Convergência de séries p-ádicas

João Lourenço

Faculdade de Ciências da Universidade do Porto

2°ano da Licenciatura em Matemática

Programa Novos Talentos em Matemática

Fundação Calouste Gulbenkian

26 de Maio de 2014

Analogia de Hensel

Consideremos o espaço $\mathbb{C}[X]$ dos polinómios com coeficientes complexos. Os elementos **primos** de $\mathbb{C}[X]$ são os polinómios da forma $(X - \alpha)$, a menos de associados, com um papel análogo aos primos de $\mathbb{N}$.

- Todo o natural maior do que 1 é um produto finito de primos.
- Dado um primo p, todo o natural pode ser escrito em base p como

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

sendo $0 \leq a_i < p$ inteiros e $n \in \mathbb{N} \cup \{0\}$.

Analogia de Hensel

Analogamente, é possível exprimir todo o polinómio não constante de $\mathbb{C}[X]$ como

- um produto finito de polinómios primos;
- uma soma

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

onde $a_i \in \mathbb{C}$ e $n \in \mathbb{N} \cup \{0\}$.

Analogia de Hensel

Além disso, sabemos que toda a fracção

$$\frac{P(X)}{Q(X)}$$

de elementos $P(X), Q(X) \in \mathbb{C}(X)$ admite uma expansão em série da forma

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

onde $k \geq 0$.

Se considerarmos todas as funções que podem ser expressas deste modo, obtemos um corpo que contém estritamente $\mathbb{C}(X)$, e onde se incluem, por exemplo, as funções exponencial e seno.

Analogia de Hensel

Querendo extender a analogia, teríamos de simultaneamente encontrar um modo de escrever todo o racional em base p, cujas expansões (em $\mathbb{R}$) geram somas como

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

mas também de admitir expressões da forma

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

cuja convergência em $\mathbb{R}$ não está assegurada.

Embora pudéssemos tratar estas expressões de modo formal, seria interessante dar-lhes um significado de convergência.

Espaços métricos

Definição

Um **espaço métrico** é um par (M, d), onde M é um conjunto e d uma função de $M \times M$ em $\mathbb{R}$ satisfazendo 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. $d(x, z) \leq d(x, y) + d(y, z)$

Exemplo

$M = \mathbb{R}^n, \quad d(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}$ (métrica usual em $\mathbb{R}^n$)

Completamento de um espaço métrico

Definição

Um espaço métrico diz-se **completo** se todas as sucessões de Cauchy desse espaço são convergentes.

Proposição

Seja (M, d) um espaço métrico. Então existe um espaço métrico completo (M^*, d^*) e uma função $\mathcal{C} : M \to M^*$ que preserva a métrica e tal que $\mathcal{C}(M)$ é denso em M^*, sendo M^* único a menos de isometria.

O espaço M^* diz-se um **completamento** do espaço métrico M.

Normas em $\mathbb{Q}$

Definição

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

1. $\|x\| \geq 0$, com igualdade se e só se $x = 0$
2. $\|xy\| = \|x\| \cdot \|y\|$
3. $\|x + y\| \leq \|x\| + \|y\|$

Para cada norma $\|\,.\,\|$, a função $d(x, y) = \|x - y\|$ define uma métrica em $\mathbb{Q}$, tornando assim $(\mathbb{Q}, d)$ num espaço métrico.

Métrica p-ádica

Definição

Dado um número primo p, a **norma p-ádica** $\|\cdot\|_p$ em $\mathbb{Q}$ é dada por

$$\|r\|_p = \begin{cases} p^{-n} & \text{se} \quad r \neq 0 \\ 0 & \text{se} \quad r = 0 \end{cases}$$

onde n é o único inteiro tal que $r = p^n \frac{a}{b}$, com $a, b \in \mathbb{Z}$, $b > 0$ e $(a, p) = (b, p) = 1$.

