§6. Елементарні властивості лишків: мала теорема Ферма, її узагальнення та китайська теорема про лишки

Озн-я $m \in \mathbb{Z}$, $m \neq 0$

$a, b \in \mathbb{Z}$ є конгруентними за модулем m якщо $m \mid (a-b)$.

Позначення: $a \equiv b \pmod m$

або

$a \equiv b \ (m)$

відношення еквівалентності на $\mathbb{Z}$:

- рефлексивне $a \equiv a \ (m)$
- симетричне $a \equiv b \ (m) \Leftrightarrow b \equiv a \ (m)$
- транзитивне $a \equiv b, \ b \equiv c \ (m) \Rightarrow a \equiv c \ (m)$

Класи еквівалентності над-ся лишками за модулем m

$a \in \mathbb{Z}$

$\bar{a} := \{ b \in \mathbb{Z} : a \equiv b \ (m) \}$

лишок

Лишки утворюють кільце:

$a \equiv a' \ (m)$, $b \equiv b' \ (m) \Rightarrow$ $a+b \equiv a'+b' \ (m)$, $ab \equiv a'b' \ (m)$

$\bar{a} + \bar{b} := \overline{a+b}$ $\bar{a} \cdot \bar{b} := \overline{ab}$

Позначення:

$\mathbb{Z}/m\mathbb{Z}$ кільце лишків за модулем m

$m \geq 1$ $\quad \mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$

* $m=1$: $\bar{0} = \bar{1}$ кільце без одиниці

* коли m складене $\mathbb{Z}/m\mathbb{Z}$ не є областю цілісності:

нап. $m=6$ $\quad \bar{2} \cdot \bar{3} = \bar{0}$

(дільники нуля)

Відтепер: $\boxed{m \geq 2}$

Задача: описати групу одиниць кільця лишків

$$(\mathbb{Z}/m\mathbb{Z})^\times - ?$$

Лема 1 Для $a \in \mathbb{Z}$ існує $b \in \mathbb{Z}$ т.ц. $ab \equiv 1 \ (m)$ т.т.т.к. $(a, m) = 1$

Дов-ня: $\Rightarrow$ $ab = 1 + mk \Rightarrow (a,m)=1$

$\Leftarrow$ $(a,m)=1 \Rightarrow \exists x, y \in \mathbb{Z}$:

$ax + my = 1 \Rightarrow ax \equiv 1 \ (m)$ ☒

$(\mathbb{Z}/m\mathbb{Z})^\times = \{\bar{a} : 1 \leq a \leq m, \ (a,m)=1\}$

Озн-ня Функція Ейлера

$m \in \mathbb{Z}_{\geq 1}$

$\varphi(m) = \#\{1 \leq a \leq m : (a,m) = 1\}$

Зокрема: $\varphi(1) = 1$

$\varphi(m) = \#(\mathbb{Z}/m\mathbb{Z})^\times \quad m \geq 2$

$\varphi(p) = p-1$

↑ просте

і

$\varphi(m) = m-1$ т.т.т.к.

m просте

PARI/GP: eulerphi(•)

$\varphi(p^e) = p^e - p^{e-1}$

$\varphi(m)$ - ?

p - просте число

Тв-ня 2 (мала теорема Ферма)

$\forall a \quad a^p \equiv a \ (p)$

Дов-ня Якщо $p \mid a$ то $a \equiv a^p \equiv 0 \ (p)$.

Якщо $p \nmid a$ тоді достатньо показати що $a^{p-1} \equiv 1 \ (p)$.

Лишок $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$

↑ скінченна група порядку $p-1$

Тобто наше твердження випливає з загального факту:

нехай G, $\#G < \infty$ скінченна група

то для $\forall g \in G$ маємо $g^{\#G} = 1$.

