Convergência de séries p-ádicas

Maria Pires de Carvalho, João Nuno P. Lourenço[1]

Departamento de Matemática / Centro de Matemática
Faculdade de Ciências da Universidade do Porto
Rua do Campo Alegre, 687, 4169-007 Porto
e-mail: mpcarval@fc.up.pt; up201200326@fc.up.pt

Resumo: Habituados a trabalhar com os números reais e a noção usual de distância, estranhamos o impacto que uma mudança na métrica pode provocar. Fixado um primo p, a norma p-ádica nos racionais mede cada número relativamente às potências de p, indicando que uma fracção irredutível é pequena se o numerador for divisível por uma potência positiva elevada de p. Este modo aritmético de estimar distâncias é drasticamente distinto do valor absoluto usual e, em particular, a família de sucessões convergentes é diferente da que encontramos em $\mathbb{R}$. Daremos aqui atenção à existência de séries de termos racionais cuja convergência não dependa da norma utilizada e tais que os respectivos limites, embora variem com a métrica, o façam de um modo que saibamos controlar.

Abstract: Accustomed to working with the real numbers and the usual notion of distance, we wonder at the impact that a change in the metric can cause. Given a prime p, the p-adic norm of a rational number measures its size with respect to the powers of p, declaring that an irreducible fraction is small if its numerator is divisible by a high positive power of p. This arithmetic method to estimate distances is quite different from the common absolute value and, in particular, the family of convergent sequences is distinct from the real one. We will concern ourselves with the existence of series with rational terms whose convergence holds no matter the chosen norm and such that, though their limits vary with the metric, we know how to master this dependence.

palavras-chave: Número primo; série; norma p-ádica.

keywords: Prime number; series; p-adic norm.

[1]Este artigo foi escrito no âmbito do Programa Novos Talentos em Matemática, da Fundação Calouste Gulbenkian. MPC tem sido parcialmente financiada pelo CMUP (UID/MAT/00144/2013) através da FCT (Portugal), com fundos nacionais (MEC) e europeus estruturais do programa FEDER, no âmbito do acordo PT2020. Os autores agradecem os comentários do revisor, que permitiram melhorar a redacção deste texto.

1 Introdução

É possível exprimir todo o elemento não constante do espaço $\mathbb{C}[X]$ dos polinómios com coeficientes complexos, cujos elementos irredutíveis são os polinómios $(X-\alpha)$, como uma soma

$$a_0 + a_1(X-\alpha) + \cdots + a_n(X-\alpha)^n$$

sendo $a_i \in \mathbb{C}$, $a_n \neq 0$ e $n \in \mathbb{N}$. Além disso, toda a fracção $\frac{P(X)}{Q(X)}$ de elementos $P(X), Q(X) \in \mathbb{C}[X]$, sendo $Q(X) \not\equiv 0$, admite uma expansão em série de Laurent na vizinhança de qualquer $\alpha \in \mathbb{C}$ da forma

$$\frac{P(X)}{Q(X)} = \frac{a_{-k}}{(X-\alpha)^k} + \cdots + \frac{a_{-1}}{(X-\alpha)} + a_0 + a_1(X-\alpha) + \ldots$$

onde $k \geq 0$. As funções que podem ser expressas deste modo formam o corpo das funções racionais, que contém estritamente $\mathbb{C}[X]$, e onde se incluem, por exemplo, as funções exponencial e seno.

Esta descrição das funções racionais tem uma analogia nos números racionais. Note-se que, dado um primo p, todo o natural pode ser escrito em base p como uma combinação finita de potências de p

$$a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n$$

com coeficientes $0 \leq a_i < p$ inteiros e sendo $n \in \mathbb{N} \cup \{0\}$; e que, do mesmo modo, todo o racional tem expansão em base p, gerando-se desse modo somas, possivelmente infinitas mas periódicas,

$$\sum_{-\infty}^{k} a_i\, p^i, \quad k \geq 0, \quad 0 \leq a_i < p.$$

Contudo, para concretizar a semelhança, sugerida por K. Hensel em [3], com o espaço das fracções de polinómios, teríamos de admitir também expressões como

$$\sum_{i=-k}^{+\infty} a_i\, p^i, \quad k \geq 0, \quad 0 \leq a_i < p$$

e encontrar, para cada número racional, uma escrita nesta forma. Mas a convergência destas séries em $\mathbb{R}$ não está assegurada. E, embora pudéssemos tratar estas expressões de modo formal, seria interessante encontrar a extensão adequada de $\mathbb{Q}$ onde convirjam. Para o conseguirmos, bastará que aceitemos estimar a distância entre os racionais de um modo distinto

do da métrica euclidiana; e que apliquemos o procedimento usual de completamento de um espaço métrico, como o utiliuzado para se obter o corpo completo de números reais [8].

Consideraremos de seguida os completamentos de $\mathbb{Q}$ relativamente a métricas que provêm de normas. Uma vez descrita a família (infinita mas não muito variada, como veremos) de extensões possíveis de $\mathbb{Q}$, é natural procurar sucessões que convirjam em alguns desses completamentos mas não em todos; que divirjam qualquer que seja o completamento; ou que, pelo contrário, convirjam sempre e, nesse caso, analisar como variam os limites com o completamento. São estas as questões que estudaremos neste texto.

2 Construção do corpo de números p-ádicos

O objectivo desta secção é o de introduzir a norma p-ádica, que depende do primo escolhido p e é distinta da norma euclidiana, e descrever um espaço que, dotado da norma p-ádica, contém os racionais e é completo. Uma referência clássica neste âmbito é [5], mas há textos mais recentes, como [4, 2], que incluem amplas oportunidades para se compararem propriedades aritméticas, algébricas ou analíticas do mundo p-ádico com o dos números reais.

2.1 Normas em $\mathbb{Q}$

Um espaço métrico é um par (M, d), onde M é um conjunto não vazio e $d : M \times M \to \mathbb{R}$ é uma função que satisfaz as seguintes condições:

1. $d(x, y) \geq 0$, com igualdade se e só se $x = y$;
2. $d(x, y) = d(y, x)$;
3. $d(x, z) \leq d(x, y) + d(y, z)$.

Por exemplo, $(\mathbb{R}^n, d_E)$ é um espaço métrico, onde

$$d_E(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}$$

é a métrica euclidiana.

Uma **norma** em $\mathbb{Q}$ é uma funçao $\| \cdot \| : \mathbb{Q} \to \mathbb{R}$ tal que:

P1. $\|x\| \geq 0$, com igualdade se e só se $x = 0$.

P2. $\|xy\| = \|x\| \cdot \|y\|$.

P3. $\|x+y\| \leq \|x\| + \|y\|$.

Para cada norma $\|\,.\,\|$, a função $d(x,y) = \|x-y\|$ define uma métrica em $\mathbb{Q}$. Por exemplo, a métrica usual d_E provém da norma dada pelo valor absoluto

$$|x| = \begin{cases} x & \text{se } x \geq 0 \\ -x & \text{caso contrário.} \end{cases}$$

2.2 Métrica p-ádica

Fixado um número primo p, consideremos a função $r \in \mathbb{Q} \quad \mapsto \quad v_p(r)$ que dá o expoente da potência de base p que surge na factorização prima de r, isto é,

$$v_p(r) = \begin{cases} \text{a maior potência de } p \text{ que divide } r & \text{se } r \in \mathbb{Z} \setminus \{0\}; \\ v_p(a) - v_p(b) & \text{se } r = \frac{a}{b}, a, b \in \mathbb{Z}, b \neq 0; \\ +\infty & \text{se } r = 0. \end{cases}$$

Note-se que, se $r \neq 0$, $v_p(r)$ é o único inteiro tal que $r = p^{v_p(r)} \frac{m}{n}$, sendo $\frac{m}{n}$ uma fracção irredutível (isto é, o máximo divisor comum, que designaremos por mdc, entre os inteiros m e $n > 0$ é 1) tal que p não divide m nem n.

A **norma p-ádica** $\|\cdot\|_p$ em $\mathbb{Q}$ é definida por

$$r \in \mathbb{Q} \quad \mapsto \quad \|r\|_p = \begin{cases} p^{-v_p(r)} & \text{se } r \neq 0; \\ 0 & \text{se } r = 0. \end{cases}$$

Por exemplo,

$$\|25\|_5 = \frac{1}{5^2}; \quad \|24\|_5 = 1; \quad \|\frac{1}{5^4}\|_5 = 5^4; \quad \|24\|_2 = \frac{1}{2^3}; \quad \|-\frac{1}{343}\|_7 = 7^3.$$

Denotaremos a respectiva **métrica p-ádica** por d_p. É de notar que esta distância só toma valores no conjunto discreto $\{p^n : n \in \mathbb{Z}\} \cup \{0\}$; e que, se p_1 e p_2 são primos distintos, a norma $\|\cdot\|_{p_1}$ não é equivalente à norma $\|\cdot\|_{p_2}$, uma vez que para a sucessão de termo geral $a_n = \left(\frac{p_1}{p_2}\right)^n$ se tem $\|a_n\|_{p_1} \to 0$ mas $\|a_n\|_{p_2} \to +\infty$.

