que $|\ \ |_1 = |\ \ |_2^{\alpha}$.

Prova: veja [$G2$] p.42 □

Proposição 1.3: Dois quaisquer valores absolutos arquimedianos sobre um mesmo corpo K são sempre equivalentes.

Prova: veja [L], p.285. □

1.2 Os valores absolutos de $\mathbb{Q}$. O corpo dos Números p-Ádicos

Aqui estamos interessados em $K = \mathbb{Q}$, e queremos salientar que existem outros valores absolutos em $\mathbb{Q}$ além do valor absoluto usual, que muitas vezes denotaremos por $|\ \ |_\infty$.

Inicialmente, observamos que se $x \in \mathbb{Q}$, digamos, $x = \frac{a}{b} \neq 0$ com $a \in \mathbb{Z}$, $b \in \mathbb{Z}_+^*$ e $mdc(a,b) = 1$, então podemos escrever, utilizando o Teorema Fundamental da Aritmética, $\frac{a}{b} = a.b^{-1} = \pm\ p_1^{r_1}\ \dots\ p_r^{r_n}.q_1^{-s_1}\ \dots\ q_s^{-s_m}$ onde $a = \pm p_1^{r_1}\ \dots\ p_r^{r_n}$ e $b = q_1^{s_1}\ \dots\ q_s^{s_m}$, p_i e q_j números primos distintos (positivos), para todo i e todo j. Esta representação é única, pela unicidade da fatoração em $\mathbb{Z}$ e pelo fato de a e b não possuirem fatores comuns, já que $mdc(a,b) = 1$. Assim, para um primo p qualquer, podemos garantir que existem $p_1,\dots,p_l$ primos distintos de p e $\alpha, \alpha_1,\dots,\alpha_l \in \mathbb{Z}$(alguns talvez nulos, mas todos únicos) tais que

$$\frac{a}{b} = \pm\ p^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2}\ \dots\ p_l^{\alpha_l} \qquad (1)$$

Definição: O expoente α em (1) é dito **valorização p-ádica de $x = \frac{a}{b}$** e é denotado por $v_p(x)$. Convenciona-se $v_p(0) = \infty$.

Proposição 1.4: A função $|\ \ |_p : \mathbb{Q} \to \mathbb{R}_+$ definida por

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

para cada $x \in \mathbb{Q}$, é um valor absoluto.

Definição: $|\ \ |_p$: $\mathbb{Q} \to \mathbb{R}_+$ construida acima é denominada **valor absoluto p-ádico.**

A idéia é que o valor absoluto p-ádico de x mede o "tamanho aritmético" de x com respeito a p, no sentido de que x será p-adicamente pequeno se uma potência grande de p divide o numerador de x.

Assim, por exemplo 20 é 2-adicamente muito pequeno pois, $|20|_2 = 2^{-2} = \frac{1}{4}$, enquanto $\frac{1}{24}$ é 2-adicamente maior do que 20, pois $\left|\frac{1}{24}\right|_2 = 8$. Para $\frac{140}{297} = 2^2.3^{-3}.5.7.11^{-1}$ temos: $\left|\frac{140}{297}\right|_2 = \frac{1}{4}$, $\left|\frac{140}{297}\right|_3 = 27$, $\left|\frac{140}{297}\right|_5 = \frac{1}{5}$, $\left|\frac{140}{297}\right|_7 = \frac{1}{7}$, $\left|\frac{140}{297}\right|_{11} = 11$ e $\left|\frac{140}{297}\right|_p = 1$, para todo p diferente de 2, 3, 5, 7 ou 11. Daí, já podemos deduzir que o valor absoluto p-ádico é dramaticamente diferente do valor absoluto usual em $\mathbb{Q}$. Mais ainda, mostra-se que a desigualdade triangular é muito mais forte quando estamos trabalhando com valor absoluto p-ádico.

Proposição 1.5: Seja p um primo; então o valor absoluto p-ádico $|\ \ |_p$ satisfaz as seguintes propriedades:

(i) $\forall\ x \in \mathbb{Z}, |x|_p \leq 1$

(ii) A função $|\ \ |_p$ é um valor absoluto não-arquimediano em $\mathbb{Q}$

(iii) $|\ \ |_p$ é um ultra valor absoluto; mais ainda se $|x|_p \neq |y|_p$ então

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

Queremos agora relacionar o valor absoluto usual e os valores absolutos p-ádicos entre si.

Proposição 1.6 :

(i) Dois quaisquer valores absolutos do conjunto $A = \{\ |\ \ |_p,\ p \in V_{\mathbb{Q}}\}$ são não equivalentes.

(ii) (Ostrowski, 1935) Qualquer valor absoluto não trivial de $\mathbb{Q}$ é equivalente a um dos valores absolutos $|\ \ |_p$ para p primo ou $p = \infty$.

(iii) **Fórmula do produto**: Dado $x \in \mathbb{Q}^*$, temos $\prod_{p \in V_{\mathbb{Q}}} |x|_p = 1$. Ou, equivalentemente, $\sum_{p \in V_{\mathbb{Q}}} \log\ |x|_p = 0$

(iv) Seja $x \in \mathbb{Q}^*$, $x \neq 1$. Então $|x|_p$ não pode ser pequeno para todo $p \in V_{\mathbb{Q}}$, ou seja: $\exists\ p \in V_{\mathbb{Q}}, |x|_p > 1$.

Prova:

(i) Basta ver que para quaisquer $p,\ q \in V_{\mathbb{Q}}$

$$|p|_q = \begin{cases} 1 \text{ se } q \neq p \text{ ambos primos} \\ \frac{1}{p} \text{ se } q = p \\ p \text{ se } q = \infty \end{cases}$$

de modo que, para qualquer $a > 0$, temos $\frac{1}{p} \neq 1^{\alpha} \neq p$, o que comprova, pelo teorema acima, que dois quaisquer valores absolutos p-ádicos com $p \in V_{\mathbb{Q}}$ são não equivalentes.

(ii) veja [G] ou [Sk].

(iii) Suponha que x é um número racional diferente de zero,

$$x = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_l^{\alpha_l}$$

onde $p_1, \dots, p_l$ são primos distintos, $\alpha_l \in \mathbb{Z}$ e $\alpha_l \neq 0$. Então

$$\Pi_{p \in V_{\mathbb{Q}}} |x|_p = |x| \, \Pi_{p\ primo} |x|_p = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_l^{\alpha_l} p_1^{-\alpha_1} p_2^{-\alpha_2} \dots p_l^{-\alpha_l} = 1$$

(iv) Se $x \in \mathbb{Q}^*$, $x \neq 1$, $x = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_l^{\alpha_l}$ com $p_1, \dots, p_l$ primos distintos, como $\Pi_{p \in V_{\mathbb{Q}}} |x|_p = 1$ e

$$\begin{cases} 1 \neq |x| = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_l^{\alpha_l} \\ |x|_{p_i} = p_i^{-\alpha_i} \end{cases}$$ basta ver que, se $p_i^{\alpha_i} < 1$ então $p_i^{-\alpha_i} > 1$.

□

Finalmente, salientamos que o valor absoluto p-ádico conduz a uma nova métrica sobre $\mathbb{Q}$:

$$d : \mathbb{Q} \times \mathbb{Q} \mapsto \mathbb{R}, \text{ dada por } d(x,y) = |x - y|_p \text{ para todo } x,\ y \in \mathbb{Q}.$$

Para cada primo p, denotaremos por $\mathbb{Q}_p$ o completamento de $\mathbb{Q}$ com relação à métrica induzida pelo valor absoluto p-ádico $|\ \ |_p$. Isto significa que $\mathbb{Q}_p$ é o menor corpo que contém $\mathbb{Q}$ e no qual toda seqüência de Cauchy de racionais converge com relação a $|\ \ |_p$. Ou seja: se $(x_n)_{n \in \mathbb{N}}$ é uma seqüência de racionais que satisfaz

$$\forall\ \varepsilon \in \mathbb{R}_+^*,\ \exists\ N \in \mathbb{N}\ [n,\ m \geq N \Rightarrow\ |x_n - x_m|_p < \varepsilon]$$

então existe $x \in \mathbb{Q}_p$ tal que

$$\forall\ \varepsilon \in \mathbb{R}_+^*,\ \exists\ N \in \mathbb{N}\ [n \geq N \Rightarrow\ |x_n - x|_p < \varepsilon].$$

Escrevemos $x = \lim_p x_n$.

A construção de $\mathbb{Q}_p$ é portanto análoga à construção de $\mathbb{R}$. Para maiores detalhes veja [G] e [G-R-S].

Queremos estender o valor absoluto p-ádico a $\mathbb{Q}_p$. O lema a seguir mostra que isto pode ser feito.

Lema 1.7: Seja (x_n) uma seqüência de números racionais que, com relação a $|\ \ |_p$, é de Cauchy mas não converge a zero. Então a seqüência de números reais $|x_n|_p$ se estabiliza, isto é, existe N tal que, para $m, n > N$ temos que $|x_n|_p = |x_m|_p$.

Prova: Como (x_n) não tende a zero, existe $\varepsilon > 0$ tal que para todo $n_0 \in \mathbb{N}$, existe $n > n_0$ tal que

$$|x_n|_p \geq \varepsilon$$

Por outro lado, como a seqüência é de Cauchy, para tal ε existe $n_1 \in \mathbb{N}$ tal que

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

Logo, se $N = \max\{n_0, n_1\}$, temos que, para $n,\ m > N$,

$$|x_n|_p \geq \varepsilon \quad \text{e} \quad |x_m|_p \geq \varepsilon.$$

Como

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

temos, pela Proposição 1.5(*iii*), $|x_n|_p = |x_m|_p$ □

Definição: Se $\delta \in \mathbb{Q}_p$ e (x_n) é qualquer representante da classe δ, definimos

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

Prova-se que este prolongamento de $|\ \ |_p$ a $\mathbb{Q}_p$ ainda é um valor absoluto.

Salientamos aqui uma propriedade de séries de racionais na métrica p-ádica que difere da análise real, e que é conseqüência da desigualdade triangular forte:

Proposição 1.8: Uma série de números racionais $\sum_{n=0}^{\infty} a_n$ converge em $\mathbb{Q}_p$ se, e somente se, seu termo geral tende a zero, isto é:

$$\lim_p a_n = 0$$

Prova: Suponhamos $\lim_p a_n = 0$. Então

$$\forall\ \varepsilon \in \mathbb{R}_+^*,\ \exists\ N \in \mathbb{N}\ [n \geq N \Rightarrow |a_n|_p < \varepsilon\ ]$$

Denotando por S_n a soma dos n primeiros termos, temos para $m \geq n$:

$$|S_m - S_n|_p = \left| \sum_{j=n+1}^{m} a_j \right|_p \leq \max\ \{|a_{n+1}|_p, ..., |a_m|_p\} < \varepsilon$$

de modo que (S_n) é de Cauchy, logo convergente em $\mathbb{Q}_p$.

A recíproca é análoga à demonstração que se faz para séries convergindo em $\mathbb{R}$. □

Como podemos pensar nos elementos de $\mathbb{Q}_p$?

Afirmamos que os elementos de $\mathbb{Q}_p$ têm uma representação bem acessível, a saber, generalizam a representação de um natural em base p, de maneira bem análoga à expansão decimal de um número real (na qual expressamos $\alpha \in \mathbb{R}$ como uma série convergente $\alpha = \sum_{n=l}^{\infty} d_n 10^{-n}$ onde $l \in \mathbb{Z}$ e cada d_n é um inteiro satisfazendo $0 < d_n \leq 9$).

De fato, podemos expressar $\delta \in \mathbb{Q}_p$ como o limite de uma série convergente de um tipo bem particular:

$$\delta = \sum_{n=l}^{\infty} d(p,n)\ p^n$$

onde l é um inteiro (que pode ser negativo) e cada $d(p,n)$ é um inteiro satisfazendo $0 \leq d(p,n) \leq p - 1$, e isto de maneira única. Chamamos esta série de **expansão p-ádica de** δ.

Chamamos atenção para os sinais contrários dos expoentes na expansão em $\mathbb{R}$ e na expansão em $\mathbb{Q}_p$ (Maiores detalhes em [G-R-S] e[K])

Com tal representação para os números p-ádicos, as operações de adição e multiplicação em $\mathbb{Q}_p$ funcionam de maneira análoga às operações com números reais escritos na forma decimal. Ainda: se $d(p,l) \neq 0$ então $v_p(\delta) = l$, de modo que $|\delta|_p = p^{-l}$

1.3 Exemplos

1.3.1 Exemplos de expansão p-ádica de inteiros

(i) $\alpha \in \mathbb{N}^* \Leftrightarrow \alpha$ tem expansão finita: (que coincide com sua expansão usual em base p) ou seja: $\alpha = a_0 + a_1 p + ... + \alpha_l p^l$.

Exemplo: Se $p = 7$ e $\alpha = 335$ então $335 = 6 + 5.7 + 6.7^2$

(ii) De (i) obtemos que, se α for um inteiro negativo então α tem expansão p-ádica infinita.

Por exemplo, para todo p primo afirmamos que a expansão p-ádica de -1 é dada por:

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

De fato:

$$\begin{aligned} 1 + \textstyle\sum_{n=0}^{\infty} (p-1)p^n &= 1 + (p-1) + (p-1)p + (p-1)p^2 + ... \\ &= p + (p-1)p + (p-1)p^2 + ... \\ &= p^2 + (p-1)p^2 + (p-1)p^3 + ... \\ &= p^3 + (p-1)p^3 + ... \\ &= ... \\ &= 0. \end{aligned}$$

Seguindo a mesma idéia acima, se $p = 7$ e $\alpha = -31$ então $31 = 3 + 4.7$, e portanto precisamos adicionar $4 + 2.7 + 6.7^2 + 6.7^3 + ...$ para se obter zero, ou seja,

$$-31 = 4 + 2.7 + \sum_{k=2}^{\infty} 6.7^k$$

Maiores detalhes podem ser vistos em [Sk] p.7.

1.3.2 Exemplo de expansão p-ádica de racional não inteiro

$p = 7;\quad \frac{31}{20} = \frac{3+4.7}{6+2.7} = (3 + 4.7).(6 + 2.7)^{-1}$

Inicialmente determinemos a expansão de $(6 + 2.7)^{-1}$

$(6 + 2.7)^{-1} = x_0 + x_1.7 + x_2.7^2 + ...$ é tal que

$$(6+2.7).\left(x_0+x_1.7+x_2.7^2+...\right) = 1;$$

então:

$$6x_0 \equiv 1\left(\text{mod } 7\right) \quad \Rightarrow x_0 = 6$$

Daí

$$(6x_0-1)7^{-1}+2x_0+6x_1 \equiv 0\left(\text{mod } 7\right) \Rightarrow$$

$$5+12+6x_1 \equiv 0\left(\text{mod } 7\right) \Rightarrow 6x_1+17 \equiv 0\left(\text{mod } 7\right) \Rightarrow x_1 = 3$$

Daí

$$(6x_1+17)7^{-1}+2x_1+6x_2 \equiv 0\left(\text{mod } 7\right) \Rightarrow$$

$$5+6+6x_2 \equiv 0\left(\text{mod } 7\right) \Rightarrow 6x_2+11 \equiv 0\left(\text{mod } 7\right) \Rightarrow x_2 = 4$$

Daí

$$(6x_2+11)7^{-1}+2x_2+6x_3 \equiv 0\left(\text{mod } 7\right) \Rightarrow$$

$$5+8+6x_3 \equiv 0\left(\text{mod } 7\right) \Rightarrow 6x_3+13 \equiv 0\left(\text{mod } 7\right) \Rightarrow x_3 = 6$$

Daí

$$(6x_3+13)7^{-1}+2x_3+6x_4 \equiv 0\left(\text{mod } 7\right) \Rightarrow$$

$$7+12+6x_4 \equiv 0\left(\text{mod } 7\right) \Rightarrow 6x_4+19 \equiv 0\left(\text{mod } 7\right) \Rightarrow x_4 = 5$$

Daí

$$(6x_4+19)7^{-1}+2x_4+6x_5 \equiv 0\left(\text{mod } 7\right) \Rightarrow$$

$$7+10+6x_5 \equiv 0\left(\text{mod } 7\right) \Rightarrow 6x_5+17 \equiv 0\left(\text{mod } 7\right) \Rightarrow x_5 = 3$$

Logo, temos que

$$(6+6.7)^{-1} = 6+3.7+4.7^2+6.7^3+5.7^4+3.7^5+4.7^6+6.7^7+5.7^8+3.7^9+...$$

Assim, $\frac{31}{20} = (3+4.7).(6+2.7)^{-1}$

$$= (3+4.7).\left(6+3.7+4.7^2+6.7^3+5.7^4+3.7^5+..\right)$$

$$= 4+7^2+3.7^3+2.7^4+7^6+3.7^7+2.7^8+7^{10}+...$$

Prova-se que um número p-ádico é racional se e só se sua expansão p-ádica é periódica a partir de um certo ponto. Note a periodicidade encontrada nos exemplos acima. Maiores detalhes podem ser vistos em [Ma] Teorema 1 p.12.

1.3.3 Outros exemplos de séries

(i) A seqüência $(3^n)_{n\in\mathbb{N}}$ é exemplo de uma seqüência $(a_n)_{n\in\mathbb{N}}$ (de números inteiros positivos) tal que

$$\sum_{n=0}^{\infty} {}_{p\text{-ádico}} a_n$$

converge em $\mathbb{Q}_p$ para algum $p \in V_{\mathbb{Q}}$ e diverge em todos os demais: de fato $\sum_{n=0}^{\infty} 3^n$ é uma expansão 3-ádica, logo um elemento de $\mathbb{Q}_3$.

No entanto, para todo $p \in V_{\mathbb{Q}} - \{3\}$ temos que para todo $n \in \mathbb{N}$,

$$|3^n|_p = \begin{cases} 1, & \text{se } p \neq \infty \\ 3^n, & \text{se } p = \infty \end{cases},$$

logo o termo geral 3^n não tende a zero, de modo que, pela proposição 1.8, a série $\sum_{n=0}^{\infty} 3^n$ diverge em $\mathbb{Q}_p$ para todo $p \in V_{\mathbb{Q}} - \{3\}$.

Observamos ainda que, como se trata de uma expansão periódica esta série representa um número racional em $\mathbb{Q}_3$. Ainda, por ser uma série geométrica de razão conhecida, conseguimos até calcular seu valor em $\mathbb{Q}_3$:

$$\lim_3(S_n) = \lim_3\left(1 + 3 + 3^2 + \ldots + 3^n\right) = \lim_3 \frac{3^{n+1}-1}{3-1} = -\frac{1}{2}$$

(ii) Exemplo de uma série que converge em $\mathbb{R}$ e diverge em $\mathbb{Q}_p$ para todo primo p :

$$\sum_{n=0}^{\infty} \frac{1}{n!}$$

(iii) Exemplo de uma série que diverge em $\mathbb{Q}_p$, para todo $p \in V_{\mathbb{Q}}$:

$$\sum_{n=0}^{\infty} \frac{1}{n}$$

(iv) Exemplo de uma série que converge em $\mathbb{Q}_p$, para todo primo p, mas diverge em $\mathbb{R}$:

$$\sum_{n=0}^{\infty} n!$$

De fato, note que para todo primo p, $(v_p(n!))$ é uma seqüência não decrescente e não estacionária de números naturais donde $|n!|_p$ tende a zero.

(v) Exemplo de uma série que converge em $\mathbb{Q}_p$ para todo $p \in V_{\mathbb{Q}}$.

Temos a série $\sum_{n=0}^{\infty} n!$ que converge também com respeito a cada valor absoluto p-ádico. Vamos modificá-la para que seja convergente também com respeito ao valor absoluto usual. Note que a série $\sum_{n=0}^{\infty} \frac{n!}{n!^2}$, converge em $\mathbb{R}$, mas infelizmente diverge com respeito a cada valor absoluto p –ádico. A idéia é colocar no denominador um número cada vez maior mas que não envolva nenhum dos primos que estão no numerador, assim teremos chance de fazê-la convergir em $| \ |_\infty$ sem mexer na convergência $| \ |_p$; afirmamos que a série

$$\sum_{n=0}^{\infty} \frac{n!}{n!^2 + 1}$$

converge com respeito a todo valor absoluto em $\mathbb{Q}$. De fato, é claro que tal série converge em $\mathbb{Q}_p$ para todo primo p e converge também em $\mathbb{R}$, pois $\frac{n!}{n!^2+1} \leq \frac{1}{n!}$, isto é, a série $\sum_{n=0}^{\infty} \frac{n!}{n!^2+1}$ é majorada pela série $\sum_{n=0}^{\infty} \frac{1}{n!}$ que converge.

