por **Graciano de Oliveira**
[Universidade Lusófona de Lisboa]

O Corpo dos *p*-ádicos

A construção do corpo dos números reais via sucessões de Cauchy é bem conhecida. Existem muitos corpos mas o corpo dos reais e o seu fecho algébrico, o dos complexos, desempenham na matemática um papel ímpar. Será possível fazer o mesmo, mas com uma métrica para os racionais diferente da habitual (caso exista outra!)? A resposta é sim e isso leva-nos a um outro e estranho reino, o dos *p*-ádicos.

1. Introdução

Há anos publiquei numa Folha Informativa distribuída na época pela Sociedade Portuguesa de Matemática o seguinte texto com o título "Uma Equação do Primeiro Grau".

A um matemático (não se sabe se caloiro se muito avançado) foi posto o seguinte problema:
Resolva a equação $x=1+3x$.
O enunciado do problema era este, nem mais palavra nem menos palavra.
O matemático pensou assim: vou utilizar um método iterativo como a forma da equação sugere.
Escreveu

$$x_{n+1}=1+3x_n$$

e tomou para x_0 *o valor 1. Obteve sucessivamente*

$$x_0=1$$
$$x_1=1+3$$
$$x_2=1+3+3^2$$
$$\ldots$$
$$x_n=1+3+3^2+\ldots+3^n.$$

Em seguida tomou limites e concluiu que a solução a seria

$$a=\sum_{i=0}^{\infty} 3^i.$$

Pensou que não seria bom apresentar a solução como sendo a soma de uma série. Depois de pensar um momento recordou-se de que

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

Substituiu α *por* **3** *e obteve* $-\frac{1}{2}$. *Como era cuidadoso voltou à equação, escreveu* $-\frac{1}{2}$ *em vez de x e verificou que de facto era raiz. Satisfeito, arrumou os papéis onde tinha feito os cálculos e embrenhou-se noutro problema na esperança de se sair tão bem como neste.*

Perguntas: 1. Que comentários faria a esta maneira de resolver a equação? 2. A resolução está certa ou errada? 3. Há razões para dizer que houve milagre?

Só um colega me abordou com respostas (diferentes das que me tinham motivado) a estas perguntas.

Quais seriam as respostas a esperar às perguntas acima formuladas? Provavelmente a grande maioria dos leitores esperaria respostas do tipo:

1. Fez-se o que se faz noutras circunstâncias mas está errado e é surpreendente que o resultado final esteja certo.

2. Errado. A série

$$1+\alpha+\alpha^2+\ldots$$

não converge para $|\alpha|\geq 1$, logo não se pode substituir α por 3.

3. Até parece que houve milagre. Muito estranho.

Mas, na minha terceira pergunta, muitos não se limitariam a uma resposta tão sucinta. Diriam que quando alguma coisa funciona sem se perceber porquê ou há coincidências ou semelhanças inexplicáveis, há uma razão escondida para isso. Em tais casos, deve procurar-se se é possível construir uma teoria que dê racionalidade, elimine os milagres e torne tudo compreensível. O problema reside em descobrir os conceitos apropriados. Pode recordar-se a Teoria das Distribuições e a função de Dirac, o início dos números complexos e muitos outros exemplos. E vale a pena lembrar as teorias unificadoras (dão unidade a factos dispersos que parecem coincidências) como a Teoria dos Matróides em conjunção com o artigo fundador de H. Whitney publicado na década de trinta.

Voltando ao raciocínio do nosso matemático, verifica-se que só há um ponto fraco: a série $1+3+3^2+\cdots$ não converge. Será possível fazê-la convergir? Substituamos a série pela sucessão associada em que o elemento u_n é a soma das primeiras $n+1$ parcelas da série. Convergência ou divergência de sucessões é uma questão de topologia, no nosso caso simplesmente uma questão de métrica. No caso vertente, só lidamos com números racionais (para efeitos de convergência até é com inteiros, mas há vantagem em utilizarmos os racionais uma vez que constituem um corpo e assim todos os elementos, distintos de zero, têm inverso). Então atentemos nos números racionais. Dada uma sucessão $u_0, u_1, \ldots$ de racionais, é possível fazê-la convergir? Melhor (no nosso caso) será possível definir uma métrica nos racionais de modo que convirja? É melhor começar pelo início, como diria Lapalisse. Vejamos o que é uma métrica e que métricas são possíveis em $\mathbb{Q}$.

Qual é a métrica usual ou, se preferirmos, o que é a distância de dois números racionais? A distância é definida à custa da noção de valor absoluto: a distância de r a s é o valor absoluto da diferença $r-s$. E o que é o valor absoluto dum racional? Como sabemos, se o racional $\frac{m}{n}$ é positivo, o seu valor absoluto é ele próprio, se é negativo, é o seu simétrico e se é zero, o valor absoluto é zero.

Notemos que o valor absoluto começa por ser uma aplicação ϕ de $\mathbb{Q}$ em $\mathbb{Q}_+$ (racionais não negativos). Aplicação essa que, provavelmente, deverá satisfazer certas condições.