↑

$H = \{1, g, g^2, \dots\} \subset G$ підгрупа породжена g

$H = \{1, g, \dots, g^{e-1}\}$ $e = \#H$

і $e = \min\{m \geq 1 : g^m = 1\}$

G розкладається в диз'юнктне об'єднання класів екв-ті:

$g_1 \sim g_2$ якщо $g_1 \in g_2 H$

$$G = \bigsqcup_{i=1}^{s} g_i H$$

$\Rightarrow \#G = s \cdot \#H$

$\Rightarrow$ $e = \#H \mid \#G$

$g^{\#G} = (g^e)^s = 1^s = 1$ ⊠

Тв-ка 3 (теорема Ейлера-Ферма)

нехай $(a, m) = 1$

то $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Довід $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$ ← скінченна група порядку $\varphi(m)$

Далі ті самі міркування ⊠

Ще кілька застосувань групової структури:

Тв-ня 4 (теорема Вільсона)

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

Дов-ня $p = 2$ $\bar{1} = -\bar{1}$ (2) вірно

Нехай $p \geq 3$ непарне просте

$$\overline{(p-1)!} = \bar{1} \cdot \bar{2} \cdot \ldots \cdot \overline{(p-1)}$$

↑

множники розбиваються на пари $\bar{a}, \bar{b}$ т.ч. $\bar{a} \cdot \bar{b} = \bar{1}$

$$\bar{b} = \bar{a}^{-1}$$

крім випадку $\bar{a}^{-1} = \bar{a}$,

тобто $\bar{a}^2 = \bar{1}$

$$p \mid (a^2 - 1) = (a-1)(a+1)$$

$$\Rightarrow p \mid (a-1) \text{ або } p \mid (a+1)$$

$$\bar{a} = \bar{1} \text{ або } \bar{a} = -\bar{1}$$

Тому

$$\overline{(p-1)!} = \overline{-1} \quad \boxtimes$$

У кільці $\mathbb{Z}/p\mathbb{Z}$ кожен ненульовий елт має обернений $\Rightarrow$ це поле

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \ldots, \overline{p-1}\}$$

поле з p елементів

Тв-ня 5 Нехай k - поле і $f \in k[x]$ многочлен степеня $n \geq 1$.
Тоді рівняння $f(a) = 0$ має не більше n різних коренів $a \in k$.

Дов-ня Індукція за n

Коли $n = 1$ $f(x) = ax + b$, $a \neq 0$

Тоді $x = -b/a \in k$ єдиний корінь ✓

Нехай $n > 1$ і твердження виконується для всіх многочленів меншого степеня.

Якщо f не має коренів в k то тв-ня для f виконується.

Інакше, нехай $a \in k$ є коренем $f(x)$. Тоді

$$f(x) = q(x)(x-a) + r$$

r — остача, степеня 0

Підставляючи $x = a \Rightarrow r = 0$

$$f(x) = q(x)(x-a)$$

$$\deg(q) = n-1$$

За припущенням індукції q має $\leq n-1$ різних коренів в k $\Rightarrow$ f має $\leq n$ коренів. ☒

В Теоремі Вільсона
$f(x) = x^2 - 1$ має
два корені в $\mathbb{F}_p$, $p \geq 3$.
Розглянемо $f(x) = x^2 + 1$.

Тв-ня 6 Конгруенція
$$x^2 \equiv -1 \pmod p$$
має розв'язки
для $p = 2$ та $p \equiv 1 \pmod 4$.

Дов-ня $p = 2$ ✓
Нехай $p \geq 3$.
За теоремою Вільсона

$$\underbrace{(1 \cdot 2 \cdot \ldots \cdot \tfrac{p-1}{2})}_{\psi} \cdot \underbrace{(\tfrac{p+1}{2} \cdot \ldots \cdot p-1)}_{\psi} \equiv -1 \ (p)$$

для $\forall$ j маємо $(p-j)$
і $j \cdot (p-j) \equiv -j^2 \ (p)$

$$\prod_{j=1}^{\frac{p-1}{2}} (-j^2) \equiv -1 \ (p)$$

$$\left(\prod_{j=1}^{\frac{p-1}{2}} j \right)^2 \equiv (-1)^{\frac{p+1}{2}} \ (p)$$

Якщо $p \equiv 1 \pmod 4$ то $\frac{p+1}{2}$
парне, і маємо розв'язок
$x = \prod_{j=1}^{\frac{p-1}{2}} j$.

Навпаки, нехай маємо
x таке що $x^2 \equiv -1 \ (p)$

$x^2 \equiv -1 \pmod p$

Тоді

$$1 \equiv x^{p-1} = (x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \ (p)$$

$\Rightarrow \frac{p-1}{2}$ є парним

$\Rightarrow p \equiv 1 \pmod 4$ ⊠

Повернемося до

$(\mathbb{Z}/n\mathbb{Z})^\times$ — ?