Observe no entanto que, apesar de termos assegurada a convergência em relação a todos os valores absolutos possíveis de $\mathbb{Q}$, não sabemos determinar seus limites. Também não sabemos determinar se algum dos limites é um número p-ádico algébrico sobre $\mathbb{Q}$ ou não. Os próximos capítulos continuam tratando da construção de séries convergentes em $\mathbb{Q}_p$, para todo $p \in V_{\mathbb{Q}}$.

No capítulo 2 vamos construir uma série que converge em $\mathbb{Q}_p$, para todo $p \in V_{\mathbb{Q}}$ e, mais até, tal que todos os seus limites são transcendentes sobre $\mathbb{Q}$.

1.4 Uma estimativa para $|n!|_p$

No capítulo seguinte vamos precisar de uma majoração para $|n!|_p$ onde p é primo e n é um número inteiro positivo arbitrário. Aqui calculamos também o valor preciso de $|n!|_p$.

Definição: Sejam p um primo e n um inteiro positivo cuja expansão p-ádica é dada por:

$$n = a_0 + a_1 p + a_2 p^2 + \ldots + a_l p^l$$

(isto é, os a_i são inteiros satisfazendo $0 \leq a_i \leq p - 1$. Definimos:

$$A_p(n) = a_0 + a_1 + ... + a_l$$

Lema 1.9: (Legendre, 1808) Se p é um número primo e n um inteiro positivo, então:

$$|n!|_p = p^{-(n-A_p(n))\ /(p-1)}$$

ou equivalentemente,

$$v_p(n!) = \frac{n - A_p(n)}{p-1}$$

Prova: Provaremos por indução sobre n.

Se $n = 1$, então é facil ver que vale a afirmação.

Suponhamos agora que o resultado vale para $n = N-1$, digamos, $N - 1 = a_0 + a_1p + a_2p^2 + ... + a_lp^l$;

então

$A_p(N-1) = \sum_{i=0}^{l} a_i$ e

$$N = \begin{cases} (a_0+1) + \sum_{i=1}^{l} a_ip^i & \text{se } a_0 < p-1 \\ p^{l+1} & \text{se } a_0 = a_1 = ... = a_l = p-1 \\ (a_T+1)p^T + \sum_{i=T+1}^{l} a_ip^i & \text{se } a_0 = a_1 = ... = a_{T-1} = p-1 \\ & \text{e } a_T < p-1,\ T < l. \end{cases}$$

donde,

$$A_p(N) = \begin{cases} A_p(N-1)+1 & \text{se } a_0 < p-1 \\ 1 & \text{se } a_0 = a_1 = ... = a_l = p-1 \\ A_p(N-1) - T.(p-1) + 1 & \text{se } a_t = p-1, 0 \leq t \leq T-1, \\ & \text{e } a_T \neq p-1,\ T < l. \end{cases}$$

1°Caso: $a_0 < p-1$. Neste caso, $v_p(N) = 0$ donde $|N|_p = 1$.

Daí, pela hipótese de indução, temos que:

$$|N!|_p = |N|_p\ |(N-1)!|_p = |(N-1)!|_p = p^{-[N-1-A_p(N-1)]\ /(p-1)}$$

$$= p^{-[N-(A_p(N-1)+1)]\ /(p-1)}$$

e, como $A_p(N) = A_p(N-1) + 1$, temos

$$|N!|_p = p^{-[N-A_p(N)]\,/(p-1)}$$

2^oCaso: $a_0 = a_1 = ... = a_l = p-1$. Neste caso $N = p^{l+1}$ donde $v_p(N) = l+1$ e $|N|_p = p^{-(l+1)}$.

Daí

$$|N!|_p = |N|_p|(N-1)!|_p = p^{-(l+1)}p^{-[N-1-A_p(N-1)]\,/(p-1)}$$

$$= p^{-[(l+1)(p-1)+N-1-A_p(N-1)]\,/(p-1)}$$

Mas aqui $A_p(N-1) = (l+1)(p-1)$, de modo que

$$|N!|_p = p^{-[N-1]\,/(p-1)} = p^{-[N-A_p(N)]/(p-1)}$$

3^oCaso: $a_t = p-1$ para $0 \le t \le T-1$ e $a_T \neq p-1$, para algum $T < l$.
Neste caso, $v_p(N) = T$ e portanto $|N|_p = p^{-T}$.
Daí, pela hipótese de indução , temos que:

$$|N!|_p = |N|_p\ |(N-1)!|_p = p^{-T}\ p^{-[N-1-A_p(N-1)]\,/(p-1)}$$

$$= p^{-[T(p-1)+N-1-A_p(N-1)]\,/\,(p-1)}$$

$$= p^{-(N-A_p(N))\,/(p-1)}$$

□

Corolário 1.10: Se p é um número primo, então para todo inteiro n suficientemente grande,

$$|n!|_p \le p^{-\,n\,/(2p-2)}$$

Prova: Escrevemos $n = a_0 + a_1p + a_2p^2 + ... + a_lp^l$,
onde os a_i são inteiros satisfazendo $0 \le a_i \le p-1$, $a_l \neq 0$. Desta forma $n \ge p^l$ então, $\log\ n \ge l\ \log\ p$ e daí,

$$l \le \frac{\log\ n}{\log\ p}$$

Isto nos dá:

$$A_p(n) = a_0 + a_1 + a_2 + ... + a_l$$

$$\leq (l+1)\ .\ (p-1) = l(p-1) + (p-1)$$

$$\leq \frac{p-1}{\log\ p}\ \log\ n + (p-1)$$

Afirmamos que, para n suficientemente grande, $\frac{p-1}{\log p}\log n + (p-1) \leq \frac{n}{2}$ já que:

$$\lim_{n\to\infty} \frac{\frac{n}{2}}{\frac{p-1}{\log p}\log n + (p-1)} = \lim_{n\to\infty} \frac{\frac{1}{2}}{\frac{p-1}{\log p}\frac{\log n}{n} + \frac{p-1}{n}} = \infty,$$

donde existe M_1 tal que $n > M_1$

$$\frac{\frac{n}{2}}{\frac{p-1}{\log p}\log n + (p-1)} \geq 1$$

Assim, $A_p(n) \leq \frac{n}{2}$ para n suficientemente grande.

Do Lema anterior,

$$|n!|_p = p^{-[n-A_p(n)]\ /(p-1)}$$

Segue que, para n suficientemente grande,

$$|n!|_p \leq p^{-(n-\frac{n}{2})\ /(p-1)} = p^{-\frac{n}{2}\ /(p-1)} = p^{-n\ /(2p-2)}$$

$\square$

CAPÍTULO 2

Números transcendentes e o Teorema de Liouville nas versões real e p-ádica

2.1 Números Reais Transcendentes e o Teorema de Liouville real

Liouville (1844) foi o primeiro matemático a provar a existência de números transcendentes e a exibir exemplos: ele apresentou uma condição suficiente para que um número real seja transcendente. Usando esse resultado é possivel apresentar explicitamente alguns números transcendentes.

Passamos a apresentar tal resultado e um exemplo de número real transcendente para depois apresentar suas versões p-ádicas. A referência para esta seção é [Sm].

Antes no entanto introduzimos um resultado para polinômios sobre um domínio de característica zero envolvendo derivada formal:

Definição: Seja A um anel. A **derivada formal** de um polinômio $f(X) = a_0 + a_1X + ... + a_nX^n \in A[X]$ é denotada por $f'(x)$ e dada por

$$f'(x) = a_1 + 2a_2X + 3a_3X^2 + ... + na_nX^{n-1}.$$

Proposição 2.1: Sejam A um domínio de característica zero, $n \in \mathbb{N}^*$ e $Q(X), Q_1(X), Q_2(X), ..., Q_s(X) \in A[X]$. Então:

$(i) \left[\sum_{i=1}^{s} Q_i(X)\right]' = \sum_{i=1}^{s} Q_i'(X)$

$(ii)\ [kQ(X)]' = kQ'(X)$

$(iii)\ [(X-a)^n]' = n(X-a)^{n-1}$

Prova: (i) e (ii) são verificadas facilmente.

(iii) Escrevemos $(X-a)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}X^k$; então

$$[(X-a)^n]' = \sum_{k=1}^{n} k \binom{n}{k} a^{n-k}X^{k-1}$$

$$= \sum_{r=0}^{n-1}(r+1)\binom{n}{r+1}a^{n-r-1}X^r$$

Por outro lado,

$$(X-a)^{n-1} = \sum_{r=0}^{n-1}\binom{n-1}{r}a^{n-1-r}X^r$$

Observe agora que para $r \in \{0, 1, ..., n-1\}$. temos:

$$n\binom{n-1}{r} = n\frac{(n-1)!}{r!(n-1-r)!}$$

$$= \frac{n!}{r!(n-1-r)!}$$

$$= (r+1)\frac{n!}{(r+1)!(n-r-1)!}$$

$$= (r+1)\binom{n}{r+1}$$

Logo, $[(X-a)^n]' = n(X-a)^{n-1}$. □

Proposição 2.2: Seja K um corpo de característica zero e seja $a \in K$. Então todo polinômio $P(X) \in K[X]$ de grau n pode ser escrito na forma

$$P(X) = P(a) + \frac{P'(a)}{1!}(X-a) + \frac{P''(a)}{2!}(X-a)^2 + ... + \frac{P^{(n)}(a)}{n!}(X-a)^n,$$

onde $P^{(n)}(X)$ denota a derivada formal de ordem n de $P(X)$.

Prova: Sabemos que para todo $a \in K$, $P(X)$ pode se escrever em potências de $(X-a)$. Suponhamos $P(X) = c_0 + c_1(X-a) + c_2(X-a)^2 + ... + c_n(X-a)^n$.

$P(a) = c_0$

Queremos mostrar que, para todo i, $c_i = \frac{P^{(i)}(a)}{i!}$

Utilizando (i), (ii), (iii) da Proposição anterior,

$P'(X) = \sum_{i=1}^{n} ic_i(X-a)^{i-1}$

$P'(a) = c_1$

e, novamente utilizando a Proposição anterior,

$P''(X) = \sum_{i=2}^{n} i(i-1)c_i(X-a)^{i-2}$

$P''(a) = 2c_2 \Rightarrow c_2 = \frac{P''(a)}{2}$

Para $1 \leq k \leq n$ obtemos, por indução,

$P^{(k)}(X) = \sum_{i=k}^{n} i(i-1). \ldots .c_i(X-a)^{i-k}$ donde

$P^{(k)}(a) = k(k-1)\ldots 1.c_k$ e portanto

$c_k = \frac{P^{(k)}(a)}{k!}$ para $0 \leq k \leq n$. $\square$

Teorema 2.3: (Liouville-versão real,1844) Seja α um número algébrico real cujo polinômio minimal tem grau $d \geq 1$. Então existe uma constante $C = C(\alpha) > 0$ tal que para todo racional $\frac{r}{s} \neq \alpha$

$$|\alpha - \frac{r}{s}| > \frac{C}{s^d}$$

Prova: Seja $P(X) \in \mathbb{Z}[X]$ um polinômio de grau d que se anula em α:

$$P(X) = a_d X^d + a_{d-1}X^{d-1} + \ldots + a_1 X + a_0$$

Note que se existisse alguma raiz racional para $P(X)$ diferente de α então o polinômio minimal de α não teria grau d. Assim, podemos afirmar que:

$$x \in \mathbb{Q}, x \neq \alpha \Longrightarrow P(x) \neq 0.$$

Seja $\frac{r}{s} \in \mathbb{Q}$, $\frac{r}{s} \neq \alpha$ (e, portanto, $s > 0$).

Inicialmente observe que:

$$\begin{aligned} |P(\tfrac{r}{s})| &= \left|a_d(\tfrac{r}{s})^d + a_{d-1}(\tfrac{r}{s})^{d-1} + \ldots + a_1(\tfrac{r}{s}) + a_0\right| \\ &= \left|a_d r^d + a_{d-1}r^{d-1}s + \ldots + a_1 r s^{d-1} + a_0 s^d\right| \left|\tfrac{1}{s^d}\right| \\ &\geq \tfrac{1}{s^d} \quad \text{pois } \alpha_i, r, s, \text{ são todos inteiros.} \end{aligned}$$

Expressando $P(X)$ em potências de $(X - \alpha)$ conforme teorema 2.1 obtemos

$$P(\tfrac{r}{s}) = P(\alpha) + \frac{P'(\alpha)}{1!}(\tfrac{r}{s} - \alpha) + \frac{P''(\alpha)}{2!}(\tfrac{r}{s} - \alpha)^2 + \ldots + \frac{P^{(d)}(\alpha)}{d!}(\tfrac{r}{s} - \alpha)^d,$$

donde, como $P(\alpha) = 0$,

$$\begin{aligned} |P(\tfrac{r}{s})| &= \left|P'(\alpha)(\tfrac{r}{s} - \alpha) + \frac{P''(\alpha)}{2!}(\tfrac{r}{s} - \alpha)^2 + \ldots + \frac{P^{(d)}(\alpha)}{d!}(\tfrac{r}{s} - \alpha)^d\right| \\ &\leq |\tfrac{r}{s} - \alpha|\left[\,|P'(\alpha)| + \left|\frac{P''(\alpha)}{2!}\right||\tfrac{r}{s} - \alpha| + \ldots + \left|\frac{P^{(d)}(\alpha)}{d!}\right||\tfrac{r}{s} - \alpha|^{d-1}\right] \end{aligned}$$

A partir daqui dividimos a prova em dois casos:

1^o caso: $|\frac{r}{s} - \alpha| \leq 1$

Temos então

$$|P(\tfrac{r}{s})| \leq |\tfrac{r}{s} - \alpha|\left[\,|P'(\alpha)| + \left|\frac{P''(\alpha)}{2!}\right| + \ldots + \left|\frac{P^{(d)}(\alpha)}{d!}\right|\,\right]$$

Afirmamos que $|P'(\alpha)| + \left|\frac{P''(\alpha)}{2!}\right| + ... + \left|\frac{P^{(d)}(\alpha)}{d!}\right|$ é não nulo. De fato, se isto ocorresse teríamos necessariamente cada parcela nula, em particular $P'(\alpha) = 0$. Mas $P'(X)$ é um polinômio de grau $d-1$ com coeficientes racionais, logo não poderá se anular para α.

Seja $D = D(\alpha)$ um número real positivo que satisfaz,

$$|P'(\alpha)| + \left|\frac{P''(\alpha)}{2!}\right| + ... + \left|\frac{P^d(\alpha)}{d!}\right| = \frac{1}{(2D)^d}$$

Então

$$|\tfrac{r}{s} - \alpha| \geq (2D)^d\, |P(\tfrac{r}{s})| \geq \frac{(2D)^d}{s^d} > \frac{C}{s^d}$$

onde tomamos $C = D^d$.

2^o caso: $|\frac{r}{s} - \alpha| > 1$

Neste caso temos

$$\begin{aligned}
|P(\tfrac{r}{s})| &\leq |\tfrac{r}{s} - \alpha|\Big[\,|P'(\alpha)| + \left|\frac{P''(\alpha)}{2!}\right||\tfrac{r}{s} - \alpha| + ... + \left|\frac{P^{(d)}(\alpha)}{d!}\right||\tfrac{r}{s} - \alpha|^{d-1}\Big] \\
&\leq |\tfrac{r}{s} - \alpha|^d\Big[\left|\frac{P'(\alpha)}{(\frac{r}{s}-\alpha)^{d-1}}\right| + \left|\frac{P''(\alpha)}{2!(\frac{r}{s}-\alpha)^{d-2}}\right| + ... + \left|\frac{P^{(d)}(\alpha)}{d!}\right|\Big] \\
&\leq |\tfrac{r}{s} - \alpha|^d\Big[\,|P'(\alpha)| + \left|\frac{P''(\alpha)}{2!}\right| + ... + \left|\frac{P^{(d)}(\alpha)}{d!}\right|\Big]
\end{aligned}$$

Escolhendo novamente $D = D(\alpha)$ um número real positivo que satisfaz

$$|P'(\alpha)| + \left|\frac{P''(\alpha)}{2!}\right| + ... + \left|\frac{P^d(\alpha)}{d!}\right| = \frac{1}{(2D)^d}$$

Então

$|P(\frac{r}{s})| \leq |\frac{r}{s} - \alpha|^d \frac{1}{(2D)^d}$ donde

$|\frac{r}{s} - \alpha|^d \geq (2D)^d |P(\frac{r}{s})| \geq \frac{(2D)^d}{s^d}$ donde

$|\alpha - \frac{r}{s}| \geq \frac{2D}{s} > \frac{C}{s} > \frac{C}{s^d}$ onde aqui tomamos $C = D$. □

Corolário 2.4: (Liouville) O número real $\alpha = \sum_{\lambda=1}^{\infty} 2^{-\lambda!}$ é transcendente sobre $\mathbb{Q}$.

Prova: Inicialmente observamos que, para cada $\lambda \in \mathbb{N}$, $\frac{1}{2^\lambda} > \frac{1}{2^{\lambda!}} > 0$. Assim a série $\sum_{\lambda=1}^{\infty} 2^{-\lambda!}$ é majorada pela série geométrica $\sum_{\lambda=1}^{\infty} 2^{-\lambda}$ que converge, e portanto é também convergente.

Escrevemos, para $k \geq 1$, $y(k) = 2^{k!}$ e $x(k) = 2^{k!} \sum_{\lambda=1}^{k} 2^{-\lambda!}$.

Então $x(k), y(k) \in \mathbb{Z}^*$ e

$$\alpha - \frac{x(k)}{y(k)} = \sum_{\lambda=k+1}^{\infty} 2^{-\lambda!}$$

e, como a série $\sum_{\lambda=k+1}^{\infty} 2^{-\lambda!}$ é também convergente, podemos escrever:

$$\alpha - \frac{x(k)}{y(k)} = \frac{1}{2^{(k+1)!}}\left(1 + \frac{1}{2^{(k+2)!-(k+1)!}} + \frac{1}{2^{(k+3)!-(k+1)!}} + \ldots\right)$$

$$= \frac{1}{2^{(k+1)!}} \sum_{j=k+1}^{\infty} \frac{1}{2^{j!-(k+1)!}}$$

$$= \frac{1}{2^{(k+1)!}} \sum_{s=0}^{\infty} \frac{1}{2^{(k+1+s)!-(k+1)!}}$$

É facil provar por indução que, para cada $s \in \mathbb{N}$, $(k+1+s)! - (k+1)! > s$.

Daí, para cada $s \in \mathbb{N}$, temos $0 < \frac{1}{2^{(k+1+s)!-(k+1)!}} < \frac{1}{2^s}$ e portanto a série de termos positivos $\sum_{i=1}^{\infty} \frac{1}{2^{(k+i)!-(k+1)!}}$ converge porque é majorada pela série geométrica $\sum_{i=0}^{\infty} \frac{1}{2^i}$ que converge para 2.

Portanto, podemos afirmar que

$$\alpha - \frac{x(k)}{y(k)} < \frac{2}{2^{(k+1)!}} = \frac{2}{y(k+1)}$$

Mas, como

$$\frac{2}{2^{(k+1)!}} = \frac{2}{2^{(k+1)k!}} = \frac{2}{2^{k.k!+k!}} = \frac{2}{(2^{k!})^k.2^{k!}} < \frac{1}{(2^{k!})^k} = \frac{1}{(y(k))^k},$$

temos,

$$\alpha - \frac{x(k)}{y(k)} < \frac{1}{y(k)^k}$$

Afirmamos agora que, para todo $C > 0$ e $d \geq 1$ existe k suficientemente grande tal que $\frac{1}{y(k)^k} \leq \frac{C}{y(k)^d}$.

De fato, como a sequência $(y(k))$ é crescente e ilimitada, temos:

Se $C \geq 1$ então, para $k \geq d$ temos $\frac{1}{y(k)^k} \leq \frac{1}{y(k)^d} \leq \frac{C}{y(k)^d}$.

Se $C < 1$ então existe k suficientemente grande tal que $y(2k) > \frac{1}{C}$. Daí, se tomamos ainda $k \geq d$,

$$\frac{1}{y(2k)^{2k}} = \frac{1}{y(2k)^k}\frac{1}{y(2k)^k} < \frac{1}{y(2k)}\frac{1}{y(2k)^k} < \frac{C}{y(2k)^k} < \frac{C}{y(2k)^d}$$

Assim, mostramos que para todo $C > 0$ e $d \geq 1$ existe k suficientemente grande tal que

$$\alpha - \frac{x(k)}{y(k)} < \frac{C}{y(k)^k} < \frac{C}{y(2k)^d},$$

o que, pelo Teorema de Liouville implica que α não é algébrico de grau d; como d é arbitrário, concluimos que α é um número transcendente. □

2.2 Prolongamentos de um valor absoluto de $\mathbb{Q}$ a uma extensão finita de $\mathbb{Q}$

Esta seção é preparatória para a demonstração da versão p-ádica do Teorema de Liouville, e uma referência para ela é [L].