Um pouco de estudo leva-nos à conclusão de que o importante não é a concretização da aplicação de $\mathbb{Q}$ em $\mathbb{Q}+$ mas sim certas propriedades que ela pode ter (ou não ter). Se se examinarem as demonstrações cuidadosamente, conclui-se que o que essencialmente se utiliza para os grandes resultados são certas propriedades de ϕ, não sendo importante o que ϕ é de facto. São elas as seguintes:

1. $\phi(r)=0 \Leftrightarrow r=0$
2. $\phi(rs)=\phi(r)\phi(s)$
3. $\phi(r+s)\leq \phi(r)+\phi(s)$

Qualquer que seja ϕ, praticamente todas as consequências continuam válidas, e com as mesmas demonstrações, desde que satisfaça estas três propriedades.

Surge então a pergunta: existirão outras aplicações $\phi: \mathbb{Q}\to\mathbb{Q}_+$ que satisfaçam 1, 2 e 3?

A resposta é sim. Uma delas é $\phi(0)=0$, $\phi\left(\frac{m}{n}\right)=1$ sempre que $\frac{m}{n}\neq 0$. É o caso chamado trivial, pois não conduz a nada de interessante (tanto quanto se sabe).

Mas há mais, como vamos ver. Pode ser que alguma delas torne convergente a série $\sum_{i=0}^{\infty} 3^i$.

Fixemos um número primo (positivo) p qualquer. Dado um racional $\frac{m}{n}$, onde supomos que m e n são inteiros sem factores comuns, ele pode escrever-se, de maneira única, na forma

$$\frac{m}{n}=p^k\frac{m'}{n'},$$

onde k é um inteiro (positivo, negativo ou nulo) e m' e n' são inteiros não divisíveis por p.

Por exemplo, se tomarmos p=5, a fracção $\frac{3}{10}$ escreve-se

$$\frac{3}{10}=5^{-1}\frac{3}{2}.$$

Definamos um novo valor absoluto (ou norma) de $\frac{m}{n}$, designado por $\rho_p\left(\frac{m}{n}\right)$, do seguinte modo:

$$\rho_p\left(\frac{m}{n}\right)=p^{-k}.$$

No caso do nosso exemplo, será

$$\rho_\infty\left(\frac{3}{10}\right)=5.$$

O valor absoluto habitual de $\frac{m}{n}$ será designado por $\rho_\infty\left(\frac{m}{n}\right)$ (há boas razões para escolher o índice ∞, que aqui não nos interessam). Assim

$$\rho_\infty\left(\frac{3}{10}\right)=\frac{3}{10}.$$

É um exercício fácil mostrar que ρ_p satisfaz as propriedades 1., 2. e 3. acima. Quanto à propriedade 3., verifica-se, na realidade, uma relação mais forte $\rho_p(r+s)\leq \max\{\rho_p(r),\rho_p(s)\}$como facilmente se prova.

Vejamos outro exemplo com o número 93.750. Claro que

$$\rho_\infty(93.750)=93.750.$$

Calculemos a norma ρ_5 deste número.

Como $93.750=5^6\times 6$, teremos

$$\rho_5(93.750)=5^{-6}=\frac{1}{15.625}=0{,}000064.$$

Em termos intuitivos dir-se-ia que na norma ρ_∞ o número em causa é grande, mas na norma ρ_5 é muito pequeno. Como consequência, na norma ρ_∞ os números 93.751 e 1 estão a grande distância, mas na norma ρ_5 estão próximos. Depois destas observações, não é de espantar que os resultados que se obtêm a respeito de convergência sejam muito diferentes.

Com $p=3$, $\lim_{n\to\infty}3^n=0$. De facto, $\rho_3(3^n)=\frac{1}{3^n}$. Como

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

tomando limites quando $n\to\infty$ podemos escrever

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

Significa que a série que apareceu a propósito da resolução da equação $x=1+3x$ é convergente com a norma ρ_3.

E mais, converge para $-\frac{1}{2}$ pelo que o raciocínio do nosso matemático está correcto. Basta supor que a norma utilizada era a norma ρ_3. A situação só parece insólita quando se pressupõe a utilização da norma habitual ρ_∞.

2. A construção dos números reais

Vamos explorar mais o conceito de ρ_p. Como veremos, chegaremos a um mundo novo de cuja existência nem suspeitávamos.

É bem conhecida a construção dos números reais a partir dos racionais. Vamos recordá-la rapidamente.

Uma sucessão de racionais $u_0,u_1,...$ diz-se de Cauchy se para todo o número racional, positivo mas arbitrário ε, existe um número natural n_0 tal que

$$n>_0 n \Rightarrow |u_{n+r}-u_n|<\varepsilon,$$

qualquer que seja o número natural r.

