25 квітня

§15. p-адичні неперервні функції

$$\mathbb{Z}_p = \{ x = (x_n)_{n\geq 1} : \; x_n \in \{0, 1, \dots, p^n - 1\}, \; x_{n+1} \equiv x_n \pmod{p^n} \}$$

кільце p-адичних цілих чисел

$$x_{n+1} = x_n + a_n p^n \qquad 0 \leq a_n \leq p-1$$
$$(a_0 = x_1)$$

$$x = a_0 + a_1 p + a_2 p^2 + \dots$$

p-адичний розклад

$x \neq 0$ $\quad \mathrm{ord}_p(x) = \min\{n \geq 0 : x_{n+1} \neq 0\}$
$\quad = \min\{n \geq 0 : a_n \neq 0\}$

$\rho \in (0,1)$ фіксоване

$$|x|_p = \begin{cases} \rho^{\mathrm{ord}_p(x)} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

$\mathbb{Z}_p$ є поповненням метричного пр-ру $(\mathbb{Z}, |\cdot|_p)$

$\mathbb{Z}$ щільне в $\mathbb{Z}_p$

Зауважимо що $\mathbb{N} = \mathbb{Z}_{\geq 1}$ також є щільними в $\mathbb{Z}_p$.

Тому функції $f: \mathbb{N} \to \mathbb{Z}$ (це послідовності цілих чисел $f(1), f(2), f(3), \dots$) які є неперервними у p-адичній метриці однозначно продовжуються до

$$f: \mathbb{Z}_p \to \mathbb{Z}_p.$$

<u>Озн-ня</u> Функція $f: \mathbb{N} \to \mathbb{Z}$ є p-адично неперервною якщо для $\forall \varepsilon > 0 \ \exists \delta > 0$ т.щ. $|f(x) - f(y)|_p < \varepsilon$

коли $|x-y|_p < \delta$.

Еквівалентно: $\forall M \ \exists N$ т.щ.

$$p^N \mid (x-y) \Rightarrow p^M \mid (f(x) - f(y)).$$

<u>Приклад 1</u> $f(x) \in \mathbb{Z}[x]$

$$f(x) = \sum_{i=0}^{k} a_i x^i$$

$$f(x) - f(y) = \sum a_i (x^i - y^i)$$

$$= (x-y) \sum_{i=1}^{k} a_i (x^{i-1} + x^{i-2} y + \dots + y^{i-1})$$

$$p^N \mid (x-y) \Rightarrow p^N \mid (f(x) - f(y))$$

(Не-)приклад 2

$f(x) = a^x \quad a \in \mathbb{N}$

$f(x) - f(y) = a^y(\underbrace{a^{x-y} - 1}_{\text{не ділиться на } p \text{ коли } a \not\equiv 1\ (p)})$

нехай $x > y$

зафіксуємо y

візьмемо $x = y + p^N$

Мала т. Ферма $\Rightarrow a^p \equiv a \pmod p$

$\Rightarrow a^{p^N} \equiv a \mod p$

Якщо $a \not\equiv 1 \pmod p$ то $f(x)$ не є p-адично неперервною.

Тв-ня 1 Коли $a \equiv 1\ (p)$ $f(x) = a^x$ є p-адично неперервною.

Дов-ня Нехай $p^N \mid (x-y)$

$x = y + kp^N$

$a^k \equiv 1 \mod p$

$a^{kp} \equiv 1 \mod p^2$

$\dots$

$a^{kp^N} \equiv 1 \mod p^{N+1}$

$p^N \mid (x-y) \Rightarrow p^{N+1} \mid (f(x) - f(y))$

$\boxtimes$

(Не-)приклад 3 $f(x) = x!$

не є p-адично неперервною:

$$f(x)-f(y) = y!\left(\underbrace{\prod_{y<j\le x} j}_{} - 1\right)$$

$x > y$

Якщо $x = y + p^N$

цей добуток ділиться на p, тому

(добуток $-$ 1) на p не ділиться.

Спробуємо прибрати з добутка j т. щ. $p \mid j$.

$$f(x) = \prod_{1\le j\le x,\ p\nmid j} j$$

Узагальнена конгруенція Вільсона (д/з №5)

$$\prod_{\substack{1\le j< p^N \\ p\nmid j}} \equiv -1 \mod p^N$$

коли $p \neq 2$

$\boxed{\text{Відтепер нехай } p \text{ непарне, для простоти}}$

Тв-ня 2 Функція

$$f(x) = (-1)^x \prod_{\substack{1\le j\le x \\ p\nmid j}} j$$

є p-адично неперервною.