Nesta seção e na próxima será útil mudarmos um pouco a notação de valor absoluto, pois trabalharemos com vários. Assim, se $E|K$ denota uma extensão de corpos, denotaremos por $|\ \ |_v$ um valor absoluto de K, e se $|\ \ |_w$é um valor absoluto de E que prolonga $|\ \ |_v$, então escreveremos $w|v$. Denotaremos também por K_v e E_w os completamentos de K e E em relação aos valores absolutos $|\ \ |_v$ e $|\ \ |_w$, respectivamente.

Proposição 2.5: Se $(K,|\ \ |_v)$ é completo e $|\ \ |_v$ é um valor absoluto não trivial, então $|\ \ |_v$ tem um único prolongamento a qualquer extensão algébrica de K. Além disso, se $E|K$ for uma extensão finita, então $(E,|\ \ |_w)$ é também completo, onde $|\ \ |_w$ denota o prolongamento de $|\ \ |_v$ a E.

Prova: Veja [L], pag 291, Proposição 4. □

Suponhamos agora que K é um corpo munido de um valor absoluto $|\ \ |_v$, e que E é uma extensão finita de K. Queremos descrever como $|\ \ |_v$ se prolonga a E.

Denotando por $\widetilde{K}_v$ o fecho algébrico do completamento K_v temos, pelo exposto acima, que existe um único prolongamento $|\ \ |_w$ de $|\ \ |_v$ a $\widetilde{K}_v$. Sendo $\widetilde{K}_v$ algebricamente fechado e $E|K$ uma extensão algébrica, sabemos que existe um K-monomorfismo $\sigma : E \to \widetilde{K}_v$. Daí, a restrição de $|\ \ |_w$ a $\sigma(E)$ é um valor absoluto de

$\sigma(E)$ que prolonga $| \ |_v$. É fácil agora verificar que, definindo para cada $\alpha \in E$,

$$|\alpha| = |\sigma(\alpha)|_w,$$

temos um valor absoluto em E que prolonga $| \ |_v$ pois, para cada $x \in K$, $\sigma(x) = x$, e portanto $|x| = |x|_w = |x|_v$.

Portanto, a liberdade que temos para prolongar $| \ |_v$ a E vem do número de monomorfismos distintos $\sigma : E \to \widetilde{K}_v$ que podemos construir. E tal número sabemos ser finito, no máximo igual ao grau da extensão $[E : K]$.

Finalmente salientamos que dois prolongamentos distintos de $| \ |_v$ a E são não equivalentes. De fato, se $| \ |_{w_1}$ e $| \ |_{w_2}$ são dois prolongamentos equivalentes então existe $\rho > 0$ tal que $| \ |_{w_1} = | \ |_{w_2}^{\rho}$. Daí, para cada $x \in K$,

$$|x|_v = |x|_{w_1} = |x|_{w_2}^{\rho} = |x|_v^{\rho},$$

donde concluimos que $\rho = 1$.

Afirmamos agora que se $| \ |_v$ for o valor absoluto usual de $\mathbb{Q}$ então todos os prolongamentos de $| \ |_v$ a uma extensão finita E de $\mathbb{Q}$ são também arquimedianos e portanto são todos equivalentes, pela proposição 1.4. Pela afirmação acima, temos então:

Proposição 2.6: A menos de equivalência, existe um único prolongamento do valor absoluto usual de $\mathbb{Q}$ a qualquer extensão finita E de $\mathbb{Q}$.

Proposição 2.7: Se $| \ |_w$ é o prolongamento de um valor absoluto $| \ |_v$ de $\mathbb{Q}$ a uma extensão finita E de $\mathbb{Q}$ então E_w pode ser identificado com o compositum $E\mathbb{Q}_v$. Em particular, $[E_w : \mathbb{Q}_v] \leq [E : \mathbb{Q}]$

Prova: Veja [L], pag 292, Proposição 6. □

Proposição 2.8: Sejam E uma extensão finita de $\mathbb{Q}$ e $| \ |_v$ um valor absoluto de $\mathbb{Q}$. Então

$$\sum_{w|v}[E_w : \mathbb{Q}_v] = [E : \mathbb{Q}],$$

onde por $\sum_{w|v}$ denotamos a soma sobre todos os valores absolutos w de E que prolongam v.

Prova: Veja [L], pag 293, Proposição 8. □

Queremos agora provar que, para uma extensão finita E de $\mathbb{Q}$, vale também uma fórmula do Produto, como a da Proposição 1.6. Para tal, no entanto, vamos precisar substituir cada prolongamento dos valores absolutos que existem em $\mathbb{Q}$ por valores absolutos equivalentes, escolhendo para cada um deles uma potência adequada.

Notação: Se $|\ \ |_w$ denota um valor absoluto de E que prolonga o valor absoluto $|\ \ |_v$ de $\mathbb{Q}$, denotaremos por $\|\ \ \|_w$ o valor absoluto de E equivalente a $|\ \ |_w$ dado por

$$\|\alpha\|_w = |\alpha|_w^{[E_w:\mathbb{Q}_v]/[E:\mathbb{Q}]},$$

para todo $\alpha \in E$.

Proposição 2.9: Seja E uma extensão finita de $\mathbb{Q}$, e seja $|\ \ |_v$ um valor absoluto de $\mathbb{Q}$. Então, para cada $x \in \mathbb{Q}$,

$$\prod_{w|v} \|x\|_w = |x|_v,$$

onde por $\prod_{w|v}$ denotamos o produto sobre todos os valores absolutos $|\ \ |_w$ de E que prolongam $|\ \ |_v$.

Prova: De fato, para cada $x \in \mathbb{Q}$,

$$\begin{aligned}\prod_{w|v} \|x\|_w &= \prod_{w|v} |x|_w^{[E_w:\mathbb{Q}_v]/[E:\mathbb{Q}]} \\ &= \prod_{w|v} |x|_v^{[E_w:\mathbb{Q}_v]/[E:\mathbb{Q}]} \\ &= |x|_v^{\sum_{w|v}[E_w:\mathbb{Q}_v]/[E:\mathbb{Q}]} \\ &= |x|_v^{[E:\mathbb{Q}]/[E:\mathbb{Q}]} \\ &= |x|_v\end{aligned}$$

□

Corolário 2.10: Seja E uma extensão finita de $\mathbb{Q}$. Então para cada $x \in \mathbb{Q},\ x \neq 0$

$$\prod_w |x|_w = 1,$$

onde por $\prod_w$ denotamos o produto sobre todos os valores absolutos $|\ \ |_w$ de E.

Prova: De fato, pela proposição acima,

$$\prod_w |x|_w = \prod_{p \in V_{\mathbb{Q}}} \prod_{w/v_p} |x|_w = \prod_{p \in V_{\mathbb{Q}}} |x|_{v_p} = 1,$$

onde na última igualdade utilizamos a fórmula do produto em $\mathbb{Q}$, uma vez que x é não nulo. $\square$

Proposição 2.11: Sejam E uma extensão finita de $\mathbb{Q}$, $|\ \ |_v$ um valor absoluto de $\mathbb{Q}$ e $|\ \ |_w$ um prolongamento de $|\ \ |_v$ a E. Então, para cada $\alpha \in E$,

$$\prod_{w|v} |\alpha|_w^{[E_w:\mathbb{Q}_v]} = \left|N_{\mathbb{Q}}^E(\alpha)\right|_v,$$

onde $\left|N_{\mathbb{Q}}^E(\alpha)\right|_v$ denota a norma do elemento α.

Prova: veja [*L*], p. 296, Proposição 11. Lembramos que $N_{\mathbb{Q}}^E(\alpha) \in \mathbb{Q}$, e portanto $\left|N_{\mathbb{Q}}^E(\alpha)\right|_v$ faz sentido. $\square$

Corolário 2.12: (A fórmula do produto em E) Seja E uma extensão finita de $\mathbb{Q}$. Então, para cada $\alpha \in E$, $\alpha \neq 0$,

$$\prod_w \|\alpha\|_w = 1,$$

onde por $\prod_w$ denotamos o produto sobre todos os valores absolutos de E. Ou, equivalentemente,

$$\sum_w \log\|\alpha\|_w = 0$$

Prova: De fato, pela proposição anterior temos:

$$\prod_w \|\alpha\|_w = \prod_{p\in V_{\mathbb{Q}}} \prod_{w|v_p} \|\alpha\|_w$$

$$= \prod_{p\in V_{\mathbb{Q}}} \prod_{w|v_p} |\alpha|_w^{[E_w:\mathbb{Q}_p]/[E:\mathbb{Q}]}$$

$$= \prod_{p\in V_{\mathbb{Q}}} \left|N_{\mathbb{Q}}^E(\alpha)\right|_{v_p}^{1/[E:\mathbb{Q}]}$$

$$= 1,$$

uma vez que $N_{\mathbb{Q}}^{E}(\alpha) \neq 0$. □

2.3 Números p-ádicos transcendentes

O que desenvolvemos nesta seção pode ser encontrado em [B], após algumas adaptações. Faremos uso das definições e notações introduzidas na seção anterior.

Para apresentarmos a versão p-ádica do Teorema de Liouville, introduzimos ainda duas definições que nos serão úteis:

Definição: *Dado* $\alpha \in \mathbb{R}_+$, definimos

$$log^+\alpha = \max\{\log\ \alpha, 0\} = \begin{cases} \log\ \alpha\ , \text{ se } \alpha > 1 \\ 0\ , \text{ se } 0 < \alpha \leq 1 \end{cases}$$

Proposição 2.13: Para todo $\alpha, \beta \in \mathbb{R}_+$,

(i) $\log^+\alpha \geq 0$ e $\log^+\alpha \geq \log\alpha$

(ii) $\log^+\alpha\beta \leq \log^+\alpha + \log^+\beta$

(iii) Se K é um corpo e $|\ \ |$ é um ultra valor absoluto de K então, para cada $n \geq 2$ e $x_1, x_2, ..., x_n \in K$,

$$\log^+|x_1 + ... + x_n| \leq \max_{1 \leq i \leq n} \{\log^+|x_i|\}\ ,$$

(iv) Se K é um corpo e $|\ \ |$ é um valor absoluto qualquer então, para cada $n \geq 2$ e $x_1, x_2, ..., x_n \in K$,

$$\log^+|x_1 + ... + x_n| \leq \log n + \max_{1 \leq i \leq n} \{\log^+|x_i|\}\ ,$$

(v) Se E é uma extensão finita de $\mathbb{Q}$ e $|\ \ |_w$ denota um prolongamento de v_p a E para algum primo p, então, dados $\alpha_1, \alpha_2, ..., \alpha_n \in E$,

$$\log^+ \|\alpha_1 + \alpha_2 + ... + \alpha_n\|_w \leq \max_{1 \leq i \leq n}\{\log^+\|\alpha_i\|_w\}$$

Prova :

(i) É conseqüência imediata da definição.

(ii) Se $\alpha\beta > 1$ então

$$\log^+\alpha\beta = \log\alpha\beta = \log\alpha + \log\beta \leq \log^+\alpha + \log^+\beta,$$

sendo a última desigualdade válida por (i).

Se $\alpha\beta \leq 1$ então

$$\log^+\alpha\beta = 0 = 0 + 0 \leq \log^+\alpha + \log^+\beta$$

(iii) Utilizando indução sobre n, nos restringimos à prova para $n = 2$. E aqui também consideramos casos:

1^0 caso: $|x_1 + x_2| > 1$.

Como $|x_1 + x_2| \leq \max\{|x_1|, |x_2|\}$ temos $|x_1| > 1$ ou $|x_2| > 1$

Vamos supor sem perda de generalidade $|x_1| > 1$; então, como log é uma função crescente,

$$\begin{aligned}\log^+|x_1 + x_2| = \log|x_1 + x_2| &\leq \log[\max\{|x_1|, |x_2|\}] = \\ &= \max\{\log|x_1|, \log|x_2|\} \\ &\leq \max\{\log^+|x_1|, \log^+|x_2|\}\end{aligned}$$

2^0 caso: $|x_1 + x_2| \leq 1$.

Então $\log^+|x_1 + x_2| = 0 \leq \max\{\log^+|x_1|, \log^+|x_2|\}$ uma vez que $\log^+x \geq 0$ para todo $x \in \mathbb{R}_+$.

(iv) Lembramos inicialmente que, pela desigualdade triangular, temos

$$|x_1 + ... + x_n| \leq |x_1| + ... + |x_n| \leq n \max\{|x_1|, ..., |x_n|\}$$

E, daí

$$\log|x_1 + ... + x_n| \leq \log(n \max\{|x_1|, ..., |x_n|\}) = \log n + \max_{1\leq i\leq n} \{\log |x_i|\},$$

1^0 caso: $|x_1 + ... + x_n| > 1$ então

$$\begin{aligned}\log^+|x_1 + ... + x_n| &= \log |x_1 + ... + x_n| \\ &\leq \log n + \max\{\log |x_1|, ..., \log |x_n|\} \\ &\leq \log n + \max\{\log^+|x_1|, ..., \log^+|x_n|\},\end{aligned}$$

sendo esta última desigualdade válida por (i).

2^0 caso: $|x_1 + ... + x_n|_p \leq 1$.

$$\log^+|x_1 + ... + x_n| = 0 \leq \log n + \max\{\log^+|x_1|, ..., \log^+|x_n|\}$$

(v) Basta notar que se $|\ \ |_w$ prolonga $|\ \ |_{v_p}$ então $|\ \ |_w$ é também um ultra valor absoluto, e o mesmo ocorre com $\|\ \ \|_w$; daí, por (iii) acima,

$$\log^+ \|\alpha_1 + \alpha_2 + ... + \alpha_n\|_w \leq \max_{1\leq i\leq n}\{\log^+\|\alpha_i\|_w\}.$$

□

Definição: Dada uma extensão finita E de $\mathbb{Q}$ definimos $h : E^* \to \mathbb{R}$ por:

$$\log h(\alpha) = \sum_w \log^+\|\alpha\|_w$$

para cada $\alpha \in E$, $\alpha \neq 0$, onde por $\sum_w$ denotamos a soma sobre todos os valores absolutos de E que são prolongamentos dos valores absolutos de $\mathbb{Q}$. O número $h(\alpha)$ é denominado a **altura** de α.

Prova-se que o valor $h(\alpha)$ independe do corpo E que o contém. Maiores detalhes podem ser encontrados em [B].

Proposição 2.14: Seja E uma extensão finita de $\mathbb{Q}$, e sejam $\alpha, \beta, \alpha_1, .., \alpha_n \in E$, sempre que necessário não nulos. Então:

(i) $h(\alpha) > 0$

(ii) $h(\alpha) = h(\alpha^{-1})$

(iii) $h(\alpha\beta) \leq h(\alpha)h(\beta)$

(iv) $h(\alpha_1 + \alpha_2 + ... + \alpha_n) \leq n\ h(\alpha_1)h(\alpha_2)...h(\alpha_n)$

(v) Se $\alpha \in \mathbb{Q}^*$ então

$$h(\alpha) = \max\{|r|, |s|\},$$

onde $r,\ s \in \mathbb{Z}^*$ são tais que $\alpha = \frac{r}{s}$ e $mdc(r,s) = 1$.

Prova:

(i) Segue direto da definição pois $h(\alpha) = \exp\left(\sum_w \log^+\|\alpha\|_w\right)$, e como $\log^+\|\alpha\|_w \geq 0$ temos até $h(\alpha) \geq 1$ para todo $\alpha \in E$ não nulo.

(ii) Inicialmente observe que

$$\begin{aligned} \log^+\|\alpha\|_w = 0 \Leftrightarrow\ & \|\alpha\|_w \leq 1 \Leftrightarrow \\ \Leftrightarrow\ & \|\alpha^{-1}\|_w \geq 1 \Leftrightarrow \\ \Leftrightarrow\ & \log^+\|\alpha^{-1}\|_w = \log\ \|\alpha^{-1}\|_w = -\log\ \|\alpha\|_w \end{aligned}$$

e também

$$\begin{aligned} \log^+\|\alpha\|_w = \log\ \|\alpha\|_w \Leftrightarrow\ & \|\alpha\|_w \geq 1 \Leftrightarrow \\ \Leftrightarrow\ & \|\alpha^{-1}\|_w \leq 1 \Leftrightarrow \\ \Leftrightarrow\ & \log^+\|\alpha^{-1}\|_w = 0 \end{aligned}$$

Daí,

$$\log\ h(\alpha) = \sum_w \log^+\|\alpha\|_w = \sum_{w \text{ tal que } \|\alpha\|_w \geq 1} \log\ \|\alpha\|_w$$

e

$$\begin{aligned} \log\ h(\alpha^{-1}) &= \sum_w \log^+\|\alpha^{-1}\|_w \\ &= \sum_{w \text{ tal que } \|\alpha\|_w \leq 1} -\log\ \|\alpha\|_w \\ &= -\sum_{w \text{ tal que } \|\alpha\|_w \leq 1} \log\ \|\alpha\|_w \end{aligned}$$

Mas, da fórmula do produto (Proposição 2.10), temos:

$$0 = \sum_w \log\ \|\alpha\|_w$$

$$= \sum_{w \text{ tal que } \|\alpha\|_w \geq 1} \log \|\alpha\|_w + \sum_{w \text{ tal que } \|\alpha\|_w \leq 1} \log \|\alpha\|_w$$
$$= \log h(\alpha) - \log h(\alpha^{-1}),$$

donde obtemos $\log h(\alpha) = \log h(\alpha^{-1})$, ou ainda, $h(\alpha) = h(\alpha^{-1})$.

(*iii*) Da Proposição 2.13 (ii) temos:

$$\begin{aligned}
\log h(\alpha\beta) &= \sum_w \log^+\|\alpha\beta\|_w \\
&\leq \sum_w (\log^+\|\alpha\|_w + \log^+\|\beta\|_w) \\
&= \sum_w \log^+\|\alpha\|_w + \sum_w \log^+\|\beta\|_w \\
&= \log h(\alpha) + \log h(\beta) \\
&= \log h(\alpha)h(\beta),
\end{aligned}$$

e portanto $h(\alpha\beta) \leq h(\alpha)h(\beta)$.

(*iv*) $\log h(\alpha_1 + \alpha_2 + \ldots + \alpha_n) = \sum_w \log^+\|\alpha_1 + \alpha_2 + \ldots + \alpha_n\|_w$

$$= \sum_{p \text{ primo}} \left(\sum_{w|v_p} \log^+\|\alpha_1 + \alpha_2 + \ldots + \alpha_n\|_w\right) + \log^+\|\alpha_1 + \alpha_2 + \ldots + \alpha_n\|_v,$$

onde por $| \ |_v$ estamos denotando o (único) valor absoluto de E que prolonga o valor absoluto usual de $\mathbb{Q}$. Daí, pela Proposição 2.11,temos:

$\log h(\alpha_1 + \alpha_2 + \ldots + \alpha_n) \leq$

$$\begin{aligned}
&\leq \sum_{p \text{ primo}} \left(\sum_{w|v_p} \max_{1\leq i\leq n}\{\log^+\|\alpha_i\|_w\}\right) + \log n + \max_{1\leq i\leq n}\{\log^+\|\alpha_i\|_v\} \\
&\leq \sum_{p \text{ primo}} \left(\sum_{w|v_p} \max_{1\leq i\leq n}\{\log^+\|\alpha_i\|_w\}\right) + \log n + \max_{1\leq i\leq n}\{\log^+\|\alpha_i\|_v\} \\
&\leq \sum_{p \text{ primo}} \sum_{w|v_p} \sum_{i=1}^n \log^+\|\alpha_i\|_w + \log n + \sum_{i=1}^n \log^+\|\alpha_i\|_v \\
&= \sum_{p\in V_{\mathbb{Q}}} \sum_{w|v_p} \sum_{i=1}^n \log^+\|\alpha_i\|_w + \log n \\
&= \sum_{i=1}^n \log h(\alpha_i) + \log n \\
&= \log(n.h(\alpha_1)...h(\alpha_n)),
\end{aligned}$$

donde concluimos que

$$h(\alpha_1 + \alpha_2 + \ldots + \alpha_n) \leq n.h(\alpha_1)...h(\alpha_n)$$

(*v*) Inicialmente escrevemos

$$\begin{aligned}
\log h(\tfrac{r}{s}) &= \sum_w \log^+\|\tfrac{r}{s}\|_w \\
&= \log^+\|\tfrac{r}{s}\|_v + \sum_{p \text{ primo}} \sum_{w|v_p} \log^+\|\tfrac{r}{s}\|_w, \qquad (1)
\end{aligned}$$

onde por $| \ |_v$ estamos denotando o (único) valor absoluto de E que prolonga o valor absoluto usual de $\mathbb{Q}$.