Que se trata efectivamente de uma norma resulta das propriedades de v_p. A primeira condição da definição de norma é claramente satisfeita por $\|\cdot\|_p$. Quanto às outras duas exigências, basta verificar que

Lema 1. *Para todo o $x, y \in \mathbb{Q}$,*

$$\begin{aligned} v_p(x\,y) &= v_p(x) + v_p(y) \\ v_p(x+y) &\geq \min\{v_p(x), v_p(y)\}. \end{aligned}$$

Daqui resulta que

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

Esta última propriedade mostra que a norma p-ádica satisfaz uma desigualdade mais forte do que a desigualdade triangular, dita *propriedade não-arquimediana*, que generaliza o facto de, se uma potência natural de p divide dois inteiros, então divide a sua soma e a sua diferença. O que, naturalmente, tem consequências.

Proposição 2. *As seguintes afirmações são equivalentes sobre uma norma $\|\cdot\|$ em $\mathbb{Q}$:*

(a) $\|\cdot\|$ é não-arquimediana.

(b) $\|z\| \leq 1 \quad \forall\, z \in \mathbb{Z}$.

Demonstração. Comecemos por provar que $(a) \Rightarrow (b)$. Tem-se $\|1\| = 1$ uma vez que $\|1\| > 0$ e a norma é multiplicativa. Fixemos $n \in \mathbb{N}$ e suponhamos que $\|k\| \leq 1$ para todo o $k \in \{1, \cdots, n-1\}$; então

$$\|n\| = \|(n-1)+1\| \leq \max\{\|n-1\|, \|1\|\} = 1$$

Por indução, tem-se $\|n\| \leq 1$ para todo o natural n. Uma vez que $\|0\| = 0 \leq 1$ e $\|-n\| = \|n\|$, concluímos que $\|z\| \leq 1$ para todo o inteiro z.

Reciprocamente, sejam $x, y \in \mathbb{Q}$ e $k \in \mathbb{N}$. Pela propriedade multiplicativa da norma e por (b), tem-se

$$\begin{aligned} \|x+y\|^k &= \|(x+y)^k\| = \|\sum_{j=0}^{k} \binom{k}{j} x^j\, y^{k-j}\| \\ &\leq \sum_{j=0}^{k} \|\binom{k}{j}\|\,\|x\|^j\,\|y\|^{k-j} \\ &\leq \sum_{j=0}^{k} \|x\|^j\,\|y\|^{k-j} \\ &\leq (k+1)\,(\max\{\|x\|, \|y\|\})^k\,. \end{aligned}$$

Consequentemente, para todo o natural k,

$$\|x+y\| \leq \sqrt[k]{k+1}\ \max\{\|x\|, \|y\|\}.$$

Deixando k tender para $+\infty$, obtemos

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

□

Podemos acrescentar que a propriedade arquimediana de uma norma $\|\cdot\|$ em $\mathbb{Q}$ garante que

$$\sup\{\|z\| : z \in \mathbb{Z}\} = +\infty$$

(e reciprocamente). De facto, se $z_0 \in \mathbb{Z}$ é tal que $\|z_0\| > 1$, então

$$\lim_{k \to +\infty} \|z_0^k\| = \lim_{k \to +\infty} \|z_0\|^k = +\infty.$$

Designe-se cada terno de racionais não nulos $(x, y, x-y)$ por «triângulo» em $\mathbb{Q}$, com a métrica p-ádica, de lados com comprimentos $\|x\|_p$, $\|y\|_p$ e $\|x-y\|_p$. Se $a \in \mathbb{Q}$ e $\varrho > 0$, a bola, na métrica p-ádica, centrada em a e de raio ϱ é o conjunto $B_\varrho(a) := \{x \in \mathbb{Q} : \| x - a \|_p < \varrho\}$.

Proposição 3.

(a) Todos os «triângulos» em $\mathbb{Q}$ com a métrica p-ádica são isósceles e o comprimento da base não excede o comprimento dos lados.

(b) Todo o ponto de cada bola é centro da bola ou, equivalentemente, dadas duas quaisquer bolas não-disjuntas, uma delas contém a outra.

(c) Uma sucessão de pontos é de Cauchy se e só se a distância entre os termos adjacentes tende para zero.

Demonstração. Sejam $\|x\|_p$, $\|y\|_p$ e $\|x-y\|_p$ os lados de um «triângulo» em $(\mathbb{Q}, \|\,.\,\|_p)$, e suponhamos que $\|x\|_p < \|y\|_p$. Então

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

e

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

Consideremos $a \in \mathbb{Q}$, $\varrho > 0$ e $b \in B_\varrho(a)$. Então, dado $x \in B_\varrho(a)$, tem-se

$$\| b - a \|_p < \varrho, \quad \| x - a \|_p < \varrho$$

e, portanto,

$$\| x - b \|_p = \| (x - a) + (a - b) \|_p \leq \max \{ \| x - a \|_p, \| b - a \|_p \} < \varrho.$$

Logo $B_\varrho(a) \subseteq B_\varrho(b)$. Analogamente se conclui que $B_\varrho(b) \subseteq B_\varrho(a)$.

Finalmente, seja $(a_n)_{n\in\mathbb{N}}$ uma sucessão de Cauchy em $\mathbb{Q}$ para a métrica p-ádica: dado $\epsilon > 0$, podemos encontrar $N \in \mathbb{N}$ tal que

$$m > n \geq N \quad \Rightarrow \quad \|a_n - a_m\|_p < \epsilon.$$

Então, obviamente,

$$n \geq N \quad \Rightarrow \quad \|a_n - a_{n+1}\|_p < \epsilon.$$

E vale o recíproco uma vez que, se $m > n$,

$$\|a_n - a_m\|_p \leq \max \{ \|a_n - a_{n+1}\|_p, \|a_{n+1} - a_{n+2}\|_p, \cdots, \|a_{m-1} - a_m\|_p \}.$$

□

Em particular, se $\varrho > 0$, qualquer esfera $S_\varrho(a) = \{x \in \mathbb{Q} : \|x - a\|_p = \varrho\}$ é um aberto na métrica p-ádica (além de ser fechado, como em qualquer métrica): se $x \in S_\varrho(a)$ e $0 < \delta < \varrho$, então $B_\delta(x) \subset S_\varrho(a)$ porque, se $z \in B_\delta(x)$, então

$$\|x - z\|_p < \delta < \varrho = \|x - a\|_p$$

e, portanto, como vimos na Proposição 3 (a),

$$\|z - a\|_p = \|x - a\|_p = \varrho.$$

2.3 Completamento de um espaço métrico

Um espaço métrico diz-se completo se todas as suas sucessões de Cauchy são convergentes. É o caso de $\mathbb{R}$ com a métrica d_E. Pelo contrário, o espaço $\mathbb{Q}$ com a mesma métrica não é completo. E $\mathbb{Q}$ com a métrica $\| \cdot \|_p$ também não é completo. Há, porém, um procedimento geral para se completar um espaço métrico.

Proposição 4. [10] *Seja (M, d) um espaço métrico. Então existe um (único) espaço métrico completo (M^*, d^*), dito completamento de M, e uma isometria $\mathcal{C} : M \to M^*$ tal que $\mathcal{C}(M)$ é denso em M^*.*

A utilização do método descrito na prova desta proposição no caso da métrica euclidiana constrói o corpo dos números reais. Se usarmos a métrica p-ádica, obtemos o corpo dos números p-ádicos, que designaremos por $\mathbb{Q}_p$. Naturalmente a propriedade não-arquimediana da norma $\|\,.\,\|_p$ e as afirmações da Proposição 3 mantêm-se válidas em $\mathbb{Q}_p$. Além disso:

Proposição 5. [4]

(a) $\mathbb{Q}$ *é denso em* $\mathbb{Q}_p$.

(b) Para $\varrho > 0$, *cada bola* $B_\varrho(a) = \{x \in \mathbb{Q}_p : \|x - a\|_p < \varrho\}$ *é um conjunto aberto e fechado.*

(c) A família de todas as bolas em $\mathbb{Q}_p$ *é numerável.*

(d) O conjunto de inteiros p-ádicos, $\mathbb{Z}_p := \{x \in \mathbb{Q}_p : \|x\|_p \leq 1\}$, *é compacto.*

(e) $\mathbb{N}$ *é denso em* $\mathbb{Z}_p$.

Em particular, se $\varrho > 0$, a esfera $S_\varrho(a) = \{x \in \mathbb{Q}_p : \|x - a\|_p = \varrho\}$ não é o bordo da bola $B_\varrho(a)$; e, para cada natural k, a bola fechada $\{x \in \mathbb{Q}_p : \|x - a\|_p \leq p^k\}$, que é igual a $\{x \in \mathbb{Q}_p : \|x - a\|_p < p^{k+1}\}$, não é a aderência da bola aberta $\{x \in \mathbb{Q}_p : \|x - a\|_p < p^k\}$.

Podemos também atribuir a $\mathbb{Q}_p$ uma estrutura de corpo, beneficiando do facto de $\mathbb{Q}$ ser denso em $\mathbb{Q}_p$. Por exemplo, se $x, y \in \mathbb{Q}_p$ são limite, na norma $\|\cdot\|_p$, de sucessões de racionais $(r_n)_{n\in\mathbb{N}}$ e $(s_n)_{n\in\mathbb{N}}$, respectivamente, então está bem definida a soma

$$x + y = \lim_{n\to+\infty}(r_n + s_n).$$

Contudo, o corpo $\mathbb{Q}_p$ assim obtido não é algebricamente fechado: a equação $x^2 - p = 0$ não tem soluções em $\mathbb{Q}_p$ (para o comprovar, basta calcular a norma p-ádica de ambos os membros desta igualdade).

