§1. Подільність та алгоритм Евкліда

<u>Озн-ня</u> $a, b \in \mathbb{Z}$, $a \neq 0$

$a \mid b$ якщо $\exists c \in \mathbb{Z}$ т.щ. $b = a \cdot c$

a ділить b

a є дільником b

b ділиться на a

$0 = 0 \cdot a \Rightarrow 0$ ділиться на будь-яке число

$(b \neq 0)$ $|b| = |a| \cdot |c| \Rightarrow |a| \leq |b|$

кожне $b \neq 0$ має скінченну кількість дільників

<u>Озн-ня</u> Якщо $a \neq 0$ або $b \neq 0$

$(a, b) = \max\{c \geq 1 : c \mid a \text{ та } c \mid b\}$

найбільший спільний дільник

н.с.д.

$(a_1, \ldots, a_n) = \max\{c \geq 1 : c \mid a_i \ \forall i\}$

Числа $a_1, \ldots, a_n$ наз-ся взаємнопростими якщо $(a_1, \ldots, a_n) = 1$

<u>Твердження 1</u> Існують $x, y \in \mathbb{Z}$ такі що

$$(a, b) = x \cdot a + y \cdot b.$$

"ділення з остачею"

Лема 2 Для будь-яких $a, b \in \mathbb{Z}$, $a > 0$ існують єдині $q, r \in \mathbb{Z}$ т. щ.

$$b = q \cdot a + r, \quad 0 \leq r < a.$$

Дов-ня Візьмемо r = найменше число в

$$\{b + a \cdot s : s \in \mathbb{Z}\} \cap \mathbb{Z}_{\geq 0}.$$

Тоді $r \geq 0$ і якщо $r > a$ тоді $r - a$ також належить цій множині і $< r$, суперечність.

Тобто $0 \leq r < a$.

Єдиність:

$$b = q_1 \cdot a + r_1$$
$$b = q_2 \cdot a + r_2$$

і $r_2 < r_1$. Тоді

$$(q_1 - q_2) a + (r_1 - r_2) = 0$$
$$\Rightarrow a \mid (r_1 - r_2)$$

але

$$0 < r_1 - r_2 < r_1 < a,$$

суперечність.

$\boxtimes$

<u>Тв-ня 1</u> $\exists\ x, y \in \mathbb{Z}$ т. щ.

$(a, b) = x \cdot a + y \cdot b$.

<u>Дов-ня</u> Нехай c = найменший елемент у множині

$\{xa + yb : x, y \in \mathbb{Z}\} \cap \mathbb{Z}_{>0}$.

Хочемо довести що $c \mid a, b$.

$a = c \cdot q + r \ , 0 \le r < c$

$c = x_0 a + y_0 b$

$0 \le r = (1 - x_0 q) a - y_0 b$

$\Rightarrow \ r = 0$

Аналогічно, $c \mid b$

Максимальність:

Нехай $d \mid a$, $d \mid b$

$a = d \cdot e \qquad b = d \cdot f$

Тоді

$c = x_0 a + y_0 b = (x_0 e + y_0 f) d$

ділиться на d

$\Rightarrow \quad c = (a, b)$ $\boxtimes$

<u>Наслідок 3</u>

$$\{xa + yb : x, y \in \mathbb{Z}\}$$
$$\parallel$$
$$\{z(a, b) : z \in \mathbb{Z}\}$$

застосування:

Лінійні діофантові рівняння

$a, b, c \in \mathbb{Z}$
$a, b \neq 0$

$$ax + by = c \quad (*)$$

Знайти всі розв'язки $x, y \in \mathbb{Z}$.

Якщо $(a,b) \nmid c \Rightarrow$ немає розв'язків

Нехай $(a,b) \mid c$

$$c = (a,b) c_1$$
$$a = (a,b) \cdot a_1$$
$$b = (a,b) \cdot b_1 \qquad (a_1, b_1) = 1$$

Насл.3 $\Rightarrow \exists\, x_0, y_0$ т.ч.

$$a_1 x_0 + b_1 y_0 = c_1$$

Тоді $a x_0 + b y_0 = c$.

