24 березня

4 Квадратичний закон взаємності

p просте число

Озн-ня Ненульовий лишок $0 \neq a \bmod p$ наз-ся квадратичним лишком (відп. кв-ним нелишком) коли рівняння $x^2 \equiv a \pmod p$ має розв'язки (відп. не має розв'язків).

Ин. mod 7

x	$\bar 1$	$\bar 2$	$\bar 3$	$\bar 4$	$\bar 5$	$\bar 6$
x^2	$\bar 1$	$\bar 4$	$\bar 2$	$\bar 2$	$\bar 4$	$\bar 1$

$\bar 1, \bar 2, \bar 4$ кв. лишки

$\bar 3, \bar 5, \bar 6$ кв. нелишки

Озн-ня Для $p \neq 2$ простого $a \in \mathbb{Z}$

символ Лежандра

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & a \equiv 0 \ (p) \\ 1, & a \in \text{кв. лишок } (p) \\ -1, & a \in \text{кв. нелишок } (p) \end{cases}$$

Тв-ня 1 (елементарні властивості)

(i) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

(ii) $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

(iii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & p \equiv 1 \pmod 4 \\ -1, & p \equiv 3 \pmod 4 \end{cases}$

Дов-ня (i)

Якщо $\left(\frac{a}{p}\right)=1$, тоді
$\exists x$ т.що. $a \equiv x^2 \pmod p$.

$\Rightarrow a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p$

за малою теоремою Ферма.

Якщо $\left(\frac{a}{p}\right)=-1$:

Для кожного $1 \le b \le p-1$ існує єдине $1 \le b' \le p-1$ таке що $b \cdot b' \equiv a \pmod p$.
Оскільки a не кв-нелишок, то $b \neq b'$, і тому

$$(p-1)! \equiv a^{\frac{p-1}{2}} \pmod p$$

↑ к-сть пар

За теоремою Вільсона

$$(p-1)! \equiv -1 \pmod p.$$

$$\Rightarrow a^{\frac{p-1}{2}} \equiv -1 = \left(\frac{a}{p}\right) \pmod p$$

що доводить (i).
(ii), (iii) випливають з (i) ⊠

Вправа: Якщо g не первісний корінь за модулем p, то квадратичні лишки це

$$g^2, g^4, \dots, g^{p-1}=1$$

і нелишки це

$$g, g^3, \dots, g^{p-2}.$$

Квадратичний закон взаємності (К.Ф. Гаусс)

p, q різні непарні прості

то

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Лема 2 (лемма) Для ненульового $0 \neq a \bmod p$

нехай

$$\sigma_a : \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\} \to \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$$

це перестановка множини лишків задана множенням на a. Тоді

$$\left(\frac{a}{p}\right) = \operatorname{sgn}(\sigma_a).$$

Перестановки

X множина з n елементів

Перестановка це бієкція

$\sigma : X \to X$

Можна впорядкувати X

$\cong \{1, 2, \ldots, n\}$ і тоді

σ діє на цій стандартній множині.

$S_n = \{$ всі перестановки n елементів $\}$

$$\#S_n = n!$$

S_n є групою з операцією композиції:

$$X \xrightarrow{\sigma_1} X \xrightarrow{\sigma_2} X$$

$$\sigma_2 \circ \sigma_1$$

Група S_n породжена транспозиціями:

перестановка $\tau = \tau_{x,y}$ є транспозицією якщо вона переставляє два елементи $x, y \in X$:

$\tau(x) = y$

$\tau(y) = x$

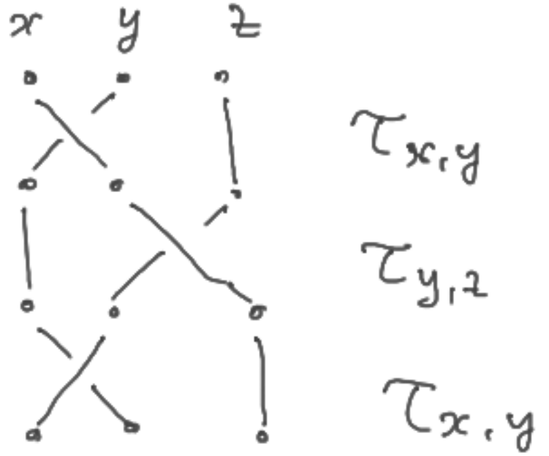
$\tau(z) = z \quad \forall z \neq x, y$

В будь-якому представленні $\sigma \in S_n$ як добутку транспозицій

$$\sigma = \tau_1 \circ \dots \circ \tau_r$$

парність числа r буде тою самою.