2.4 Completamentos de $\mathbb{Q}$

Uma norma diz-se trivial se $\|x\| = 1$ para todo o $x \neq 0$. Esta norma induz a métrica discreta em $\mathbb{Q}$, para a qual este espaço é completo uma vez que uma sucessão de racionais é de Cauchy para esta norma se e só é constante a partir de certa ordem. Como vimos, os racionais suportam normas mais interessantes, como as p-ádicas e a euclidiana, e tanto o espaço

dos números reais como o dos p-ádicos são corpos que contêm os racionais e dotados de métricas relativamente às quais são completos (o corpo dos reais tem a propriedade adicional de admitir uma ordenação compatível com as operações). E, no caso das métricas provenientes de normas em $\mathbb{Q}$, não há mais possibilidades.

Teorema 6 (Ostrowski, [4]). *Seja $\bar{\mathbb{Q}}$ o completamento de $\mathbb{Q}$ com uma norma não trivial. Então $\bar{\mathbb{Q}}$ é homeomorfo a $\mathbb{R}$ ou a $\mathbb{Q}_p$ para algum número primo p.*

Essencialmente, a demonstração separa as normas em dois tipos: ou a norma é limitada nos inteiros (caso em que o completamento é um espaço p-ádico) ou não é (e o completamento é $\mathbb{R}$).

Pode mostrar-se que todo o $a \in \mathbb{Q}_p$ admite uma e uma só expansão p-ádica da forma

$$a = \sum_{i=-k}^{+\infty} \alpha_i \, p^i, \quad k \in \mathbb{Z}, \quad 0 \leq \alpha_i < p, \quad \alpha_{-k} \neq 0$$

sendo $\|a\|_p = p^k$ (detalhes em [4]). Formalmente, isto significa que a é o limite, na métrica p-ádica, das somas parciais desta série. Os inteiros p-ádicos são precisamente os elementos de $\mathbb{Q}_p$ para os quais $k \geq 0$. Note-se que a existência de uma expansão p-ádica dos elementos de $\mathbb{Z}_p$ corresponde a afirmar que $\mathbb{N}$ é denso em $\mathbb{Z}_p$.

Por exemplo, os inteiros estão em $\mathbb{Z}_p$; e, como

$$\frac{1}{1-p} = \sum_{i=0}^{+\infty} p^i,$$

a fracção racional $\frac{1}{1-p}$ é também um inteiro p-ádico. À semelhança do que acontece em $\mathbb{R}$, uma condição necessária e suficiente para que a expansão p-ádica de $a \in \mathbb{Q}_p$ seja finita é que a seja um número racional não-negativo cujo denominador seja uma potência de p. Além disso, $a \in \mathbb{Q}_p$ é um número racional se e só se a sua expansão p-ádica é periódica a partir de uma certa ordem.

Estamos agora em condições de verificar que $\mathbb{Q}$ com a métrica p-ádica não é um espaço completo, isto é, que existem sucessões de Cauchy de racionais que não são convergentes. Uma tal sucessão de racionais que seja de Cauchy para a métrica p-ádica mas não convirja em $\mathbb{Q}$ pode obter-se a partir da expansão p-ádica de $\sqrt{a}$, onde $a \in \mathbb{Z}$ não é quadrado perfeito mas tem raiz quadrada em $\mathbb{Q}_p$. Por exemplo, $\sqrt{-7} \in \mathbb{Q}_2$; e $\sqrt{1-p} \in \mathbb{Q}_p$ para todo o primo $p > 2$; mais pormenores em [4].

2.5 $\mathbb{Q}_p$ quando p não é primo

Consideremos um natural composto q. Dado um inteiro $x \neq 0$, podemos considerar a maior potência v de q que divide x. Contudo, se x é um racional não inteiro, dado pela fracção irredutível $\frac{a}{b}$, a presença de q na fracção pode distribuir-se por a e por b sem que q divida algum deles. Tem-se, porém, o seguinte:

Lema 7. *Para toda a fracção $\frac{a}{b}$, com $a \in \mathbb{Z}$, $b \in \mathbb{N}$ e $mdc\,(a,b) = 1$, existe um (único) $v \in \mathbb{Z}$ e um par de inteiros a' e $b' > 0$ tais que $q \nmid a'$, $q \nmid b'$ $mdc\,(a',b') = 1$ e*

$$\frac{a}{b} = q^v \, \frac{a'}{b'}.$$

Demonstração. Se $q \nmid a$ e $\mathrm{mdc}\,(b,q) = 1$, escolhemos $v = 0$, $a' = a$ e $b' = b$. Se $q \mid a$, então $\mathrm{mdc}\,(b,q) = 1$ porque a e b são, por hipótese, primos entre si. Seja $v \in \mathbb{N}$ a maior potência de q que divide a e consideremos

$$a' = a\, q^{-v} \quad \text{e} \quad b' = b.$$

Desse modo, temos $q \nmid a'$, $\mathrm{mdc}\,(a',b') = 1$ e

$$\frac{a}{b} = q^v \, \frac{a'}{b'}.$$

Se $q \nmid a$ e $\mathrm{mdc}\,(b,q) > 1$, podemos escrever $b = b_1 b_2$, sendo b_1 e b_2 inteiros positivos tais que todos os factores primos de b_1 dividem q e $\mathrm{mdc}\,(b_2,q) = 1$. Analogamente, $q = q_1 q_2$ para um par de naturais q_1 e q_2 com a propriedade de todos os factores primos de q_1 dividirem b_1 e $\mathrm{mdc}\,(q_2,b_1) = \mathrm{mdc}\,(q_2,b) = 1$. Seja β o menor inteiro positivo tal que $b_1 \mid q^\beta$. Então

$$q^\beta \, \frac{a}{b} = \frac{q_1^\beta \, q_2^\beta}{b_1 \, b_2} \, a$$

sendo $\frac{q_1^\beta}{b_1}$ um inteiro. E, portanto,

$$\frac{a}{b} = q^{-\beta} \, \frac{a'}{b'}$$

se

$$a' = \frac{q_1^\beta \, q_2^\beta \, a}{b_1} \quad \text{e} \quad b' = b_2.$$

Note-se que $q \nmid a'$ e $\mathrm{mdc}\,(a',b') = \mathrm{mdc}\,(q,b') = \mathrm{mdc}\,(q,b_2) = 1$. Seja então $v = -\beta$. □

Por exemplo, se $q = 10$, então

- para $\frac{2}{3}$, tem-se $a' = 2$, $b' = 3$ e $v = 0$.
- para $\frac{40}{17}$, tem-se $a' = 4$, $b' = 17$, $v = 1$ e reescrevemos $\frac{40}{17} = 10\,\frac{4}{17}$.
- para $\frac{1}{20}$, como $q \nmid 1$ e $\mathrm{mdc}\,(20, 10) = 10$, tomamos

$$b_1 = 2^2\,5, \quad b_2 = 1, \quad q_1 = 10, \quad q_2 = 1, \quad a' = 5, \quad b' = 1, \quad \beta = 2$$

logo $v = -2$ e reescrevemos $\frac{1}{20} = 10^{-2}\,\frac{5}{1}$.

Dado um natural $q \geq 2$ e uma fracção $\frac{a}{b}$ com $a \in \mathbb{Z}$, $b \in \mathbb{N}$ e $\mathrm{mdc}\,(a, b) = 1$, consideremos o inteiro v obtido no Lema 7.

Definição 1.

$$\left\| \frac{a}{b} \right\|_q = \begin{cases} q^{-v} & \text{se } a \in \mathbb{Z} \setminus \{0\}; \\ 0 & \text{se } a = 0. \end{cases}$$

Note-se que, se q é primo, a definição anterior coincide com a norma q-ádica. Por exemplo, se $q = 10$, então $\|50\|_{10} = \frac{1}{10}$, $\|51\|_{10} = 1$, $\|\frac{1}{20}\|_{10} = 10^2$ e $\|\frac{1}{50}\|_{10} = 10^2$. Observe-se agora que

$$\|\frac{1}{20} \times \frac{1}{50}\|_{10} = 10^3 < \|\frac{1}{20}\|_{10} \times \|\frac{1}{50}\|_{10}$$

o que significa que a função $x \in \mathbb{Q} \mapsto \|x\|_{10}$ não é uma norma. Tem, contudo, as seguintes propriedades:

- $x = 0 \;\Leftrightarrow\; \|x\|_q = 0$
- $\|x\,y\|_q \leq \|x\|_q\,\|y\|_q$
- $\|x + y\|_q \leq \|x\|_q + \|y\|_q$.

Por isso, a função $d_q : (x, y) \in \mathbb{Q} \times \mathbb{Q} \mapsto \|x - y\|_q$ é uma métrica em $\mathbb{Q}$. Relativamente a d_q, o conjunto de racionais também não é completo; seja $\mathbb{Q}_q$ o seu completamento. Este espaço, com a soma e o produto como definidos anteriormente, é um anel, mas tem divisores de zero. Um resultado de Hensel [4] informa que, se $q = p_1 p_2 \cdots p_k$ é um produto de primos distintos, então o anel $\mathbb{Q}_q$ é isomorfo à soma directa dos corpos $\mathbb{Q}_{p_1} \bigoplus \cdots \bigoplus \mathbb{Q}_{p_k}$.