Afirmamos agora que

$$\log^+\|\tfrac{r}{s}\|_v = \log^+|\tfrac{r}{s}|_\infty \qquad (2)$$

e

$$\sum_{w\nmid\infty} \log^+ \|\tfrac{r}{s}\|_w = \log |s|_\infty \qquad (3)$$

De fato:

$$\log^+\|\tfrac{r}{s}\|_v = \log^+|\tfrac{r}{s}|_v^{[E_v:\mathbb{R}]/[\mathbb{E}:\mathbb{Q}]} = \log^+|\tfrac{r}{s}|_\infty^{[E_v:\mathbb{R}]/[\mathbb{E}:\mathbb{Q}]},$$

uma vez que w prolonga o valor absoluto usual e $\frac{r}{s} \in \mathbb{Q}$.

Mas sendo $|\ \ |_v$ o único valor absoluto de E que prolonga o valor absoluto usual de $\mathbb{Q}$ temos, pela Proposição 2.8, que $[E_v : \mathbb{R}] = [\mathbb{E} : \mathbb{R}]$, e portanto

$$\log^+\|\tfrac{r}{s}\|_v = \log^+|\tfrac{r}{s}|_\infty,$$

o que completa a prova de (2).

Para provar (3), observe que, se p é um primo tal que $p|s$, então $p \not| \ r$, e daí:

$$\begin{aligned} 0 = v_p(r) < v_p(s) &\Rightarrow \\ v_p(\tfrac{r}{s}) &\leq -1 \\ |\tfrac{r}{s}|_p &\geq p > 1 \end{aligned}$$

Portanto, se w prolonga o valor absoluto p-ádico, então

$$\begin{aligned} \log^+\|\tfrac{r}{s}\|_w &= \log^+|\tfrac{r}{s}|_w^{[E_w:\mathbb{Q}_p]/[E:\mathbb{Q}]} \\ &= \log^+|\tfrac{r}{s}|_{v_p}^{[E_w:\mathbb{Q}_p]/[E:\mathbb{Q}]} \\ &= \log\ |\tfrac{r}{s}|_{v_p}^{[E_w:\mathbb{Q}_p]/[E:\mathbb{Q}]} \\ &= \log\ \|\tfrac{r}{s}\|_w \end{aligned}$$

E, se p é um primo tal que $p \not| \ s$ então

$$\begin{aligned} 0 = v_p(s) \leq v_p(r) &\Rightarrow \\ v_p(\tfrac{r}{s}) \geq 1 &\Rightarrow \\ |\tfrac{r}{s}|_p \leq 1 &\Rightarrow \\ |\tfrac{r}{s}|_p^{[E_w:\mathbb{Q}_p]/[E:\mathbb{Q}]} \leq 1 &\Rightarrow \\ \log^+\|\tfrac{r}{s}\|_w &= 0, \end{aligned}$$

de modo que

$$\begin{aligned} \sum_{p \text{ primo}} \sum_{w|v_p} \log^+\|\tfrac{r}{s}\|_w &= \sum_{p \text{ primo},\, p|s} \sum_{w|v_p} \log^+\|\tfrac{r}{s}\|_w \\ &= \sum_{p \text{ primo},\, p|s} \sum_{w|v_p} \log\ \|\tfrac{r}{s}\|_w \\ &= \sum_{p \text{ primo},\, p|s} \log \prod_{w|v_p} \|\tfrac{r}{s}\|_w \\ &= \sum_{p \text{ primo},\, p|s} \log\ |\tfrac{r}{s}|_p, \end{aligned}$$

onde na última igualdade utilizamos a Proposição 2.9.

Daí, se $s = p_1^{t_1} \ldots p_n^{t_n}$ é a fatoração de s em fatores primos então

$$|\tfrac{r}{s}|_{p_i} = p_i^{t_i},$$

para cada $i \in \{1, \ldots, n\}$, donde

$$\sum_{p \text{ primo}} \sum_{w|v_p} \log^+\|\tfrac{r}{s}\|_w = \sum_{i=1}^{n} \log\ |\tfrac{r}{s}|_{p_i}$$

$$= \log\ |s|_\infty,$$

o que completa a prova de (3).

Utilizando agora (1), (2) e (3) obtemos:

$$\log\ h(\tfrac{r}{s}) =$$

$$= \log^+\|\tfrac{r}{s}\|_v + \textstyle\sum_{p \text{ primo}} \sum_{w|v_p} \log^+\|\tfrac{r}{s}\|_w$$

$$= \log^+|\tfrac{r}{s}|_\infty + \log\ |s|_\infty$$

Note agora que, se $|r|_\infty \leq |s|_\infty$ então $|\frac{r}{s}|_\infty \leq 1$, donde

$$\log^+|\tfrac{r}{s}|_\infty + \log\ |s|_\infty = \log\ |s|_\infty$$

$$= \log\ \max\{|r|_\infty, |s|_\infty\}$$

E, se $|r|_\infty > |s|_\infty$ então $|\frac{r}{s}|_\infty > 1$, donde

$$\log^+|\tfrac{r}{s}|_\infty + \log\ |s|_\infty = \log\ |\tfrac{r}{s}|_\infty + \log\ |s|_\infty$$

$$= \log\ |r|_\infty$$

$$= \log\ \max\{|r|_\infty, |s|_\infty\}$$

Em qualquer caso portanto, temos

$$\log\ h(\tfrac{r}{s}) = \log\ \max\{|r|_\infty, |s|_\infty\},$$

ou seja,

$$h(\tfrac{r}{s}) = \max\{|r|_\infty, |s|_\infty\}$$

□

Teorema 2.15: (Versão p-ádica do Teorema de Liouville) Dado $p \in V_{\mathbb{Q}}$, seja $\alpha \in \mathbb{Q}_p$ um número algébrico cujo polinômio minimal tem grau $d \geq 1$. Então existe uma constante $C = C(\alpha) > 0$ tal que, para todo número racional não nulo $\frac{r}{s}$, $\alpha \neq \frac{r}{s}$,

$$|\alpha - \tfrac{r}{s}|_p \geq \frac{C}{h(\frac{r}{s})^d}$$

Prova: Consideremos a extensão finita $E = \mathbb{Q}(\alpha)$ e suponhamos, sem perda de generalidade $\mathrm{mdc}(r,s) = 1$. Daí:

$$\log|\alpha - \tfrac{r}{s}|_p = \log\|\alpha - \tfrac{r}{s}\|_w^{[E:\mathbb{Q}]/[E_w:\mathbb{Q}_p]}$$

$$= \frac{[E:\mathbb{Q}]}{[E_w:\mathbb{Q}_p]} \log\|\alpha - \tfrac{r}{s}\|_w$$

Mas, pelo Corolário 2.12,

$$\log\|\alpha - \tfrac{r}{s}\|_w = -\textstyle\sum_{v\neq w} \log\|\alpha - \tfrac{r}{s}\|_v$$

$$\geq -\textstyle\sum_{v\neq w} \log^+\|\alpha - \tfrac{r}{s}\|_v$$

$$\begin{aligned}
\log\|\alpha - \tfrac{r}{s}\|_w &= -\textstyle\sum_{v\neq w} \log\|\alpha - \tfrac{r}{s}\|_v \\
&\geq -\textstyle\sum_{v\neq w} \log^+\|\alpha - \tfrac{r}{s}\|_v \\
&\geq -\textstyle\sum_{v} \log^+\|\alpha - \tfrac{r}{s}\|_v \\
&= -\log\ h(\alpha - \tfrac{r}{s}) \\
&\geq -\log\ [2h(\alpha)h(\tfrac{r}{s})],
\end{aligned}$$

sendo esta última desigualdade válida pela Proposição anterior. Daí,

$$\begin{aligned}
\log|\alpha - \tfrac{r}{s}|_p &= \frac{[E:\mathbb{Q}]}{[E_w:\mathbb{Q}_p]} \log\|\alpha - \tfrac{r}{s}\|_w \\
&\geq -\frac{[E:\mathbb{Q}]}{[E_w:\mathbb{Q}_p]} \log\ [2h(\alpha)h(\tfrac{r}{s})] \\
&= \log\left[[2h(\alpha)h(\tfrac{r}{s})]^{-\frac{[E:\mathbb{Q}]}{[E_w:\mathbb{Q}_p]}} \right],
\end{aligned}$$

donde obtemos, já que $d = [E : \mathbb{Q}] \geq [E_w : \mathbb{Q}_p]$,

$$\begin{aligned}
|\alpha - \tfrac{r}{s}|_p &\geq [2h(\alpha)h(\tfrac{r}{s})]^{-\frac{d}{[E_w:\mathbb{Q}_p]}} \\
&\geq [2h(\alpha)h(\tfrac{r}{s})]^{-d} \\
&= \frac{[2h(\alpha)]^{-d}}{[h(\frac{r}{s})]^d} \\
&= \frac{C}{[h(\frac{r}{s})]^d},
\end{aligned}$$

onde $C = [2h(\alpha)]^{-d}$ é uma constante positiva (pois $h(\alpha) > 0$) que depende de α. □

2.4 Séries que convergem para um número p -ádico transcendente, com $p \in V_{\mathbb{Q}}$

Queremos agora, fixado um primo p, dar exemplos de números p-ádicos transcendentes. E faremos isto utilizando o Teorema de Liouville p -ádico. Faremos mais até: vamos construir uma série formal de potências, $F(X) = \sum_{n=0}^{\infty} \beta_n X^n \in \mathbb{Q}[[X]]$ tal que para todo racional $\gamma \neq 0$, $F(\gamma)$ converge para um transcendente de $\mathbb{Q}_p$, gerando assim uma infinidade de elementos de $\mathbb{Q}_p$ transcendentes sobre $\mathbb{Q}$.

Para $\gamma \in \mathbb{Q}$, continuaremos a denotar por $h(\gamma)$ a altura de γ e introduzimos uma nova definição.

Definição: Dados $\alpha_1, ...\alpha_N$ números racionais, definimos

$$h_1(\alpha_1, \alpha_2, ..., \alpha_N) = \max_{1 \leq i \leq N} \{h(\alpha_i)\},$$

Teorema 2.16: Seja $p \in V_{\mathbb{Q}}$ fixado e suponhamos que existe uma sequência de racionais $\{\beta_0, \beta_{1,...}\}$ satisfazendo:

$$0 < |\beta_N|_p \leq N^{-N} h_1(\beta_0, \beta_1, ...\beta_{N-1})^{-(N-1)^2} \qquad (*)$$

para cada $N \in \mathbb{N}^*$.

Então, para todo $\gamma \in \mathbb{Q}$, $\gamma \neq 0$, a série $F(\gamma) = \sum_{n=0}^{\infty} \beta_n \gamma^n$ converge em $\mathbb{Q}_p$ e, mais até, é um número transcendente.

Prova: Inicialmente observe que, para cada $\gamma \in \mathbb{Q}$, $\gamma \neq 0$, a série $\sum_{n=0}^{\infty} \beta_n \gamma^n$ realmente converge em $\mathbb{Q}_p$, pois, se $h(\gamma) = M$ então para cada n,

$$|\beta_n \gamma^n|_p \leq n^{-n} h_1(\beta_0, \beta_1, ...\beta_{n-1})^{-(n-1)^2} |\gamma|_p^n$$
$$\leq n^{-n} h_1(\beta_0, \beta_1, ...\beta_{n-1})^{-(n-1)^2} M^n$$

Daí, para $n > 2M$,

$n^{-n}.M^n < 2^{-n} M^{-n} M^n = 2^{-n}$, donde

$|\beta_n \gamma^n|_p < 2^{-n} h_1(\beta_0, \beta_1, ...\beta_{n-1})^{-(n-1)^2}$

Note agora que $h_1(\beta_0, \beta_1, ...\beta_{n-1}) \geq h_1(\beta_0) = h(\beta_0) \geq 1$, e portanto

$|\beta_n \gamma^n|_p < \frac{1}{2^n h_1(\beta_0, \beta_1, ...\beta_{n-1})^{(n-1)^2}} \leq \frac{1}{2^n}$

e então, se p é primo, o termo geral da série $\sum_{n=0}^{\infty} \beta_n \gamma^n$ converge p-adicamente a zero, para cada $\gamma \in \mathbb{Q}$, $\gamma \neq 0$ e daí a série realmente converge em $\mathbb{Q}_p$. E se $p = \infty$ então a série $\sum_{n=0}^{\infty} |\beta_n \gamma^n|$ é majorada pela série $\sum_{n=0}^{\infty} \frac{1}{2^n}$ que converge, de modo que $\sum_{n=0}^{\infty} \beta_n \gamma^n$ é absolutamente convergente e portanto converge.

Queremos agora mostrar que $F(\gamma)$ é transcendente sobre $\mathbb{Q}$.

Por absurdo, se $F(\gamma)$ fosse algébrico, então, supondo que o grau de seu polinômio minimal é d, pelo Teorema 2.15 teríamos que existe uma constante $C > 0$ tal que, para todo número racional não nulo $\frac{r}{s}$ com $\frac{r}{s} \neq \gamma$,

$$\left|F(\gamma) - \frac{r}{s}\right|_p \geq \frac{C}{h(\frac{r}{s})^d}$$

Em particular tal desigualdade deve ser válida para os racionais

$Q_N = \sum_{n=0}^{N} \beta_n \gamma^n$ onde $N \in \mathbb{N}$. Ou seja, para cada $N \in \mathbb{N}$,

$$|F(\gamma) - Q_N|_p \geq \frac{C}{h(Q_N)^d}$$

Mas, se notarmos $\beta_i = \frac{a_i}{b_i}$ e $\gamma = \frac{x}{y}$ com $mdc(a_i, b_i) = 1 = mdc(x, y)$, teremos:

$$h(Q_N) = h\left(\beta_0 + \beta_1\gamma + \beta_2\gamma^2 + ... + \beta_N\gamma^N\right)$$
$$= h\left(\frac{a_0b_1b_2...b_Ny^N + b_0a_1b_2...b_Nxy^{N-1} + ... + b_0b_1...b_{N-1}a_Nx^N}{b_0b_1b_2...b_Ny^N}\right)$$

Como $h\left(\frac{a}{b}\right) < \max\{|a|, |b|\}$ se $mdc(a,b) \neq 1$, temos

$$h(Q_N) \leq \max\left\{\left|a_0b_1b_2...b_Ny^N + ... + b_0b_1...b_{N-1}a_Nx^N\right|, \left|b_0b_1b_2...b_Ny^N\right|\right\}$$

Ainda, pondo $a = h_1(\beta_0, \beta_1, ..., \beta_N)$ temos

$$a = \max \ \{h(\beta_0), ..., h(\beta_N)\} = \max\{|a_0|, |b_0|, |a_1|, |b_1|, ..., |a_n|, |b_n|\}$$

e portanto, como $M = h(\gamma) = \max\{|x|, |y|\}$, temos

$$\left|a_0b_1b_2...b_Ny^N + b_0a_1b_2...b_Nxy^{N-1} + ... + b_0b_1...b_{N-1}a_Nx^N\right| \leq (N+1)a^{N+1}M^N$$

e também $\left|b_0b_1b_2...b_Ny^N\right| \leq a^{N+1}M^N$

Portanto

$$h(Q_N) \leq \max\{(N+1)a^{N+1}M^N, a^{N+1}M^N\} = (N+1)a^{N+1}M^N$$
$$= (N+1)h_1(\beta_0, \beta_1, ..., \beta_N)^{N+1}.M^N,$$

de modo que

$$|F(\gamma) - Q_N|_p \geq \frac{C}{h(Q_N)^d} \geq \frac{C}{(N+1)^d h_1(\beta_0, \beta_1, ..., \beta_N)^{d(N+1)}.M^{dN}} \qquad (**)$$

Vamos agora majorar $|F(\gamma) - Q_N|_p$, utilizando o fato que os β_i's satisfazem $(*)$

Inicialmente note que

$F(\gamma) - Q_N = \sum_{n=N+1}^{\infty} \beta_n\gamma^n$ ainda converge.

Observe agora que, como já mostramos anteriormente

$|\beta_n\gamma^n|_p \leq n^{-n}h_1(\beta_0, \beta_1, ..., \beta_{n-1})^{-(n-1)^2}M^n$, de modo que, para $N > M$ teremos que, para $n > N$, $n^{-n}M^n = \left(\frac{M}{n}\right)^n < 1$.

Daí, para $N > M$, temos, para todo $n > N$,

$$|\beta_n\gamma^n|_p < h_1(\beta_0, \beta_1, ..., \beta_{n-1})^{-(n-1)^2} \leq h_1(\beta_0, \beta_1, ..., \beta_N)^{-(n-1)^2}$$

Assim, para todo $N > M = h(\gamma)$ a série de números reais positivos $\sum_{n=N+1}^{\infty} |\beta_n\gamma^n|_p$ é majorada pela série

$$\sum_{n=N+1}^{\infty} h_1(\beta_0, \beta_1, ..., \beta_N)^{-(n-1)^2} = \sum_{n=N+1}^{\infty} h_1(\beta_0, \beta_1, ..., \beta_N)^{-N^2} h_1(\beta_0, \beta_1, ..., \beta_N)^{-(n-1)^2+N^2}$$

Queremos agora mostrar que a série $\sum_{n=N+1}^{\infty} h_1(\beta_0, \beta_1, ..., \beta_N)^{-(n-1)^2+N^2}$ converge, pois daí teremos que $\sum_{n=N+1}^{\infty} h_1(\beta_0, \beta_1, ..., \beta_N)^{-N^2} h_1(\beta_0, \beta_1, ..., \beta_N)^{-(n-1)^2+N^2}$ converge para $h_1(\beta_0, \beta_1, ..., \beta_N)^{-N^2} \sum_{n=N+1}^{\infty} h_1(\beta_0, \beta_1, ..., \beta_N)^{-(n-1)^2+N^2}$.

Introduzindo a mudança de variável $j = n - (N+1) = n - N - 1$ obtemos

$$-(n-1)^2 + N^2 = -(j+N)^2 + N^2 = -\left(j^2 + 2jN\right) = -j(j+2N) < -j$$

e portanto

$$h_1(\beta_0, \beta_1, ..., \beta_N)^{-(n-1)^2+N^2} \leq h_1(\beta_0, \beta_1, ..., \beta_N)^{-j}$$

Assim, por sua vez, a série

$\sum_{n=N+1}^{\infty} h_1(\beta_0, \beta_1, ..., \beta_N)^{-(n-1)^2+N^2} = \sum_{j=0}^{\infty} h_1(\beta_0, \beta_1, ..., \beta_N)^{-j(j+2N)}$ é majorada pela série $\sum_{j=0}^{\infty} h_1(\beta_0, \beta_1, ..., \beta_N)^{-j}$.

Afirmamos agora que para $N > M$, temos $h_1(\beta_0, ..., \beta_N) > 2$, e portanto a série $\sum_{j=0}^{\infty} h_1(\beta_0 ... \beta_N)^{-j}$ é majorada pela série $\sum_{j=0}^{\infty} 2^{-j}$ que converge para 2.

De fato: $N > M = h(\gamma) \geq 1$ implica $N \geq 2$. Assim $h_1(\beta_0, ..., \beta_N) \geq h(\beta_2)$. Observe agora que

$h_1(\beta_0, \beta_1) = \max\{h(\beta_0), h(\beta_1)\} \geq 1$ e portanto

$$|\beta_2|_p \leq 2^{-2} h_1(\beta_0, \beta_1)^{-1} \leq 2^{-2}.$$

Logo $p^{-v_p(\beta_2)} = |\beta_2|_p \leq 2^{-2}$ ou seja $p^{v_p(\beta_2)} \geq 4$. Daí $h(\beta_2) \geq 4 > 2$.