Ил.



$\tau_{x,y}$

$\tau_{y,z}$

$\tau_{x,y}$

$\tau_{x,y} \circ \tau_{y,z} \circ \tau_{x,y} = \tau_{x,z}$

Сигнатура $\sigma \in S_n$ це

$$\operatorname{sgn}(\sigma) = (-1)^r.$$

↑

Мультиплікативна функція (тобто характер)

$$\operatorname{sgn}: S_n \longrightarrow \{1, -1\}$$

Коли на X заданий порядок $X \cong \{1, 2, \dots, n\}$

то пари $(i, j) \in X^2$

т.ч. $i < j$ та $\sigma(i) > \sigma(j)$

називаються інверсіями перестановки σ. Множина інверсій σ залежить від вибраного порядку на X. Але парність кількості інверсій не залежить від порядку:

$$\operatorname{sgn}(\sigma) = (-1)^{\#\text{ інверсій } \sigma}$$

(Вправа *)

Довести Лему 2

Нехай g не первісний корінь за модулем p.

Тоді $\left(\frac{g}{p}\right) = -1$ оскільки $g^{\frac{p-1}{2}} \neq 1 \pmod p$.

Впорядкуємо множину лишків так:

$$X = \mathbb{Z}/p\mathbb{Z} = \{\bar{0}, g, g^2, \dots, g^{p-1} = \bar{1}\}$$

Множення $\times g$ має першому точку $\bar{0}$ то цикл довжини $p-1$:

$$\bar{0} \xrightarrow{\times g} \bar{0}$$

$$g \to g^2 \to g^3 \to \dots \to g^{p-2} \to g^{p-1} \to g$$

σ_g

(2) (3) (4) . (p-1) (1)

1 1 $p-2$ транспозиції

цикл довжини m це добуток $m-1$ транспозицій

$$\operatorname{sgn}(\sigma_g) = (-1)^{p-2} = -1 = \left(\frac{g}{p}\right)$$

Для інших елементів тв-ня випливає з мультиплікативності $\operatorname{sgn}(-)$ та $\left(\frac{-}{p}\right)$:

$a = g^k$

$$\left(\frac{a}{p}\right) = \left(\frac{g}{p}\right)^k = \operatorname{sgn}(\sigma_g)^k = \operatorname{sgn}(\sigma_g^k)$$

↑ Т-ма 1 (ii)

↑ щойно

$$= \operatorname{sgn}(\sigma_{g^k}) = \operatorname{sgn}(\sigma_a)$$

↑ т

$\sigma_a \cdot \sigma_b = \sigma_{ab}$ ☒

Теорема 3 (i) Якщо p, q — різні непарні прості то $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

(ii) p непарне просте

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p \equiv 1,7 \pmod 8 \\ -1, & p \equiv 3,5 \pmod 8 \end{cases}$$

Дов-ня (ii) Впорядкуємо лишки mod p адитивно

$$X = \mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{\tfrac{p-1}{2}}\} \cup \{\overline{\tfrac{p+1}{2}}, \dots, \overline{p-1}\}$$

$$= S_1 \qquad\qquad = S_2$$

Порахуємо інверсії для $\sigma_{\bar{2}}$:

- для $(\bar{i}, \bar{j}) \in S_1^2$

  $\bar{i} < \bar{j} \Rightarrow \overline{2i} < \overline{2j}$

  тобто в S_1 інверсій немає
- для $(\bar{i}, \bar{j}) \in S_2^2$

  $\left(\overline{\tfrac{p+u}{2}}, \overline{\tfrac{p+v}{2}}\right)$

$$S_2 = \left\{\overline{\tfrac{p+1}{2}}, \overline{\tfrac{p+3}{2}}, \dots, \overline{\tfrac{p+(p-2)}{2}}\right\}$$