Duas sucessões de Cauchy $u_0, u_1, ...$ e $v_0, v_1, ...$ dizem-se equivalentes se para todo o racional, positivo, arbitrário ε existe um inteiro n_0 tal que

$$n>n_0 \Rightarrow |u_n-v_n|<\varepsilon.$$

Trata-se de uma relação de equivalência compatível com as operações de adição e produto. Isto significa que se

$$u_0,u_1,...u_n,...\sim v_0,v_1,...v_n,...$$

e

$$u'_0,u'_1,...u'_n,...\sim v'_0,v'_1,...v'_n,...$$

então

$$u_0+u'_0,u_1+u'_1,...u_n+u'_n,...\sim v_0+v'_0,v_1+v'_1,...v_n+v'_n,...$$

e

$$u_0u'_0,u_1u'_1,...u_nu'_n,...\sim v_0v'_0,v_1v'_1,...v_nv'_n,...$$

Devido a estas propriedades, as classes de equivalência podem somar-se e multiplicar-se, obtendo-se um corpo. Não entraremos em mais pormenores, diremos só que o que se obtém é o corpo dos números reais. E depois pode estender-se aos números reais a noção de valor absoluto que já existia nos racionais do seguinte modo. Seja $u_0,u_1,...u_n,...$ uma sucessão qualquer da classe de equivalência do real r. Será, por definição,

$$\rho_\infty(r)=\lim_{n\to\infty}\rho_\infty(u_n)$$

que existe e não depende da sucessão particular escolhida para representar r como se pode demonstrar. Agora, define-se a distância de r a s como sendo $\rho_\infty(r-s)$.

O corpo dos reais tem uma propriedade importantíssima que os racionais não tinham: toda a sucessão de Cauchy de números reais converge para um número real.

Como representar um número real (que não é mais do que uma classe de equivalência, contendo uma infinidade de sucessões)? Haverá, em cada classe, uma sucessão canónica? Vamos estudar este problema.

Por exemplo o número π (real, mas não racional) costuma representar-se pela sucessão

$$3,3+\frac{1}{10},3+\frac{1}{10}+\frac{4}{10^2},3+\frac{1}{10}+\frac{4}{10^2}+\frac{1}{10^3},3+\frac{1}{10}+\frac{4}{10^2}+\frac{1}{10^3}+\frac{5}{10^4},...$$

ou seja, como soma da série

$$3+\frac{1}{10}+\frac{4}{10^2}+\frac{1}{10^3}+\frac{5}{10^4},...$$

De maneira notacionalmente mais simples, costuma escrever-se π=3,1415… o que nos dá os coeficientes das sucessivas potências de 10 na série, como é bem conhecido. Além de nos dar os coeficientes das sucessivas potências de 10, não encerra qualquer ambiguidade, representando um número real bem definido. A 3,1415… chama-se dízima. Temos pois a seguinte propriedade: todo o número real se pode representar como soma

de uma série cujos termos são certos coeficientes (um número de 0 a 9) multiplicados pelas sucessivas potências de 10, as de expoente positivo em número finito, as de expoente negativo em número finito ou infinito.

Vejamos a questão da unicidade, ou seja, vamos tentar responder a esta pergunta: um número tem sempre uma só dízima? Nem sempre é assim, há casos em que tem duas. É bem sabido que

$$31{,}2574=31{,}257399999\ldots$$

Designemos este número por r. Quando escrevemos $r=31{,}2574$ queremos dizer que

$$r=3\times10+1+\frac{2}{10}+\frac{5}{10^2}+\frac{7}{10^3}+\frac{4}{10^4}$$

e quando escrevemos $r=31{,}25739999\ldots$ queremos dizer que

$$r=3\times10+1+\frac{2}{10}+\frac{5}{10^2}+\frac{7}{10^3}+\frac{3}{10^4}+\frac{9}{10^5}+\frac{9}{10^6}+\frac{9}{10^7}+\cdots.$$

Reconhece-se que não há qualquer contradição, notando que

$$\frac{9}{10^5}+\frac{9}{10^6}+\frac{9}{10^7}+\cdots=\frac{1}{10^4}.$$

Portanto o número 31,2574 tem duas dízimas distintas, o que significa que pode escrever-se como soma de uma série de potências de 10 de duas maneiras diferentes. São os casos deste tipo os únicos em que não há unicidade da dízima. Não apresentaremos aqui os pormenores das demonstrações, pois pressupomos esta matéria bem conhecida, só pretendemos recordar.

3. A construção dos números p-ádicos

Depois desta digressão pelos números reais, imaginemos o seguinte. Façamos o mesmo que fizemos para, a partir dos racionais, construir os reais com uma ligeira alteração: sempre que necessitarmos de uma norma, utilizemos a norma ρ_p (p um primo qualquer) em vez da norma habitual ρ_∞.

