$d = (a,b)$ $\quad |d| = (|a|+|b|)$ $\quad \exists u,v: d = ua + vb$

Св. (АЕ) $\quad (da, db) = d(a,b)$

Д-во Като „умножаваме" АЕ за a_2 и b_2 с d, получаваме АЕ за da и db

Св. $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$

Опр. Ако $(a,b) = 1$ – взаимно прости

Д-во $\left((a,b)\frac{a}{(a,b)}, (a,b)\frac{b}{(a,b)}\right) = (a,b)\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right)$

Св. $a \mid bc$, $(a,b) = 1 \Rightarrow a \mid c$

Д-во $\exists u,v: ua + vb = 1 \Rightarrow uac + vbc = c \Rightarrow a \mid c$

Ц $a \mid bc \Rightarrow \frac{a}{(a,b)} \mid c$

Д-Ц $\exists k : bc = ak \Rightarrow \frac{b}{(a,b)} c = \frac{a}{(a,b)} k$

$\Rightarrow \frac{a}{(a,b)} \mid \frac{b}{(a,b)} c \Rightarrow \frac{a}{(a,b)} \mid c$

$\left(\left(\frac{a}{(a,b)}, \frac{b}{(a,b)} \right) = 1 \right)$

Т. $a \mid m, b \mid m \Leftrightarrow \exists t : m = \frac{ab}{(a,b)} t$

Зам. $\forall t$ от $\frac{ab}{(a,b)} t$ и $b \mid \frac{ab}{(a,b)} t$

$\frac{ab}{(a,b)} t = a \frac{b}{(a,b)} t = b \frac{a}{(a,b)} t$

Сл. $\{$ОД на a и $b\} = \left\{ \frac{ab}{(a,b)} t \mid t \in \mathbb{Z} \right\}$

В частност $[a,b] = \frac{ab}{(a,b)}$

Д-во $a \mid m \Rightarrow m = ak$

$b \mid ak \Rightarrow \frac{b}{(a,b)} \mid k \Rightarrow k = \frac{b}{(a,b)} t \Rightarrow m = \frac{ab}{(a,b)} t$

Т. $a \mid c$, $b \mid c$, $(a,b) = 1 \Rightarrow ab \mid c$

Д-во $\exists [a,b] \mid c$

$\| \frac{ab}{(a,b)} = ab$

Опр. p - простое, если $p \mid ab \Rightarrow p \mid a$ или $p \mid b$

$\Leftrightarrow (ab) \subseteq (p) \Rightarrow (a) \subseteq (p)$ или $(b) \subseteq (p)$

$\Leftrightarrow ab \in (p) \Rightarrow a \in (p)$ или $b \in (p)$

(только идеал с простым числом)

$\Leftrightarrow (a)(b) \subseteq p \Rightarrow (a) \subseteq (p)$ или $(b) \subseteq (p)$

2) p – неразложим, ако $d \mid p \Rightarrow d = \pm 1, \pm p$ ($d = \varepsilon, \varepsilon p$; $\varepsilon \in \mathbb{Z}^{\times} = \{\pm 1\}$)

$\Leftrightarrow \big((p) \subseteq (d) \Rightarrow (d) = \mathbb{Z}$ или $(d) = (p) \big)$

(Такива идеали се наричат максимални)

Зад: По-нататък ще докажем, че $\forall$ max идеал е и прост. Обратното в общия случай не е вярно

Тв. p – прост $\Leftrightarrow$ p – неразложим

Д-во $(\Rightarrow)$ Нека p е разложим $\Rightarrow \exists a, b : p = ab \;\Big|\; \begin{matrix} 1 < |a| < |p| \\ 1 < |b| < |p| \end{matrix}$

($a = d$, $b = \frac{p}{d}$, $d \neq \pm 1, \pm p$)

$\Rightarrow p \mid ab$, но $p \nmid a$ и $p \nmid b$

$(\Leftarrow)$ Нека $p \mid ab$; $(p, a) \mid p \Rightarrow (p, a) = 1, p$

- $(p, a) = p \Rightarrow p \mid a$
- $(p, a) = 1 \Rightarrow p \mid b$ ($p \mid ab$)

Деф. 1) p - просто $\forall a\,(p,a)=1,\ p \mid a$ $\Leftarrow$ ($(p,a)=1$, $p \mid a$)

2) p/q ; p-q - пр. $\Rightarrow p=q$ $\quad (p>0,\ q>0)$

3) ± 1 не е прости $\quad (\pm 1)=\mathbb{Z}$

Основна теорема на аритметиката на целите числа

$\forall n>1\ \exists p_1 \dots p_k$ - прости $\wedge\ p_i>0$: $n=p_1 \dots p_k$

Представянето е единствено с точност до реда на множ.