$\bar{i} < \bar{j} \iff u < v$

$\iff \overline{2i} = \bar{u} < \overline{2j} = \bar{v}$

Тобто $2 * S_2$ це всі непарні лишки, і в S_2 інверсій немає

- пара $\left(\bar{i}, \bar{j} = \overline{\tfrac{p+u}{2}}\right) \in S_1 \times S_2$ буде інверсією якщо

  $\overline{2j} = \bar{u} < \overline{2i}$.

Зафіксуємо $\bar{i}$. Кількість таких інверсій це кіл-сть непарних серед $1, 2, \dots, 2i$, тобто i.

інверсій для $\sigma_{\bar{2}}$ це

$$\sum_{i=0}^{\frac{p-1}{2}} i = \frac{\frac{p-1}{2} \cdot \frac{p+1}{2}}{2} = \frac{p^2-1}{8}.$$

З леми 2

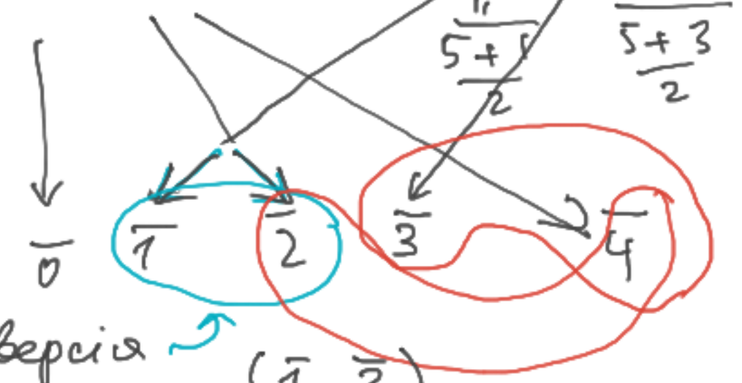
$$\left(\frac{2}{p}\right) = \operatorname{sgn}(\sigma_{\bar{2}}) = (-1)^{\#\text{інверсій}}$$

$$= (-1)^{\frac{p^2-1}{8}} \qquad \boxtimes$$

Приклад: $p = 5$

S_1 $\qquad$ S_2

$\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\} \cup \{\bar{3}, \bar{4}\}$



$\bar{i} = \bar{1}$: 1 інверсія $(\bar{1}, \bar{3})$

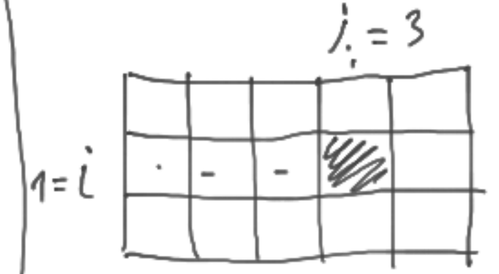
$\bar{i} = \bar{2}$: 2 інверсії $(\bar{2}, \bar{3})$ та $(\bar{2}, \bar{4})$

$$\sum_{i=0}^{\frac{p-1}{2}} i = 1 + 2 = 3$$

(i) $p \neq q$ непарні прості

Розглянемо множину з pq елементів

$$X = \{(i,j) : \begin{matrix} 0 \le i \le p-1 \\ 0 \le j \le q-1 \end{matrix}\}$$



$p = 3$
$q = 5$

і три різні порядки на X:

$n \longmapsto (n \bmod p, \lfloor \frac{n}{p} \rfloor)$

0	3	6	9	12
1	4	7	10	13
2	5	8	11	14

$n = 0, 1, \ldots, pq-1$

→ $n \longmapsto \left(\left\lfloor \frac{n}{q} \right\rfloor , n \bmod q \right)$