Obtém-se igualmente um corpo que se chama corpo dos números p-ádicos e se representa por $\mathbb{Q}_p$. Claramente contém os racionais mas é muito diferente do corpo dos reais em diversos aspectos. Por exemplo, a série

$$1+p+p^2+p^3+\cdots+p^n+\cdots$$

é convergente. Isso é fácil de provar. É claro que

$$1+p+p^2+\cdots+p^n=\frac{1-p^{n+1}}{1-p}.$$

Como $\rho_p(p^{n+1})=\frac{1}{p^{n+1}}$, $\lim_{n\to\infty} p^{n+1}=0$. Então podemos escrever

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

Outro exemplo de uma propriedade inesperada é o seguinte:

Dada uma série de p-ádicos

$$\sum_{i=0}^{\infty} u^i,$$

ela converge se e só se $\lim u_n=0$.

A demonstração é fácil. Sabemos que qualquer que seja a métrica (designemos uma métrica não especificada por ρ), para que uma série de termo geral u_i convirja é necessáro e suficiente que dado um número real positivo ε exista sempre um n_0 tal que

$$n>n_0\Rightarrow\rho(u_n+u_{n+1}+\cdots+u_{n+t})<\varepsilon$$

para todo o t.

Isto vale para qualquer norma e implica $u_n \to 0$.
Se considerarmos a norma ρ_p e recordarmos que

$$\rho_p(u_n+u_{n+1}+\cdots+u_{n+t}) \leq \max\{\rho_p(u_n), \rho_p(u_{n+1}),\ldots, \rho_p(u_{n+t})\},$$

deduz-se facilmente que $u_n \to 0$ implica a convergência da série.

A situação no caso dos *p*-ádicos é, portanto, muito mais simples do que no caso dos reais.

Voltemos ao problema de como representar cada número *p*-ádico. Existirá algo de parecido com a dízima? Pode provar-se que sim. Cada *p*-ádico pode representar-se como soma de uma série do tipo

$$s=\frac{a_{-k}}{p^k}+\cdots+\frac{a_{-1}}{p}+a_0+a_1p+\cdots+a_np^n+\cdots \qquad (1)$$

onde cada coeficiente a_i é um número inteiro satisfazendo $0 \leq a_i \leq p-1$.

Esta representação é única, sem qualquer excepção.

Há outra diferença importante em relação aos reais. O número de potências de expoente negativo de p é sempre finito e é o número de potências de expoente positivo que pode ser finito ou infinito. Obviamente o *p*-ádico acima pode, de maneira mais simples, escrever-se na forma

$$a_{-k}\cdots a_0, a_1\cdots a_n\cdots \qquad (2)$$

com $a_i \in \{0,1,\ldots, p-1\}$.

A convenção é que a_j é o coeficiente de p^j e que a vírgula se põe depois do coeficiente de p^0.

É como no caso dos reais em que, em vez de

$$b_k10^k+\cdots+b_{-1}10+b_0+\frac{b_1}{10}+\cdots+\frac{b_n}{10^n}+\cdots,$$

onde cada b_i é um inteiro satisfazendo $0 \leq b_i \leq 9$, costuma escrever-se

$$b_k\cdots b_{-1}b_0, b_1\cdots b_n\cdots$$

Com os números reais nesta forma, existem algoritmos (que antigamente se aprendiam na Escola Primária, hoje 1.º ciclo do Ensino Básico) para as 4 operações fundamentais e outras, como a raiz quadrada.

Para os *p*-ádicos a situação é idêntica, existem também esses algoritmos e são fáceis de utilizar.

Vamos exemplificar com a soma (atenção aos casos em que há *transporte* como nos reais). De um exemplo, apreende-se facilmente o algoritmo e começaremos por um caso em que não há *transporte*. Utilizaremos a forma (1) em vez da forma (2).

Com $p=5$ calculemos a soma dos números

$$2\,p^{-3}+1p^{-2}+0\,p^{-1}+4+3p+1p^2+\cdots$$

e

$$3p^{-2}+4\,p^{-1}+0+1p+1p^2+\cdots$$

Pode fazer-se assim

$$\begin{array}{r} 2p^{-3}+1p^{-2}+0p^{-1}+4+3p+1p^2+\cdots \\ 3p^{-2}+4p^{-1}+0+1p+1p^2+\cdots \\ \hline 2p^{-3}+4p^{-2}+4p^{-1}+4+4p+2p^2+\cdots \end{array}$$

Este esquema compreende-se sem mais explicações.

Quando há transporte, é ligeiramente mais complicado como, aliás, no caso dos reais, havendo mesmo quem defenda que o seu ensino aos muito jovens pode traumatizar para toda a vida. Se, por exemplo, onde, na primeiro parcela, está $1p^{-2}$ estivesse 4 p^{-2} é claro que como soma de $4p^{-2}$ com $3p^{-2}$ se obteria $7p^{-2}$. O coeficiente 7 excede p, que é 5, em 2 unidades. Faz-se como no caso de transporte com os reais: $7\,p^{-2} = (p+2)\,p^{-2} = 2\,p^{-2} + p^{-1}$, pelo que, na soma, onde está $4p^{-2}$ dever-se-ia pôr 2 p^{-2} e adicionar p^{-1} à parcela seguinte que levaria a substituir 4 p^{-1} por $5p^{-1}$. Como $5p^{-1}=1$ e este adicionado a 4 dá p, deveríamos substituir $4p$ por $5p = p^2$ que com 2 p^2 dará $3p^2$. O total passaria a ser

$$2\,p^{-3}+2\,p^{-2}+0\,p^{-1}+0+0\,p+3p^{2}+\cdots$$

O estudo cuidado deste exemplo é suficiente para compreender a ideia. O leitor mais desejoso de dominar a técnica só tem uma coisa a fazer: praticar.