Дов-ня $\quad f(x)=(-1)^x \prod\limits_{\substack{1\le j\le x \\ p\nmid j}} j$

$$f(x)-f(y) = f(y)\times$$

$x>y$

$$x = y + kp^N \qquad \left(\underbrace{(-1)^{x-y} \prod_{\substack{y<j\le x \\ p\nmid j}} j}_{\equiv \ \bmod p^N} - 1 \right)$$

$kp^N \equiv k \pmod 2$

$$(-1)^k \Big(\underbrace{\prod_{y<j\le y+p^N} j}_{\equiv (-1)^k \bmod p^N} \Big)^k - 1$$

уз-ня Вільсона

$$\equiv 0 \mod p^N$$

$$p^N \mid (x-y) \Rightarrow p^N \mid (f(x)-f(y)) \quad \boxtimes$$

Зауважимо, що $f(x)$ приймає значення у $\{m\in\mathbb{Z} : p\nmid m\} \subset \mathbb{Z}_p^\times$.

Тому її p-адичне продовження за неперервністю

$$f : \mathbb{Z}_p \to \mathbb{Z}_p^\times .$$

Продовження (у заг. випадку):

$$f(s) = \lim_{\substack{x\in\mathbb{N} \\ x\to s}} f(x)$$

$s\in\mathbb{Z}_p$

p-адична границя

Історично,

$$-f(x-1) =: \Gamma_p(x)$$

називаеться p-адичною гамма функцією

$$\Gamma_p(x) = (-1)^x \prod_{\substack{1\le j<x \\ p\nmid j}} j$$

$$= (-1)^x \frac{j!}{\lfloor j/p \rfloor !\, p^{\lfloor j/p \rfloor}}$$

$x \in \mathbb{N}$

Порівняйте з:

$$\Gamma(s) = \int_0^\infty x^{s-1} e^{-x}\, dx \qquad s>0$$

класична гамма-функція

$$\Gamma(s+1) = s\,\Gamma(s)$$

$$\Gamma(x+1) = x! \qquad x \in \mathbb{N}$$

Вправа:

$\Gamma_p(0)$ – ?

$\Gamma_p(1)$ – ?

$\Gamma_p\left(\frac{1}{2}\right)$ – ?

$\Gamma_p(-1)$ – ?

$$\Gamma_p : \mathbb{Z}_p \to \mathbb{Z}_p^\times$$

Властивості:

i) $$\frac{\Gamma_p(s+1)}{\Gamma_p(s)} = \begin{cases} -s, & s \in \mathbb{Z}_p^\times \\ -1, & s \in p\mathbb{Z}_p \end{cases}$$

ii) $s \in \mathbb{Z}_p \quad s = s_0 + p s_1 \quad s_0 \in \{1, 2, \dots, p\}$

$$\Gamma_p(s)\,\Gamma_p(1-s) = (-1)^{s_0}$$

(Вправа)

Функції задані степеневими рядами

$$\sum_{n=0}^{\infty} a_n \qquad a_n \in \mathbb{Q}_p$$

збігається за озн-ням коли $A_N = \sum_{n=0}^{N} a_n$, $N \geq 0$

це пос-ть Коші.

$\mathbb{Q}_p$ повний метричний пр-р

$\Rightarrow$ сума збіжного ряду належить $\mathbb{Q}_p$

$M > N$

$$|A_M - A_N|_p = \left|\sum_{n=N+1}^{M} a_n\right|_p$$

$$\leq \max_{N < n \leq M} |a_n|_p$$

Ряд збігається т.т.т.к. $|a_n|_p \to 0$, $n \to \infty$

(вправа)

$$f(x) = \sum_{n=0}^{\infty} a_n x^n \qquad a_n \in \mathbb{Q}_p$$

$$R = \frac{1}{\limsup |a_n|_p^{1/n}}$$

збігається коли $|x|_p < R$

розбігається коли $|x|_p > R$

На колі $|x|_p = R$ ряд або збігається або роз-ся для всіх x залежно від того чи

$$|a_n|_p \cdot R^n \to 0, \quad n \to \infty.$$

<u>Приклад 4</u> $f(x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$

(розклад Тейлора $\log(1+x)$)

$$|a_n|_p^{1/n} = p^{-\frac{ord_p(n)}{n}}$$

$ord_p(n) \in \left[\frac{\log n}{\log p}\right]$

$\frac{ord_p(n)}{n} \xrightarrow[n\to\infty]{} 0$

$$\lim_{n\to\infty} |a_n|_p^{1/n} = 1$$

в $\mathbb{R}$

$3! \cdot 1$

Ряд збігається для x т.щ. $|x|_p < 1$, тобто $x \in p\mathbb{Z}_p$.

Коли $|x|_p = 1$ $(x \in \mathbb{Z}_p^\times)$

$$|a_n|_p = p^{-ord_p(n)} \not\to 0, \quad n \to \infty$$

ряд розбігається.