$n = 0, \dots, pq-1$

0	1	2	3	4
5	6	7	8	9
10	11	12	13	14

↘ $n \longmapsto (n \bmod p, n \bmod q)$

0	6	12	3	9
10	1	7	13	4
5	11	2	8	14

$n = 0, \dots, pq-1$

Кожна пара впорядкувань задає перестановку на X, наприклад

$\sigma_{\rightarrow\downarrow} : (n \bmod p, \left\lfloor \frac{n}{p} \right\rfloor) \to \left(\left\lfloor \frac{n}{q} \right\rfloor, n \bmod q \right)$

$\sigma_{\searrow\rightarrow} : \left(\left\lfloor \frac{n}{q} \right\rfloor, n \bmod q \right) \to (n \bmod p, n \bmod q)$

$\sigma_{\downarrow\searrow} : (n \bmod p, n \bmod q) \to (n \bmod p, \left\lfloor \frac{n}{p} \right\rfloor)$

$\sigma_{\downarrow\searrow} \circ \sigma_{\searrow\rightarrow} \circ \sigma_{\rightarrow\downarrow} = id$ тотожна перестановка на X

⇓

$\operatorname{sgn}(\sigma_{\downarrow\searrow}) \operatorname{sgn}(\sigma_{\searrow\rightarrow}) \operatorname{sgn}(\sigma_{\rightarrow\downarrow}) = 1$

$\left(\frac{p}{q}\right) \quad \left(\frac{q}{p}\right) \quad (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ Ми показали що

$\sigma_{\searrow\rightarrow} : \left(\left\lfloor \frac{n}{q} \right\rfloor, n \bmod q\right) \longmapsto (n \bmod p,\ n \bmod q)$

це перестановка зберігає стовпчики

В j-му стовпчику:

$$i \longmapsto iq + j \bmod p$$

(i, j)

$n = iq + j$

перестановка j-го стовпчика $= \left(\sigma_{+1}\right)^j \circ \sigma_{\bar{q}}$

(σ_{+1} — цикл довжини p)

$\operatorname{sgn}(-//-) = ((-1)^{p-1})^j \cdot \left(\frac{q}{p}\right)$

($((-1)^{p-1})$ — цикл довжини p як добуток $p-1$ транспозиції; $\left(\frac{q}{p}\right)$ — лема 2)

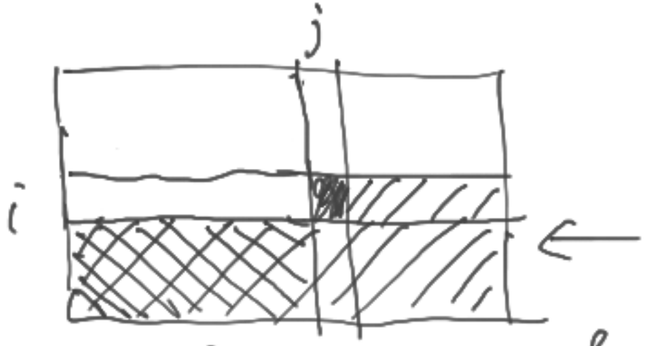
$$\operatorname{sgn}\left(\sigma_{\searrow\rightarrow}\right) = \prod_{\text{стовпчик}} \operatorname{sgn}\left(\begin{matrix}\text{в}\\ \text{стовпчику}\end{matrix}\right)$$

$$= \left(\frac{q}{p}\right)^q = \left(\frac{q}{p}\right)$$

$$\sigma_{\downarrow\searrow} = \sigma_{\searrow\downarrow}^{-1}$$

$$\operatorname{sgn}\left(\sigma_{\downarrow\searrow}\right) = \operatorname{sgn}\left(\sigma_{\searrow\downarrow}\right) = \left(\frac{p}{q}\right)$$

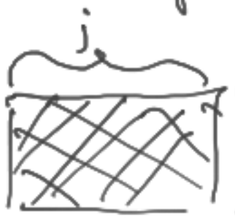
$\sigma_{\to\downarrow}$: порахуємо кількість інверсій



для (i,j)

тут розташовані більші елементи в порядку $\Rightarrow$

з них елементи є меншими в порядку $\downarrow$



рахуємо інверсії для порядку $\downarrow$

інверсій для $\sigma_{\to\downarrow}$

$$= \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} \underbrace{(p-1-i)}_{\text{парне}} j$$

$$\overset{(\mathrm{mod}\,2)}{\equiv} \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} i \cdot j = \frac{(p-1)p}{2} \cdot \frac{(q-1)q}{2}$$

$$\overset{(\mathrm{mod}\,2)}{\equiv} \frac{p-1}{2} \cdot \frac{q-1}{2}$$

$$\operatorname{sgn}(\sigma_{\to\downarrow}) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

$\boxtimes$

Застосування: розщеплення простих p у квадратичних полях $K = \mathbb{Q}(\sqrt{m})$.

