2 травня

§16. Числа Бернуллі

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

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

$\ldots$

$1^k+2^k+\ldots+n^k =$ многочлен степени $k+1$

<u>Оз-ня</u> Коефіцієнти Тейлора

$$\frac{t}{e^t-1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}$$

наз-ся числами Бернуллі.

$B_0=1$ $B_1=-\frac{1}{2}$ $B_2=\frac{1}{6}$ $B_3=0$ $B_4=-\frac{1}{30}$
$B_5=0$ $B_6=\frac{1}{42}$

Вправа: покажіть що коли $k>1$, непарне то $B_k=0$.

Многочлени Бернуллі $B_k(x)$, $k\geq 0$ визначаются твірною функцією

$$\frac{t\,e^{tx}}{e^t-1} = \sum_{k=0}^{\infty} B_k(x)\frac{t^k}{k!}$$

- $B_k(0) = B_k$
- $B_k(x) = \sum_{m=0}^{k}\binom{k}{m}B_{k-m}x^m$

$\deg B_k = k$

$$\frac{t\,e^{tx}}{e^t-1} = \sum_{l\geq 0} B_l\frac{t^l}{l!}\cdot\sum_{m\geq 0}\frac{x^m t^m}{m!}$$
$$= \sum_{k\geq 0}\frac{t^k}{k!}\sum_{l+m=k}\binom{k}{m}B_l x^m$$

• $B_k(x+1) - B_k(x) = k\, x^{k-1}, \quad k \geq 1$

$$\frac{t\, e^{t(x+1)}}{e^t - 1} - \frac{t\, e^{tx}}{e^t - 1} = \sum_{k=0}^{\infty} \left(B_k(x+1) - B_k(x)\right) \cdot t^k / k!$$

$$\| $$

$$\frac{t\, e^{tx}}{\cancel{e^t - 1}} \left(\cancel{e^t - 1} \right) = \sum_{k=1}^{\infty} \left(k\, x^{k-1}\right) \frac{t^k}{k!}$$

Тв-ня $\quad k \geq 0$

$$1^k + 2^k + \ldots + n^k = \frac{B_{k+1}(n+1) - B_{k+1}}{k+1}$$

Дов-ня $\quad k = 0$ ясно

бо $B_1(x) = x - \frac{1}{2}$

$k \geq 1$

$$\sum_{i=1}^{n} i^k = \sum_{i=0}^{n} \frac{B_{k+1}(i+1) - B_{k+1}(i)}{k+1}$$

$$= \frac{B_{k+1}(n+1) - B_{k+1}(0)}{k+1} \qquad \boxtimes$$

$B_0(x) \equiv 1$

$B_1(x) = x - \frac{1}{2}$

$B_2(x) = x^2 - x + \frac{1}{6}$

$B_3(x) = x^3 - \frac{3}{2}x^2 + \frac{x}{2}$

...

Мета: довести наступну властивість чисел Бернуллі

p просте

<u>Теорема</u> Якщо $(p-1) \nmid k$, то $\frac{B_k}{k} \in \mathbb{Z}_p$.

Якщо $(p-1) | k$ і k парне (або $p=2$, $k=1$) то

$$p B_k \equiv -1 \pmod p.$$

$$\left(\Leftrightarrow B_k + \sum_{\substack{p \text{ просте} \\ (p-1)|k}} \frac{1}{p} \in \mathbb{Z} \right)$$

Вправа

$B_2 = \frac{1}{6}$ $\quad \frac{1}{6} + \frac{1}{2} + \frac{1}{3} = \frac{1+3+2}{6} = 1$

$B_4 = -\frac{1}{30}$ $\quad -\frac{1}{30} + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} = \frac{-1+15+10+6}{30} = 1$

$B_6 = \frac{1}{42}$ $\quad \frac{1}{42} + \frac{1}{2} + \frac{1}{3} + \frac{1}{7} = 1$

$B_8 = -\frac{1}{30}$ $\quad -\frac{1}{30} + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} = 1$

$B_{10} = \frac{5}{66}$ $\quad \frac{5}{66} + \frac{1}{2} + \frac{1}{3} + \frac{1}{11} = 1$

$B_{12} = -\frac{691}{2730}$ $\quad \ldots = 1$

$B_{14} = \frac{7}{6}$ $\quad \frac{7}{6} + \frac{1}{2} + \frac{1}{3} = 2$

...