3 Séries em $\mathbb{Q}_p$

Uma vez que $\mathbb{Q}_p$ é simultaneamente um corpo e um espaço métrico, é possível definir séries em $\mathbb{Q}_p$ tal como no caso real. Como sabemos, uma condição necessária para a convergência de uma série em $\mathbb{R}$ é que a norma dos seus termos tenda para zero. Este critério não é, no entanto, suficiente, como mostra a série $\sum_{n=1}^{+\infty} \frac{1}{n}$. No caso dos p-ádicos, a situação não é a mesma.

Lema 8. *Seja* $\sum_{n=0}^{+\infty} a_n$ *uma série em* $\mathbb{Q}_p$. *Então*

$$\lim_{n\to+\infty} \|a_n\|_p = 0 \quad \Leftrightarrow \quad \text{a série converge.}$$

Demonstração. Seja $(S_n)_{n\in\mathbb{N}}$ a sucessão de somas parciais da série $\sum_{n=0}^{+\infty} a_n$. Para mostrar que a condição sobre o termo geral da série é necessária para a convergência, basta notar que a convergência da sucessão das somas parciais implica que esta é de Cauchy, e como tal

$$\lim_{n\to+\infty} \|a_{n+1}\|_p = \lim_{n\to+\infty} \|S_{n+1} - S_n\|_p = 0.$$

Reciprocamente, suponhamos que essa condição sobre o termo geral da série se verifica. Como $\mathbb{Q}_p$ é completo, é suficiente mostrar que a sucessão das somas parciais é de Cauchy. Observemos que, se n e m são naturais tais que $m > n$, então, por aplicação sucessiva da propriedade não-arquimediana de d_p,

$$\|S_m - S_n\|_p \leq \max_{n\leq i\leq m-1} \|S_{i+1} - S_i\|_p$$

logo

$$\lim_{n,m\to+\infty} \|S_m - S_n\|_p \leq \lim_{n,m\to+\infty} \max_{n\leq i\leq m-1} \|a_i\|_p = 0.$$

□

3.1 Exemplos

3.1.1 $\sum_{n=1}^{\infty} n\, n!$

Para qualquer primo p, esta série, que diverge em $\mathbb{R}$, tem soma -1 em $\mathbb{Q}_p$. De facto, para todo o $k \in \mathbb{N}$,

$$1 + \sum_{n=1}^{k} n\, n! = (k+1)!$$

e, portanto,

$$\left\| \left(\sum_{n=1}^{k} n\, n! \right) - (-1) \right\|_p = \|(k+1)!\|_p$$

que converge para 0 quando $k \to +\infty$, uma vez que, para todo o natural m, a potência p^m divide $(k+1)!$ para todo o natural k suficientemente grande.

3.1.2 $\sum_{n=1}^{\infty} n!$

Esta série, divergente em $\mathbb{R}$, converge em $\mathbb{Q}_p$ para qualquer primo p. Efectivamente, a fórmula de Legendre [4] indica que, se $\mathbb{D}_p(n)$ é a soma dos dígitos de n quando representado na base p, então

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

onde

$$v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor = \frac{n - \mathbb{D}_p(n)}{p-1}.$$

Além disso,

Lema 9. *Para cada primo p e todo o natural n,*

$$\mathbb{D}_p(n) \leq (p-1) \left[\frac{\ln(n)}{\ln(p)} + 1 \right].$$

Demonstração. Se $n = c_0 + c_1\, p + c_2\, p^2 + \cdots + c_N\, p^N$ na base p, sendo $0 \leq c_j \leq p-1$ e $c_N \neq 0$, então $n \geq p^N$, o que indica, calculando logaritmos, que

$$N \leq \frac{\ln(n)}{\ln(p)}.$$

E, portanto, como cada dígito é menor ou igual a $p-1$, a soma dos dígitos da expansão de n na base p é majorada por

$$\mathbb{D}_p(n) \leq (p-1)\, \frac{\ln(n)}{\ln(p)} + (p-1).$$

□

Consequentemente, se n é suficientemente grande, $\mathbb{D}_p(n) \leq \frac{n}{2}$. E, da fórmula de Legendre, obtemos finalmente

$$v_p(n!) = \frac{n - \mathbb{D}_p(n)}{p-1} \geq \frac{n}{2p-2}$$

o que garante que $\lim_{n\to+\infty} \|n!\|_p = 0$.

Para cada primo p, seja $L_p = \sum_{n=1}^{\infty} n!$ em $\mathbb{Q}_p$. Note-se que L_p é um inteiro p-ádico uma vez que, para todo o natural k,

$$\left\| \sum_{n=1}^{k} n! \right\|_p \leq \max_{1\leq n\leq k} \{\|n!\|_p\} = 1.$$

Para a maioria dos primos p é ainda um problema em aberto saber qual o valor de L_p, se é racional ou mesmo se é não-nulo (embora seja certo que L_p não pode ser racional para todos os primos p; mais detalhes em [6]).

3.1.3 Séries de potências

A série $\sum_{n=0}^{+\infty} x^n$ converge em $x \in \mathbb{Q}_p$ para $\frac{1}{1-x}$ se e só se $\|x\|_p < 1$. Por exemplo, a série $\sum_{n=0}^{+\infty} 3^n$ converge para $-\frac{1}{2}$ em $\mathbb{Q}_3$, mas diverge em $\mathbb{Q}_p$ para $p \neq 3$.

Em geral, uma série de potências $\sum_{n=0}^{+\infty} a_n\, x^n$, onde $a_n \in \mathbb{Q}_p$, converge se e só se $\lim_{n\to+\infty} \|a_n\, x^n\|_p \to 0$, e portanto o raio de convergência de uma tal série é

$$R_c = \sup\{r \geq 0 : \|a_n\|_p\, r^n \to 0\}.$$

Por isso, tal como em $\mathbb{R}$,

$$R_c = \frac{1}{\limsup_{n\to+\infty} (\|a_n\|_p)^{\frac{1}{n}}}.$$

E o que acontece no bordo, quando $\|x\|_p = R_c$? Em $\mathbb{R}$, o comportamento de uma série de potências no bordo do intervalo de convergência pode ser bastante complicado. Em $\mathbb{Q}_p$ a situação é muito mais simples de formular porque a convergência depende não de x mas de $\|x\|_p$: o domínio de convergência de uma série de potências p-ádica $\sum_{n=0}^{+\infty} a_n\, x^n$ é um disco

$$\mathcal{D} = \{x : \|x\|_p \leq R\},$$

onde a convergência é de facto uniforme, sendo $R \in \{p^k : k \in \mathbb{Z}\} \cup \{0\} \cup \{+\infty\}$ e satisfazendo exclusivamente uma das duas condições seguintes:

- $R = R_c$ e a série converge para todo o x tal que $\|x\|_p = R_c$;
- $R = \frac{R_c}{p}$ e a série diverge para todo o x tal que $\|x\|_p = R_c$.

3.1.4 Séries exponencial, logaritmo e trigonométricas

A série $\displaystyle\sum_{n=0}^{+\infty} \frac{1}{n!}$ converge em $\mathbb{R}$, para e, mas diverge em $\mathbb{Q}_p$ para todo o primo p porque se tem

$$\left\| \frac{1}{n!} \right\|_p = p^{v_p(n!)} \geq 1 \quad \forall\, n \in \mathbb{N}.$$

Mais geralmente, a série $\displaystyle\sum_{n=0}^{+\infty} \frac{1}{n!}\, x^n$, que em $\mathbb{R}$ converge para qualquer x, tem no espaço $\mathbb{Q}_p$ um domínio de convergência que se reduz ao disco

$$\mathcal{D}_p = \{x \in \mathbb{Q}_p : \|x\|_p < p^{-\frac{1}{p-1}}\}.$$

De facto, uma vez que, pelo Lema 9, se tem

$$0 \leq \mathbb{D}_p(n) \leq (p-1)\, \left[\frac{\ln(n)}{\ln(p)} + 1 \right]$$

concluímos que

$$\begin{aligned} \frac{1}{p-1} &\geq \lim_{n\to+\infty} \frac{n - \mathbb{D}_p(n)}{n\,(p-1)} \\ &\geq \lim_{n\to+\infty} \frac{n - (p-1)\, \left[\frac{\ln(n)}{\ln(p)} + 1 \right]}{n\,(p-1)} \\ &= \frac{1}{p-1}. \end{aligned}$$

Consequentemente, tendo em conta que $v_p(n!) = \frac{n - \mathbb{D}_p(n)}{p-1}$ (veja-se a Secção 3.1.2),

$$\begin{aligned} \limsup_{n\to+\infty} \left(\|\frac{1}{n!}\|_p \right)^{\frac{1}{n}} &= \limsup_{n\to+\infty} p^{\frac{v_p(n!)}{n}} \\ &= \limsup_{n\to+\infty} p^{\frac{n - \mathbb{D}_p(n)}{n\,(p-1)}} \\ &= p^{\frac{1}{p-1}}. \end{aligned}$$

Logo, $R_c = p^{-\frac{1}{p-1}}$, e a série $\displaystyle\sum_{n=0}^{+\infty} \frac{1}{n!}\, x^n$ converge se $\|x\|_p < p^{-\frac{1}{p-1}}$ e diverge se $\|x\|_p > p^{-\frac{1}{p-1}}$.

