11 квітня

§13. Кільце p-адичних цілих чисел

p просте число

Озн-ня p-адичне ціле число це послідовність

$x = (x_1, x_2, x_3, \dots)$ де

$$x_n \in \mathbb{Z}/p^n\mathbb{Z}$$

та

$$x_{n+1} \equiv x_n \pmod{p^n}$$

для всіх $n \geq 1$.

Пригадаємо, що для $\forall m, k$

$$\mathbb{Z}/mk\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z}$$

є сюр'єктивним.

$a \equiv b \bmod mk \Rightarrow a \equiv b \bmod m$

Зокрема

$$\mathbb{Z}/p^{n+1}\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^n\mathbb{Z}$$

є сюр'єктивним.

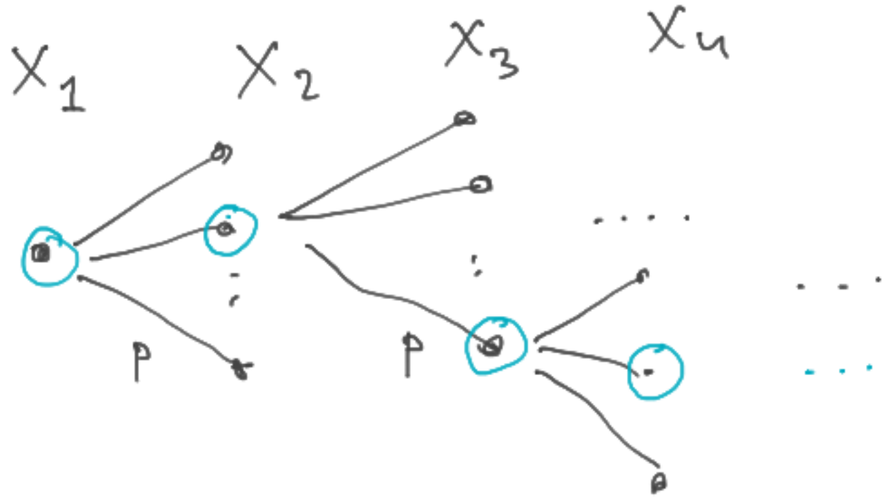
Зручно ідентифікувати

$$\mathbb{Z}/p^n\mathbb{Z} = \{0, 1, \dots, p^n - 1\}.$$

Тоді прообразами $\tilde{a}$ будуть

$$a,\ a + p^n,\ a + 2p^n,\ \dots,\ a + (p-1)p^n.$$

Тобто маємо p прообразів.



Порівняйте це з тим, коли ми думали про дійсні числа як про послідовності раціональних апроксимацій. Напр.:

$$\pi = (3,\ 3.1,\ 3.14,\ 3.141,\ 3.1415,\ \dots)$$

Спостереження:

- для кожного n компонента x_n визначає всі попередні:

$$x_1 = x_n \bmod p$$
$$x_2 = x_n \bmod p^2$$
$$\dots$$
$$x_{n-1} = x_n \bmod p^{n-1}$$

- для $\forall n$ при фіксованому x_n маємо p можливостей для x_{n+1}:

$$x_n \in \{0, \dots, p^n - 1\}$$
$$x_{n+1} = x_n + a_n \cdot p^n$$
$$a_n \in \{0, 1, \dots, p-1\}$$

- додавання, відніманння і множення покомпонентно:

$$X \pm Y = (x_1 \pm y_1, x_2 \pm y_2, \dots)$$

$$X \cdot Y = (x_1 \cdot y_1, x_2 \cdot y_2, \dots)$$

добре визначені операції бо

$$\mathbb{Z}/p^{n+1}\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^n\mathbb{Z}$$

є гомоморфізмом кілець: суми переходять в суми і добутки в добутки

тм. $(x_{n+1} + y_{n+1}) \bmod p^n$

$= x_{n+1} \bmod p^n + y_{n+1} \bmod p^n$

$= x_n + y_n$

Позначення:

$\mathbb{Z}_p$ це кільце p-адичних цілих чисел з цими операціями

$1 = (1, 1, 1, \dots)$

$0 = (0, 0, 0, \dots)$

- $\mathbb{Z} \subset \mathbb{Z}_p$ як кільця

$m \longmapsto X = (x_1, x_2, x_3, \dots)$

де $x_n = m \bmod p^n$

Наприклад:

$-1 \longmapsto (p-1, p^2-1, p^3-1, \dots)$

якщо ми ідентифікуємо $\mathbb{Z}/p^n\mathbb{Z}$ з $\{0, 1, \dots, p^n-1\}$

- еквівалентний спосіб запису $x \in \mathbb{Z}_p$ це його p-адичний розклад:

$$X_{n+1} = X_n + a_n p^n$$

$$a_n \in \mathbb{Z}/p\mathbb{Z} \cong \{0, 1, \dots, p-1\}$$

$$X_1 \in \mathbb{Z}/p\mathbb{Z} =: a_0$$

$$X_2 = a_0 + a_1 p$$

$$X_3 = a_0 + a_1 p + a_2 p^2$$

$$\dots$$

$$X = a_0 + a_1 p + \dots = \sum_{k=0}^{\infty} a_k p^k$$

Порівняйте з записом натуральних чисел у системі числення з основою p.

Вправа: запишіть p-адичний розклад числа -1.

$$p^{n+1} - 1 = p^n - 1 + \underbrace{(p-1)}_{a_n} p^n$$

p-адичні цифри

- Наведемо приклад $x \in \mathbb{Z}_p \setminus \mathbb{Z}$

$p \neq 2$

$$x = \frac{p-1}{2} + \frac{p-1}{2} p + \frac{p-1}{2} p^2 + \dots$$

всі цифри p-адичного розкладу $a_k = \frac{p-1}{2}$

$$x_n = \frac{p-1}{2}(1 + p + \dots + p^{n-1})$$

$$= \frac{p-1}{2} \cdot \frac{p^n - 1}{p-1} = \frac{p^n - 1}{2}$$

$$x = \left(\frac{p^n - 1}{2} ; n \geq 1 \right) \in \mathbb{Z}_p$$

Вправа: перевірити, що $x_{n+1} \equiv x_n \mod p^n$.

Помітимо, що

$$2 \cdot x = \left(p^n - 1 ; n \geq 1 \right) = -1$$

<u>Озн-ня</u> p-цілі дроби (же кільце)

$$\mathbb{Z}_{(p)} = \left\{ \frac{m}{k} : p \nmid k \right\} \subset \mathbb{Q}.$$

- $\mathbb{Z}_{(p)} \subset \mathbb{Z}_p$ як кільця

$\frac{m}{k} \longmapsto x = (x_1, x_2, \dots)$ де

$$x_n = \frac{m}{k} \mod p^n$$

оскільки $k \in (\mathbb{Z}/p^n\mathbb{Z})^\times$, то $\frac{1}{k} \in \mathbb{Z}/p^n\mathbb{Z}$.

Нп. $x = \left(\frac{p^n - 1}{2} ; n \geq 1 \right) = -\frac{1}{2}$ коли $p \neq 2$

• Приклад p-адичного числа

$x \in \mathbb{Z}_p \setminus \mathbb{Z}_{(p)}$?

Лема Гензеля $f(X) \in \mathbb{Z}[X]$

Нехай простий корінь $f(X)$ за модулем p, тобто $\alpha \in \mathbb{Z}/p\mathbb{Z}$ т.що.

$$f(\alpha) \equiv 0, \quad f'(\alpha) \not\equiv 0 \pmod{p},$$

має <u>єдине</u> підняття до кореня $f(X)$ за модулем p^n для всіх $n \geq 1$:

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

т.що. $f(x_n) \equiv 0 \mod p^n$

та $x_n \equiv \alpha \mod p$.

При доведенні леми отримали x_n з рекурентної формули:

$$x_1 = \alpha$$

$$x_{n+1} = x_n - f'(\alpha)^{-1} f(x_n) \mod p^{n+1}$$

(дуже коротке нагадування доведення леми Гензеля)

З <u>єдиності</u> випливає, що

$$x_{n+1} \equiv x_n \mod p^n.$$

Тобто $x = (x_1, x_2, x_3, \dots) \in \mathbb{Z}_p$.

Нове формулювання леми Гензеля:

$f \in \mathbb{Z}[X]$

кожен простий корінь $f \bmod p$ має єдине підняття до кореня в $\mathbb{Z}_p$.

Тобто, якщо $\alpha \in \mathbb{Z}/p\mathbb{Z}$ це простий корінь $f \bmod p$ то $\exists!\ x \in \mathbb{Z}_p$

$(x_1, x_2, x_3, \dots)$ т.ад.