Зад. 1) $n \in \mathbb{Z}$ $\quad n=\pm p_1 \dots p_k$; $p_1 \dots p_k = q_1 \dots q_s \Rightarrow \Big|_{q_i=\pm p_i}^{k=s}$

2) $n=p_1^{\alpha_1} \dots p_k^{\alpha_k}$; $p_1, \dots, p_k$ - прост. - канонично разлагане

3) $d/n \Rightarrow d=\pm p_1^{\beta_1} \dots p_k^{\beta_k}$, $0 \le \beta_i \le \alpha_i$

4) $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $\alpha_i \geq 0$

$b = p_1^{\beta_1} \cdots p_k^{\beta_k}$, $\beta_i \geq 0$

$\Rightarrow$ • $(a,b) = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$ $\quad \gamma_i = \min\{\alpha_i, \beta_i\}$

• $[a,b] = p_1^{\delta_1} \cdots p_k^{\delta_k}$ $\quad \delta_i = \max\{\alpha_i, \beta_i\}$

<u>Зад.</u> Дко $\ldots a_n | a_{n-1} | \cdots | a_2 | a_1$

$\Leftrightarrow (a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq \cdots$

$(\sigma) = \bigcup_{i=1}^{\infty} (a_i) \lhd \mathbb{Z} \Rightarrow \exists i : a \in (a_i) \Rightarrow (\sigma) \subseteq (a_i)$

$(a_i) \subseteq (\sigma)$ $\Big\} (a_i) = (\sigma)$

$\Rightarrow (a_i) = (a_{i+1}) = \cdots = (\sigma)$

Д-во (∃) ще го док. с мат. индукция по n

- $n = 2$. OK
- Нека е вярно $\forall k < n$
- док. за n

  ≥ n - просто $\Rightarrow n = n$

  ≥ n - съставно $\Rightarrow n = ab$, $1 < a, b < n$

  ОТ инд. хип. $\Rightarrow \exists p_1 \ldots p_k : a = p_1 \ldots p_k$ $\quad p_i, q_i$ - прости

  $\exists q_1 \ldots q_s : b = q_1 \ldots q_s$

  $\Rightarrow n = p_1 \ldots p_k q_1 \ldots q_s$

(Единственост) $n = p_1 \ldots p_k = q_1 \ldots q_s$ (p_i, q_i - прости)

$p_k \mid q_1 \ldots q_s \Rightarrow \exists i : p_k \mid q_i \Rightarrow p_k = q_i$. БОО $i = s$

(формально по конструкции $\frac{k}{}$)

$p_1 - p_{k-1} = q_1 - q_{s-1}$ и т. д. –

Сравнения

Опр. $a \equiv b \pmod n$ ($\frac{a}{}$ и $\frac{b}{}$ сравнимо с "$\frac{b}{}$" по модулю "$\frac{n}{}$"),

если $n \mid a-b$

Св-ва: ($\frac{n}{}$ – фикс.) (Часто пишем просто $a = b$ или $a \equiv b (n)$)

1) $a \equiv a$

2) $a \equiv b \Rightarrow b \equiv a$

3) $a \equiv b$, $b \equiv c \Rightarrow a \equiv c$

} "$\equiv$" – ОЭ

4) $a \equiv b \Leftrightarrow \exists c : a = b + nc \quad (\Leftarrow \forall c)$

5) $a \equiv b, a = nq_1 + r_1, b = nq_2 + r_2, 0 \le r_1, r_2 < n \Rightarrow r_1 = r_2$

$(n \mid a-b = n(q_1-q_2) + r_1 - r_2 \Rightarrow n \mid r_1 - r_2 \xrightarrow{|r_1-r_2|<n} r_1 - r_2 = 0)$

6) $a \equiv b, c \equiv d \Rightarrow a \pm c \equiv b \pm d$

7) $a \equiv b, c \equiv d \Rightarrow ac \equiv bd$

$(a = b + c_1 n, c = d + c_2 n \Rightarrow ac = bd + n(bc_2 + c_1 d + n c_1 c_2))$