Por exemplo, em $\mathbb{Q}_2$, a série converge em $\{x \in \mathbb{Q}_2 : \|x\|_2 \leq \frac{1}{4}\} = 4\mathbb{Z}_2$, e, por isso, não existe neste espaço um elemento análogo a $e = \exp(1)$. Se $p > 2$, o valor $p^{-\frac{1}{p-1}}$ não é válido para a norma p-ádica; como $\frac{1}{p} < p^{-\frac{1}{p-1}} < 1$, a série converge precisamente em $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : \|x\|_p \leq \frac{1}{p}\}$.

No domínio $\mathcal{D}_p$, a série define a *exponencial p-ádica*, que se designa por $\exp_p$ e verifica:

- $exp_p(0) = 1$.
- $\exp_p(x+y) = \exp_p(x)\,\exp_p(y) \quad \forall\, x, y \in \mathcal{D}_p$.
- $\exp_p' = \exp_p$.

Analogamente, a série de potências $\displaystyle\sum_{n=1}^{+\infty}(-1)^{n+1}\frac{(x-1)^n}{n}$ representa a função *logaritmo p-ádico*, que designaremos por $\ln_p$. A série converge em $\mathcal{E}_p = \{x \in \mathbb{Q}_p : \|x-1\|_p \leq \frac{1}{p}\} = 1 + \mathcal{D}_p$ e satisfaz as igualdades:

- $\ln_p(1) = 0$.
- $\ln_p(xy) = \ln_p(x) + \ln_p(y) \quad \forall\, x, y \in \mathcal{E}_p$.
- $\ln_p'(x) = \frac{1}{x} \quad \forall\, x \in \mathcal{E}_p$.

As funções

$$\exp_p : \mathcal{D}_p \to 1 + \mathcal{D}_p \quad \text{e} \quad \ln_p : 1 + \mathcal{D}_p \to \mathcal{D}_p$$

são inversas, isto é,

$$\ln_p(\exp_p(x)) = x \quad \text{e} \quad \exp_p(\ln_p(1+x)) = 1 + x \quad \forall\, x \in \mathcal{D}_p$$

e são isometrias, ou seja, para todo o $x, y \in \mathcal{D}_p$,

$$\|\exp_p(x) - \exp_p(y)\|_p = \|x-y\|_p \quad \text{e} \quad \|\ln_p(1+x) - \ln_p(1+y)\|_p = \|x-y\|_p$$

Por exemplo, quando $p = 2$, como $\|-1-1\|_2 = \frac{1}{2} < 1$, a função $\ln_2$ está definida em -1 e temos, por um lado

$$\ln_2(-1) = -\left(2 + \frac{2^2}{2} + \frac{2^3}{3} + \cdots\right)$$

e, por outro,

$$0 = \ln_2(1) = \ln_2((-1).(-1)) = \ln_2(-1) + \ln_2(-1) = 2\ln_2(-1).$$

Logo, $\ln_2(-1) = 0$. O que significa que, quando n tende para $+\infty$, a soma $2 + \frac{2^2}{2} + \frac{2^3}{3} + \cdots + \frac{2^n}{n}$ tende para 0 em $\mathbb{Q}_2$, ou seja, é divisível por potências cada vez maiores de 2.

De modo análogo se definem as funções $\cos_p$ e $\sin_p$ como as séries

$$\cos_p(x) = \sum_{n=0}^{+\infty} \frac{(-1)^n\, x^{2n}}{(2n)!}$$

e

$$\sin_p(x) = \sum_{n=0}^{+\infty} \frac{(-1)^n\, x^{2n+1}}{(2n+1)!}$$

que convergem no disco

$$\{x \in \mathbb{Q}_p : \|x\|_p < p^{-\frac{1}{p-1}}\}.$$

Ao contrário do que acontece em $\mathbb{R}$, estas funções não são periódicas, a função $\cos_p$ não se anula e $\sin_p$ só se anula em 0. Mas continua válida a relação

$$\cos_p^2(x) + \sin_p^2(x) = 1.$$

E, se o primo p é tal que $p \equiv 1 \pmod 4$, então existe $i \in \mathbb{Q}_p$ tal que $i^2 = -1$ e a fórmula

$$\exp_p(ix) = \cos_p(x) + i \sin(x)$$

vale no domínio (comum) de convergência das séries que definem estas funções.

3.1.5 Série harmónica

A série $\displaystyle\sum_{n=1}^{+\infty} \frac{1}{n}$ diverge em todos os espaços $\mathbb{Q}_p$ e também em $\mathbb{R}$. De facto, a sucessão de somas parciais da série harmónica não é limitada em $\mathbb{R}$; e $\lim_{n\to\infty} \frac{1}{n} \neq 0$ em $\mathbb{Q}_p$ uma vez que

$$\left\|\frac{1}{n}\right\|_p = p^{-v_p(\frac{1}{n})} = p^{v_p(n)} \geq 1 \quad \forall\, n \in \mathbb{N}.$$

De modo análogo se verifica que a série $\displaystyle\sum_{n=1}^{\infty} n$ diverge em $\mathbb{Q}_p$, para todo o p primo, e em $\mathbb{R}$: a sucessão de somas parciais não é limitada em $\mathbb{R}$; e $\lim_{n\to\infty} n \neq 0$ em $\mathbb{Q}_p$ pois a norma p-ádica de cada elemento da subsucessão $\Big((p+1)^k\Big)_{k\in\mathbb{N}}$ é 1.

3.1.6 $\displaystyle\sum_{n=1}^{\infty} \frac{n!}{(n!)^2+1}$

O termo geral desta série junta a vantagem de ter $n!$ no denominador, o que lhe garante a convergência em $\mathbb{R}$, com a presença de $n!$ no numerador, o que a faz herdar a convergência em todos os espaços $\mathbb{Q}_p$ que encontrámos no Exemplo 3.1.2.

4 Séries convergentes em $\mathbb{Q}_p$, para todo o primo p, e em $\mathbb{R}$

Os exemplos anteriores mostram que é possível uma série de termos racionais não identicamente nula convergir apenas em $\mathbb{R}$; ou só convergir num dos espaços $\mathbb{Q}_p$; ou divergir relativamente a todas as normas não triviais em $\mathbb{Q}$; ou convergir em $\mathbb{R}$ e em $\mathbb{Q}_p$ para qualquer primo p. Vejamos como construir mais exemplos deste último tipo de séries. A estratégia para as obter deve garantir que cada primo aparece com potência cada vez maior no termo geral da série, mas também que em cada etapa se junta, no denominador do termo geral, uma potência elevada de um primo de ordem superior para se controlar a convergência em $\mathbb{R}$.

Seja $2 < 3 < 5 < \cdots < p_k < \ldots$ a enumeração usual de todos os primos. Para cada natural n, defina-se

$$\begin{aligned}
a_1 &= \frac{2}{(3).5^2} \\
a_2 &= \frac{2^2.3}{(5.7^2).11^2} \\
a_3 &= \frac{2^3.3^2.5}{(7.11^2.13^3).17^2} \\
a_4 &= \frac{2^4.3^3.5^2.7}{(11.13^2.17^3.19^4).23^2} \\
&\vdots \\
a_n &= \frac{2^n\, 3^{n-1} \ldots p_{n-1}^2\, p_n}{(p_{n+1} \ldots p_{2n}^n)\, p_{2n+1}^2}.
\end{aligned}$$

Claramente, para todo o primo p,

$$\lim_{n\to+\infty} \|a_n\|_p = 0$$

pelo que a série de termo geral $(a_n)_{n\in\mathbb{N}}$ converge em todos os espaços $\mathbb{Q}_p$. Além disso,

$$|a_n| \leq \left(\frac{1}{p_{2n+1}}\right)^2$$

logo, em $\mathbb{R}$, pelo critério de comparação temos

$$\sum_{n=1}^{+\infty} a_n \leq \sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

5 Controle dos limites

A questão natural que se coloca face ao resultado anterior é se podemos escolher os limites da série em cada um dos corpos.

Teorema 10. *Consideremos a ordenação usual $p_1 < \cdots < p_k < \ldots$ dos primos e escolhamos $\beta \in \mathbb{R}$ e, para cada $k \in \mathbb{N}$, $\gamma_k \in \mathbb{Q}_p$. Então existe uma série de termos racionais que converge para γ_k em $\mathbb{Q}_{p_k}$, para todo o k, e converge para β em $\mathbb{R}$.*

A construção da série a que se refere este resultado, que apresentaremos de seguida, inspirou-se no procedimento da secção anterior, acrescentando-se uma maior atenção à proximidade da sucessão de somas parciais dos limites pretendidos. Como veremos, para conseguir este controle, bastará uma versão em $\mathbb{Q}_p$ do Teorema Chinês dos Restos [7].