Note-se que a norma p-ádica só toma valores no conjunto discreto

$$\{p^n : n \in \mathbb{Z}\} \cup \{0\}.$$

Exemplo

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

Propriedade não-arquimediana

É possível mostrar que a métrica p-ádica verifica uma desigualdade mais forte que a triangular:

$$\|r+s\|_p \leq \max\{\|r\|_p, \|s\|_p\}$$

É interessante notar que esta desigualdade conduz a certas propriedades topológicas exóticas. Por exemplo:

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

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

III. *Uma sucessão de pontos é de Cauchy se e só se a distância entre os termos consecutivos tende para zero.*

$\mathbb{Q}_p$

O espaço métrico $(\mathbb{Q}, \|\,.\,\|_p)$ não é completo.

Definição

Denotemos por $\mathbb{Q}_p$ o completamento de $\mathbb{Q}$ relativo à norma $\|\cdot\|_p$.

Em $\mathbb{Q}_p$:

- $\mathbb{Q}$ é denso.
- Cada bola $B(a;\varrho)$ é um conjunto aberto e fechado.
- O conjunto de inteiros p-ádicos, $\mathbb{Z}_p = B[0;1]$, é compacto.
- $\mathbb{N}$ é denso em $\mathbb{Z}_p$.

$\mathbb{Q}_p$

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 $\|\,.\,\|_p$, de sucessões de racionais $(r_n)_{n\in\mathbb{N}}$ e $(s_n)_{n\in\mathbb{N}}$,

$$x = \lim_{n\to+\infty} r_n \quad \text{e} \quad y = \lim_{n\to+\infty} s_n$$

então está bem definida a soma

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

Observe-se que as propriedades multiplicativa e não-arquimediana da norma $\|\,.\,\|_p$ se mantêm em $\mathbb{Q}_p$.

Completamentos de $\mathbb{Q}$

Uma norma diz-se trivial se $\|0\| = 0$ e $\|x\| = 1$ para todo o $x \neq 0$.

Teorema (Ostrowski)

Seja $\|\cdot\|$ uma norma em $\mathbb{Q}$ e $\bar{\mathbb{Q}}$ o seu completamento. 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 $\mathbb{R}$).

Analogia de Hensel revisitada

É possível agora mostrar que todo o elemento de $\mathbb{Q}_p$ admite uma e uma só expansão p-ádica da forma descrita anteriormente:

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

Reduzindo ao caso $x \in \mathbb{Z}_p$, tratar-se-ia de encontrar uma sucessão de naturais $(\alpha_n)_n$ tal que

$$\alpha_{i+1} \equiv \alpha_i \ (mod\, p^i), \quad 0 \leq \alpha_i < p^i \quad \text{e} \quad \lim_{n \to +\infty} \alpha_n = x.$$

e verificar que é única. Note-se que isto corresponde também a afirmar que $\mathbb{N}$ é denso em $\mathbb{Z}_p$.

Critério de convergência

Em $\mathbb{R}$, uma condição necessária para a convergência de uma série é a de que a norma dos seus termos tenda para zero. Este critério não é, no entanto, suficiente, como mostra a série $\sum \frac{1}{n}$.

No caso dos p-ádicos, a situação não é a mesma.

Lema

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

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

Exemplo

A série $\sum_{n=1}^{\infty} n\, n!$ não converge em $\mathbb{R}$. Em $\mathbb{Q}_p$, qualquer que seja o primo p, tem-se

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

De facto, para todo o $k \in \mathbb{N}$,

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

e, portanto,

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

que converge para 0 quando k tende para $+\infty$.

Outros exemplos

- A série $\sum_{n=0}^{+\infty} \frac{1}{n!}$ converge para e em $\mathbb{R}$, mas diverge em $\mathbb{Q}_p$ para todo o primo p.
- A série $\sum_{n=0}^{+\infty} x^n$ converge em $\mathbb{Q}_p$ para $\frac{1}{1-x}$ se e só se $\|x\|_p < 1$.