8) $a \equiv b \Rightarrow ac \equiv bc$

9) $a \equiv b \Rightarrow a^k \equiv b^k$

10) $a + b \equiv c \Rightarrow a \equiv c - b$

(1) $f \in \mathbb{Z}[X]$, $a \equiv b \Rightarrow f(a) \equiv f(b)$

Th. $ka \equiv kb \ (n) \Rightarrow a \equiv b \left(\frac{n}{(k,n)}\right)$

D-ea $n \mid k(a-b) \Rightarrow \frac{n}{(k,n)} \mid a-b$

Def „$\equiv$" e RE

$\bar{a} = [a] = \{ b \mid a \equiv b \pmod n \}$ – clasa lui echiv.

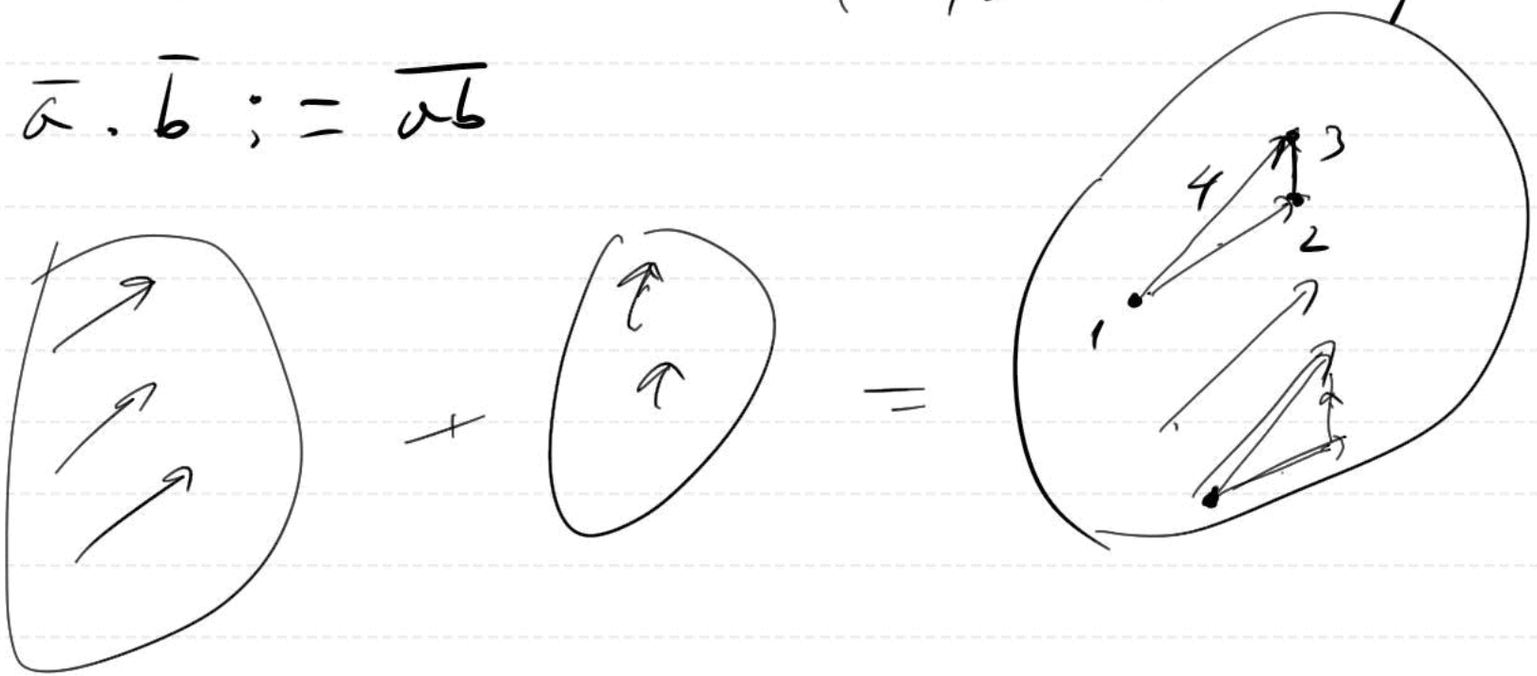
$a \sim b \Leftrightarrow [a] = [b]$, sau $[a] \cap [b] = \emptyset$