Após todas estas majorações obtemos que, $\sum_{n=N+1}^{\infty} |\beta_n \gamma^n|_p$ converge e para todo $\gamma \in \mathbb{Q}^*$ e todo $N > M = h(\gamma)$

$$\begin{aligned}
\sum_{n=N+1}^{\infty} |\beta_n \gamma^n|_p &\leq \sum_{n=N+1}^{\infty} h_1(\beta_0, \beta_1, ..., \beta_N)^{-(n-1)^2} \\
&\leq h_1(\beta_0, \beta_1, ..., \beta_N)^{-N^2} \sum_{n=N+1}^{\infty} h_1(\beta_0, \beta_1, ..., \beta_N)^{-j} \\
&\leq 2 h_1(\beta_0, \beta_1, ..., \beta_N)^{-N^2}
\end{aligned}$$

Observe agora que,

$$\begin{aligned}
\left|\sum_{n=N+1}^{\infty} \beta_n \gamma^n\right|_p &= \left|\lim_{T\to\infty} \sum_{n=N+1}^{T} \beta_n \gamma^n\right|_p \\
&= \lim_{T\to\infty} \left|\sum_{n=N+1}^{T} \beta_n \gamma^n\right|_p \\
&\leq \lim_{T\to\infty} \sum_{n=N+1}^{T} |\beta_n \gamma^n|_p \\
&= \sum_{n=N+1}^{\infty} |\beta_n \gamma^n|_p
\end{aligned}$$

Mas então, para todo $\gamma \in \mathbb{Q}^*$ e todo $N > M = h(\gamma)$,

$$|F(\gamma) - Q_N|_p = \left|\sum_{n=N+1}^{\infty} \beta_n \gamma^n\right|_p \leq \sum_{n=N+1}^{\infty} |\beta_n \gamma^n|_p \leq 2\, h_1(\beta_0, \beta_1, ... \beta_N)^{-N^2}$$

Então, por $(**)$ temos

$$0 < \frac{C}{(N+1)^d h_1(\beta_0, \beta_1, ..., \beta_N)^{d(N+1)} . M^{dN}} \leq |F(\gamma) - Q_N|_p \leq 2\ h_1(\beta_0, \beta_1, ...\beta_N)^{-N^2}$$

E daí,

$$0 < \frac{C}{2} \leq (N+1)^d\ M^{dN}\ h_1(\beta_0, \beta_1, ...\beta_N)^{d(N+1)}\ h_1(\beta_0, \beta_1, ...\beta_N)^{-N^2}$$

Isto é,

$$0 < \frac{C}{2} \leq \frac{(N+1)^d}{h_1(\beta_0, \beta_1, ...\beta_N)^{\frac{N^2}{3}}} . \frac{M^{dN}}{h_1(\beta_0, \beta_1, ...\beta_N)^{\frac{N^2}{3}}} . \frac{h_1(\beta_0, \beta_1, ...\beta_N)^{d(N+1)}}{h_1(\beta_0, \beta_1, ...\beta_N)^{\frac{N^2}{3}}}$$

Contudo, a expressão acima é impossível, já que os fatores aproximam-se de zero para N suficientemente grande.

Desta forma $F(\gamma) \in \mathbb{Q}_p$ não é algébrico sobre $\mathbb{Q}$, ou seja, é transcendente sobre $\mathbb{Q}$, para todo $\gamma \in \mathbb{Q} - \{0\}$.. □

Para efetivamente apresentarmos um exemplo de elementos transcendentes de $\mathbb{Q}_p$, resta-nos mostrar a existência de uma sequência (β_N) de racionais satisfazendo a condição $(*)$ do Teorema 2.16.

Teorema 2.17: Seja $F(X)$ a série de potências definida por:

$$F(X) = \sum_{n=0}^{\infty} \left(\frac{n!}{n!^2 + 1} \right)^{n!^3} X^n,$$

Então para todo número racional α diferente de zero e para todo $p \in V_{\mathbb{Q}}$, $F(\alpha)$ converge para um número em $\mathbb{Q}_p$. transcendente sobre $\mathbb{Q}$.

Prova: Para cada $n \in \mathbb{N}$, nós definimos

$$\beta_n = \left(\frac{n!}{n!^2 + 1} \right)^{n!^3}$$

Inicialmente afirmamos que basta mostrar que, para todo $p \in V_{\mathbb{Q}}$ existe N_0 suficientemente grande tal que

$$N > N_0,\ 0 < |\beta_N|_p \leq N^{-N} h_1(\beta_0, \beta_1, ...\beta_{N-1})^{-(N-1)^2}$$

De fato, se tal N_0 existir então consideramos a sequência α_n definida por $\alpha_n = \beta_{N_0+n}$; teremos $|\alpha_n|_p$ tal que

$$\begin{aligned} 0 < |\alpha_n|_p = |\beta_{N+n}|_p &\leq (N+n)^{-(N+n)} h_1(\beta_0, \beta_1, ... \beta_{N+n-1})^{-(N+n-1)^2} \\ &\leq n^{-n} h_1(\beta_N, \beta_{N+1}, ... \beta_{N+n-1})^{-(n-1)^2} \\ &= n^{-n} h_1(\alpha_0, \alpha_1, ..., \alpha_{n-1})^{-(n-1)^2}. \end{aligned}$$

Daí, pelo Teorema 2.16, a série $\sum_{n=0}^{\infty} \alpha_n \gamma^n$ converge para um transcendente p –ádico, para cada $\gamma \in \mathbb{Q}$, $\gamma \neq 0$ e portanto

$$\begin{aligned} \sum_{n=0}^{\infty} \beta_n \gamma^n &= \sum_{n=0}^{N_0-1} \beta_n \gamma^n + \sum_{n=N_0}^{\infty} \beta_n \gamma^n \\ &= \sum_{n=0}^{N_0-1} \beta_n \gamma^n + \sum_{n=0}^{\infty} \beta_{n+N_0} \gamma^{n+N_0} \\ &= \sum_{n=0}^{N_0-1} \beta_n \gamma^n + \gamma^{N_0} \sum_{n=0}^{\infty} \alpha_n \gamma^n \text{ é um transcendente.} \end{aligned}$$

Assim, vamos mostrar que, para cada $p \in V_{\mathbb{Q}}$ fixado, para N suficientemente grande temos

$$0 < |\beta_N|_p \leq N^{-N} h_1(\beta_0, \beta_1, ... \beta_{N-1})^{-(N-1)^2} \qquad (*)$$

Inicialmente observe que, para cada $j \in \mathbb{N}^*$, $h(\beta_i) = \left[j!^2 + 1\right]^{j!^3}$ e portanto

$$\begin{aligned} h_1(\beta_0, \beta_1, ... \beta_{N-1}) &= \max\{h(\beta_0), h(\beta_1), ..., h(\beta_{N-1})\} \\ &= [(N-1)!^2 + 1]^{(N-1)!^3} \end{aligned}$$

donde, para N suficientemente grande:

$$\begin{aligned} N^{-N}\, h_1(\beta_0, \beta_1, ... \beta_{N-1})^{-(N-1)^2} &= N^{-N} \left[(N-1)!^2 + 1\right]^{-(N-1)^2 (N-1)!^3} \\ &\geq N!^{-N - (N-1)^2(N-1)!^3} \end{aligned}$$

e como para N suficientemente grande,

$$N + (N-1)^2(N-1)!^3 < [N + (N-1)^2](N-1)!^3 < N^3(N-1)!^3 = N!^3$$

temos

$$N^{-N}\, h_1(\beta_0, \beta_1, ... \beta_{N-1})^{-(N-1)^2} \geq N!^{-N!^3}$$

Mostremos agora que a seqüência (β_N) satisfaz $(*)$ para N suficientemente grande quando $p = \infty$. De fato, temos

$$\frac{N!}{N!^2 + 1} = \frac{1}{N! + \frac{1}{N!}} < \frac{1}{N!}$$

e portanto,

$$0 < |\beta_N| = \left(\frac{N!}{N!^2 + 1}\right)^{N!^3} \leq (N!)^{-(N!)^3} \leq N^{-N}\, h_1(\beta_0, \beta_1, ... \beta_{N-1})^{-(N-1)^2}$$

Agora, seja p um número primo. Então, para $N > p$, temos

$$|\beta_N|_p = \left|\left(\frac{N!}{N!^2+1}\right)^{N!^3}\right|_p = |N!|_p^{N!^3} > 0$$

pois $v_p(N!^2+1) = 0$ para todo primo p.

Pelo Corolário 1.10 temos $v_p(N!) \geq \frac{N}{2p-2}$, donde

$0 < |\beta_N|_p = |N!|_p^{N!^3} = [p^{-v_p(N!)}]^{N!^3} \leq p^{-N!^3 N/(2p-2)}$

Afirmamos agora que, para N suficientemente grande, temos

$p^{N!^3 \frac{N}{2p-2}} \geq N!^{N+(N-1)^2(N-1)!^3}$

De fato:

$$\log\left[p^{N!^3 \frac{N}{2p-2}}\right] = N!^3 N \frac{\log p}{2p-2} \quad \text{e} \quad \log\left[N!^{N+(N-1)^2(N-1)!^3}\right] = [N+(N-1)^2(N-1)!^3]\log N!$$

Mas

$$\frac{[N+(N-1)^2(N-1)!^3]\log N!}{N!^3 N \frac{\log p}{2p-2}} \leq \frac{[N+(N-1)^2(N-1)!^3]\log N}{N!^3} \cdot \frac{2p-2}{\log p}$$

$$= \left[\frac{N}{N!^3} + \frac{(N-1)^2}{N^3}\right]\log N \frac{2p-2}{\log p}$$

$$= \left[\frac{N}{N^2(N-1)!^3} + \frac{(N-1)^2}{N^2}\right]\frac{\log N}{N}\,\frac{2p-2}{\log p}$$

É facil ver que a última igualdade tende a zero para N suficientemente grande, e daí

$$\log\left[p^{N!^3 \frac{N}{2p-2}}\right] \geq \log\left[N!^{N+(N-1)^2(N-1)!^3}\right]$$

De modo que, para N suficientemente grande,

$$0 < |\beta_N|_p \leq p^{-N!^3 N/(2p-2)}$$
$$\leq N!^{-N-(N-1)^2(N-1)!^3}$$
$$\leq N^{-N} h_1(\beta_0, \ldots, \beta_{N-1})^{-(N-1)^2} \qquad \square$$

CAPÍTULO 3

Séries que convergem para números p-ádicos prescritos, com $p \in V_{\mathbb{Q}}$

3.1 Enunciado e demonstração do resultado

No exemplo 1.3.3(v) do capítulo 1 construimos uma série que converge em $\mathbb{Q}_p$, para todo $p \in V_{\mathbb{Q}}$, mas não sabemos responder se seus limites são números algébricos ou transcendentes. E, no capítulo anterior apresentamos exemplo de uma série formal $F(X) = \sum_{i=0}^{\infty} \beta_i X^i \in \mathbb{Q}[[X]]$ tal que, para todo $\alpha \in \mathbb{Q} - \{0\}$, $F(\alpha)$ converge em $\mathbb{Q}_p$ sendo seu limite, para todo $p \in V_{\mathbb{Q}}$, um número transcendente.sobre $\mathbb{Q}$.

Neste capítulo formulamos uma nova questão, colocada e respondida por Burger e Struppeck, em [B-S]:

É possível construir uma seqüência de números racionais não nulos tal que para cada $p \in V_{\mathbb{Q}}$ a série por eles originada converge em $\mathbb{Q}_p$ e, para cada $p \in V_{\mathbb{Q}}$, a soma da série é um número racional prescrito? Esta questão foi colocada por Koblitz (veja [K] p.85), e na página 142 ele diz que até aquele momento não se conhecia a resposta.

Teorema 3.1 (Burger, Struppeck): Para cada $p \in V_{\mathbb{Q}}$, fixemos $\alpha_p \in \mathbb{Q}_p$. Então existe uma seqüência de números racionais $(a_n)_{n \in \mathbb{N}}$, com $a_n > 0$ para todo $n \geq 1$, tal que, para cada $p \in V_{\mathbb{Q}}$, a série

$$\sum_{n=0}^{\infty}{}_{p\text{-ádico}}\, a_n = \alpha_p$$

A demonstração do Teorema acima vai nos fornecer um algoritmo para gerar tal série.

Estabelecemos primeiramente preliminares para sua demonstração.

Definição: Definimos para cada $m \in \mathbb{N}$, $m \geq 2$:

$$U(m) = \left\{\tfrac{r}{s} \in \mathbb{Q},\ r \equiv s \equiv 1(\mathrm{mod}\, m)\right\}$$

Lema 3.2: Seja m um produto de primos: $m = p_1 \dots p_n$. Se $\mu \in U(m)$, então $\mu \in U(p_i)$ para todo $i \in \{1, \dots, n\}$.

Prova: Basta observar que, $r \equiv 1(\mathrm{mod}\ m)$ se e somente se $r \equiv 1(\mathrm{mod}\ p_i)$, $i = 1, \dots n$. □

Lema 3.3: Seja $m \geq 2$ um inteiro. Então $U(m)$ é um subconjunto denso de $\mathbb{R}$.

Prova: Como $\mathbb{Q}$ é denso em $\mathbb{R}$, basta-nos mostrar que $U(m)$ é denso em $\mathbb{Q}$. Fixados $\frac{a}{b} \in \mathbb{Q}$ e $\varepsilon > 0$, afirmamos que existe $n \in \mathbb{Z}$ tal que

$$\frac{anm+1}{bnm+1} \in U(m), \qquad \left|\frac{a}{b} - \frac{anm+1}{bnm+1}\right| < \varepsilon$$

De fato, é claro que $\frac{anm+1}{bnm+1} \in U(m)$. Ainda, note que:

$$\left|\frac{a}{b} - \frac{anm+1}{bnm+1}\right| = \left|\frac{abnm + a - abnm - b}{b(bnm+1)}\right| = \frac{|a-b|}{b|bnm+1|},$$

de modo que

$$\frac{|a-b|}{b|bnm+1|} < \varepsilon \Longleftrightarrow$$

$$\frac{|a-b|}{\varepsilon b} < |bnm+1|$$

E, se n for natural, teremos: $|bnm+1| = bnm+1$ e

$$\frac{|a-b|}{\varepsilon b} < bnm+1 \Longleftrightarrow$$

$$n > \left(\frac{|a-b|}{\varepsilon b} - 1\right)\frac{1}{bm} \Longleftrightarrow$$

$$n > \frac{|a-b| - \varepsilon b}{\varepsilon b^2 m}$$

Assim, se escolhermos para tal $\varepsilon > 0$ um $n \in \mathbb{N}$ satisfazendo, $n > \frac{|a-b| - \varepsilon b}{\varepsilon b^2 m}$, teremos satisfeita a desigualdade $\left|\frac{a}{b} - \frac{anm+1}{bnm+1}\right| < \varepsilon$, e daí podemos concluir que $U(m)$ é denso em $\mathbb{Q}$. $\square$

Teorema 3.4 (Chinês de Restos): Dados inteiros $m_1, ..., m_k$ dois a dois primos entre si e inteiros arbitrários $r_1, ..., r_k$, existe uma solução inteira para o sistema de congruências

$$\begin{cases} X \equiv r_1 \pmod{m_1} \\ \ldots \\ X \equiv r_k \pmod{m_k} \end{cases}$$

Além disso, tal solução é única módulo $N = m_1 ... m_k$

Prova: Consideremos

$$t_i = \frac{N}{m_i}, \qquad i \in \{1, ..., k\}$$

Como $m_1, ..., m_k$ são dois a dois relativamente primos então temos para todo i, $mdc\ (t_i, m_i) = 1$, isto é, existem $\mu_i,\ v_i \in \mathbb{Z}$ tais que

$$\mu_i t_i + v_i m_i = 1;$$

assim já temos garantido $\mu_i t_i \equiv 1 \pmod{m_i}$. Notemos que para $j \neq i$, m_j divide t_i, de modo que $\mu_i t_i \equiv 0 \pmod{m_j}$. Portanto, tomando

$$M = \mu_1 t_1 r_1 + ... + \mu_k t_k r_k$$

teremos

$$\begin{cases} \mu_i t_i r_i \equiv r_i \pmod{m_i} \\ \mu_j t_j r_j \equiv 0 \pmod{m_i},\ i \neq j \end{cases} \Rightarrow M \equiv r_i \pmod{m_i},\ \forall\ i$$

Assim, M é uma solução para o sistema de congruência dado.

Afirmamos agora que se $y \equiv r_i \pmod{m_i}$, para todo i então $M \equiv y \pmod{m_1 ... m_k}$

De fato: Se $y \equiv r_i \equiv M \pmod{m_i}$, para todo i então $y \equiv M \pmod{m_i}$, para todo i, isto é, m_i divide $y - M$, para todo $i \in \{1, ..., k\}$

Como $m_1, ..., m_k$ são dois a dois relativamente primos temos daí que o produto $m_1 . \ ... \ .m_k$ divide $y - M$, ou seja,

$$y \equiv M \pmod{m_1 ... m_k}$$

provando assim que existe uma única solução módulo $m_1. \ldots .m_k$. □

Corolário 3.5: Dados inteiros $m_1, ..., m_k$, $a_1, ..., a_k$, $r_1, ..., r_k$ satisfazendo:

(i) $m_1, ..., m_k$ são dois a dois primos entre si

(ii) $mdc(a_i, m_i) = 1$, para cada $i \in \{1, ..., k\}$

existe uma solução inteira para o sistema de congruências

$$\begin{cases} a_1 X \equiv r_1 (\text{mod } m_1) \\ \ldots \\ a_k X \equiv r_k (\text{mod } m_k) \end{cases}$$

Além disso, tal solução é única módulo $N = m_1 ... m_k$

Prova: Basta observar que se $mdc(a_i, m_i) = 1$ então existe $b_i,\ c_i \in \mathbb{Z}$ tais que

$$a_i b_i + c_i m_i = 1$$

e assim, $a_i b_i \equiv 1 \ (\text{mod } m_i)$.

Note agora que, se $x \in \mathbb{Z}$ for tal que $x \equiv b_i r_i (\text{mod } m_i)$, então $a_i x \equiv r_i (\text{mod } m_i)$.

Assim, passamos a considerar o sistema

$$\begin{cases} X \equiv b_1 r_1 (\text{mod } m_1) \\ \ldots \\ X \equiv b_k r_k (\text{mod } m_k) \end{cases}$$

E, pelo Teorema Chinês de Restos, tal sistema admite solução da forma

$$M = \mu_1 t_1 r_1 b_1 + \ldots + \mu_k t_k r_k b_k \ ,$$

onde, para cada $i \in \{1, ..., k\}$, $\mu_i t_i + v_i m_i = 1$ com $t_i = \frac{N}{m_i}$, e já sabemos que tal solução é única mod N. □

Para enunciar os próximos resultados, introduzimos a seguinte notação:

Notação 1: Seja F uma coleção finita de primos distintos.

Para cada $p \in F$, seja δ_p um elemento diferente de zero de $\mathbb{Q}_p$, e denotemos sua expansão p-ádica como

$$\delta_p = \sum_{n=l_p}^{\infty} d(p,n) p^n$$

(onde $l_p \in \mathbb{Z}$ e $0 \le d(p,n) \le p-1$ para cada $n \ge l_p$). Como os δ_p são todos não nulos suporemos $d(p,l_p) \ne 0$, de modo que $v_p(\delta_p) = l_p$ e portanto $|\delta_p|_p = p^{-l_p}$.

Para tal escolha, definimos o número racional $\Upsilon = \Upsilon(\{\delta_p\}_{p\in F})$ por $\Upsilon = \prod_{p\in F} p^{l_p}$ (que está bem definido pois cada δ_p é não nulo).

Lema 3.6: Para F, $\{\delta_p\}_{p\in F}$ e Υ conforme Notação 1 acima, existe um inteiro $M > 0$ tal que:

$$\forall\ p\ \in F,\ |\delta_p - M\Upsilon|_p < |\delta_p|_p.$$

Ou seja, para cada $p \in F$, $M\Upsilon$ na métrica p-ádica está mais próximo de δ_p do que o zero

Prova: Inicialmente observamos que $v_p(\delta_p) = l_p$, de modo que queremos encontrar $M \in \mathbb{N}$ tal que, para todo $p \in F$, $v_p(\delta_p - M\Upsilon) > l_p$. Assim, queremos encontrar $M\Upsilon$ de tal forma que $M\Upsilon = \sum_{n=l_p}^{\infty} d'(p,n)p^n$ onde $d'(p,l_p) = d(p,l_p)$, o primeiro termo da expansão p –ádica de δ_p.

Para isso definimos, para cada primo $p \in F$, $\Upsilon_p = \Upsilon p^{-l_p}$ e escrevemos $\Upsilon_p = \frac{m_p}{n_p}$ onde m_p e n_p são inteiros relativamente primos com p.

Agora consideremos a seguinte coleção finita de congruências lineares simultâneas:

$$\left\{\ m_pX \equiv n_pd(p,l_p) \qquad (\text{mod } p)\ \right\}_{p\in F}$$

Pelo Corolário 3.5, podemos encontrar infinitas soluções inteiras para o sistema, todas elas no entanto congruentes módulo $\prod_{p\in F} p$. Assim, tomando uma solução $x = M > 0$ para o sistema, teremos que, para cada $p \in F$, existe algum inteiro t_p tal que:

$$m_pM = n_pd(p,l_p) + pt_p$$

Daí

$$\frac{m_p}{n_p}M = d(p,l_p) + p\frac{t_p}{n_p}$$

donde

$$\Upsilon_pM = d(p,l_p) + p\frac{t_p}{n_p}$$

e, como $\Upsilon_p p^l = \Upsilon$,

$$\Upsilon M = d(p,l_p)p^{l_p} + p^{l_p+1}.\ \frac{t_p}{n_p}.$$

Como n_p não é congruente a zero módulo p, temos que $v_p(p^{l_p+1}.\ \frac{t_p}{n_p}) \geq l_p + 1$. Assim, o primeiro termo da expansão p-ádica para $M\Upsilon$ é $d(p,l_p)p^{l_p}$, como queríamos. □

A demonstração acima, junto com o Corolário 3.5, nos permite até sermos um pouco mais específicos sobre tal constante M:

Lema 3.6$'$: Para F, $\{\delta_p\}_{p\in F}$ e Υ conforme Notação 1, existe um único inteiro $M \in \left\{1,2,3,\ldots,\prod_{p\in F} p-1\right\}$ tal que

$$|\delta_p - M\Upsilon|_p < |\delta_p|_p$$

para todo primo $p \in F$. Em particular, $|M\Upsilon|_p = |\delta_p|_p$.