$f(x) = 0$ та $x_1 = \alpha$.

("корінь") ("підняття α")

Приклад

$p = 7$ 7-адичний розклад

$$\sqrt{2} = 3 + 1\cdot 7 + 2\cdot 7^2 + 6\cdot 7^3 + 1\cdot 7^4 + \dots$$

або

$$4 + 5\cdot 7 + 4\cdot 7^2 + 0\cdot 7^3 + 5\cdot 7^4 + \dots$$

$f(X) = X^2 - 2$

не має коренів $\bmod 3$, $\bmod 5$

(2 не є квадратичним лишком $\bmod p = 3, 5$)

Наступні p такі що $\left(\frac{2}{p}\right) = 1$ це $p = 17$ та $p = 23$.

Приклад $f(X) = X^{p-1} - 1$

має $p-1$ коренів в $\mathbb{Z}/p\mathbb{Z}$
(1 простих)

тобто є $p-1$ корінь в $\mathbb{Z}_p$.

Вони називаються одиницями Тейхмюллера

Ин. $p=5$

$$1$$
$$2 + 1\cdot 5 + 2\cdot 5^2 + 1\cdot 5^3 + \dots$$
$$3 + 3\cdot 5 + 2\cdot 5^2 + 3\cdot 5^3 + \dots$$
$$-1 = 4 + 4\cdot 5 + 4\cdot 5^2 + 4\cdot 5^3 + \dots$$

Одиниці Тейхмюллера є $(p-1)$-ми коренями з 1 подібно до комплексних чисел

$$\exp\left(2\pi i \frac{m}{p-1}\right) \in \mathbb{C}$$

$m = 0, 1, \dots, p-2$.

Вправа: доведіть, що в $\mathbb{Z}_p$ немає інших коренів з 1 крім одиниць Тейхмюллера. Тобто якщо $x \in \mathbb{Z}_p$ т.що. $x^m = 1$ для деякого $m \geq 2$, то $x^{p-1} = 1$.

● $\mathbb{Z}_p^\times$ — ?

одиниці кільця

$$\mathbb{Z}_p^\times = \{ x = (x_1, x_2, \dots) \in \mathbb{Z}_p : x_1 \neq 0 \}$$

$$\Updownarrow$$

$$x_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times \quad \forall n$$

$$\mathbb{Z}_p = \mathbb{Z}_p^\times \sqcup p\mathbb{Z}_p$$

$x_1 = 0 \iff a_0 = 0$ у p-адичному розкладі

$\iff x \in p\mathbb{Z}_p$

$$\mathbb{Z}_p = \mathbb{Z}_p^\times \underset{\text{диз'юнктне об'єднання}}{\sqcup} p\mathbb{Z}_p$$

$$= \mathbb{Z}_p^\times \sqcup p\mathbb{Z}_p^\times \sqcup p^2\mathbb{Z}_p$$

$$\dots$$

$$\mathbb{Z}_p \setminus \{0\} = \bigsqcup_{k \geq 0} p^k \mathbb{Z}_p^\times$$

Кожне ненульове $x \in \mathbb{Z}_p$ може бути єдиним способом записане як

$$x = p^k \cdot y$$

де $k \in \mathbb{Z}_{\geq 0}$, $y \in \mathbb{Z}_p^\times$.

- Множина

$$\mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right]$$

$$= \mathbb{Z}_p \sqcup p^{-1}\mathbb{Z}_p^{\times} \sqcup p^{-2}\mathbb{Z}_p^{\times} \dots$$

є полем, яке називається полем p-адичних чисел.

Додавання: $p^k y + p^m z$ $(=)$

$k \geq m$, $y, z \in \mathbb{Z}_p^{\times}$

$(=)$ $p^m\left(z + y\,p^{k-m}\right)$

↖ звичайне додавання в $\mathbb{Z}_p$

$$\mathbb{Q}_p \setminus \{0\} = \bigsqcup_{k \in \mathbb{Z}} p^k \mathbb{Z}_p^{\times}$$

- $\mathbb{Q} \subset \mathbb{Q}_p$ вкладення полів

$\Downarrow$

$\frac{m}{k} = p^s \frac{l}{t}$ $\qquad \frac{l}{t} \in \mathbb{Z}_p^{\times}$

$p \times l, t$

$s \in \mathbb{Z}$

$\frac{m}{k} \in p^s \mathbb{Z}_p^{\times} \subset \mathbb{Q}_p$