Теорема 7 (китайська теорема про лишки)

Нехай $m_1, \dots, m_r \in \mathbb{Z}_{\geq 2}$ є попарно взаємно простими:

$(m_i, m_j) = 1 \quad \forall\ i \neq j$.

Тоді для будь яких $a_1, \dots, a_r \in \mathbb{Z}$ система конгруенцій

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \dots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

має розв'язок, і кожні два розв'язки відрізняються на число кратне

$m := m_1 \cdot \dots \cdot m_r$.

Інтерпретація Теореми 7
в термінах кілець:

розглянемо відображення

$$(*)\quad \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_2\mathbb{Z}$$

$$\bar{a} \longmapsto (\overline{a \bmod m_1}, \dots, \overline{a \bmod m_2})$$

Ик.

$$\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

$$\{\bar{0}, \dots, \bar{5}\} \qquad \{\bar{0}, \bar{1}\} \qquad \{\bar{0}, \bar{1}, \bar{2}\}$$

$$\begin{aligned}
\bar{0} &\longmapsto (\bar{0}, \bar{0}) \\
\bar{1} &\longmapsto (\bar{1}, \bar{1}) \\
\bar{2} &\longmapsto (\bar{0}, \bar{2}) \\
\bar{3} &\longmapsto (\bar{1}, \bar{0}) \\
\bar{4} &\longmapsto (\bar{0}, \bar{1}) \\
\bar{5} &\longmapsto (\bar{1}, \bar{2})
\end{aligned}$$

бієкція

(*) це гомоморфізм кілець

ін'єктивний:
якщо $m_i \mid a \quad \forall i = 1, \dots, 7$

то $m \mid a$
(з єдиності розкладу на прості множники в $\mathbb{Z}$)

сюр'єктивність:
китайська теорема про лишки

Дов-ко Теореми 7

$$(*)\begin{cases} x \equiv a_1 \ (m_1) \\ \vdots \\ x \equiv a_r \ (m_r) \end{cases}$$

Позначимо $n_i = \frac{m}{m_i} = \prod\limits_{\substack{j=1 \\ j\neq i}}^{r} m_j$

Оскільки $(m_j, m_i) = 1 \ \forall j \neq i$ то $(n_i, m_i) = 1$.

Тоді існує $b_i \in \mathbb{Z}$ т.ш.

$n_i \cdot b_i \equiv 1 \pmod{m_i}$.

Нехай $x_0 = \sum\limits_{i=1}^{r} n_i b_i a_i$.

Перевіримо що це розв'язок $(*)$:

Для $\forall j$ та $\forall i \neq j$

маємо $m_j \mid \frac{m}{m_i} = n_i$ і тому

$$x_0 \equiv n_j b_j a_j \ (m_j) \equiv a_j \ (m_j).$$

Нехай x_1 це деякий інший розв'язок. Тоді

$$m_j \mid (x_0 - x_1) \quad \forall j = 1, \dots, 2$$

$$\Rightarrow \ m \mid (x_0 - x_1) \qquad \boxtimes$$

Наприклад:

$$\begin{cases} x \equiv 13 \pmod{25} \\ x \equiv 3 \pmod{4} \end{cases}$$

$m = 25 \cdot 4 = 100$

$4 \cdot 19 \equiv 1 \pmod{25}$ PARI/GP:

Mod(4, 25)^(-1)

% = Mod(19, 25)

$25 \cdot 1 \equiv 1 \pmod{4}$

$x_0 = 4 \cdot 19 \cdot 13 + 25 \cdot 1 \cdot 3$

$= 1063 = 63 \pmod{100}$

ізоморфізм кілець

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_2\mathbb{Z}$$

$\Rightarrow$ групи одиниць також ізоморфні (вправа)

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/m_1\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/m_2\mathbb{Z})^\times$$

$\Rightarrow$

$$\varphi(m) = \varphi(m_1) \dots \varphi(m_2)$$

<u>Наслідок 8</u> Нехай $m = p_1^{e_1} \dots p_2^{e_2}$ це розклад на прості множники

Тоді

$$\varphi(m) = \prod_{i=1}^{2} \left(p_i^{e_i} - p_i^{e_i - 1} \right) = m \prod_{i=1}^{2} \left(1 - \frac{1}{p}\right)$$

p просте

Наступного разу:

$$(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times$$

є циклічною групою:

$\exists\ \bar{a} \in \mathbb{F}_p^\times$ що

$$\{\bar{1}, \bar{a}, \bar{a}^2, \dots, \bar{a}^{p-2}\} = \mathbb{F}_p^\times.$$

Доведіть!