Функція $f(x-1) =: \log_p(x)$ наз-ся p-адичним логарифмом.

$$\log_p : 1 + p\mathbb{Z}_p \to p\mathbb{Z}_p$$

(вправа)

Приклад 5

$$f(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} =: \exp_p(x)$$

p-адична експонента

$$|a_n|_p = \rho^{-\mathrm{ord}_p(n!)} = \rho^{\frac{S_p(n)-n}{p-1}}$$

$$|a_n|_p^{1/n} = \rho^{\frac{S_p(n)/n - 1}{p-1}} \longrightarrow \rho^{-\frac{1}{p-1}}$$

$$R = \rho^{\frac{1}{p-1}} < 1. \qquad 0 < \frac{1}{p-1} < 1$$

$\Rightarrow$

$$\exp_p : p\mathbb{Z}_p \longrightarrow 1 + p\mathbb{Z}_p$$

$$\exp_p(py) - 1 = \sum_{n \geq 1} \frac{p^n y^n}{n!}$$

$y \in \mathbb{Z}_p$

$$\mathrm{ord}_p\left(\frac{p^n}{n!}\right) = n - \frac{n - S_p(n)}{p-1}$$

$$= \frac{S_p(n)}{p-1} + \frac{p-2}{p-1} n > 0$$

$p^n/n! \in p\mathbb{Z}_p$

$\Rightarrow \exp_p(py) - 1 \in p\mathbb{Z}_p$

Тв-ня 3 $\forall x, y \in p\mathbb{Z}_p$

$$\exp_p(x+y) = \exp_p(x)\, \exp_p(y)$$

$$\exp_p(x)\exp_p(y) = \sum_{n\geq 0}\frac{x^n}{n!}\sum_{m\geq 0}\frac{y^m}{m!}$$

$$= \sum_{k\geq 0}\sum_{n+m=k}\frac{x^n y^m}{n!\,m!}$$

У збіжного p-адичного ряду будь-яке перегрупування членів не змінює суми. (вправа)

$$\sum_{k\geq 0}\frac{(x+y)^k}{k!} = \exp_p(x+y)$$

В подібний спосіб доводиться, що

<u>Тв-ня 4</u> $\forall\, x, y \in p\mathbb{Z}_p$

$$\log_p((1+x)(1+y)) = \log_p(1+x) + \log_p(1+y)$$

Зауваження:

$$(1+x)(1+y) = 1 + \underbrace{x+y+xy}_{\in p\mathbb{Z}_p}$$

Ліва частина

$$\sum_{m\geq 1}(-1)^m\frac{(x+y+xy)^m}{m} = \sum_{k,l\geq 0} c_{k,l}x^k y^l$$

З того, що для дійсних розкладів Тейлора маємо

$$\log(1+x+y+xy) = \log(1+x) + \log(1+y)$$

$\Rightarrow$ $C_{k,l} = 0$ коли $k \neq 0$ і $l \neq 0$.

$\Rightarrow$ для p-адичних рядів тоді також

$$\sum C_{k,l}\, x^k y^l = \log_p(1+x) + \log_p(1+y).$$

З подібних міркувань $\Rightarrow$

<u>Тв-ня 5</u> Для $x \in p\mathbb{Z}_p$

$$\log_p(\exp_p(x)) = x$$

та

$$\exp_p(\log_p(1+x)) = 1+x.$$

Наприклад, доведемо перше:

$$\log_p(\exp_p(x)) = \sum_{m=1}^{\infty} \frac{(-1)^{m+1}}{m} \left(\sum_{n=1}^{\infty} \frac{x^n}{n!} \right)^m$$

є p-адично збіжним

$$= \sum_{k=1}^{\infty} C_k x^k \qquad C_k = \sum_{n \cdot m = k} \frac{(-1)^{m+1}}{m \cdot n!}$$

але ця формула не важлива

Цей перехід робить розклади Тейлора для функцій дійсного аргумента!

$$\log(\exp(x)) = x \qquad x \in \mathbb{R}$$

$$\Rightarrow \quad c_1 = 1$$
$$c_k = 0, \quad k > 0$$

Це доводить нашу рівність для p-адичного аргумента x. $\boxtimes$

$$\underset{\substack{\text{з}\\ \text{операцією}\\ +}}{p\mathbb{Z}_p} \underset{\log_p}{\overset{\exp_p}{\rightleftarrows}} \underset{\substack{\text{з}\\ \text{операцією}\\ \cdot}}{1 + p\mathbb{Z}_p}$$

Ці функції мають продовження на $\mathbb{Q}_p$ з такими самими алгебраїчними властивостями (див. N. Koblitz)