Prova: Esclarecemos porque $M \neq \prod_{p\in F} p$. De fato, para todo $p \in F$, n_p, m_p e $d(p,l_p)$ são relativamente primos com p e $m_p M \equiv n_p d(p,l_p) \pmod{p}$. Logo $M \neq 0 \pmod{p}$ para todo $p \in F$, donde $M \neq \prod_{p\in F} p$. □

Corolário 3.7: Sejam F, $\{\delta_p\}_{p\in F}, \Upsilon$, e M como no Lema 3.6. Fixado $p \in F$, temos, para cada $\mu \in U(p)$,

$$|\delta_p - \mu M\Upsilon|_p < |\delta_p|_p$$

Prova: Se $\mu = \frac{r}{s}$ com $r \equiv s \equiv 1(\text{mod } p)$, então $r = np + 1$ e $s = mp + 1$ para convenientes m, n inteiros. Temos assim $|s|_p = 1$. Além disso, $|1 - \mu|_p < 1$ pois

$$|1-\mu|_p = \left|1 - \frac{r}{s}\right|_p = \left|\frac{s-r}{s}\right|_p = |s-r|_p =$$

$$= |mp + 1 - np - 1|_p = |p(m-n)|_p \leq p^{-1} < 1$$

Daí:

$$|\delta_p - \mu M\Upsilon|_p = |\delta_p - M\Upsilon + M\Upsilon - \mu M\Upsilon|_p$$

$$\leq \max\left\{|\delta_p - M\Upsilon|_p\,,\, |M\Upsilon - \mu M\Upsilon|_p\right\}$$

$$= \max \left\{ |\delta_p - M\Upsilon|_p \, , \, |M\Upsilon|_p |1 - \mu|_p \right\}.$$

Mas,

$$|M\Upsilon|_p |1 - \mu|_p < |M\Upsilon|_p = |\delta_p|_p$$

(veja Lema 3.6$'$) e pelo Lema 3.6,

$$|\delta_p - M\Upsilon|_p < |\delta_p|_p \, .$$

Portanto

$$|\delta_p - \mu M\Upsilon|_p < |\delta_p|_p \qquad \square$$

Finalmente antes de passarmos à prova do Teorema 3.1, introduzimos a

Notação 2: Indicamos por F_n o conjunto dos n primeiros primos, isto é, $F_0 = \{ \}$, $F_1 = \{2\}$, $F_2 = \{2,3\}$, e assim por diante, e indicamos por P_n o produto dos n primeiros primos.

Prova do Teorema 3.1:

Definiremos os números racionais a_n indutivamente.

A idéia que vamos perseguir para construir uma série de racionais $\sum a_n$ que convirja para α_p, é que para construirmos a_{N+1}, estejamos levando em conta os $N+1$ primeiros primos e aproximando-nos mais dos N primeiros p-ádicos $\alpha_2, \ \alpha_3, \ \alpha_5, ..., \alpha_N$ fixados.

Note que, se construirmos (a_n) satisfazendo:

(i) $a_n \in \mathbb{Q}$ e $a_n > 0$, para todo $n \neq 0$;

(ii) se $S_N = \sum_{n=0}^{N} a_n$ é a soma parcial dos N primeiros termos, então

$$0 < \alpha_\infty - S_N < 2^{-(N-1)};$$

(iii) para cada primo p em F_N, $S_{N-1} = \alpha_p$ ou

$$|\alpha_p - S_N|_p < |\alpha_p - S_{N-1}|_p,$$

estaremos garantindo com (i) que os elementos da série são números racionais a_n, com $a_n > 0$ para todo $n \geq 1$, com (ii) a convergência da série em $\mathbb{Q}_\infty = \mathbb{R}$ para α_∞, e com (iii) temos garantidas todas as convergências para $\alpha_p \in \mathbb{Q}_p$ com p primo, visto que, para cada primo p, sendo $\{S_N\}_{n=0}^{\infty}$ uma seqüência monotonamente crescente de números racionais, então $\alpha_p = S_J$ para no máximo um J; daí conclui-se que existe um N tal que $0 < |\alpha_p - S_{n+1}|_p < |\alpha_p - S_n|_p$ para todo $n \geq N$, e portanto a sequência $\left\{|\alpha_p - S_n|_p\right\}_{n=N}^{\infty}$ é uma sequência estritamente decrescente de potências inteiras de p. Então $\lim_{n\to\infty} |\alpha_p - S_n|_p = 0$, ou seja, a série $\sum_{n=0}^{\infty} a_n$ converge para $\alpha_p \in \mathbb{Q}_p$.

Começamos por colocar:

$$a_0 = [\alpha_\infty - 1]$$

onde por $[x]$ estamos denotando a parte inteira de x.

Note que, desta forma, para $N = 0$ as três condições acima são satisfeitas. De fato:

(i) $a_0 = [\alpha_\infty - 1] \in \mathbb{Q}$;

(ii) $0 < \alpha_\infty - a_0 < 2$;

(iii) Como $F_0 = \{\ \}$, esta condição é satisfeita por vacuidade.

Suponhamos agora $N \geq 0$ e que a_0, a_1, ..., a_N estão todos construidos de tal forma que obedecem às três condições acima.

Para construirmos a_{N+1}, consideremos, para cada primo $p \in F_{N+1}$,

$$\delta_p = \alpha_p - S_N$$

Seja $\widetilde{F}_{N+1} = \{p \in F_{N+1} : \delta_p \neq 0\}$

Se $\widetilde{F}_{N+1} = \{\ \}$ façamos $M\Upsilon = 1$; caso contrário, pelo Lema 3.6 existe um inteiro $M > 0$ tal que:

$$|\delta_p - M\Upsilon|_p < |\delta_p|_p \text{para todo primo } p \in \widetilde{F}_{N+1}$$

Em qualquer caso, como P_{N+1} denota o produto dos $N+1$ primeiros primos temos, pelo Lema 3.3 que $U(P_{N+1})$ é denso em $\mathbb{R}$; assim, existe $\mu \in U(P_{N+1})$ tal que:

$$\left|\frac{\alpha_\infty - S_N}{M\Upsilon} - \mu\right| < \frac{1}{2}\frac{\alpha_\infty - S_N}{M\Upsilon}$$

É fácil ver que podemos até escolher μ satisfazendo

$$0 < \mu < \frac{\alpha_\infty - S_N}{M\Upsilon}$$

isto é,

$$\frac{\alpha_\infty - S_N}{2M\Upsilon} < \mu < \frac{\alpha_\infty - S_N}{M\Upsilon}$$

Pelo Corolário 3.7, temos que, para um tal μ,

$$|\delta_p - \mu M\Upsilon|_p < |\delta_p|_p, \quad \forall\, p \in \widetilde{F}_{N+1},$$

ou seja,

$$|\alpha_p - S_N - \mu M\Upsilon|_p < |\alpha_p - S_N|_p, \quad \forall\, p \in \widetilde{F}_{N+1}$$

Definimos então $a_{N+1} = \mu M\Upsilon$. Afirmamos que a_{N+1} satisfaz também as três condições acima citadas. De fato:

(i) $a_{N+1} \in \mathbb{Q}$ e $a_{N+1} > 0$ pois escolhemos $\mu > 0$, μ racional, M inteiro positivo e $\Upsilon = \prod_{p\in\widetilde{F}_{N+1}} p^{l_p} \in \mathbb{Q}$ também positivo.

(ii) Por construção $0 < \frac{\alpha_\infty - S_N}{M\Upsilon} - \mu < \frac{\alpha_\infty - S_N}{2M\Upsilon}$. Daí

$0 < \alpha_\infty - (S_N + \mu M\Upsilon) < 2^{-1}(\alpha_\infty - S_N) \Rightarrow$

$0 < \alpha_\infty - (S_N + a_{N+1}) < 2^{-1}(\alpha_\infty - S_N) \Rightarrow$

$0 < \alpha_\infty - S_{N+1} < 2^{-1}(\alpha_\infty - S_N) < 2^{-1}2^{-(N-1)} = 2^{-(N+1-1)}$

Logo,

$$0 < \alpha_\infty - S_{N+1} < 2^{-(N+1-1)}.$$

(iii) para cada primo $p \in F_{N+1}$, temos $\alpha_p = S_N$ se $p \notin \widetilde{F}_{N+1}$ ou então $p \in \widetilde{F}_{N+1}$, e neste caso $|\delta_p - \mu M\Upsilon|_p < |\delta_p|_p$ onde $\delta_p = \alpha_p - S_N$.

Mas

$|\delta_p - \mu M\Upsilon|_p < |\delta_p|_p \Leftrightarrow$

$\Leftrightarrow |\alpha_p - S_N - \mu M\Upsilon|_p < |\alpha_p - S_N|_p \Leftrightarrow$

$\Leftrightarrow |\alpha_p - S_{N+1}|_p < |\alpha_p - S_N|_p$

Assim, para todo $n \in \mathbb{N}$, a_n satisfaz as três condições exigidas e o teorema 3.1 está demonstrado. □

As observações a seguir têm o objetivo de facilitar a elaboração do algoritmo que a demonstração acima sugere.

Observação 1: A escolha $a_0 = [\alpha_\infty - 1]$ ao invés de $a_0 = [\alpha_\infty]$ na demonstração acima, evita o caso $a_0 = \alpha_\infty$, o que acarretaria $0 = \alpha_\infty - a_0$, e a escolha de μ não seria possivel neste caso.

O que podemos no entanto observar é que no caso $\alpha_\infty \notin \mathbb{Z}$ nunca ocorrerá $[\alpha_\infty] = \alpha_\infty$, e então neste caso podemos tomar $a_0 = [\alpha_\infty]$.

Observação 2: Como observamos no Lema 3.6', M pode ser escolhido univocamente se nos restringirmos ao conjunto $\left\{1, 2, \ldots, \prod_{p \in \widetilde{F}_{N+1}} p - 1\right\}$. No entanto, não há chances de escolhermos μ univocamente uma vez que $U(P_{N+1})$ é denso em $\mathbb{Q}$. Mas poderíamos tentar selecionar um pouco a escolha de μ; queremos $\mu \in U(P_{N+1})$ e $\frac{\alpha_\infty - S_N}{2M\Upsilon} < \mu < \frac{\alpha_\infty - S_N}{M\Upsilon}$, poderíamos tentar encontrar $\mu = \frac{1}{\eta}$ com $\begin{cases} \eta \equiv 1 \pmod{P_{N+1}} \\ \frac{\alpha_\infty - S_N}{2M\Upsilon} < \mu < \frac{\alpha_\infty - S_N}{M\Upsilon} \end{cases}$

ou ainda

$$\mu = \frac{1}{\eta} \text{ com } \eta \text{ tal que } \begin{cases} \eta \equiv 1 \pmod{P_{N+1}} \\ \frac{M\Upsilon}{\alpha_\infty - S_N} < \eta < \frac{2M\Upsilon}{\alpha_\infty - S_N} \end{cases}$$

Infelizmente, como veremos adiante no exemplo 2, um $\mu \in U(P_{N+1})$ na forma $\mu = \frac{1}{\eta}$ pode não existir satisfazendo a condição $\frac{\alpha_\infty - S_N}{2M\Upsilon} < \mu < \frac{\alpha_\infty - S_N}{M\Upsilon}$.

3.2 Algoritmo para a construção da série

Fixados $\alpha_\infty \in \mathbb{Q}_\infty = \mathbb{R}$ e $\alpha_p \in \mathbb{Q}_p$ para cada primo p, construimos uma série $\sum_{n=0}^{\infty} a_n$ de números racionais que converge para α_∞ em $\mathbb{Q}_\infty = \mathbb{R}$ e converge para α_p em $\mathbb{Q}_p$ para cada primo p através do seguinte Algoritmo, que leva em conta as observações 1 e 2 acima, além da demonstração do Teorema 3.1.

1. Defina $a_0 = \begin{cases} [\alpha_\infty - 1], & \alpha_\infty \in \mathbb{Z} \\ [\alpha_\infty], & \alpha_\infty \notin \mathbb{Z} \end{cases}$

2. Para a determinação de a_N, $N > 0$, supondo-se conhecidos $a_0, a_1, \ldots, a_{N-1}$

a) Define-se:

$$\delta_p = \alpha_p - S_{N-1}, \text{ para todo } p \in F_N$$

$$\widetilde{F}_N = \{p \in F_N : \delta_p \neq 0\}$$

$$P_N = \Pi_{p \in F_N}\, p$$

$$\Upsilon = \Pi_{p \in \widetilde{F}_N}\, p^{l_p} \text{ onde } l_p = v_p(\delta_p)$$

b) Se $\widetilde{F}_N = \{\ \}$, define-se $M\Upsilon = 1$.

Se $\widetilde{F}_N \neq \{\ \}$, determina-se o inteiro $M \in \{1, 2, ..., P_N - 1\}$, tal que:

$$|\delta_p - M\Upsilon|_p < |\delta_p|_p \ , \forall\ p \in \widetilde{F}_N$$

ou equivalentemente

$$v_p(\delta_p - M\Upsilon) > v_p(\delta_p)$$

c) Procura-se $\mu \in U(P_N)$ tal que:

$$\frac{\alpha_\infty - S_{N-1}}{2M\Upsilon} < \mu < \frac{\alpha_\infty - S_{N-1}}{M\Upsilon}$$

ou, se possível $\mu = \frac{1}{\eta}$, $\eta \equiv 1 \pmod{P_N}$ onde

$$\frac{M\Upsilon}{\alpha_\infty - S_{N-1}} < \eta < \frac{2M\Upsilon}{\alpha_\infty - S_{N-1}}$$

d) Define-se então $a_N = \mu M\Upsilon$.

3.3 Exemplos

Exemplo 1. Construção de uma série $\sum_{n=0}^{\infty} a_n$ de números racionais positivos que converge para "e" em $\mathbb{Q}_\infty = \mathbb{R}$ e converge para zero em $\mathbb{Q}_p$, para todo p primo.

Temos aqui $\alpha_\infty = e \simeq 2,71828182846... \in \mathbb{R}$ e $\alpha_p = 0 \in \mathbb{Q}_p$, para todo p primo

Portanto $a_0 = [e] = 2$ então $S_0 = 2$.

Aqui neste caso já temos algumas simplificações no algoritmo:

a) Como $S_0 = 2 \neq 0$ e (S_N) é uma sequência monótona crescente, teremos $S_N \neq 0$ sempre.

b) Para cada primo p e para cada $N \in \mathbb{N}$, como $\alpha_p = 0$,

$$\delta_p = \alpha_p - S_N = -S_N \neq 0$$

de modo que

$$\widetilde{F}_N = F_N$$

♦ Determinação de a_1:

Temos $\delta_2 = -S_0 = -2$, $\widetilde{F}_1 = \{2\}$, $\Upsilon = 2^1 = -\delta_2$ e $P_1 = 2$.

Determinamos $M \in \{1,...,P_1 - 1\} = \{1\}$ tal que $v_2(\delta_2 - M\Upsilon) > v_2(\delta_2)$ ou seja, $M = 1$.

E portanto $M\Upsilon = 2 = S_0$.

Procuramos agora, se possível, $\mu = \frac{1}{\eta}$ com

$$\begin{cases} \eta \equiv 1(\mathrm{mod}\, 2) \\ \frac{M\Upsilon}{a_\infty - S_0} < \eta < \frac{2M\Upsilon}{a_\infty - S_0} \end{cases}$$

o que é equivalente a:

$$\begin{cases} \eta \equiv 1 \ (\mathrm{mod}\ 2) \\ \frac{2}{0{,}718...} < \eta < \frac{4}{0{,}718...} \end{cases}$$

isto é,

$$2,7855... < \eta < 5,5710...$$

E, como $\eta \equiv 1(\mathrm{mod}\, 2)$ então $\eta \in \{3, 5\}$.

Façamos aqui uma escolha que simplifique de alguma forma nossas somas parciais

$$\mu = \frac{1}{\eta} \Rightarrow a_1 = \frac{M\Upsilon}{\eta} = \frac{S_0}{\eta} \Rightarrow S_1 = S_0 + a_1 = S_0(1 + \frac{1}{\eta}) = 2(\frac{\eta+1}{\eta})$$

Ora, queremos neste momento apenas "dar conta "do primeiro primo 2, de modo que queremos que no numerador de S_1 cresça a potência de 2. Note que conseguimos que nenhum outro primo apareça no numerador de S_1 se escolhermos $\eta = 3$. Assim, com $\eta = 3$, temos $a_1 = \frac{2}{3}$ donde $S_1 = 2 + \frac{2}{3} = \frac{8}{3}$

$S_1 = \frac{8}{3} = \frac{2^3}{3} = 2.666...$, um número mais próximo de e do que 2 na métrica usual e também mais próximo de 0 do que 2 na métrica 2-ádica.

♦ Determinação de a_2 :

Temos $\delta_2 = \ \delta_3 = -S_1 = -\frac{8}{3}$,

$\widetilde{F}_2 = \{2, 3\}$, $\Upsilon = 2^3.3^{-1} = S_1 = -\delta_p$ para $p \in \{2, 3\}$ e $P_2 = 6$.

Determinamos $M \in \{1,...,P_2 - 1\} = \{1, 2,...,5\}$ tal que:

$$\begin{cases} v_2(\delta_2 - M\Upsilon) > v_2(\delta_2) \\ v_3(\delta_3 - M\Upsilon) > v_3(\delta_3) \end{cases}$$

ou seja, como $\Upsilon = -\delta_p$ para $p \in \{2, 3\}$,

$$\begin{cases} v_2(\delta_2) + v_2(1+M) > v_2(\delta_2) \\ v_3(\delta_3) + v_3(1+M) > v_3(\delta_3) \end{cases}$$

ou ainda

$$\begin{cases} 1 + M \equiv 0 \pmod{2} \\ 1 + M \equiv 0 \pmod{3} \end{cases}$$

que nos dá $1 + M \equiv 0 \ (\text{mod} 2.3)$

Mas $M \in \{1, 2, ..., 5\}$ e $1 + M \equiv 0(\text{mod} 2.3)$ implica $M = 5$ e portanto $M\Upsilon = \frac{40}{3}$

Procuramos agora, se possível, $\mu = \frac{1}{\eta}$ com

$$\begin{cases} \eta \equiv 1(\text{mod} 6) \\ \frac{M\Upsilon}{\alpha_\infty - S_1} < \eta < \frac{2M\Upsilon}{\alpha_\infty - S_1} \end{cases}$$

ou seja

$$\begin{cases} \eta \equiv 1(\text{mod} 6) \\ \frac{40}{3\left|e - \frac{8}{3}\right|} < \eta < \frac{80}{3\left|e - \frac{8}{3}\right|} \end{cases}$$

ou ainda

$$\begin{cases} \eta \equiv 1(\text{mod} 6) \\ 258,32.. < \eta < 516,64... \end{cases}$$

o que nos dá $\eta \in \{259, 265, ..., 511\}$.

Mas, novamente tentamos aqui fazer uma escolha que simplifique de alguma forma nossas somas parciais: seria ótimo se nesta série que estamos construindo, apenas um novo número primo fosse introduzido no numerador da soma parcial.

Assim, como

$$S_2 = S_1 + a_2 = \tfrac{8}{3} + \mu\tfrac{40}{3} = \tfrac{8}{3}(1 + \mu.5) = \tfrac{8}{3}(1 + \tfrac{5}{\eta}) = \tfrac{8}{3}\left(\tfrac{\eta+5}{\eta}\right),$$

podemos notar que, se escolhermos $\eta + 5 \equiv 0(\text{mod} 2)$, teremos $v_2\left(\frac{\eta+5}{\eta}\right) > 0$; mas também se $\eta + 5 \equiv 0\left(\text{mod} 3^2\right)$, teremos $v_3\left(\frac{8}{3}\frac{\eta+5}{\eta}\right) > 0$; e, finalmente, se $\eta + 5 \equiv 0(\text{mod} 5)$, teremos $v_5\left(\frac{\eta+5}{\eta}\right) \geq 0$. Portanto, se $\eta + 5 \equiv 0\left(\text{mod} 2.3^2.5\right)$, teremos chances de no numerador de S_2 obter apenas potências de 2 e 3.