§17. p-адичне інтегрування

$N \geq 0$

Кожний $x \in \mathbb{Z}_p$ міститься у деякій множині виду

$a + p^N \mathbb{Z}_p$, $0 \leq a \leq p^N - 1$.

$$\mathbb{Z}_p = \bigsqcup_{a=0}^{p^N-1} a + p^N \mathbb{Z}_p$$

диз'юнктне об'єднання

Будемо називати множини виду $a + p^N \mathbb{Z}_p$, $0 \leq a \leq p^N - 1$ **дисками**.

В термінах загальної топології:

- диск є відкритою множиною
- диск є замкненою множиною

Більше того, диск є компактною множиною.

В метричних просторах компактність еквівалентна тому, що з кожної пос-ті ел-тів множини можна вибрати збіжну підпослідовність.

Вправа, для бажаючих: $X \subseteq \mathbb{Z}_p$ підмножина є відкритою і компактною тттк X є об'єднанням скінченної кількості дисків.

Ми будемо працювати зі скінченними об'єднаннями дисків і називати їх відкритими компактними множинами, з огляду на цей факт-вправу.

$X \subseteq \mathbb{Z}_p$ ком-ка від-та

Озн-ня p-адичний розподіл μ на X це адитивна функція

$$\mu : \{ U \subseteq X \text{ від-та ком-на} \} \to \mathbb{Q}_p .$$

Тобто: $U = U_1 \sqcup \ldots \sqcup U_n$

$\Rightarrow \mu(U) = \mu(U_1) + \ldots + \mu(U_n)$.

Тв-ня 1 Функція

$$\mu : \{ \text{диски які містяться в } X \} \to \mathbb{Q}$$

однозначно продовжується до розподілу на X т.т.т.к.

$$\mu(a + p^N \mathbb{Z}_p) = \sum_{b=0}^{p-1} \mu(a + b p^N + p^{N+1} \mathbb{Z}_p) \qquad (*)$$

для кожного диска $a + p^N \mathbb{Z}_p \subset X$.

Дов-ня - вправа.

__Приклад 1__ $X = \mathbb{Z}_p$

$$\mu_{Haar}(a+p^N\mathbb{Z}_p) \stackrel{def}{=} \frac{1}{p^N}$$

(*) очевидна

і має властивість інваріантності відносно зсувів

$\forall U \subset \mathbb{Z}_p$ комп. від-та

$\forall \alpha \in \mathbb{Z}_p$

$$\mu_{Haar}(\alpha+U) = \mu_{Haar}(U).$$

Цю властивість достатньо перевірити на дисках.

Для $x \in \mathbb{Z}_p$ позначимо $\{x\}_N \in \{0,1,\dots,p^N-1\}$ таке єдине число, що $x-\{x\}_N \in p^N\mathbb{Z}_p$.

Тоді для диска $U = a+p^N\mathbb{Z}_p$

$\alpha+U = \{\alpha+a\}_N + p^N\mathbb{Z}_p$

є диском того самого "розміру" $1/p^N$
$\quad \shortparallel$
μ_{Haar}

Приклад 2 Розподіл Мазура

$$\mu_{\text{Mazur}}(a+p^N\mathbb{Z}_p) = \frac{a}{p^N} - \frac{1}{2}$$

Barry Mazur

Вправа: перевірити (*).

Ми доведемо більш загальний факт.

Тв-ня 2 $k \geq 1$

$B_k(x)$ ми-н Бернуллі

Функція задана на дисках як

$$\mu_k(a+p^N\mathbb{Z}_p) = p^{N(k-1)} B_k\left(\frac{a}{p^N}\right)$$

однозначно продовжується за адитивністю до розподілу на $\mathbb{Z}_p$. Він наз-ся k-м розподілом Бернуллі.

Дов-ня Треба перевірити (*)

$$\Leftrightarrow B_k\left(\frac{a}{p^N}\right) = p^{k-1}\sum_{b=0}^{p-1} B_k\left(\frac{a+bp^N}{p^{N+1}}\right).$$

Нехай $\lambda = \frac{a}{p^{N+1}}$.

Права сторона $= p^{k-1}\sum_{b=0}^{p-1} B_k\left(\lambda + \frac{b}{p}\right)$

$$= \underset{\text{в}}{\overset{\text{коеф-т}}{\text{при}}}\ t^k \quad p^{k-1}\sum_{b=0}^{p-1} \frac{t\, e^{t(\lambda+\frac{b}{p})}}{e^t-1}$$

$$p^{k-1}\frac{te^{\lambda t}}{e^t-1}\sum_{b=0}^{p-1}\left(e^{t/p}\right)^b$$

$$= p^{k-1}\frac{te^{t\lambda}}{\cancel{e^t-1}}\,\frac{\cancel{\left(e^{t/p}\right)^p-1}}{e^{t/p}-1}$$

$$= p^k\,\frac{t/p\;e^{p\lambda\cdot t/p}}{e^{t/p}-1} = p^k\sum_{m=0}^{\infty}B_m(p\lambda)\left(\frac{t}{p}\right)^m$$