  Assim, tem-se que a série $\sum_{n=0}^{+\infty} 3^n$ converge para $-\frac{1}{2}$ em $\mathbb{Q}_3$, mas diverge em $\mathbb{Q}_p$ para $p \neq 3$.
- A série harmónica $\sum_{n=1}^{+\infty} \frac{1}{n}$ diverge em todos os $\mathbb{Q}_p$ e também em $\mathbb{R}$.
- A série $\sum_{n=1}^{+\infty} \frac{n!}{(n!)^2+1}$ converge em todos os $\mathbb{Q}_p$ e também em $\mathbb{R}$.

Série convergente em todos os $\mathbb{Q}_p$ e em $\mathbb{R}$

Vejamos um outro modo de construir uma série que converge em todos os $\mathbb{Q}_p$ e em $\mathbb{R}$. Seja $2 < 3 < 5 < \cdots < p_k < \ldots$ a enumeração usual de todos os primos. Para cada natural n, definamos

$$a_n = \left(2^n\, 3^{n-1} \ldots p_{n-1}^2\, p_n\right)\left(p_{n+1}^{-1} \ldots p_{2n}^{-n}\right) p_{2n+1}^{-2}.$$

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 todo o $\mathbb{Q}_p$. Além disso,

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

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

Problema

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

Proposição

Consideremos a ordenação usual $p_1 < \cdots < p_k < \ldots$ *dos primos e escolhamos*

$$\beta \in \mathbb{R}$$

e, para cada $k \in \mathbb{N}$,

$$\gamma_k \in \mathbb{Q}_{p_k}.$$

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* $\mathbb{R}$.

Congruências

Definição

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 $x \equiv y \pmod{p^n}$ se

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

Trata-se de uma relação de equivalência (para a transitividade, basta aplicar a propriedade não-arquimediana de $\|\,.\,\|_p$) que não só se reduz à noção de congruência usual em $\mathbb{Z} \subseteq \mathbb{Q}_p$ como também satisfaz as propriedades usuais das congruências em inteiros.

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 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

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

Porém, se nos restringirmos a $\mathbb{Z}_p$, a congruência é preservada pelo produto.

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

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

$$\begin{cases} x \equiv x_1 \ (mod\ p_1^{\alpha_1}) \\ x \equiv x_2 \ (mod\ p_2^{\alpha_2}) \\ \vdots \\ x \equiv x_k \ (mod\ p_k^{\alpha_k}) \end{cases}$$

onde $x_i \in \mathbb{Q}_{p_i}$ e os p_i são todos distintos.

Podemos assumir sem perda de generalidade que $x_i \in \mathbb{Z}_{p_i}$, $1 \leq i \leq k$. Como $\mathbb{N}$ é denso nos inteiros p-ádicos, podemos escolher naturais n_i tais que

$$x_i \equiv n_i \ (mod\ p_i^{\alpha_i})$$

Obtemos assim o sistema equivalente

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

Este sistema é solúvel em $\mathbb{Z}$, 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

$$x_1 \equiv x_0 \ (mod\ p_i^{\alpha_i}).$$

Daqui resulta que

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

onde $q \in \mathbb{Q}$ é tal que

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

Também é claro que qualquer racional x_1 satisfazendo esta condição

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

onde $q \in \mathbb{Q}$ é tal que

$$\|q\|_{p_i} \leq 1,$$

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

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

onde

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

Solução do problema

Recorde-se que, dados $\gamma_k \in \mathbb{Q}_{p_k}$ e $\beta \in \mathbb{R}$, queremos encontrar uma série 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

$$S_n \equiv \gamma_k \ (mod\ p_k^{n+1-k})$$

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 $n \to +\infty$.