Queremos então

$$\eta = 259 + s \quad \text{e} \quad \eta + 5 \equiv 0(\text{mod} 90)$$

Mas

$$259 + s + 5 \equiv 0(\text{mod} 90) \iff s \equiv 6(\text{mod} 90)$$

Assim,

$$\eta = 259 + s = 259 + 6 + 90t = 265 + 90t \ ,$$

o que nos dá

$$\eta + 5 = 270 + 90t.$$

Tomando $t = 0$ temos

$$\eta + 5 = 270 = 2.3^3.5 \Rightarrow$$

$$\begin{aligned} S_2 &= \frac{8}{3}\left(\frac{\eta+5}{\eta}\right) \\ &= \frac{8}{3}\left(\frac{2.3^3.5}{5.53}\right) \\ &= \frac{144}{53} = \frac{2^4 3^2}{53} \cong 2,71698113... \end{aligned}$$

Como $M\Upsilon = \frac{40}{3}$, temos que $a_2 = \frac{40}{3}.\frac{1}{265} = \frac{8}{159}$

S_2 é um número mais próximo de e do que $S_1 = 2,666...$ na métrica usual e também mais próximo de 0 do que $S_1 = \frac{2^3}{3}$ nas métricas 2-ádica e 3-ádica.

Note que a congruência $\eta + 5 \equiv 0(\mathrm{mod}\,5)$ serve apenas para diminuir o numerador, portanto as potênias de 2 e 3 do numerador de S_2 não são tão altas. Se o valor de η satisfazendo $\eta + 5 \equiv 0\left(\mathrm{mod}\,2.3^2.5\right)$ ultrapassasse os limites de η, isto é, $\eta > 511$, teríamos que abrir mão desta condição $\eta + 5 \equiv 0(\mathrm{mod}\,5)$. Tal situação ocorrerá na determinação de a_4.

♦ Determinação de a_3 :

Temos $\delta_2 = \delta_3 = \delta_5 = -S_2 = -\frac{144}{53}$, $\widetilde{F}_3 = \{2,3,5\}$,
$\Upsilon = 2^4.3^2 5^0 = 53.S_2 = -53.\delta_p$, para $p \in \{2,3,5\}$ e $P_3 = 30$.
Determinamos $M \in \{1,2,...,29\}$ tal que:

$$\begin{cases} v_2(\delta_2 - M\Upsilon) > v_2(\delta_2) \\ v_3(\delta_3 - M\Upsilon) > v_3(\delta_3) \\ v_5(\delta_5 - M\Upsilon) > v_5(\delta_5) \end{cases}$$

ou seja como $\Upsilon = -53\delta_p$ para $p \in \{2,3,5\}$,

$$\begin{cases} v_2(\delta_2 - 53M\delta_2) > v_2(\delta_2) \\ v_3(\delta_3 - 53M\delta_3) > v_3(\delta_3) \\ v_5(\delta_5 - 53M\delta_5) > v_5(\delta_5) \end{cases}$$

ou ainda

$$\eta + 53.13 \equiv 0\left(\text{mod } 2.3.5.53^2.13\right) \text{ com } \eta = 1439251 + s. \Leftrightarrow$$
$$1439251 + s + 53.13 \equiv 0\left(\text{mod } 2.3.5.53^2.13\right) \Leftrightarrow$$
$$344430 + s \equiv 0\left(\text{mod } 1095510\right) \Leftrightarrow$$
$$s \equiv 751080\left(\text{mod } 1095510\right) \Leftrightarrow$$
$$s = 751080 + 1095510t$$

Assim,

$$\eta = 1439251 + 751080 + 1095510t$$
$$\eta = 2190331 + 1095510t.$$

Pondo t = 0 temos

$$\eta = 2190331 = 11.13.17^2.53, \text{ donde}$$
$$\eta + 53.13 = 2191020 = 2^2 3.5.13.53^2$$

Assim,

$$S_3 = \frac{144}{53}\left(\frac{\eta+53.13}{\eta}\right)$$
$$= \frac{2^4.3^2.2^2.3.5.13.53^2}{53.11.13.17^2.53}$$

$S_3 = \frac{2^6.3^3.5}{11.17^2} \cong 2,71783579...$, um valor mais próximo de e do que $S_2 \cong 2,7169813...$ na métrica usual e mais próximo de zero do que $S_2 = \frac{2^4.3^2}{53}$ nas métricas 2-ádica, 3-ádica e 5-ádica.

Como $M\Upsilon = 689$ então $a_3 = 689.\frac{1}{2190331} = \frac{2^4.3^2}{11.17^2.53}$

♦ Determinação de a_4 :

Temos $\delta_2 = \delta_3 = \delta_5 = \delta_7 = -S_3 = -\frac{2^6.3^3.5}{11.17^2} = -\frac{8640}{3179}$

$\widetilde{F}_4 = \{2,3,5,7\}$, $\Upsilon = 2^6.3^3.5.7^0 = 8640 = -11.17^2.\delta_p$ e $P_4 = 210$.

Determinamos $M \in \{1,2,3,...,209\}$ tal que:

$$\begin{cases} v_2(\delta_2 - M\Upsilon) > v_2(\delta_2) \\ v_3(\delta_3 - M\Upsilon) > v_3(\delta_3) \\ v_5(\delta_5 - M\Upsilon) > v_5(\delta_5) \\ v_7(\delta_7 - M\Upsilon) > v_7(\delta_7) \end{cases}$$

ou seja , como $\Upsilon = -11.17^2\delta_p$ para $p \in \{2,3,5,7\}$,

$$\begin{cases} v_2(\delta_2 + 11.17^2M\delta_2) > v_2(\delta_2) \\ v_3(\delta_3 + 11.17^2M\delta_3) > v_3(\delta_3) \\ v_5(\delta_5 + 11.17^2M\delta_5) > v_5(\delta_5) \\ v_7(\delta_7 + 11.17^2M\delta_7) > v_7(\delta_7) \end{cases}$$

ou ainda

$$\begin{cases} v_2(1+11.17^2.M) > 0 \\ v_3(1+11.17^2.M) > 0 \\ v_5(1+11.17^2.M) > 0 \\ v_7(1+11.17^2.M) > 0 \end{cases}$$

o que nos dá $M \in \{1,2,...,209\}$ e $1+3179M \equiv 0\left(mod\ 2.3.5.7\right)$.

Mas

$1+3179M \equiv 0\left(\text{mod}\ \ 210\right) \Leftrightarrow$

$3179M \equiv -1\left(\text{mod}\ \ 210\right) \Leftrightarrow$

$29M \equiv -1\left(\text{mod}\ \ 210\right)$

$M \equiv -1.29^{-1}\left(\text{mod}\ \ 210\right)$, já que $mdc(29,210) = 1$

$M \equiv 181\left(\text{mod}\ \ 210\right)$

Assim $M \in \{1,2,...,209\}$ e $M \equiv 181\left(mod\ 210\right)$ o que implica $M = 181$, donde $M\Upsilon = 181.2^6.3^3.5$

Procuramos agora, se possível, $\mu = \frac{1}{\eta}$ com

$$\begin{cases} \eta \equiv 1(\text{mod}210) \\ \frac{M\Upsilon}{|\alpha_\infty - S_3|} < \eta < \frac{2M\Upsilon}{|\alpha_\infty - S_3|} \end{cases}$$

ou seja

$$\begin{cases} \eta \equiv 1(\text{mod}210) \\ \frac{1563840}{|e-\frac{8640}{3179}|} < \eta < \frac{2.1563840}{|e-\frac{8640}{3179}|} \end{cases}$$

o que nos dá

$$\begin{cases} \eta \equiv 1(\text{mod}210) \\ 3506123699,3... < \eta < 7012247398,7... \end{cases}$$

Como $\eta \equiv 1(\text{mod}210)$ então :

$\eta \in \{3506123881 + 210n'/\ n' = 0,1,2,....,16695826\}$

Novamente tentamos escolher um η que simplifique a nova soma parcial.

Note que $S_4 = S_3 + \mu M\Upsilon = \frac{8640}{3179} + \mu 1563840$

$$= \frac{2^6.3^3.5}{11.17^2} + \mu 2^6.3^3.5.181$$

$$= \frac{2^6.3^3.5}{11.17^2}\left(1+11.17^2.181\mu\right)$$

$$= \frac{2^6.3^3.5}{11.17^2}\left(\frac{\eta+11.17^2.181}{\eta}\right)$$

Assim, procuramos $\eta = 3506123881 + s$, tal que

$$\eta + 11.17^2.181 \equiv 0\left(\mathrm{mod}\ 2.3.5.7.11^2.17^4\right)$$

Teremos $3506123881 + s + 11.17^2.181 \equiv 0(\mathrm{mod}\, 2122268610) \Leftrightarrow$

$$s + 3506699280 \equiv 0\left(\mathrm{mod}\ 2122268610\right) \Leftrightarrow$$

$$s \equiv -3506699280\left(\mathrm{mod}\ 2122268610\right) \Leftrightarrow$$

$$s \equiv 737837940\left(\mathrm{mod}\ 2122268610\right) \Leftrightarrow$$

$$s = 737837940 + 2122268610\, t$$

Assim, $\eta = 3506123881 + 737837940 + 2122268610\, t$

$$\eta = 4243961821 + 2122268610\, t.$$

Pondo t = 0 temos

$$\eta = 4243961821 = 11 \times 17^2 439 \times 3041 \text{ donde,}$$

$$\eta + 11.17^2.181 = 4244537220 = 2^2 3 \times 5 \times 7 \times 11^2 17^4$$

Daí,

$$S_4 = \frac{2^6.3^3.5}{11.17^2}\left(\frac{\eta + 11.17^2.181}{\eta}\right)$$

$$= \frac{2^6.3^3.5}{11.17^2}\left(\frac{2^2 \times 3 \times 5 \times 7 \times 11^2.17^4}{11 \times 17^2 \times 439.3041}\right)$$

$$S_4 = \frac{2^8.3^4.5^2.7}{439.3041} \cong 2.7182042833$$

Como $M\Upsilon = 181.2^6.3^3.5$ então

$$a_4 = 181.2^6.3^3.5.\frac{1}{11 \times 17^2 439 \times 3041} = \frac{1563840}{4243961821}$$

♦ Determinação de a_5 :

Temos $\delta_2 = \delta_3 = \delta_5 = \delta_7 = \delta_{11} = -S_4 = -\frac{2^8.3^4 5^2.7}{439.3041} = -\frac{3628800}{1334999}$

$\widetilde{F}_5 = \{2,3,5,7,11\}$, $\Upsilon = 2^8 3^4 5^2 7.11^0 = -1334999\delta_p$ e $P_5 = 2310$

Determinamos $M \in \{1,2,3,...,2309\}$ tal que:

$$\begin{cases} v_2(\delta_2 - M\Upsilon) > v_2(\delta_2) \\ v_3(\delta_3 - M\Upsilon) > v_3(\delta_3) \\ v_5(\delta_5 - M\Upsilon) > v_5(\delta_5) \\ v_7(\delta_7 - M\Upsilon) > v_7(\delta_7) \\ v_{11}(\delta_{11} - M\Upsilon) > v_{11}(\delta_{11}) \end{cases}$$

ou seja como $\Upsilon = -439.3041\delta_p = -1334999\delta_p$

$$\begin{cases} \nu_2(\delta_2 + 1334999\delta_2 M) > \nu_2(\delta_2) \\ \nu_3(\delta_3 + 1334999\delta_3 M) > \nu_3(\delta_3) \\ \nu_5(\delta_5 + 1334999\delta_5 M) > \nu_5(\delta_5) \\ \nu_7(\delta_7 + 1334999\delta_7 M) > \nu_7(\delta_7) \\ \nu_{11}(\delta_{11} + 1334999\delta_{11} M) > \nu_{11}(\delta_{11}) \end{cases}$$

ou ainda

$$\begin{cases} \nu_2(1 + 1334999M) > 0 \\ \nu_3(1 + 1334999M) > 0 \\ \nu_5(1 + 1334999M) > 0 \\ \nu_7(1 + 1334999M) > 0 \\ \nu_{11}(1 + 1334999M) > 0 \end{cases}$$

O que nos dá $M \in \{1, 2, ..., 2309\}$ e $1334999M + 1 \equiv 0 \pmod{2.3.5.7.11} \Leftrightarrow$

$$2129M + 1 \equiv 0 \pmod{2310} \Leftrightarrow$$
$$M \equiv -1.2129^{-1} \pmod{2310} \Leftrightarrow$$
$$M \equiv -1.1289 \pmod{2310} \Leftrightarrow$$
$$M \equiv 1021 \pmod{2310}$$

Assim $M = 1021$ donde $M\Upsilon = 2^8.3^4.5^2.7.1021 = 3705004800$

Procuramos agora se possível, $\mu = \frac{1}{\eta}$ com

$$\begin{cases} \eta \equiv 1(\mathrm{mod} 2310) \\ \frac{M\Upsilon}{|\alpha_\infty - S_4|} < \eta < \frac{2M\Upsilon}{|\alpha_\infty - S_4|} \end{cases}$$

ou seja

$$\begin{cases} \eta \equiv 1(\mathrm{mod} 2310) \\ \frac{3705004800}{\left|e - \frac{3628800}{1334999}\right|} < \eta < \frac{2.3705004800}{\left|e - \frac{3628800}{1334999}\right|} \end{cases}$$

o que nos dá

$$\begin{cases} \eta \equiv 1(\mathrm{mod} 2310) \\ 47778672453600 < \eta < 95557344907200 \end{cases}$$

isto é, $\eta \in \{47778672452281, 47778672452281 + 2310n', n' = 0, 1, 2, ..., 20683407988\}$

Vamos escolher um η que simplifique a nova soma parcial:

$$S_5 = S_4 + \mu M\Upsilon = \frac{2^8.3^4.5^2.7}{439.3041} + 2^8.3^4.5^2.7\ \mu$$
$$= \frac{2^8.3^4.5^2.7}{439.3041}\left(1 + 439.3041.\frac{1}{\eta}\right)$$
$$= \frac{2^8.3^4.5^2.7}{439.3041}\left(\frac{\eta + 439.3041}{\eta}\right)$$

Procuramos η tal que $\eta + 439.3041 \equiv 0\left(\text{mod } 2.3.5.7.11.439.3041^2\right)$ Mas

$$\begin{cases} \eta + 439.3041 \equiv 0 \ (\text{mod } 2.3.5.7.11.439.3041^2) \\ \eta = 47778672452281 + s \end{cases} \Leftrightarrow$$

$$47778672452281 + s + 1334999 \equiv 0\left(\text{mod } 2.3.5.7.11.439.3041^2\right) \Leftrightarrow$$
$$s \equiv -47\,778\,673\,787\,280\left(\text{mod } 9377980825290\right) \Leftrightarrow$$
$$s \equiv 8489\,211\,164\,460\left(\text{mod } 9377980825290\right)$$

Então

$$s = 8489\,211\,164\,460 + 9377980825290t$$

Daí

$$\eta = 47778672452281 + 8489\,211\,164\,460 + 9377980825290t$$
$$\eta = 56\,267\,883\,616\,741 + 9377980825290t$$

Pondo $t = 0$ temos $\eta = 56\,267\,883\,616\,741$

$$56\,267\,883\,616\,741 = 23 \times 439 \times 607 \times 3019 \times 3041$$

donde

$$\eta + 439.3041 = 2^2 3^2 5 \times 7 \times 11 \times 439 \times 3041^2$$

Daí,

$$S_5 = \frac{2^8.3^4.5^2.7}{439.3041}\left(\frac{\eta + 439.3041}{\eta}\right)$$
$$S_5 = \frac{2^8.3^4.5^2.7}{439.3041}\left(\frac{2^2.3^2.5.7.11.439.3041^2}{23.439.607.3019.3041}\right)$$
$$= \frac{2^{10}.3^6.5^3.7^2.11}{23.439.607.3019}$$

Ou $$= \frac{50295168000}{18503085701} \cong 2,71820434779$$

Como $M\Upsilon = 1021.2^8.3^4.5^2.7$ então

$$a_5 = \frac{1021.2^8.3^4.5^2.7}{23.439.607.3019.3041} = \frac{3705\,004\,800}{56\,267\,883\,616\,741}$$

♦ Determinação de a_6 :

Temos

$$\delta_2 = \delta_3 = \delta_5 = \delta_7 = \delta_{11} = \delta_{13} = -S_5 = -\frac{2^{10}.3^6.5^3.7^2.11}{18503085701} = -\frac{50295168000}{18503085701}$$

$\widetilde{F}_5 = \{2,3,5,7,11,13\}$, $\Upsilon = 2^{10}.3^6.5^3.7^2.11.13^0 = -18503085701\delta_p$

$\Upsilon = -18503085701\delta_p$ para $p \in \{2,3,5,7,11\}$ e $P_6 = 30030$.

Determinamos $M \in \{1,2,3,...,30329\}$ tal que:

$$\begin{cases} \nu_2(\delta_2 - M\Upsilon) > \nu_2(\delta_2) \\ \nu_3(\delta_3 - M\Upsilon) > \nu_3(\delta_3) \\ \nu_5(\delta_5 - M\Upsilon) > \nu_5(\delta_5) \\ \nu_7(\delta_7 - M\Upsilon) > \nu_7(\delta_7) \\ \nu_{11}(\delta_{11} - M\Upsilon) > \nu_{11}(\delta_{11}) \\ \nu_{13}(\delta_{13} - M\Upsilon) > \nu_{13}(\delta_{13}) \end{cases}$$

ou seja

$$\begin{cases} \nu_2(\delta_2 + 18503085701\delta_2 M) > \nu_2(\delta_2) \\ \nu_3(\delta_3 + 18503085701\delta_3 M) > \nu_3(\delta_3) \\ \nu_5(\delta_5 + 18503085701\delta_5 M) > \nu_5(\delta_5) \\ \nu_7(\delta_7 + 18503085701\delta_7 M) > \nu_7(\delta_7) \\ \nu_{11}(\delta_{11} + 18503085701\delta_{11} M) > \nu_{11}(\delta_{11}) \\ \nu_{13}(\delta_{13} + 18503085701\delta_{13} M) > \nu_{13}(\delta_{13}) \end{cases}$$

ou ainda

$$\begin{cases} \nu_2(1 + 18503085701M) > 0 \\ \nu_3(1 + 18503085701M) > 0 \\ \nu_5(1 + 18503085701M) > 0 \\ \nu_7(1 + 18503085701M) > 0 \\ \nu_{11}(1 + 18503085701M) > 0 \\ \nu_{13}(1 + 18503085701M) > 0 \end{cases}$$

O que nos dá $M \in \{1, 2, 3, ..., 30029\}$ e $M18503085701 + 1 \equiv 0 (\mathrm{mod}\, 2.3.5.7.11.13)$.

$$\begin{aligned} &18503085701M + 1 \equiv 0(\mathrm{mod}\, 30030) \Leftrightarrow \\ &11111M \equiv -1(\mathrm{mod}\, 30030) \Leftrightarrow \\ &M \equiv -1.11111^{-1}(\mathrm{mod}\, 30030) \Leftrightarrow \\ &M \equiv -21011(\mathrm{mod}\, 30030) \\ &M \equiv 9019(\mathrm{mod}\, 30030) \end{aligned}$$

Assim $M \in \{1, 2, 3, ..., 30029\}$ e $M \equiv 9019(\mathrm{mod}\, 30030)$, donde

$$\begin{aligned} &M\Upsilon = 2^{10}.3^6.5^3.7^2.11.9019 = \\ &2^{10} \times 3^6 \times 5^3 \times 7^2 \times 11 \times 9019 = 453\,612\,120\,192\,000 \\ &453\,612\,120\,192\,000 \div .00007748067 = 5.8545 \times 10^{18} = 5.8545 \times 10^{18} \end{aligned}$$

Procuramos agora se possível, $\mu = \frac{1}{\eta}$ com

Como $M\Upsilon = 9019.2^{10}.3^6.5^3.7^2.11$ então

$$a_6 = \frac{9019.2^{10}.3^6.5^3.7^2.11}{10022605676705441821} = \frac{453612120192000}{10022605676705441821}$$

Temos assim:

$S_o = 2$

$S_1 = 2 + \frac{2}{3} = \frac{8}{3} = \frac{2^3}{3} = 2,66666666...$

$S_2 = \frac{8}{3} + \frac{8}{159} = \frac{144}{53} = \frac{2^4 3^2}{53} \simeq 2,71698113208$

$S_3 = \frac{144}{53} + \frac{2^4.3^2}{11.17^2.53} = \frac{8640}{3179} = \frac{2^6 3^3 5}{11.17^2} \simeq 2,71783579742$

$S_4 = \frac{8640}{3175} + \frac{2^6.3^3.5.181}{11.17^2.439.3041} = \frac{2^8.3^4.5^2.7}{439.3041} \simeq 2.7182042833$

$S_5 = \frac{1814400}{667589} + \frac{3705004800}{56267883616741} = \frac{2^{10}3^6 5^3 7^2 11}{23.439.607.3019} \simeq 2,71820434779$

$S_6 = \frac{4191264000}{1542130589} + \frac{453612120192000}{10022605676705441821} = \frac{2^{12}3^7 5^4 7^3 11^2 13}{23.439.607.3019.19.109} \simeq 2,71824960668$

...