І також

$$(\mathbb{Z}/p^e\mathbb{Z})^\times = \langle \bar{b} \rangle$$

для деякого $\bar{b} \in (\mathbb{Z}/p^e\mathbb{Z})^\times$.

$K = \mathbb{Q}(\xi)$ $n = \deg(f)$

$f(x) \in \mathbb{Q}[x]$ $f(\xi) = 0$

$\theta_1, \dots, \theta_n$ базис $K/\mathbb{Q}$

$\alpha \in K$ $L_\alpha = (l_{ij}) \in \mathbb{Q}^{n \times n}$

$$\alpha \theta_j = \sum_{i=1}^{n} \theta_i l_{ij}$$

$$(\alpha \cdot Id - L_\alpha) \begin{pmatrix} \theta_1 \\ \vdots \\ \theta_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

$\Rightarrow \det(\alpha \cdot Id - L_\alpha) = 0$

$f_\alpha(\alpha) = 0$

кратні корені?

$\alpha \in \mathbb{Q}(\xi)$

$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\xi)$

$d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$

$\alpha_1, \dots, \alpha_d$ Всі різні

$[\mathbb{Q}(\xi) : \mathbb{Q}(\alpha)] = m$

Ψ

β первісний

$1, \beta, \beta^2, \dots, \beta^{m-1}$ базис

тоді

$\alpha_i \beta^j$ $i = 1, \dots, d$

$0 \le j \le m-1$

не базис $K/\mathbb{Q}$

Γ

в цьому базисі

видно що

$$f_\alpha(x) = p_\alpha(x)^m$$

$$= (x - \alpha_1) \dots (x - \alpha_d)$$

(i)

$K = \mathbb{Q}(\sqrt{m})$ m вільне від кв-тів

$m \equiv 2, 3 \ (4)$

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{m}$$

$$d_K = \det\begin{pmatrix} 1 & 1 \\ \sqrt{m} & -\sqrt{m} \end{pmatrix}^2 = 4m$$

$m \equiv 1 \ (4)$

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\,\frac{1+\sqrt{m}}{2}$$

$$d_K = \det\begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{m}}{2} & \frac{1-\sqrt{m}}{2} \end{pmatrix}^2 = m$$

(iii) Stickelberger's Discriminant relation

K числове поле

$$d_K = d(\mathcal{O}_K) \equiv 1, 0 \mod (4)$$

$$\det(\sigma_i(\theta_j)) = \sum_{\varepsilon \in S_n} (-1)^{\mathrm{sgn}(\varepsilon)} \prod_{i=1}^{n} \sigma_i(\theta_{\varepsilon(i)})$$

$= P - N$

P — сума по ε з $\mathrm{sgn}(\varepsilon) = 1$; N — сума по ε з $\mathrm{sgn}(\varepsilon) = -1$

(*)

$P+N$ і $P \cdot N$ є симетричними від вкладень ... тобто в $\mathbb{Q} \cap \overline{\mathbb{Z}}$ тобто в $\mathbb{Z}$

(ii)

$d_K \in \mathbb{Z}$?

$\theta_1, \dots, \theta_n$ $\mathbb{Z}$-базис $\mathcal{O}_K$

$\sigma_i(\theta_j) \in \overline{\mathbb{Z}}$

$\Rightarrow$ $d_K \in \overline{\mathbb{Z}}$

Чтобы $d_K \in \mathbb{Q}$? ($\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$)

Т-ма 4 (i):

$d(\theta_1, \dots, \theta_n) \in \mathbb{Q} \setminus \{0\}$

' зависс $K/\mathbb{Q}$

(iii)

$$d_K = (P - N)^2$$

$$= (P+N)^2 - 4PN$$

$$\in \mathbb{Z} \qquad \in \mathbb{Z}$$

(* z symetrii bign. $\sigma_i \leftrightarrow \sigma_{\bar{i}}$)

$$\equiv 0, 1 \pmod 4$$