Тв-ня 4 Нехай вільне від квадратів число m є таким що кільце цілих $\mathcal{O}_K \in$ ООФ. Просте число $p \nmid m$, $p \neq 2$ розщеплюється в $\mathcal{O}_K$ в добуток $p = \pi_1 \cdot \pi_2$ двох простих ел-тів т.т.т.к. $\left(\frac{m}{p}\right) = 1$.

Дов-во $(\Rightarrow)$ $p = \pi_1 \cdot \pi_2$

$\Rightarrow N(\pi_1) = \pm p$, $N(\pi_2) = \pm p$

$\Rightarrow \exists\, a, b \in \frac{1}{2}\mathbb{Z}$ т. що.

$N(a + b\sqrt{m}) = \pm p$

$a^2 - mb^2$

Позначимо $A = 2a$, $B = 2b \in \mathbb{Z}$

$(*)$ $A^2 - mB^2 = \pm 4p$

$\bar{A}^2 - \bar{m}\bar{B}^2 \equiv 0 \pmod p$

$p \nmid B$: якщо $p \mid B$ то з $(*)$ також $p \mid A$ і ліва частина ділиться на p^2, а права - ні

$\bar{x} = \bar{A} \cdot \bar{B}^{-1}$ задовольняє $\in$

$\bar{x}^2 = \bar{m} \pmod p$.

$\Rightarrow \left(\frac{m}{p}\right) = 1$.

(⇐) Нехай $\left(\frac{m}{p}\right) = 1$

$\exists\, x \in \mathbb{Z}$ т.ч $x^2 \equiv m \pmod p$

$p \mid (x^2 - m) = (x - \sqrt{m})(x + \sqrt{m})$

$\in \mathcal{O}_K \qquad \in \mathcal{O}_K$

Припустимо що p - просте в $\mathcal{O}_K$. Тоді

$p \mid x - \sqrt{m}$ або $p \mid x + \sqrt{m}$

$\Rightarrow$ або $\frac{x}{p} - \frac{\sqrt{m}}{p} \in \mathcal{O}_K$ або

$\frac{x}{p} + \frac{\sqrt{m}}{p} \in \mathcal{O}_K$. Це

суперечить тому що $\mathcal{O}_K$,

бо $\pm\frac{1}{p} \notin \frac{1}{2}\mathbb{Z}$. ⊠

Застосування Теореми 3:

$\left(\frac{m}{p}\right)$ залежить від

$p \bmod 4 \cdot |m|$.

(вправа)

Приклад $\mathbb{Q}(\sqrt{-1})$ $p \neq 2$

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \bmod 4 \\ -1 & p \equiv 3 \bmod 4 \end{cases}$$

$\mathbb{Q}(\sqrt{-3})$ $p \neq 2, 3$

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}} \left(\frac{p}{3}\right)$$

$$= \left(\frac{p}{3}\right) = \begin{cases} 1 & p \equiv 1 \bmod 3 \\ -1 & p \equiv -1 \bmod 3 \end{cases}$$

Д/з

$$a^{p-1} \equiv 1 \mod p \quad (*)$$

$$\begin{cases} a \equiv b \mod p^s \\ \Rightarrow a^p \equiv b^p \mod p^{s+1} \end{cases}$$

$$(*) \Rightarrow a^{p^{s-1}(p-1)} \equiv 1 \mod p^s$$

$$a_s = a^{p^{s-1}} \mod p^s$$

відношення розв'язку a рівняння $x^{p-1} \equiv 1 \pmod p$.