Poderíamos apresentar algoritmos para outras operações (que não são muito difíceis de reinventar para o leitor interessado).

A métrica (ou norma) ρ_p definida em $\mathbb{Q}$ pode estender-se a $\mathbb{Q}_p$ como no caso dos reais. O p-ádico s, da fórmula (1), é o limite da soma S_m dos primeiros m termos da série. Ora, qualquer que seja m, $\rho_p(S_m)=p^k$, donde $\lim_{p\to\infty}\rho_p(S_m)=p^k$ que é, por definição, a norma ρ_p do p-ádico em questão. Conclui-se que quando temos um número p-ádico escrito naquela forma, é fácil determinar a sua norma ρ_p.

Os p-*ádicos* x cuja norma satisfaz $\rho_p(x)\leq 1$ chamam-se inteiros p-ádicos. São, pois, os p-ádicos em que na forma (1) não aparecem potências de p de expoente negativo. Eles constituem um domínio de integridade contido em $\mathbb{Q}_p$. Como exercício, pode o leitor tentar provar esse facto.

4. Como encontrar as dízimas dos racionais

Como sabemos $\mathbb{Q}\subseteq\mathbb{Q}_p$. Portanto os racionais são p-ádicos e admitem desenvolvimentos do tipo (1). Como os conseguir? Quando é finita a dízima?

Se

$$q=\frac{b_m}{p^m}+\cdots+\frac{b_1}{p}+b_0+b_1p+\cdots+b_np^n,$$

é fácil verificar que q é um número racional, não negativo cujo denominador é uma potência de p. O inverso será verdadeiro? É. Comecemos com um inteiro não negativo r. Dividindo por p, teremos

$$r=pq_1+r_1,\ 0\leq r_1\leq p-1.$$

Dividindo agora o quociente q_1 por p,

$$q_1=pq_2+r_2$$

donde

$$r=p^2q_2+pr_2+r_1.$$

Prosseguindo, acaba por se ter o número r escrito segundo potências de p de expoente não negativo e coeficientes em $\{0,1,\ldots,p-1\}$. Podemos dizer que todo o inteiro positivo se pode representar como polinómio em p cujos coeficientes são não negativos e inferiores a p. Uma fracção $s=\frac{r}{p^m}$ pode obviamente representar-se como o número q acima. Para o conseguir basta escrever r na forma $a_0+a_1p+\cdots+a_np^n$ o que dá (supondo, para fixar ideias, $m<n$)

$$s=\frac{a_0}{p^m}+\frac{a_1}{p^{m-1}}+\cdots+a_np^{n-m}.$$

Como representar como série de potências de p os números fraccionários em geral, incluindo os números negativos? Por exemplo,

$$-1=(p-1)+(p-1)p+(p-1)p^2+\cdots \qquad (3)$$

e a justificação é simples.

De facto,

$$(p-1)+(p-1)p+(p-1)p^2+\cdots=(p-1)(1+p^2+p^3+\cdots)$$

e como sabemos que $1+p+p^2+\cdots=\frac{1}{1-p}$, fica a justificação completa.

Examinemos melhor o que significa $s_n=\sum_{i=0}^{n}(p-1)p^i$ convergir para -1. Para os sucessivos valores de n temos

$$s_0 = -1+p$$
$$s_1 = -1+p^2$$
$$s_2 = -1+p^3$$
$$\dots$$
$$s_n = -1+p^{n+1}$$

Ou seja, a diferença entre S^n e -1 torna-se muito pequena e, desde que tomemos n suficientemente grande, tão pequena quanto queiramos. Isto corresponde a dizer que a diferença entre S_n e -1 se torna divisível por potências de p de expoentes elevados, e, desde que tomemos n suficientemente grande, torna-se divisível por potências de p com expoentes tão grandes quanto queiramos.

Como fazer para outros números inteiros negativos? Claro que se -1 é dado por (3), será

$$-2 = (p-2) + (p-1)p + (p-1)p^2 + \cdots$$
$$-3 = (p-3) + (p-1)p + (p-1)p^2 + \cdots$$
$$\cdots$$
$$-p = (p-1)p + (p-1)p^2 + \cdots$$

Propomos agora ao leitor que procure continuar com $-p$-1,$-p$-2, etc. Não deve esquecer-se de que todos os coeficientes das potências de p devem pertencer a $\{0,1,\dots,p-1\}$. E propomos um problema mais geral: dado um número s por (1), determinar a representação (na mesma forma) do seu simétrico.