Нехай x_1, y_1 це будь-який інший розв'язок $(*)$. Тоді

$$a_1 \underbrace{(x_1 - x_0)}_{\substack{\parallel \\ \exists m:\ m b_1}} + b_1 \underbrace{(y_1 - y_0)}_{\substack{\parallel \\ -m a_1}} = 0$$

Тобто

$$\begin{cases} x = x_0 + m b_1 \\ y = y_0 - m a_1 \end{cases} \quad m \in \mathbb{Z}$$

це множина розв'язків $(*)$.

Питання: як знайти перший розв'язок x_0, y_0?

Алгоритм Евкліда

$a, b \in \mathbb{Z}$, $a > 0$

ділення з остачею

$b = a q_1 + r_1$, $0 < r_1 < a$

$a = r_1 q_2 + r_2$, $0 < r_2 < r_1$

$r_1 = r_2 q_3 + r_3$, $0 < r_3 < r_2$

$\dots$

$r_{n-2} = r_{n-1} q_n + r_n$, $0 < r_n < r_{n-1}$

$r_{n-1} = r_n q_{n+1}$ $\quad r_{n+1} = 0$

Тв-ня 4 останній ненульовий лишок

$r_n = (a, b)$

Зауваження:

$r_n \mid a$, $r_n \mid b$

$\dots$

$r_n \mid r_{n-2}$

$r_n \mid r_{n-1}$

r_n є спільним дільником a і b

за індукцією

$r_i = x_i a + y_i b$

$$\begin{cases} x_i = x_{i-2} - q_i x_{i-1} \\ y_i = y_{i-2} - q_i y_{i-1} \end{cases}$$

Приклад: $a=7 \quad b=10$

$$\begin{aligned} 10 &= 7\cdot 1 + 3 \\ 7 &= 3\cdot 2 + 1 \\ 3 &= 1\cdot 3 \end{aligned} \qquad \begin{aligned} 3 &= 10-7 \\ 1 &= 7-(10-7)2 \\ &= 3\cdot 7 - 2\cdot 10 \end{aligned}$$

$$(10,7) = 1 = 3\cdot 7 + (-2)\cdot 10$$

Лема 5 $(a,b) = (a, b + a\cdot x)$

Дов-ня Позначимо $d = (a,b)$

$g = (a, b + a\cdot x)$

Ясно що $d \mid (b + a\cdot x) \Rightarrow d \mid g$

Тв-ня 1 $\Rightarrow d = ax_0 + by_0$

$= a(x_0 - x\cdot y_0) + (b + ax)y_0$

Наслідок 2 $\Rightarrow g \mid d$

$\Rightarrow d \mid g, g \mid d \Rightarrow d = g$ $\boxtimes$

Дов-ня Тв-ня 4 (алг. Евкліда)

лема 5 $\Rightarrow$

$$\begin{aligned} b &= a q_1 + r_1 & (b,a) &= (a, r_1) \\ a &= r_1 q_2 + r_2 & (a, r_1) &= (r_1, r_2) \\ r_1 &= r_2 q_3 + r_3 & (r_1, r_2) &= (r_2, r_3) \\ &\vdots & &\vdots \\ r_{n-1} &= r_n \cdot q_{n+1} & (r_{n+1}, r_n) &= r_n \end{aligned}$$

$\boxtimes$

k поле

нп. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$

$$k[x] = \left\{ \sum_{i=0}^{n} a_i x^i : \begin{array}{l} n \geq 0 \\ a_i \in k \end{array} \right\}$$

кільце многочленів з коефіцієнтами в k

<u>Лема 6</u> ("ділення з остачею в кільці многочленів")

Нехай $f, g \in k[x]$, $g \neq 0$. Тоді існують єдині многочлени $q, r \in k[x]$ т.щ. $f = q \cdot g + r$ і або $r = 0$ або $\deg(r) < \deg(g)$.

Дов-ня: вправа.

Можна використовувати алгоритм Евкліда!

R область цілісності = комутативне ненульове ($R \neq \{0\}$) кільце без дільників нуля

$x, y \in R \quad xy = 0$
$\Rightarrow x = 0$ або $y = 0$

$I \subseteq R$ ідеал: $0 \in I$

$x, y \in I \Rightarrow x + y \in I$

$x \in I, r \in R \Rightarrow xr \in I$

Наприклад

$\langle x_1, \dots, x_n \rangle$

$= \left\{ \sum_{i=1}^{n} r_i x_i : r_i \in R \right\}$

ідеал породжений елементами $x_1, \dots, x_n \in R$

Сьогодні ми довели в $R = \mathbb{Z}$

$$\underbrace{\{xa + yb : x, y \in \mathbb{Z}\}}_{\langle a, b \rangle} = \underbrace{\{z(a,b) : z \in \mathbb{Z}\}}_{\langle (a,b) \rangle}$$

За індукцією

$\langle x_1, \dots, x_n \rangle = \langle (x_1, \dots, x_n) \rangle$ в $\mathbb{Z}$

<u>Озн-ня</u> Ідеали вигляду $\langle x \rangle$, $x \in R$ називаються головними ідеалами.