5.1 Congruências

Definição 2. *Dados $x, y \in \mathbb{Q}_p$ e $n \in \mathbb{N}$, dizemos que x e y são congruentes modulo p^n, o que denotamos por $x \equiv y \,(\mathrm{mod}\, p^n)$, se*

$$\|x - y\|_p \leq p^{-n}.$$

Trata-se de uma relação de equivalência. É claramente reflexiva e simétrica. Suponhamos agora que $x \equiv y \,(\mathrm{mod}\, p^n)$ e $y \equiv z \,(\mathrm{mod}\, p^n)$, ou seja, que

$$\|x - y\|_p \leq p^{-n} \quad \text{e} \quad \|y - z\|_p \leq p^{-n}.$$

Pela propriedade não-arquimediana de $\mathbb{Q}_p$, obtemos

$$\|x - z\|_p \leq \max\{\|x - y\|_p, \|y - z\|_p\} \leq p^{-n}$$

o que é equivalente a $x \equiv z \,(\mathrm{mod}\, p^n)$. Esta relação reduz-se à noção de congruência usual em $\mathbb{Z} \subset \mathbb{Q}_p$ e satisfaz as propriedades usuais das congruências em inteiros.

5.1.1 Operações com congruências

No que se refere às operações aritméticas em $\mathbb{Q}_p$, tem-se

$$x \equiv x' \,(\mathrm{mod}\, p^n) \quad \text{e} \quad y \equiv y' \,(\mathrm{mod}\, p^n) \quad \Rightarrow \quad x + x' \equiv y + y' \,(\mathrm{mod}\, p^n)$$

mas, contrariamente ao que acontece em $\mathbb{Z}$, o produto não preserva a relação de congruência. Por exemplo,

$$p \equiv 0 \,(\mathrm{mod}\, p) \quad \text{e} \quad \frac{1}{p} \equiv \frac{1}{p} \,(\mathrm{mod}\, p)$$

mas

$$1 \not\equiv 0 \,(\mathrm{mod}\, p).$$

O problema tem origem no facto de estarmos a dividir por inteiros não co-primos com p. Porém, se nos restringirmos a $\mathbb{Z}_p$, a congruência é preservada pelo produto uma vez que, se $x \equiv x' \,(\mathrm{mod}\, p^n)$ e $y \equiv y' \,(\mathrm{mod}\, p^n)$, então, como x e y' são inteiros p-ádicos,

$$\|xy - x'y'\|_p = \|x(y-y') - y'(x-x')\|_p \leq \max\{\|x(y-y')\|_p, \|y'(x-x')\|_p\} \leq p^{-n}$$

o que mostra que $xy \equiv x'y' \,(\mathrm{mod}\, p^n)$. De facto, observando que $p^n\mathbb{Z}_p$ é um ideal do anel $\mathbb{Z}_p$, podemos identificar as operações com congruências com as operações no anel quociente $\mathbb{Z}_p/p^n\mathbb{Z}_p$.

5.1.2 Teorema Chinês dos Restos em $\mathbb{Q}_p$

Agora que temos uma noção de congruência em $\mathbb{Q}_p$, podemos resolver um sistema de congruências da forma

$$\begin{cases} x \equiv b_1 \bmod p_1^{\alpha_1} \\ x \equiv b_2 \bmod p_2^{\alpha_2} \\ \vdots \\ x \equiv b_k \bmod p_k^{\alpha_k} \end{cases}$$

onde $b_i \in \mathbb{Q}_{p_i}$, $\alpha_i \in \mathbb{N}$ e os p_i são primos todos distintos.

Podemos supor sem perda de generalidade que $b_i \in \mathbb{Z}_{p_i}$ para todo o $1 \leq i \leq k$. De facto, tomando para cada i o menor natural ℓ_i tal que $p_i^{\ell_i} b_i \in \mathbb{Z}_{p_i}$ e denotando por

$$\begin{aligned} m &= \prod_{i=1}^{k} p_i^{\ell_i} \\ y &= m\,x \\ c_i &= m\,b_i \end{aligned}$$

verifica-se que

$$\|x - b_i\|_p \leq p_i^{-\alpha_i} \quad \Leftrightarrow \quad \|y - c_i\|_p \leq p_i^{-\alpha_i - \ell_i}$$

logo, substituindo b_i por c_i e x por y, obtemos o sistema equivalente

$$\begin{cases} y \equiv c_1 \bmod p_1^{\alpha_1+\ell_1} \\ y \equiv c_2 \bmod p_2^{\alpha_2+\ell_2} \\ \vdots \\ y \equiv c_k \bmod p_k^{\alpha_k+\ell_k}. \end{cases}$$

Como $\mathbb{N}$ é denso nos inteiros p-ádicos, podemos escolher naturais n_i tais que

$$c_i \equiv n_i \bmod p_i^{\alpha_i}.$$

Obtemos assim o sistema equivalente

$$\begin{cases} x \equiv n_1 \bmod p_1^{\alpha_1} \\ x \equiv n_2 \bmod p_2^{\alpha_2} \\ \vdots \\ x \equiv n_k \bmod p_k^{\alpha_k}. \end{cases}$$

Este sistema é solúvel em $\mathbb{Z}$, por aplicação do Teorema Chinês dos Restos usual, uma vez que todos os primos p_i são distintos, e, portanto, existe uma solução $x_0 \in \mathbb{Q}$ para o sistema de congruências inicial.

Se x_1 for outra solução racional do sistema considerado, subtraímos as i-ésimas condições respectivas, obtendo

$$x_1 \equiv x_0 \bmod p_i^{\alpha_i}.$$

Daqui resulta que

$$x_1 = x_0 + q \prod_{i=1}^{k} p_i^{\alpha_i}$$

onde $q \in \mathbb{Q}$ é tal que

$$\|q\|_{p_i^{\alpha_i}} \leq 1.$$

Também é claro que, reciprocamente, qualquer racional x_1 satisfazendo a igualdade

$$x_1 = x_0 + q \prod_{i=1}^{k} p_i^{\alpha_i}$$

em que $q \in \mathbb{Q}$ é tal que

$$\|q\|_{p_i^{\alpha_i}} \leq 1$$

é solução do sistema de congruências dado. Logo, se $\mathcal{S}$ designa o conjunto de soluções, então

$$\mathcal{S} = x_0 + \left(\prod_{i=1}^{n} p_i^{\alpha_i}\right) A$$

onde

$$A = \{q \in \mathbb{Q} : \|q\|_{p_i} \leq 1, \quad \forall\, 1 \leq i \leq n\}.$$

Observação 1. Conhecendo as expansões p-ádicas de todos os b_i's, o argumento anterior fornece um algoritmo para encontrar uma solução particular do sistema de congruências.

5.2 Prova do Teorema 10

Recorde-se que, dados $\gamma_k \in \mathbb{Q}_{p_k}$ e $\beta \in \mathbb{R}$, queremos encontrar uma série $\sum_{n=0}^{+\infty} a_n$ de termos racionais que convirja para γ_k em $\mathbb{Q}_{p_k}$, qualquer que seja o primo p_k, e para β em $\mathbb{R}$. Designemos por $(S_n)_{n\in\mathbb{N}}$ a sucessão das somas parciais da série que queremos construir. Para cada $k \in \mathbb{N}$ e todo o natural $n \geq k$, gostaríamos que S_n satisfizesse a condição

$$S_n \equiv \gamma_k \bmod p^{n+1-k}$$

pois isso garante desde logo que a série converge para γ_k em $\mathbb{Q}_{p_k}$, uma vez que

$$\|S_n - \gamma_k\|_{p_k} \leq p_k^{-(n+1-k)} \to 0$$

à medida que $n \to +\infty$.

5.2.1 Convergência em $\mathbb{Q}_{p_k}$

Se fixarmos n, queremos que S_n seja solução do sistema

$$\begin{cases} x \equiv \gamma_1 \bmod p_1^n \\ x \equiv \gamma_2 \bmod p_2^{n-1} \\ \vdots \\ x \equiv \gamma_k \bmod p_k. \end{cases} \tag{5.2.1}$$

A tabela seguinte reformula estes sistemas de congruências em termos de distâncias na métrica p_k-ádica, para cada k: a n-ésima linha da tabela representa o sistema de congruências que determina S_n; a k-ésima coluna mostra a convergência de $(S_n)_{n\in\mathbb{N}}$ para γ_k em $\mathbb{Q}_{p_k}$.

$k=1$	$k=2$	$k=3$	$k=4$	$\cdots$
$\|S_1-\gamma_1\|_2 \leq \frac{1}{2}$	-	-	-	-
$\|S_2-\gamma_1\|_2 \leq \frac{1}{4}$	$\|S_2-\gamma_2\|_3 \leq \frac{1}{3}$	-	-	-
$\|S_3-\gamma_1\|_2 \leq \frac{1}{8}$	$\|S_3-\gamma_2\|_3 \leq \frac{1}{9}$	$\|S_3-\gamma_3\|_5 \leq \frac{1}{5}$	-	-
$\|S_4-\gamma_1\|_2 \leq \frac{1}{16}$	$\|S_4-\gamma_2\|_3 \leq \frac{1}{27}$	$\|S_4-\gamma_3\|_5 \leq \frac{1}{25}$	$\|S_4-\gamma_4\|_7 \leq \frac{1}{7}$	-
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\|S_n-\gamma_1\|_2 \leq \frac{1}{2^n}$	$\|S_n-\gamma_2\|_3 \leq \frac{1}{3^{n-1}}$	$\|S_n-\gamma_3\|_5 \leq \frac{1}{5^{n-2}}$	$\|S_n-\gamma_4\|_7 \leq \frac{1}{7^{n-3}}$	$\cdots$

Sabemos que existe sempre solução para os sistemas descritos acima, pelo que está garantida a desejada convergência de $(S_n)_{n\in\mathbb{N}}$ em cada domínio p_k-ádico. Resta mostrar que a escolha de $(S_n)_{n\in\mathbb{N}}$ pode ser feita de modo a garantir a convergência em $\mathbb{R}$.