Se quisermos fazer o desenvolvimento de, por exemplo, $\frac{11}{2}$, como proceder? Se p=2, é fácil pois $11=2^3+2+1$ de onde tiramos $\frac{11}{2}=2^2+1+\frac{1}{2}$.

Suponhamos $p\neq 2$, por exemplo, p=5. Como $\rho_5\left(\frac{11}{2}\right)=1$, o desenvolvimento será da forma

$$\frac{11}{2} = a_0+a_1p+a_2p^2+\cdots$$

com $a_i\in\{0,1,\dots,p-1\}$ e certamente $a_0\neq 0$. Note-se que o segundo membro não pode ter um número finito de parcelas porque se tivesse seria um inteiro não negativo.

Podemos escrever

$$11=1+2\times 5=2a_0+2a_1p+2a_2p^2+\cdots \qquad (4)$$

onde o coeficiente $2a_0$ é um inteiro positivo satisfazendo $0\leq 2a_0\leq 2(p-1)$. Note-se que $1+2\times 5$ é um desenvolvimento da forma (1) mas $2a_0 + 2a_1p +\cdots$ não é necessariamente um desenvolvimento desse tipo porque pode haver coeficientes $2a_i$ que não pertençam a $\{0,1,\dots,p-1\}$. Não se pode, pois, invocar a unicidade dos desenvolvimentos do tipo (1) para concluir que $2a_0$=1. Mas podemos proceder de outro modo. Sendo $2a_0$ um inteiro não negativo, ele pode escrever-se na forma $2a_0=a'_0+a'_1p+\cdots+a'_tp^t$ com $a'_i\in\{0,1,\dots,p-1\}$. Agora, pela unicidade, pode concluir-se que a'_0=1 ou, o que é o mesmo, $2a_0=1 \bmod 5$, $a_0\in\{0,1,3,4\}$. Será, pois, a_0=3. Entrando com este valor em (4) e tendo em conta que $2a_0=6=1+p$ vem

$$1+2\times 5 = (1+p) + 2a_1p + 2a_2p^2 +\cdots = 1+(2a_1+1)p + 2a_2p^2 +\cdots$$

Um raciocínio simples mostra que deverá ser

$$2a_1+1 = 2 \bmod 5$$

de onde se tira a_1=3. Como $2a_1+1=7=2+p$, podemos agora escrever

$$1+2\times 5 = 1+(2+p)p + 2a_2p^2 +\cdots = 1+2p+(2a_2+1)p^2 + 2a_3p^3 +\cdots$$

donde

$$2a_2 + 1 = 0 \bmod 5$$

que dá $a_2 = 2$.

Portanto

$$1 + 2\times 5 = 1 + 2p + (2a_3 + 1)p^3 + \cdots,$$

devendo ser

$$2a_3 + 1 = 0 \bmod 5$$

o que dá $a_3 = 2$, etc.

Conhecidos os valores de $a_0, a_1, a_2, \ldots$ podemos escrever

$$\frac{11}{2} = 3 + 3p + 2p^2 + 2p^3 + \cdots$$

O que é fácil de confirmar:

$$3 + 3p + 2p^2 + 2p^3 + \cdots = 3 + 3\times 5 + 2\times 5^2 (1 + p + p^2 + \cdots) = 18 + 50\left(\frac{1}{1-5}\right) = \frac{11}{2}.$$

Ainda outro exemplo. Calculemos, com $p=5$, a raiz quadrada de 7. Como $\rho_5(7) = 1$, a raiz quadrada de 7, caso exista, será da forma

$$\sqrt{7} = a_0 + a_1 p + a_2 p^2 + \cdots$$

e deveremos ter

$$(a_0 + a_1 p + a_2 p^2 + \cdots)^2 = 7 = 2 + 1\times 5,$$

donde $a_0^2 \equiv 2 \bmod 5$. Como esta equação não tem solução, podemos afirmar que, em $\mathbb{Q}_5$, $\sqrt{7}$ não existe. Como exercício, verifique-se que para $p=17$, existem duas raízes quadradas de 7.

Vejamos o que acontece com $\sqrt{6}$, ainda no caso $p=5$. Se existir deverá ser um inteiro p-ádico e satisfazer

$$(a_0 + a_1 p + a_2 p^2 + \cdots)^2 = 1 + 1\times 5.$$

Daqui tira-se que a_0 pode ser igual a 1 ou a 4. Continuando o processo, encontram-se as duas raízes que de facto existem em $\mathbb{Q}_5$. Recordamos que $\mathbb{Q}_5$ é um corpo e portanto nunca poderia haver mais do que duas.

Procuremos as raízes quadradas de -1 em $\mathbb{Q}_5$.

$$(a_0 + a_1 p + a_2 p^2 + \cdots)^2 = -1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots$$

com $p=5$, $a_0^2 \equiv 4 \bmod 5$ donde $a_0 = 2$ ou $a_0 = 3$.