Область цілісності, у якій кожен ідеал є головним наз-ся областю головних ідеалів (ОГІ).

Приклад: $\mathbb{Z}$, $k[x]$ є ОГІ (вправа!)

k має два ідеали: $I = \{0\} = \langle 0 \rangle$ та $I = k = \langle 1 \rangle$

тобто також ОГІ

$k[x_1, \ldots, x_n]$ $n > 1$
не є ОГІ
(без доведення)

Озн-ня Область цілісності наз-ся евклідовою областю якщо існує функція

$\lambda : R \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$

т.щ. для кожних $a, b \in R$, $a \neq 0$ існують $q, r \in R$ т.щ.

$$b = q \cdot a + r$$

і або $r = 0$ або $\lambda(r) < \lambda(a)$.

λ наз-ся евклідовою нормою на кільці R

Нп. $R = \mathbb{Z}$ $\lambda(x) = |x|$

$R = k[x]$ $\lambda(f) = \deg(f)$

Теорема 7 Евклідова область є областю головних ідеалів.

План доведення: $I \neq \{0\}$

Візьмемо $x \in I$ т.щ.

$\lambda(x) = \min\{\lambda(y) : y \in I \setminus \{0\}\}$.

Можна показати що

$I = \langle x \rangle$ (вправа!)

$\boxtimes$

<u>Озн-ня</u> $x \neq 0$ є н.с.д. $x_1, \dots, x_n$ якщо x ділиться на кожен спільний дільник $x_1, \dots, x_n$.

Н.с.д. не завжди існує (приклади пізніше).

Якщо R це ОГІ тоді $\exists x \neq 0$ т.щ. $\langle x_1, \dots, x_n \rangle = \langle x \rangle$. Тоді ясно що x це н.с.д.

Єдиність ?

Нехай x, x' це н.с.д.

Тоді $x = x'u$

$x' = xv = x'uv$

$\underbrace{x'}_{\neq 0}(1 - uv) = 0$

R обл. цілісності $\Rightarrow u \cdot v = 1$

<u>Озн-ня</u> $R^\times = \left\{ u \in R : \begin{array}{l} \exists v \in R \text{ т.щ.} \\ u \cdot v = 1 \end{array} \right\}$

множина оборотних ел-тів або одиниць кільця R

є групою: $u_1, u_2 \in R \Rightarrow u_1 u_2 \in R$

Озн-ня Для $x \in R$ елементи виду $x \cdot u$, $u \in R^*$ наз-ся асоційованими з x.

$\Rightarrow$ Кожні два н.с.д. є асоційованими один з одним.

$\mathbb{Z}^\times = \{1, -1\}$ н.с.д. в $\mathbb{Z}$ єдиний з точністю до $\pm$, ми вибираємо додатній з двох ел-тів.

$k[x]^\times = k^\times = k \setminus \{0\}$

н.с.д. двох многочленів визначений з точністю до множення на ненульову сталу. Можливий вибір: нормований многочлен (старший коефіцієнт $= 1$)

У наступному прикладі немає "природного" представника множини асоційованих елементів:

$$R = \mathbb{Z} + \mathbb{Z}\sqrt{-1}$$

$$= \{ m + n\sqrt{-1} : m, n \in \mathbb{Z} \}$$

кільце гауссових цілих чисел

Вправи:

- доведіть що R є евклідовою областю з

$$\lambda(m + n\sqrt{-1}) = m^2 + n^2$$

- покажіть що

$$R^\times = \{ 1, -1, \sqrt{-1}, -\sqrt{-1} \}$$

Підказка: скористатися мультиплікативністю λ:

$$\lambda(x_1 x_2) = \lambda(x_1)\lambda(x_2)$$

- застосуйте алгоритм Евкліда: $2 + 3\sqrt{-1}$ та $4 + \sqrt{-1}$.