5.2.2 Convergência em $\mathbb{R}$

Comecemos por uma caracterização dos subgrupos aditivos de $\mathbb{R}$.

Lema 11. *Seja H um subgrupo de $(\mathbb{R},+)$ (ou de $(\mathbb{R}_+,\times)$). Então H é infinito cíclico ou denso em $\mathbb{R}$ (respectivamente, em $\mathbb{R}_+$).*

Demonstração. Seja $H \neq \{0\}$ um subgroupo de $(\mathbb{R},+)$ e consideremos

$$\tau = \inf\{x \in H : x > 0\}.$$

Note-se que τ está bem definido uma vez que $\{x \in H : x > 0\} \neq \emptyset$ pois existe $h \in H \setminus \{0\}$ e $-h \in H$.

Suponhamos que $\tau > 0$ e que $\tau \notin H$. Então existem $x, y \in H$ tal que $x < y < 2\tau$, logo $0 < y - x < \tau$ e $y - x \in H$, o que contradiz a definição de τ. Consequentemente, $\tau \in H$.

Se $a \in H$, existe $q \in \mathbb{Z}$ tal que $0 \leq a - q\tau < \tau$. Como $a - q\tau \in H$, tem de ser igual a zero, caso contrário teríamos $\tau \leq a - q\tau$. Ou seja, $a = q\tau \in \langle\tau\rangle$. O que mostra que $H = \langle\tau\rangle$, logo cíclico.

Suponhamos agora que $\tau = 0$. Então, para qualquer $\epsilon > 0$, existe $h \in H$ tal que $0 < h \leq \epsilon$. Seja $x \in \mathbb{R}$ and consideremos $q \in \mathbb{Z}$ tal que $0 \leq x - qh < h \leq \epsilon$. Como $qh \in H$, concluímos que H é denso in $\mathbb{R}$.

Para provar a afirmação para $(\mathbb{R}_+, \times)$, façamos uso da aplicação exponencial $\exp : \mathbb{R} \to \mathbb{R}_+$, que é um isomorfismo de grupos e um homeomorfismo entre os espaços topológicos $\mathbb{R}$ e $\mathbb{R}_+$. Basta agora observar que um isomorfismo preserva o carácter cíclico de um subgrupo e um homeomorfismo preserva a densidade de um subconjunto. □

Corolário 12. *Seja $\mathcal{P}$ um subconjunto de primos com cardinal $|\mathcal{P}| \geq 2$ e consideremos o subgrupo $\langle \mathcal{P} \rangle$ de $(\mathbb{R}_+, \times)$ gerado por $\mathcal{P}$. Então $A_{\mathcal{P}} = \langle \mathcal{P} \rangle \bigcup -\langle \mathcal{P} \rangle$ é denso em $\mathbb{R}_+ \cup -\mathbb{R}_+$, e, portanto, é denso em $\mathbb{R}$.*

Demonstração. Pelo lema anterior, basta observar que $\langle \mathcal{P} \rangle \simeq \oplus_{p \in \mathcal{P}} \mathbb{Z}$ não é cíclico quando $|\mathcal{P}| \geq 2$. □

Para cada natural n, consideremos o subconjunto de primos

$$\mathcal{P} = \{p_{n+1}, p_{n+2}, \cdots\}$$

e observemos que

$$A_{\mathcal{P}} = \{q \in \mathbb{Q} : \|q\|_{p_i} = 1, \quad \forall\, 1 \leq i \leq n\}.$$

Note-se agora que o conjunto de soluções do sistema (5.2.1) contém o conjunto

$$B_{\mathcal{P}} = x_0 + \left(\prod_{k=1}^{n} p^{n+1-k} \right) A_{\mathcal{P}}$$

e que resulta do corolário anterior que este é um conjunto denso em $\mathbb{R}$. Assim sendo, escolhemos

$$S_n \in B_{\mathcal{P}}$$

de modo que

$$|S_n - \beta| < \frac{1}{n}$$

o que garante a convergência de $(S_n)_{n \in \mathbb{N}}$ em $\mathbb{R}$.

Observação 2. Naturalmente, a série $\sum_{n=1}^{+\infty} a_n$ de números racionais que converge para γ_k em $\mathbb{Q}_{p_k}$, qualquer que seja o primo p_k, e para β em $\mathbb{R}$ tem termo geral

$$a_0 = 0 \quad \text{e} \quad a_n = S_n - S_{n-1} \quad \forall\, n \in \mathbb{N}.$$

É de referir ainda que, mesmo quando $\gamma_k = \beta \in \mathbb{Q}$ para todo o $k \in \mathbb{N}$, a série que se construiu não é trivial (seria trivial se verificasse $a_0 = \beta$ e $a_n = 0$ para $n \in \mathbb{N}$).

Em particular, se $(\gamma_k)_{k \in \mathbb{N}}$ designa a sucessão de todos os racionais, existe uma série de termos racionais que converge em $\mathbb{Q}_{p_k}$ para γ_k, qualquer que seja $k \in \mathbb{N}$.

6 Apêndice

Voltemos à série $\sum_{n=1}^{\infty} n!$. É que, ao tentarmos (sem sucesso, aliás) obter informação sobre a sua soma, acabámos por fazer uma digressão por várias fórmulas de recorrência e problemas em aberto que estão relacionados com esta série. É do que daremos conta nesta secção.

Se $(S_n)_{n\in\mathbb{N}}$ designa a sucessão das somas parciais e L_p é a soma da série em $\mathbb{Q}_p$, então

$$\|S_n - L_p\|_p \leq p^{-\frac{n+1}{2p-2}}$$

uma vez que,

$$\|S_n - L_p\|_p \leq \|(n+1)!\|_p = p^{-v_p((n+1)!)}$$

e, como se provou na Secção 3.1.2, para n suficientemente grande

$$p^{-v_p((n+1)!)} \leq p^{-\frac{n+1}{2p-2}}.$$

Isto mostra que a convergência desta série em cada espaço $\mathbb{Q}_p$ é exponencialmente rápida.

Já vimos também que, para cada primo p, a soma da série $\sum_{n=1}^{\infty} n!$ em $\mathbb{Q}_p$ é um inteiro p-ádico. Podemos acrescentar mais informação sobre a sua localização em $\mathbb{Z}_p$? Não muita, mas uma tal informação resolveria de uma vez várias questões interessantes.

6.1 L_p é diferente de zero?

Foi esta a questão, aparentemente simples, que começámos por tentar resolver.

Lema 13. *Se uma série $\sum_{n=1}^{\infty} a_n$ converge em $\mathbb{Q}_p$ para L, e, para cada natural n, $S_n = a_1 + a_2 + \cdots + a_n$ designa a soma parcial de ordem n, então*

$$\lim_{n\to+\infty} \|S_n\|_p = 0 \quad \textit{ou} \quad \exists\, N \in \mathbb{N} : \forall\, n \geq N \quad \|S_n\|_p = \|L\|_p.$$

Demonstração. Se $L \neq 0$, como $\|S_n - L\|_p < \|L\|_p$ para n suficientemente grande, tem-se, pela alínea (a) da Proposição 3,

$$\|S_n\|_p = \max\{\|S_n - L\|_p, \|L\|_p\}.$$

□

Como a soma parcial $S_n = 1 + 2! + 3! + \cdots + n!$ é um inteiro ímpar, para todo o $n \in \mathbb{N}$, é claro que $\|S_n\|_2 = 1$, logo, pelo lema anterior, $\|L_2\|_2 = 1$ e, portanto, $L_2 \neq 0$.

Quanto a L_p, para $p = 3, 5, 7, 11$, podemos verificar de modo análogo que

$$\begin{aligned} \|L_3\|_3 &= \frac{1}{3^2} \\ \|L_5\|_5 = \|L_7\|_7 &= 1 \\ \|L_{11}\|_{11} &= \frac{1}{11} \end{aligned}$$

e, com algum esforço de computação, comprovamos que $\|L_p\|_p = 1$ para todos os setenta mil primos seguintes. Apesar de esta evidência numérica ser quase irrelevante, talvez seja verdade que, se p é primo, então

$$p \mid L_p \quad \Leftrightarrow \quad p = 3 \text{ ou } p = 11$$

o que implicaria que $L_p \neq 0$ para todo o primo p. Contudo, nada nesta análise sugere como o provar.