коеф-т при t^k

$$= B_k(p\lambda) = B_k\left(\frac{a}{p^N}\right)$$

$=$ ліва сторона $\boxtimes$

<u>Озн-ня</u> Розподіл μ на X наз-ся <u>мірою</u> якщо його множина значень є обмеженою.
Тобто $\exists\, C>0$ т. щ. $\forall\, U\subseteq X$ комп. від-та

$$|\mu(U)|_p\leq C.$$

μ_{Haar}, μ_k не є мірами.
Зараз ми перетворимо розподіли Бернуллі на міри, так звані регуляризовані розподіли Бернуллі.

Нехай $\alpha \in \mathbb{Z}_p^\times$, $\alpha \neq 1$.

$$\mu_{k,\alpha}(U) \overset{def}{=} \mu_k(U) - \alpha^{-k}\mu_k(\alpha U)$$

<u>Теорема 3</u> $\mu_{k,\alpha}$ є мірою на $\mathbb{Z}_p$.

<u>Дов-ня</u> Для будь-якого розподілу μ на $\mathbb{Z}_p$

$$U \longmapsto \mu(\alpha U)$$

є розподілом. Лінійна комбінація розподілів є розподілом. Тому $\mu_{k,\alpha}$ є розподілом.

Треба довести обмеженість. Оскільки $|\cdot|_p$ це ультранорма, достатньо довести обмеженість значень на дисках:

$$|\mu(U_1 \sqcup \ldots \sqcup U_n)|_p \leq \max_{1 \leq i \leq n} |\mu(U_i)|_p$$

$$\leq C$$

оцінка для дисків буде оцінкою для всіх відкритих компактів U.

$\underline{k=1}$ $\boxed{p>2}$ $k>1$

$$\mu_{1,\alpha}(a+p^N\mathbb{Z}_p)$$
$$= \frac{a}{p^N} - \frac{1}{2} - \frac{1}{\alpha}\left(\frac{\{\alpha a\}_N}{p^N} - \frac{1}{2}\right)$$
$$= \underbrace{\frac{a-\alpha^{-1}\{\alpha a\}_N}{p^N}}_{\in \mathbb{Z}_p \text{ бо:}} + \underbrace{\frac{1}{2}(\alpha^{-1}-1)}_{\in\mathbb{Z}_p}$$

$$\{\alpha a\}_N \equiv \alpha a \mod p^N\mathbb{Z}_p$$
$$\Rightarrow \alpha^{-1}\{\alpha a\}_N - a \in p^N\mathbb{Z}_p$$

$$\mu_{1,\alpha}(a+p^N\mathbb{Z}_p) \in \mathbb{Z}_p$$
$$|\cdot|_p \le 1 \qquad C=1$$

<u>Лема 4</u> Нехай d_k це найменший спільний знаменник коефіцієнтів $B_k(x)$. (Зокрема $d_k B_k(x) \in \mathbb{Z}[x]$.) Тоді

$$\mu_{k,\alpha}(a+p^N\mathbb{Z}_p) \equiv k a^{k-1}\mu_{1,\alpha}(a+p^N\mathbb{Z}_p) \mod p^{N-\mathrm{ord}_p(d_k)}.$$

$$\Rightarrow \forall N > \mathrm{ord}_p(d_k)$$
$$\mu_{k,\alpha}(a+p^N\mathbb{Z}_p) \in \mathbb{Z}_p$$
$$\Rightarrow \mu_{k,\alpha}(U) \in \mathbb{Z}_p$$
$$\forall U \subseteq \mathbb{Z}_p \text{ відк. комп.} \qquad C=1$$

Дов-ня леми 4

$$B_k(x) = x^k - \frac{k}{2}x^{k-1} + \dots$$

$$d_k \mu_{k,\alpha}(a + p^N\mathbb{Z}_p)$$

$$= p^{N(k-1)} d_k \left(B_k\left(\frac{a}{p^N}\right) - \alpha^{-k} B_k\left(\frac{\{\alpha a\}_N}{p^N}\right)\right) \equiv (p^N)$$

$d_k B_k(x) \in \mathbb{Z}[x] \Rightarrow$ для $i \le k-2$ складник з x^i має знаменник p^{Ni} $\Rightarrow$ буде в $p^N\mathbb{Z}_p$ після множення на $p^{N(k-1)}$.