Construção de S_n

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

Convergência em $\mathbb{Q}_{p_k}$

Se fixarmos n, queremos que S_n seja solução do sistema

$$\begin{cases} x \equiv \gamma_1 \ (mod\ p_1^n) \\ x \equiv \gamma_2 \ (mod\ p_2^{n-1}) \\ \vdots \\ x \equiv \gamma_n \ (mod\ p_n) \end{cases}$$

Sabemos que existe sempre solução para o sistema acima, pelo que podemos garantir a desejada convergência de S_n em cada domínio p-ádico. Resta mostrar que a escolha de S_n pode ser feita de modo a garantir a convergência em $\mathbb{R}$.

Subgrupos densos de $\mathbb{R}$

Lema

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

Corolário

Seja $\mathcal{P}$ um subconjunto de primos com cardinal $|\mathcal{P}| \geq 2$ e consideremos o subgrupo $\langle \mathcal{P} \rangle$ de $(\mathbb{R}_+, \cdot)$ gerado por $\mathcal{P}$. Então $A_{\mathcal{P}} = \langle \mathcal{P} \rangle \bigcup -\langle \mathcal{P} \rangle$ 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 $|\mathcal{P}| \geq 2$. □

Convergência em $\mathbb{R}$

Para cada natural n, consideremos o subconjunto de primos

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

e observemos que

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

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

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

e resulta do corolário anterior que se trata de 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 $\mathbb{R}$.

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

Esta série não converge em $\mathbb{R}$ mas, para qualquer primo p, converge em $\mathbb{Q}_p$.

Proposição (Fórmula de Legendre)

Se $D_p(n)$ é a soma dos dígitos de n quando representado na base p, então

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

onde

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

Além disso, para n suficientemente grande, tem-se $D_p(n) \leq \frac{n}{2}$ e, portanto,

$$v_p(n!) \geq \frac{n}{2p-2}.$$

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

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

É ainda um problema em aberto saber qual o valor de L_p, se é racional ou mesmo se é não-nulo.

L_2

Como a soma parcial $S_n = 1 + 2! + 3! + \cdots + n!$ é um inteiro ímpar, para todo o $n \in \mathbb{N}$, sabemos que

$$\|S_n\|_2 = 1$$

logo

$$\|L_2\|_2 = 1$$

e, portanto, $L_2 \neq 0$.

L_p, para $p = 3, 5, 7, 11$

De modo análogo se verifica que

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

e, com algum esforço computacional, comprovámos que

$$\|L_p\|_p = 1 \quad \forall\, p \text{ primo tal que } 13 \leq p < 10^6.$$

Apesar de esta evidência computacional ser quase irrelevante, talvez seja verdade que, se p é primo, então

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

embora nada nesta análise numérica sugira como o provar.

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,

$$p \mid 1 + 2! + \cdots + (p-1)! \quad \Leftrightarrow \quad p = 3 \text{ ou } p = 11.$$

Com o Teorema de Wilson,

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

o problema reduz-se a provar que, se p é primo, então

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

e, como

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

bastaria provar que

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

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

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

Estes números satisfazem a seguinte relação de recorrência

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k.$$

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 $k \geq p$.

Proposição (Congruência de Touchard)

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,

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

Subfactorial

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

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

onde S_n é o grupo simétrico em n letras. Os primeiros valores de $!n$ são

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

Obtém-se, pelo Princípio de Inclusão-Exclusão, a fórmula fechada

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

Proposição

Seja p um primo ímpar. Então

$$1! + 2! + \ldots (p-1)! \equiv\, !(p-1) - 1 \ (mod\ p).$$

Lema

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

Demonstração.

Se $k < p-1$, basta proceder por indução, notando 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,

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

 F.Q. Gouvêa, *p-adic Numbers: An introduction*, Springer-Verlag, Berlin, 2000.

 N. Koblitz, *p-adic Numbers, p-adic Analysis and Zeta-functions*, Springer-Verlag, Berlin, 1984.