Exemplo 2. Construção de uma série $\sum_{n=0}^{\infty} a_n$ de números racionais positivos que converge para -2 em $\mathbb{Q}_p$, para todo $p \in V_{\mathbb{Q}}$. (e assim estaremos exemplificando a questão original de Koblitz)

Temos aqui que $\alpha_\infty = -2 \in \mathbb{Z}$ e $\alpha_p = -2$ para todo p.

Então $a_0 = [\alpha_\infty - 1] = -3$; assim, $S_0 = -3$

Aqui já podemos observar que, para $N \geq 1$, teremos sempre $\widetilde{F}_N = F_N$.

De fato para cada $N \geq 1$ e para cada $p \in F_N$, $\delta_p = -2 - S_{N-1}$ que é sempre não nulo pois $S_0 = -3 < -2$ e a seqüência (S_n) é monótona crescente e converge a -2.

♦ Determinação de a_1 :

Temos $\delta_2 = -2 + 3 = 1 \qquad \widetilde{F}_1 = \{2\} \qquad P_1 = 2 \qquad \Upsilon = 2^0 = 1$

Determinamos $M \in \{1\}$ tal que $|\delta_2 - M\Upsilon|_2 < |\delta_2|_2$ isto é, $|1 - M|_2 < 1$ o que nos dá $M = 1$ e $M\Upsilon = 1$

Determinamos se possível $\mu = \frac{1}{\eta}$ com

$$\begin{cases} \eta \equiv 1(\mathrm{mod}\,2) \\ \frac{M\Upsilon}{\alpha_\infty - S_0} < \eta < \frac{2M\Upsilon}{\alpha_\infty - S_0} \end{cases}$$

ou seja

$$\begin{cases} \eta \equiv 1(\mathrm{mod}\,2) \\ \frac{1}{-2+3} < \eta < \frac{2}{-2+3} \end{cases}$$

ou ainda

$$\begin{cases} \eta \equiv 1(\mathrm{mod}\,2) \\ 1 < \eta < 2 \end{cases}$$

o que não é possível.

Assim, passamos a procurar $\mu \in U(2)$ tal que $\frac{-2+3}{2} < \mu < \frac{-2+3}{1}$, isto é,

$$\mu = \frac{r}{t} \text{ com } \begin{cases} r \equiv 1(\mathrm{mod}\,2) \\ t \equiv 1(\mathrm{mod}\,2) \\ \frac{1}{2} < \frac{r}{t} < 1 \end{cases}$$

o que nos dá infinitas possibilidades: de fato note que necessariamente temos $t \geq 5$ e se tomarmos r ímpar satisfazendo $r < t < 2r$, teremos todas as condições satisfeitas. Passamos então a tentar escolher r e t de modo a simplificar a nova soma parcial; mais precisamente: simplificar $S_1 + 2$, já que (S_N) converge a -2 se e só se $(S_N + 2)$ converge a zero. Isto significa que seria ótimo se na fração $S_N + 2$ apenas os N primeiros primos aparecessem no numerador. Mas como $a_1 = \mu M\Upsilon = \mu$, temos

$$S_1 + 2 = -3 + \tfrac{r}{t} + 2 = -1 + \tfrac{r}{t} = \tfrac{r-t}{t}$$

e portanto, se tomarmos r e t ímpares com $t \geq 5$ e $t < 2r$ teremos por exemplo $a_1 = \frac{r}{t} = \frac{3}{5}$

Assim $a_1 = \mu M\Upsilon = \frac{3}{5}$ e

$S_1 = -3 + \frac{3}{5} = -\frac{12}{5}$

$S_1 = -2{,}4$

$S_1 + 2 = -\frac{12}{5} + 2 = -\frac{2}{5}$

♦ Determinação de a_2 :

Temos $\delta_2 = \delta_3 = -2 + \frac{12}{5} = \frac{2}{5}$, $\widetilde{F}_2 = \{2,3\}$ $P_2 = 6$, $\Upsilon = 2.3^0 = 2$

Determinamos $M \in \{1,2,...,5\}$ tal que

$$\begin{cases} \nu_2(\delta_2 - M\Upsilon) > \nu_2(\delta_2) \\ \nu_3(\delta_3 - M\Upsilon) > \nu_3(\delta_3) \end{cases}$$

ou seja, para $p \in \{2,\ 3\}$, $\nu_p(\frac{2}{5} - 2M) = \nu_p\left(\frac{2}{5}\right) + \nu_p(1 - 5M)$, então

$$\begin{cases} \nu_2(1 - 5M) > 0 \\ \nu_3(1 - 5M) > 0 \end{cases}$$

o que nos dá

$$1 - 5M \equiv 0 (\text{mod } 6) \Leftrightarrow$$
$$-5M \equiv -1 (\text{mod } 6) \Leftrightarrow$$
$$M \equiv 5 (\text{mod } 6) \Leftrightarrow$$

Assim $M = 5$ e $M\Upsilon = 10$

Procuramos agora, se possível, $\mu = \frac{1}{\eta}, \mu \in U(6)$ com

$$\begin{cases} \eta \equiv 1 (\text{mod} 6) \\ \frac{M\Upsilon}{-2-S_1} < \eta < \frac{2M\Upsilon}{-2-S_1} \end{cases}$$

ou seja

$$\begin{cases} \eta \equiv 1 (\text{mod} 6) \\ \frac{10}{-2+\frac{12}{5}} < \eta < \frac{20}{-2+\frac{12}{5}} \end{cases}$$

ou ainda

$$\begin{cases} \eta \equiv 1(\bmod 6) \\ 25 < \eta < 50 \end{cases}$$

o que nos dá, $\eta \in \{31, 37, 43, 49\}$

Vamos tentar fazer uma escolha que simplifique a fração $S_2 + 2$, isto é, se possível no seu numerador tenha apenas os fatores $2^2.3$.

Se $a_2 = \frac{M\Upsilon}{\eta} = \frac{10}{31}$

$S_2 + 2 = -\frac{12}{5} + \frac{10}{31} + 2 = -\frac{12}{155} = -\frac{2^2.3}{5.31}$

$S_2 = -\frac{12}{5} + \frac{10}{31} = -\frac{322}{155}$

$S_2 = -2,07741935.$ e

Note que $|S_2 + 2|_2 < |S_1 + 2|_2$ e $|S_2 + 2|_3 < |S_1 + 2|_3$

♦ Determinação de a_3 :

Temos:

$\delta_2 = \delta_3 = \delta_5 = -2 + \frac{322}{155} = \frac{12}{155}$; $P_3 = 30$; $\widetilde{F}_3 = \{2,3,5\}$ $\Upsilon = 2^2.3.5^{-1} = \frac{12}{5}$

Determinamos $M \in \{1, 2, ..., 29\}$ tal que

$$\begin{cases} v_2(\delta_2 - M\Upsilon) > v_2(\delta_2) \\ v_3(\delta_3 - M\Upsilon) > v_3(\delta_3) \\ v_5(\delta_5 - M\Upsilon) > v_5(\delta_5) \end{cases}$$

ou seja, como $\Upsilon = \frac{12}{5}$ e $v_p(\frac{12}{155} - M\frac{12}{5}) = v_p(\frac{12}{155}) + v_p(1 - M31)$ então

$$\begin{cases} v_2(1 - M31) > 0 \\ v_3(1 - M.31) > 0 \\ v_5(1 - M.31) > 0 \end{cases}$$

o que nos dá $1 - M31 \equiv 0(\bmod 30)$

$- \ M \equiv -1(\bmod 30)$

$M \equiv 1(\bmod 30)$

Assim, $M = 1$ e $M\Upsilon = \frac{12}{5}$

Procuramos agora, se possível, $\mu = \frac{1}{\eta}, \mu \in U(30)$ com

$$\begin{cases} \eta \equiv 1(\bmod 30) \\ \frac{M\Upsilon}{-2-S_2} < \eta < \frac{2M\Upsilon}{-2-S_2} \end{cases}$$

ou seja

$$\left\{\begin{array}{c} \eta \equiv 1(\bmod 30) \\ \frac{\frac{12}{5}}{-2+\frac{322}{155}} < \eta < \frac{2.\frac{12}{5}}{-2+\frac{322}{155}} \end{array}\right.$$

ou ainda

$$\left\{\begin{array}{l} \eta \equiv 1(\bmod 30) \\ 31 < \eta < 62 \end{array}\right.$$

o que nos dá, $\eta = 61$

$a_3 = \mu M\Upsilon = \frac{12}{5.61}$ então

$S_3 + 2 = S_2 + a_3 + 2 = -\frac{322}{155} + \frac{12}{305} + 2$

$= -\frac{360}{9455} = -\frac{2^3.3^2.5}{5.31.61} = \frac{2^3.3^2}{31.61}$

$S_3 = -\frac{322}{155} + \frac{12}{305} = -\frac{3854}{1891} = -2,03807509$

♦ Determinação de a_4 :

Definimos $\delta_2 = \delta_3 = \delta_5 = \delta_7 = -2 + \frac{3854}{1891} = \frac{72}{1891} = \frac{2^3.3^2}{31.61}$

$P_4 = 210$; $\Upsilon = 2^3.3^2.5^0.7^0 = 72$, $\widetilde{F}_4 = \{2,3,5,7\}$

Determinamos M tal que $v_p(\delta_p - M\Upsilon) > v_p(\delta_p)$ para $p = 2,3,5,7$. ou

$v_p(\frac{72}{1891} - M72) > v_p(\frac{72}{1891})$

Como $v_p(\frac{72}{1891} - M72) = v_p(\frac{72}{1891}) + v_p(1 - M1891)$ então

$v_p(1 - M1891) > 0$ para $p = 2,3,5,7$ o que equivale a:

$1 - M1891 \equiv 0\left(\bmod\ 210\right) \Leftrightarrow$

$-1891M \equiv -1\left(\bmod\ 210\right) \Leftrightarrow$

$-M \equiv -1\left(\bmod\ 210\right) \Leftrightarrow$

$M \equiv 1\left(\bmod\ 210\right)$

Assim $M = 1$ e $M\Upsilon = 72$

Procuramos agora, se possível, $\mu = \frac{1}{\eta}, \mu \in U(210)$ com

$$\left\{\begin{array}{c} \eta \equiv 1(\bmod 210) \\ \frac{M\Upsilon}{-2-S_3} < \eta < \frac{2M\Upsilon}{-2-S_3} \end{array}\right.$$

ou seja

$$\left\{\begin{array}{c} \eta \equiv 1(\bmod 210) \\ \frac{72}{\frac{72}{1891}} < \eta < \frac{2.72}{\frac{72}{1891}} \end{array}\right.$$

ou ainda

$$\begin{cases} \eta \equiv 1(\text{mod}\, 210) \\ 1891 < \eta < 3782 \end{cases}$$

o que nos dá, $\eta \in \{2101, 2101 + 210n', \; n' = 1, 2, ..., 8\}$

Vamos tentar fazer uma escolha que simplifique a fração $S_4 + 2$, isto é, se possível no seu numerador tenha apenas os fatores $2^4.3^3.5.7$.Então

$$S_4 + 2 = S_3 + \mu M\Upsilon + 2 = -\tfrac{19270}{9455} + \tfrac{72}{\eta} + 2$$
$$= -\tfrac{72}{1891} + \tfrac{72}{\eta}$$
$$= -\tfrac{72}{1891}(1 - \tfrac{1891}{\eta})$$
$$= -\tfrac{72}{1891}\left(\tfrac{\eta - 1891}{\eta}\right)$$

Queremos $\eta - 1891 \equiv 0(\text{mod}\, 2.3.5.7)$ com $\eta = 2101 + s$, isto é,

$2101 + s - 1891 \equiv 0(\text{mod}\, 210) \Leftrightarrow$

$s \equiv -210(\text{mod}\, 210) \Leftrightarrow$

$s = 0 + 210t$ e $\eta = 2101 + 210t$

Tomando $t = 0$, temos:

$\eta = 2101$ e $a_4 = \mu M\Upsilon = \frac{72}{2101}$

$$S_4 + 2 = -\tfrac{72}{1891}\left(\tfrac{\eta - 1891}{\eta}\right)$$
$$= -\tfrac{15120}{1891.2101} = -\tfrac{2^4.3^3.5.7}{11.31.61.191}$$
$$S_4 = S_3 + a_4 = -\tfrac{3854}{1891} + \tfrac{72}{2101}$$
$$= -\tfrac{7961102}{3972991} = -2,003805697$$

♦ Determinação de a_5 :

Definimos

$$\delta_2 = \delta_3 = \delta_5 = \delta_7 = \delta_{11} = -2 + \tfrac{7961102}{3972991} = \tfrac{15120}{3972991} = \tfrac{2^4.3^3.5.7}{11.361181}$$

$P_5 = 2310$; $\Upsilon = 2^4.3^3.5.7.11^{-1} = \frac{15120}{11}$, $\widetilde{F}_5 = \{2, 3, 5, 7, 11\}$

Determinamos M tal que $v_p(\delta_p - M\Upsilon) > v_p(\delta_p)$ para $p = 2, 3, 5, 7, 11.$ ou

$v_p(\frac{15120}{3972991} - M\frac{15120}{11}) > v_p(\frac{15120}{3972991})$

Como $v_p(\frac{15120}{3972991} - M\frac{15120}{11}) = v_p(\frac{15120}{3972991}) + v_p(1 - M361181)$ então

$v_p(1 - M361181) > 0$ para $p = 2, 3, 5, 7, 11$ o que equivale a:

$1 - M361181 \equiv 0\left(\text{mod } 2310\right) \Leftrightarrow$

$M821 \equiv 1\left(\text{mod } 2310\right) \Leftrightarrow$

$M \equiv 821^{-1}\left(\text{mod } 2310\right) \Leftrightarrow$

$M \equiv 1691 \pmod{2310}$

Assim $M = 1691$ e $M\Upsilon = \frac{1691.15120}{11} = \frac{25567920}{11}$

Procuramos agora, se possível, $\mu = \frac{1}{\eta}, \mu \in U(2310)$ com

$$\begin{cases} \eta \equiv 1 (\bmod 2310) \\ \frac{M\Upsilon}{-2-S_4} < \eta < \frac{2M\Upsilon}{-2-S_4} \end{cases}$$

ou seja

$$\begin{cases} \eta \equiv 1 (\bmod 2310) \\ \frac{\frac{25567920}{11}}{\frac{15120}{3972991}} < \eta < \frac{2.\frac{25567920}{11}}{\frac{15120}{3972991}} \end{cases}$$

ou ainda

$$\begin{cases} \eta \equiv 1 (\bmod 2310) \\ 610757071 < \eta < 1221514142 \end{cases}$$

o que nos dá, $\eta \in \{610759381, 610759381 + 2310n', \ n' = 1, 2, ..., 264300\}$

Vamos tentar fazer uma escolha que simplifique a fração $S_5 + 2$, isto é, se possível no seu numerador tenha apenas os fatores $2^5.3^4.5^2.7^2.11$.Então

$$\begin{aligned} S_5 + 2 = S_4 + \mu M\Upsilon + 2 &= -\frac{7961102}{3972991} + \frac{25567920}{11\eta} + 2 \\ &= -\frac{15120}{1891.2101} + \frac{25567920}{11\eta} \\ &= -\frac{15120}{3972991}\left(1 - \frac{610757071}{\eta}\right) \\ &= -\frac{15120}{11.31.61.191}\left(\frac{\eta - 610757071}{\eta}\right) \end{aligned}$$

Queremos $\eta - 610757071 \equiv 0 (\bmod 2.3.5.7.11^2)$ com $\eta = 610759381 + s$,

isto é,

$610759381 + s - 610757071 \equiv 0(\bmod 25410) \Leftrightarrow$

$s + 2310 \equiv 0(\bmod 25410) \Leftrightarrow$

$s = 23100 + 25410t$ e $\eta = 610759381 + 23100 + 25410t$

Tomando $t = 0$, temos:

$\eta = 610782481$ e $a_5 = \mu M\Upsilon = \frac{25567920}{11\eta} = \frac{25567920}{6718607291}$

$$\begin{aligned} S_5 + 2 &= -\frac{15120}{11.31.61.191}\left(\frac{\eta - 610757071}{\eta}\right) \\ &= -\frac{15120}{11.31.61.191}\left(\frac{610782481 - 610757071}{610782481}\right) \\ &= -\frac{15120}{11.31.61.191}\left(\frac{25410}{610782481}\right) \\ &= -\frac{2^4.3^3.5.7}{11.31.61.191} \cdot \frac{2.3.5.7.11^2}{103.109.54403} \\ &= -\frac{2^5.3^4.5^2.7^2.11}{11.31.61.191.103.109.54403} \end{aligned}$$

$$\begin{aligned} S_5 = S_4 + a_5 &= -\frac{7961102}{3972991} + \frac{25567920}{6718\,607\,291} \\ &= -\frac{53\,385\,936\,825\,545\,962}{26\,692\,966\,299\,677\,381} \\ &= -2,00000015832 \end{aligned}$$

Temos assim:

$S_0 = -3$

$S_1 = -\frac{12}{5} = -2,4$ e $S_1 + 2 = -\frac{2}{5}$

$S_2 = -\frac{322}{155} = -2,07741935484$ e $S_2 + 2 = -\frac{12}{155} = -\frac{2^2.3}{5.31}$

$S_3 = -\frac{3854}{1891} = -2,03807509254$ e $S_3 + 2 = -\frac{360}{9455} = -\frac{2^3.3^2.5}{5.31.61} = -\frac{2^3.3^2}{31.61}$

$S_4 = -\frac{7961102}{3972991} = -2,003805697$ e $S_4 + 2 = -\frac{15120}{3972991} = -\frac{2^4.3^3.5.7}{11.31.61.191}$

$S_5 = -\frac{53\,385\,936\,825\,545\,962}{26\,692\,966\,299\,677\,381} = -2,00000015832$

e $S_5 + 2 = -\frac{2^5.3^4.5^2.7^2.11}{11.31.61.191.103.109.54403}$

Referências Bibliográficas

[B]: BOMBIERI, E. *Analytic Number Theory and Diophantine Problems*, Birkhauser, 1987

[B-S]: BURGER, E.B; STRUPPECK,T. *Does* $\sum \frac{1}{n!}$ *really converge? Infinite series and p-adic analysis.* Am. Math. Monthly, vol 103 #7 (1996) 565-577

[E]: ENDLER, O.. *Valuation Theory*, Springer-Verlag, 1970

[F]: FIGUEIREDO, D. G. *Números irracionais e transcendentes. SBM*, 1980.

[G]: GOUVÊA, F. *Primeiros Passos p-Ádicos*, 17^0 Colóquio Brasileiro de Matemática. IMPA, 1989

[G2]: GOUVÊA, F. *p –Adic Numbers*, Universitext, Springer-Verlag, 1993

[G-R-S]: GODINHO, H; RIPOLL,C; SOARES, M *Mini-Curso:Funções-Zeta Clássicas e Modernas.* XV Escola de Álgebra, IM/UFRGS, 1998

[L]: LANG, S. *Algebra*, Addison-Wesley Pub.Co.Inc., Reading, USA, 1965

[Ma]: MAHLER,K. *p –Adic Numbers and their Functions*, Cambridge Univ. Press, 1981

[M]: MONTEIRO, L. H; *Elementos de Algebra.* Livros Técnicos e Científicos,Rio de Janeiro,1978

[K]: KOBLITZ, N. *p-Adic Numbers, p-adic analysis and Zeta Functions, Graduate Texts in Mathematics* 58. Springer-Verlag, 1984 (2nd. edition)

[S-S-G]: SHOKRANIAN,M; SOARES; GODINHO,H. *Teoria dos números.* Editora Universidade de Brasília, 2^aedição, 1999

[Sk]: SCHIKHOF,W.H. Schikhof, *Ultrametric Calculus -An Introduction to p-Adic Analysis.* Cambridge Univ. Press, 1984

[Sm]: SCHMIDT, W. M. *Diophantine Equations and Aproximation.* Springer Lecture Notes in Mathematics 1467, 1991

[V]: VISWANATHAN, "*Introdução à Álgebra e Aritmética*", *Monografias de Matemática* n^o33. IMPA, Rio de Janeiro, 1979