Prosseguindo, conclui-se que -1 tem duas raízes quadradas dentro de $\mathbb{Q}_5$.

Quanto às raízes cúbicas de 6 em $\mathbb{Q}_7$, devemos começar com a equação

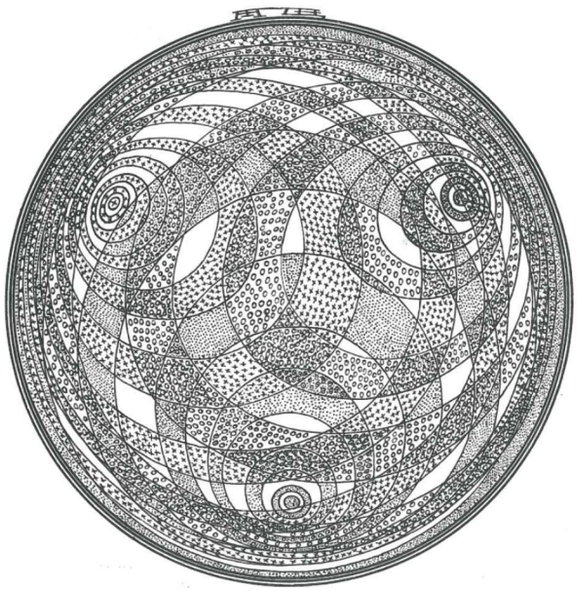
$$x^3 = 6$$

ou

$$(a_0 + a_1 p + a_2 p^2 + \cdots)^3 = 6$$

Pode ser $a_0 = 3, 5, 6$ e continuando obtêm-se três raízes.

Estes exemplos, e as analogias entre eles, levam a suspeitar de que deve existir um algoritmo mais geral. É o que vamos ver na secção a seguir.



Impressão de Anatoly Fomenko, matemático russo
e conhecido topólogo, sobre o disco unitário 3-ádico.

5. Lema de Hensel

Podemos dizer que $\mathbb{Q}_p$ é um corpo com propriedades extraordinariamente diferentes das de $\mathbb{R}$.

Nos exemplos que acabámos de dar estamos a utilizar, sem o saber, uma proposição de grande importância conhecida por Lema de Hensel. Vamos descrever essa proposição. Antes, recordemos que um inteiro p-ádico é um *p-ádico x* que satisfaz $\rho_p(x) \leq 1$.

Lema de Hensel *Seja* $f(x)=c_0+c_1x+\cdots+c_nx^n$ *um polinómio cujos coeficientes são inteiros p-ádicos. Seja* $f'(x)=c_1+2c_2x+\cdots+nc_nx^{n-1}$.

Seja $a_0=\tilde{a}_0+\tilde{a}_1p+\tilde{a}_2p^2+\cdots$ *um inteiro p-ádico que satisfaça*

$$f(a_0) = 0 \bmod p$$

e

$$f'(a_0) \neq 0 \bmod p.$$

Então existe um único inteiro p-ádico, a tal que

$$f(a) = 0 \text{ e } a = a_0 \bmod p.$$

Não daremos a demonstração, mas vamos explicar como obter aproximações sucessivas, $\tilde{a}_0$, a_1,a_2 ,..., da raiz que se diz existir.

A primeira aproximação é $\tilde{a}_0$ (primeiro coeficiente de a_0). Para as restantes é conveniente introduzir nova notação. Designaremos por $C_{p^n}(f(\alpha))$ o coeficiente de p^n no desenvolvimento de $f(\alpha)$. A segunda aproximação será dada por $a_1=\tilde{a}_0+b_1p$ com b_1 calculado por

$$b_1 = -\frac{C_p(f(\tilde{a}_0))}{f'(\tilde{a}_0)} \bmod p,\ b_1 \in \{0,1,\ldots,p-1\}.$$

A terceira aproximação será $a_2=\tilde{a}_0+b_1p+b_2p^2$ com b_2 calculado por

$$b_2 = -\frac{C_{p^2}(f(a_1))}{f'(a_1)} \bmod p,\ b_2 \in \{0,1,\ldots,p-1\}.$$

A seguinte será $a_3=\tilde{a}_0+b_1p+b_2p^2+b_3p^3$ com

$$b_3 = -\frac{C_{p^3}(f(a_2))}{f'(a_2)} \bmod p,\ b_3 \in \{0,1,\ldots,p-1\}.$$

etc.

O Lema de Hensel é o equivalente ao método de Newton para o cálculo de raízes de funções.

6. Séries de potências

Séries de potências são séries da forma

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

com $a_n \in \mathbb{Q}_p$ e $x \in \mathbb{Q}_p$. Como era de esperar, saber para que valores de x converge é um problema importante.