Observação 3. Note-se que

$$\exists\, N \in \mathbb{N} : \, p \mid S_n \quad \forall n \geq N \quad \Leftrightarrow \quad p \mid S_{p-1}$$

e que

$$\exists\, N \in \mathbb{N} : \, p \mid S_n \quad \forall n \geq N \quad \Leftrightarrow \quad p \mid L_p.$$

Logo, demonstrar uma tal conjectura corresponde a provar que, se p é primo,

$$p \text{ primo } \Rightarrow \quad [\, p \mid 1 + 2! + \cdots + (p-1)! \quad \Leftrightarrow \quad p = 3 \text{ ou } p = 11]$$

o que, com o Teorema de Wilson, isto é,

$$p \text{ é primo} \quad \Leftrightarrow \quad (p-1)! \equiv -1 \ \ (mod\ p),$$

é equivalente a provar que

$$p \text{ primo } \Rightarrow \quad [\, p \mid 2! + \cdots + (p-2)! \quad \Leftrightarrow \quad p = 3 \text{ ou } p = 11]$$

e, como

$$(p-1)! \equiv -1 \ \ (mod\ p) \quad \Rightarrow \quad (p-2)! \equiv 1 \ \ (mod\ p),$$

que

$$p \text{ primo } \Rightarrow \quad [\, p \mid 1! + \cdots + (p-3)! \quad \Leftrightarrow \quad p = 3 \text{ ou } p = 11].$$

6.1.1 Números de Bell

Seja X um conjunto. Uma partição de X é uma família $(A_i)_{i\in I}$ tal que

$$A_i \cap A_j = \emptyset \quad \text{e} \quad \bigcup_{i\in I} A_i = X.$$

Para $n \in \mathbb{N} \cup \{0\}$, o n-ésimo **número de Bell**, que designamos por B_n, conta as distintas partições de um conjunto com exactamente n elementos. Os primeiros números de Bell são

$$1, 1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975, \cdots$$

e, como se explica em [1], satisfazem a relação de recorrência

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k, \qquad \forall\, n \in \mathbb{N} \cup \{0\}.$$

O problema colocado anteriormente reformula-se em termos dos números de Bell pois pode provar-se que

$$1 + 2! + \cdots + (p-1)! \equiv B_{p-1} - 2 \mod p$$

pelo que

$$\|L_p\|_p = 1 \quad \Leftrightarrow \quad B_{p-1} \not\equiv 2 \mod p.$$

A questão da congruência de B_k módulo p encontra-se bem estudada, mas as fórmulas conhecidas são úteis somente quando $k \geq p$.

Teorema 14 (Congruência de Touchard, [1, 9])**.** *Sejam n e m inteiros não-negativos. Então*

$$B_{p+n} \equiv B_n + B_{n+1} \mod p$$

e, mais geralmente,

$$B_{p^m+n} \equiv mB_n + B_{n+1} \mod p$$

Por exemplo,

$$\begin{aligned} B_p &\equiv B_0 + B_1 \mod p \equiv 2 \mod p \\ B_{p+1} &\equiv B_1 + B_2 \mod p \equiv 3 \mod p. \end{aligned}$$

Contudo, com esta informação, obtemos apenas

$$\begin{aligned} 2 &\equiv B_p \mod p \\ &= B_0 + \binom{p-1}{1} B_1 + \binom{p-1}{2} B_2 + \cdots + \binom{p-1}{p-2} B_{p-2} + B_{p-1} \\ &\equiv B_0 - B_1 + B_2 - B_3 + \cdots - B_{p-2} + B_{p-1} \mod p \end{aligned}$$

ou, equivalentemente,

$$B_{p-1} \equiv B_3 - B_4 + \cdots + B_{p-2} \mod p.$$

6.1.2 Números subfactoriais

Outra sucessão combinatória associada ao estudo de $\|L_p\|_p$ é a dos subfactoriais, cujo termo geral é dado por

$$!n = \#\{\sigma \in \mathcal{G}_n : \sigma(i) \neq i, \quad \forall\, 1 \leq i \leq n\}$$

onde $\mathcal{G}_n$ é o grupo simétrico em n letras. Os primeiros valores de $!n$ são

$$1, 0, 1, 2, 9, 44, 265, 1854, 14833, \cdots$$

e, pelo Princípio de Inclusão-Exclusão, obtém-se a fórmula

$$!n = n! \sum_{k=0}^{n} (-1)^k \frac{1}{k!}.$$

Proposição 15. *Seja p um primo ímpar. Então*

$$1! + 2! + \ldots (p-1)! \equiv !(p-1) - 1 \quad \textit{mod } p.$$

Lema 16. $\binom{p-1}{k} \equiv (-1)^k \quad \textit{mod } p, \quad 0 \leq k \leq p-1.$

Demonstração. Se $k < p-1$, basta proceder por indução, tendo em atenção a igualdade

$$\binom{p-1}{k-1} + \binom{p-1}{k} = \binom{p}{k} \equiv 0 \mod p.$$

Se $k = p-1$, o resultado decorre de p ser ímpar. □

Do lema deduzimos que

$$\begin{aligned} !(p-1) &= \sum_{k=0}^{p-1} (-1)^k \frac{(p-1)!}{k!} \\ &= \sum_{k=0}^{p-1} (-1)^k \binom{p-1}{k} (p-1-k)! \\ &\equiv \sum_{i=0}^{p-1} i! \mod p. \end{aligned}$$ □

E, portanto,

$$\|L_p\|_p = 1 \quad \Leftrightarrow \quad !(p-1) \not\equiv 1 \mod p.$$

6.1.3 Zeros de séries de potências p-ádicas

Consideremos uma função $f : \mathbb{Z}_p \to \mathbb{Q}_p$ dada por uma série de potências

$$f(x) = \sum_{n=0}^{\infty} a_n \, x^n$$

tal que $\lim_{n\to+\infty} a_n = 0$ em $\mathbb{Q}_p$, o que garante que a série converge para todo o $x \in \mathbb{Z}_p$ e que a sucessão $(\|a_n\|_p)_{n\in\mathbb{N}\cup\{0\}}$ atinge o máximo num número finito de índices.

Teorema 17 (Lema de Hensel, [6])**.** *Suponhamos que* $\|a_n\|_p \leq 1$ *para todo o* $n \in \mathbb{N} \cup \{0\}$ *e que existe* $a \in \mathbb{Z}_p$ *tal que*

$$\|f(a)\|_p < 1 \quad e \quad \|f'(a)\|_p = 1.$$

Então existe $b \in \mathbb{Z}_p$ *tal que*

$$\|b-a\|_p \leq \|f(a)\|_p \quad e \quad f(b) = 0.$$

Por exemplo, seja $f(x) = \sum_{n=0}^{\infty} n! \, x^n$. Esta série de potências converge em $x \in \mathbb{Q}_p$ se e só se $\|x\|_p < p^{\frac{1}{p-1}}$. Como $1 < p^{\frac{1}{p-1}} < p$, o domínio de convergência da série é $\mathbb{Z}_p$. Além disso, $\|n!\|_p \leq 1$ para todo o $n \in \mathbb{N} \cup \{0\}$ e todo o primo p, e

$$\begin{aligned} f(1) &= 1 + \sum_{n=1}^{\infty} n! \\ f'(1) &= \sum_{n=1}^{\infty} n \, n! = -1. \end{aligned}$$

Se $\|f(1)\|_p < 1$, o que implica que $\sum_{n=1}^{\infty} n! \neq 0$, então o teorema anterior indica que f se anula em $b \in \mathbb{Z}_p$ tal que $\|b-1\|_p \leq \|f(1)\|_p$.

Teorema 18 (Teorema de Strassman, [4]). *Seja $N \in \mathbb{N} \cup \{0\}$ tal que*

- $\|a_N\|_p = \max_{n \in \mathbb{N} \cup \{0\}} \|a_n\|_p$.
- $\|a_n\|_p < \|a_N\|_p \quad \forall\, n > N$.

Então f tem no máximo N zeros em $\mathbb{Z}_p$.

Por exemplo, para a série de potências $\sum_{n=1}^{\infty} n!\, x^n$, que se pode reescrever como $f(x) = \sum_{n=0}^{\infty} (n+1)!\, x^n$, o número mágico N é $p-2$ e $\|a_N\|_p = 1$. Logo o teorema anterior indica que $\sum_{n=0}^{\infty} (n+1)!\, x^n$ se anula quando muito $p-2$ vezes em $\mathbb{Z}_p$. O que confirma que $L_2 = f(1) \neq 0$, mas não fornece pistas sobre as distâncias dos zeros de f a 0 quando $p > 2$.

Referências

[1] E.T. Bell, *The Iterated Exponential Integers*, Annals of Math., Second Series, Vol. 39, No. 3 (1938), 539–557.

[2] F.Q. Gouvêa, *p-adic numbers: an introduction*, Springer-Verlag, Berlin, 2000.

[3] K. Hensel, *Über die Normenreste und Nichtreste in den allgemeinsten relativ-Abelschen Zahlkörpern*, Mathematische Annalen 85, 1 (1922), 1–10.

[4] N. Koblitz, *p-adic numbers, p-adic analysis and zeta-functions*, Springer-Verlag, Berlin, 1984.

[5] K. Mahler, *p-adic numbers and their functions*, Cambridge University Press, 1973.

[6] W.H. Schikhof, *Ultrametric calculus: an introduction to p-adic analysis*, Cambridge Studies in Advanced Mathematics 4, Cambridge University Press, 1984.

[7] W. Sierpinski, *Elementary theory of numbers*, North-Holland, 1988.

[8] M. Spivak, *Calculus*, Publish or Perish, Houston, 1994.

[9] J.Touchard, *Propriétés arithmétiques de certains nombres récurrents*, Ann. Soc. Sci. Bruxelles Ser. A, 53 (1933), 21–31.

[10] S. Willard, *General Topology*, Addison-Wesley, 1970.