Нехай $\alpha \in \mathbb{Z}$, $p \nmid \alpha$, $\alpha \neq 1$

$$\equiv d_k p^{N(k-1)} \times \left(\left(\frac{a}{p^N}\right)^k - \frac{1}{\alpha^k}\left(\frac{\{\alpha a\}_N}{p^N}\right)^k \right)$$

$$- d_k p^{N(k-1)} \frac{k}{2} \left(\left(\frac{a}{p^N}\right)^{k-1} - \frac{1}{\alpha^k}\left(\frac{\{\alpha a\}_N}{p^N}\right)^{k-1} \right)$$

$$\frac{\{\alpha a\}_N}{p^N} = \left\{\frac{\alpha a}{p^N}\right\} = \frac{\alpha a}{p^N} - \left\lfloor \frac{\alpha a}{p^N} \right\rfloor$$

$$\equiv d_k \left(\frac{a^k}{p^N} - \frac{p^{N(k-1)}}{\alpha^k}\left(\frac{\alpha a}{p^N} - \left\lfloor \frac{\alpha a}{p^N}\right\rfloor\right)^k - \frac{k}{2}\left(a^{k-1} - \frac{1}{\alpha^k} p^{N(k-1)} \left(\frac{\alpha a}{p^N} - \left\lfloor\frac{\alpha a}{p^N}\right\rfloor\right)^{k-1}\right)\right)$$

$$\overset{(p^N)}{\equiv} d_k\left(\cancel{\frac{a^k}{p^N}} - \frac{1}{\alpha^k}\left(\cancel{\frac{\alpha^k a^k}{p^N}} - k\,\alpha^{k-1} a^{k-1}\left\lfloor \frac{\alpha a}{p^N}\right\rfloor\right)\right.$$

$$\left. - \frac{k}{2}\left(a^{k-1} - \frac{1}{\alpha^k}\left(\alpha^{k-1} a^{k-1}\right)\right)\right)$$

$$= d_k \cdot k \cdot a^{k-1}\left(\alpha^{-1}\left\lfloor\frac{\alpha a}{p^N}\right\rfloor - \frac{1}{2} + \frac{\alpha^{-1}}{2}\right)$$

$$\alpha^{-1}\left(\frac{\alpha a}{p^N} - \frac{\{\alpha a\}_N}{p^N}\right) + \frac{1}{2}\left(\alpha^{-1} - 1\right)$$

$$\mu_{1,\alpha}\left(a + p^N \mathbb{Z}_p\right) \qquad \boxtimes$$

$d_k(\ldots) \equiv 0 \mod p^N$

$\Rightarrow (\ldots) \equiv 0 \mod p^{N - \mathrm{ord}_p(d_k)}$

p-адичне інтегрування

Теорема 5 Нехай μ це p-адична міра на $\mathbb{Z}_p$ і $f: \mathbb{Z}_p \to \mathbb{Q}_p$ це p-адична неперервна функція. Тоді суми Рімана

$$S_{N, \{x_{a,N}\}_{a=0}^{p^N-1}} \stackrel{def}{=} \sum_{a=0}^{p^N-1} f(x_{a,N}) \cdot \mu(a+p^N\mathbb{Z}_p)$$

$x_{a,N} \in a+p^N\mathbb{Z}_p$

мають границю в $\mathbb{Q}_p$ коли $N \to \infty$, і значення цієї границі не залежить від вибору пос-тей $\{x_{a,N}\}$.

Позн-ня: $\int_{\mathbb{Z}_p} f\mu \stackrel{def}{=} \lim_{N\to\infty} S_{N,\{x_{a,N}\}}$

$\forall\, U \subseteq \mathbb{Z}_p$ відк. комп.

$f \cdot \mathbb{1}_U$ є неперервною

$$\int_U f\mu \stackrel{def}{=} \int_{\mathbb{Z}_p} f \cdot \mathbb{1}_U \cdot \mu .$$

Дов-ня залишаємо як вправу.