Teorema 6.1 *Seja*

$$R = \frac{1}{\limsup(\rho_p(a^n))^{\frac{1}{n}}}.$$

a) Se $R=0$ a série só converge para $x=0$ e se $R=\infty$, converge para todo o x de Q_p.

b) Se $R\neq 0,\infty$, há dois casos: (i) Se $\lim_{n\to\infty} \rho_p(a_n)R^n=0$, $f(x)$ converge se e só se $\rho_p(x)\leq R$; (ii) Se não se verificar aquela condição, $f(x)$ converge se e só se $\rho_p(x)<R$.

Não damos a demonstração deste teorema, que não é difícil. E salientamos uma propriedade notável: a série ou converge para todos os valores da fronteira da região de convergência ou não converge para nenhum. Logo, dada uma série, se se descobrir o que acontece num só ponto dessa fronteira, fica-se a saber o que acontece em todos. Podemos agora pensar em generalizar aos *p-ádicos* a exponencial, as funções trigonométricas, etc. Adivinha-se como o fazer. Vamos concentrar-nos no logaritmo.

Por definição (e como era de esperar)

$$\log(x+1) = \sum_{n=0}^{\infty} (-1)^{n+1}\frac{x^n}{n} = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots.$$

Para simplificar, designaremos $\log(1+x)$ por $g(x)$.

Qual o raio de convergência? Vamos estudar como se comporta $\rho_p(a_n)$ quando $n\to\infty$. Temos

$$\rho_p(a^n) = \rho_p\left(\frac{1}{n}\right) = p^{t(n)}$$

onde $t(n)$ é o expoente da maior potência de p que divide n: $n = p^{t(n)}n'$ e p não divide n'. Daqui vem $\sqrt[n]{\rho_p\left(\frac{1}{n}\right)} = p^{\frac{t(n)}{n}}$.

De $n=p^{t(n)}n'$ tira-se

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

pelo que $\frac{t(n)}{n} \to 0$ e, portanto,

$$\lim_{n\to\infty} \sqrt[n]{\rho_p\left(\frac{1}{n}\right)} = 1.$$

Por conseguinte, R=1. Que acontece para x=1? Para x=1, o termo geral da série não converge para zero. Por isso

$$g(x)=x-\frac{x^2}{2}+\frac{x^3}{3}-\frac{x^4}{4}+\cdots$$

converge se e só se $\rho_p(x)<1$.

Estes factos permitem-nos conclusões curiosas.

Como $\rho_p(-2)=\frac{1}{2}$ (estamos a tomar p=2), para x=-2 a série converge, o que nos dá

$$-\log(-1)=2-\frac{2^2}{2}+\frac{2^3}{3}-\frac{2^4}{4}+\cdots$$

Para x=0 vem log(1)=0. Ora 2log(-1) = $\log(-1)^2$ (esta propriedade mantém-se) ou seja 2log(-1)=0. Como estamos num corpo de característica zero (contém os racionais), deverá ser log(-1)=0. Podemos escrever

$$2+\frac{2^2}{2}+\frac{2^3}{3}+\cdots+\frac{2^n}{n}+\cdots=0.$$

À primeira vista (pensando em termos de números reais) esta igualdade parece absurda. Se se pensar que estamos no corpo dos reais dir-se-á que uma série de termos positivos não pode convergir para 0 e logo se notará que $\frac{2^n}{n}$ tende para infinito pelo que a série nem sequer converge. Mas como estamos no corpo $\mathbb{Q}_2$, converge!

E isso significa que se pode escolher n suficientemente grande para que o número racional positivo

$$2+\frac{2^2}{2}+\frac{2^3}{3}+\cdots+\frac{2^n}{n}$$

tenha um numerador divisível por qualquer potência de 2 de expoente previamente dado. Com mais rigor, acabámos de provar o:

Teorema 6.2 *Dado um inteiro m positivo, é sempre possível escolher n_0 tão grande que a soma*

$$\sum_{i=1}^{n}\frac{2^i}{i}$$

tenha um numerador divisível por 2^m para todo o $n \geq n_0$.

Terminamos com uma nota sobre a possibilidade de ordenar $\mathbb{Q}_p$. Dissemos que "uma série de termos positivos não pode convergir para zero" (nos reais). Em $\mathbb{Q}_p$ nem sequer se pode falar de elementos positivos porque (como acontece com o corpo dos complexos) $\mathbb{Q}_p$ não é um corpo ordenado. Vimos num exemplo atrás que, em $\mathbb{Q}_5$, -1 tem raízes quadradas. Isso mostra que $\mathbb{Q}_5$ não é formalmente real e, em consequência, não é ordenado. Pode demonstrar-se que a situação é idêntica para outros valores de p.

Bibliografia

[1] **F. Q. Gouvêa** (1993), *p-adic Numbers*. Spring Verlag.

[2] **N. Koblitz** (1977), *p-adic Numbers, p-adic Analysis and Zeta-Functions*. Spring Verlag.

[3] **L. Rédei**, *Algebra*, Pergamon Press.

[4] **H. Whitney** (1935), *On the Abstract Properties of Linear Dependence*, Amer. J. Math. Vol. 57 509-533.