- $[a] = [b] \Leftrightarrow a \equiv b$
- $\mathbb{Z} = \bigcup_{a \in \mathbb{Z}} [a] = \bigcup_{r=0}^{n-1} [r]$ / reuniune cu puse.
- $a = bn + r \Rightarrow [a] = [r]$; $[r_1] = [r_2]$, $0 \le r_1, r_2 < n \Rightarrow r_1 = r_2$

$\mathbb{Z}_n := \{ [0], [1], \dots [n-1] \}$, $|\mathbb{Z}_n| = n$

$\bar{a} + \bar{b} := \overline{a+b}$ ($a, b \in \mathbb{Z}$ – произвольные)

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



Тв. $\bar{a} = \bar{a'}$ и $\bar{b} = \bar{b'} \Rightarrow \overline{a+b} = \overline{a'+b'}$ и $\overline{ab} = \overline{a'b'}$, т.е.
($\Leftrightarrow a \equiv a'$) ↓ ($\Leftrightarrow b \equiv b'$) → ($\Leftrightarrow a+b \equiv a'+b'$) ↑ ($\Leftrightarrow ab \equiv a'b'$)
$+, \cdot$ в $\mathbb{Z}_n$ – корректно определены

Тв $(\mathbb{Z}_n, +, \cdot)$ — комут. пръстен с 1

Д-во $+, \cdot$ — коректно деф.

1) $(\bar{a}+\bar{b})+\bar{c} = \overline{a+b}+\bar{c} = \overline{(a+b)+c}$

$\bar{a}+(\bar{b}+\bar{c}) = \bar{a}+\overline{b+c} = \overline{a+(b+c)}$ $\quad \| \Leftarrow (a+b)+c = a+(b+c)$

(асоциативността в $\mathbb{Z}_n$ се „наследява" от асоциативността в $\mathbb{Z}$)

и т. н.; $\bar{0}$ – нулев; $-\bar{a} = \overline{(-a)}$; $\bar{1}$ – единичен

Пример $n=6$ $\quad \bar{2}\,\bar{3} = \bar{0}$

Тв. 1) $\bar{a}$ е делител на 0 $\Leftrightarrow (a,n) \neq 1$

2) $\bar{a}$ е обратим $\Leftrightarrow (a,n) = 1$

Δ-ια 1/(⇒) Έστω $\bar{a} \neq \bar{0}$ ε γενικά του 0 ⇒ $\exists \bar{b} \neq \bar{0} : \bar{a}\bar{b} = \bar{0}$

⇒ $\overline{ab} = \bar{0}$ ⇒ $ab \equiv 0 \Rightarrow n \mid ab$ $(n \times a, n \times b)$

Άρα $(n, a) = 1 \Rightarrow n \mid b$ ΤΣ $\Rightarrow (n, a) \neq 1$

(⇐) Έστω $(n, a) = d \neq 1 \Rightarrow \left(\frac{n}{d}\right) \neq \bar{0}$

$\bar{a} \cdot \frac{\bar{n}}{d} = \overline{a \frac{n}{d}} = \overline{n \frac{a}{d}} = \bar{n}\left(\frac{a}{d}\right) = \bar{0} \Rightarrow \bar{a}$ ε γεν. του 0

2/(⇒) $\bar{a}$ ε αδ/στον ⇒ $\exists \bar{b} : \bar{a}\bar{b} = \bar{1} \Rightarrow \overline{ab} = \bar{1} \Rightarrow ab \equiv 1$

⇒ $ab = 1 + kn$ $(\exists k) \Rightarrow (a, n) \mid 1 \Rightarrow (a, n) = 1$

(⇐) $(a, n) = 1 \Rightarrow \exists u, v : au + nv = 1 \Rightarrow au \equiv 1$

⇒ $\overline{au} = \bar{1}$ ⇒ $\bar{a}\,\bar{u} = \bar{1}$ ⇒ $\bar{a}$ αδ/στον $(\bar{a}^{-1} = \bar{u})$

R – ум.; $I \lhd R$ – идеал, ако: (главен)

– $\forall i_1, i_2 \in I \Rightarrow i_1 - i_2 \in I$ $((I, +) < (R, +))$

– $\forall i \in I, \forall r \in R \Rightarrow ir, ri \in I$

R – комут. ум. с 1 $(a) = \{ar \mid r \in R\} \lhd R$

главен