Наслідок 6

Якщо $|\mu(U)|_p \le C$

для $\forall U \subseteq \mathbb{Z}_p$

та $|f(x)|_p \le A \quad \forall x \in \mathbb{Z}_p$

то $\left|\int f \mu\right|_p \le A \cdot C.$

Дов-ня $\forall N, \{x_{a,N}\}$

$$\left|S_{N,\{x_{a,N}\}}\right|_p \le \max_a \left(\left|f(x_{a,N})\right|_p \cdot \left|\mu(a+p^N\mathbb{Z}_p)\right|_p \right) \le A \cdot C$$

$\boxtimes$

Лема 4 $\Rightarrow \forall U \subseteq \mathbb{Z}_p$

$$\boxed{\mu_{k,\alpha}(U) = k \int_U x^{k-1} \mu_{1,\alpha}}$$

Теорема 7

Kummer congruences

(i) $(p-1) \nmid k \Rightarrow B_k/k \in \mathbb{Z}_p$

(ii) $(p-1) \nmid k \quad k' \equiv k \mod (p-1)p^N$

$$\Rightarrow (1-p^{k'-1})\frac{B_{k'}}{k'} \equiv (1-p^{k-1})\frac{B_k}{k} \mod p^{N+1}$$

(iii) $(p-1) \mid k$ і k парне (або $k=1, p=2$) тоді

$$p B_k \equiv -1 \mod p.$$

Von Stadt-Clausen congruence

Дов-ня (i)

$$\mu_k(\mathbb{Z}_p) = B_k(0) = B_k$$

$$\overset{\parallel}{0 + p^0 \cdot \mathbb{Z}_p}$$

$$\mu_{k,\alpha}(\mathbb{Z}_p) = (1-\alpha^{-k})\,B_k$$

$$\parallel$$

$$k \int_{\mathbb{Z}_p} x^{k-1}\,\mu_{1,\alpha}$$

Нехай $\alpha \in \{1, \dots, p-1\}$ є первісним коренем mod p:

$$\alpha^m \equiv 1 \pmod p \iff (p-1) \mid m$$

$$(p-1) \nmid k \Rightarrow \alpha^{-k} \not\equiv 1 \pmod p$$

$$1 - \alpha^{-k} \in \mathbb{Z}_p^\times$$

$$\frac{B_k}{k} = \underbrace{\frac{1}{1-\alpha^{-k}}}_{\in\, \mathbb{Z}_p} \underbrace{\int_{\mathbb{Z}_p} x^{k-1}\,\mu_{1,\alpha}}_{\in\, \mathbb{Z}_p}$$

бо всі суми Рімана $\in \mathbb{Z}_p$

$$\Rightarrow B_k/k \in \mathbb{Z}_p$$

(ii)

$$\mu_k(p\mathbb{Z}_p) = p^{k-1} B_k$$

$a=0 \quad N=1$

$$\mu_{k,\alpha}(p\mathbb{Z}_p) = (1-\alpha^{-k})\, p^{k-1} B_k$$

$$\mu_{k,\alpha}(\mathbb{Z}_p^\times) = (1-\alpha^{-k})(1-p^{k-1}) B_k$$

$$\shortparallel$$

$$k \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha}$$

$$(1-p^{k-1})\frac{B_k}{k} = \frac{1}{1-\alpha^{-k}} \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha}$$

α вибираємо як в (i)

$$k' \equiv k \mod (p-1)p^N$$

$$\alpha^{k'-k} \equiv 1 \mod p^{N+1}$$

$$\alpha^{-k'} \equiv \alpha^{-k} \mod p^{N+1}$$

$$\frac{1}{1-\alpha^{-k'}} \equiv \frac{1}{1-\alpha^{-k}} \mod p^{N+1}$$

$(p-1) \nmid k$

Так само для $\forall x \in \mathbb{Z}_p^\times$

$$x^{k'-1} \equiv x^{k-1} \mod p^{N+1}$$

(Наслідок 6 $\Rightarrow$)

$$\int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha} \equiv \int_{\mathbb{Z}_p^\times} x^{k'-1} \mu_{1,\alpha} \mod p^{N+1}$$

бо це так для всіх сум Рімана.

(iii) Візьмемо $\alpha = 1+p$

$k \geq 2$ парне

$$pB_k = kp \cdot \frac{B_k}{k}$$

$$= \underbrace{\frac{kp}{1-\alpha^{-k}}} \underbrace{(1-p^{k-1})^{-1}}_{\equiv 1 \,(\mathrm{mod}\, p)} \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha}$$

$\downarrow$

$$1-\alpha^{-k} = 1-(1+p)^{-k} \equiv kp \mod p^{2+d} \quad d = \mathrm{ord}_p k$$

(вправа)

$$\frac{kp}{1-\alpha^{-k}} \equiv 1 \mod p$$

$(p-1) \mid k \Rightarrow x^k \equiv 1 \mod p \quad \forall x \in \mathbb{Z}_p^\times$

$$\int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha} \equiv \underbrace{\int_{\mathbb{Z}_p^\times} x^{-1} \mu_{1,\alpha} \mod p}_{\equiv -1 \mod p}$$

<u>Вправа:</u>

для нашого $\alpha = 1+p$

$\boxtimes$