$(a,b)=1 \to$ a и b са взаимнопрости

$(a)(b)=(ab)$; $a/b \Leftrightarrow (b)\subseteq(a)$

<u>Оп.</u> 1) p - просто, ако $p/ab \Rightarrow p/a$ или p/b

$\Leftrightarrow$ ако $ab\in(p)$, то $a\in(p)$ или $b\in(p)$ (прост идеал)

2) p - неразложимо, ако $p=ab$, то $|p|=|a|$ или $|p|=|b|$

$\Leftrightarrow$ ако a/p, то $|a|=p$ или $|a|=1$

$\Leftrightarrow$ ако a/p, то $a=\varepsilon p$ или $a=\varepsilon$ за $\varepsilon\in\mathbb{Z}^{*}=\{\pm1\}$

$\Leftrightarrow$ ако $(p)\subseteq(a)$, то $(a)=(p)$ или $(a)=\mathbb{Z}$

((p) е максимален идеал)

<u>Зад.</u> Да се док., че $\forall$ мах идеал е прост

Тв. p - прост $\Leftrightarrow$ p - неразл.

$(\Rightarrow)$ Доп. против., т.е. p е разложимо (съставно число)

$\Rightarrow \exists a, b :$ $\left| \begin{array}{l} p = ab \to a \mid p,\ b \mid p \\ |a| \neq 1, |p| \\ |b| \neq 1, |p| \end{array} \right.$ $\Rightarrow p : a \cdot b \mid ab$ и $p \nmid a$ и $p \nmid b$

$\to |a|, |b| \leq p \xrightarrow{\neq} |a|, |b| < |p|$ $\uparrow\downarrow$

$(\Leftarrow)$ Доп. против., т.е. p - не е прост $\Rightarrow \exists a, b : p \mid ab$, но $p \nmid a$, $p \nmid b$

$d = (p, a) \mid p$ $\qquad (p, a) = 1, p \xrightarrow{p \nmid a} (p, a) = 1 \xrightarrow{p \mid ab} p \mid b$ $\uparrow\downarrow$

$\qquad\qquad\qquad\qquad\qquad\quad\ \uparrow$ неразл.

Зад. $\ldots a_n \overset{\leq}{\mid} a_{n-1} \mid \ldots \overset{\leq}{\mid} a_2 \mid a_1 \to$ процесът е краен

$\Leftrightarrow (a_1) \subset (a_2) \subset \ldots \subset (a_n) \subset \ldots \to$ почти равенство в

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

$\to (a_i) = (a_{i+1}) = \ldots$

Основна теорема на аритметиката на целите числа

$\forall n \in \mathbb{N}, n > 1 \ \exists p_1 \ldots p_k$ – прости ($p_i > 0$) : $n = p_1 \ldots p_k$
(възможно е да са равни)

Представянето е еднозначно с точност до реда на множителите

<u>Д-во</u> ($\exists$) инд. по $\underline{n}$

$n = 2, 3$ – ок.

Нека е вярно $\forall 1 < k < n$

Ще док. за $\underline{n}$

– n – просто $\to n = n$

– n – съставно $\to \exists d \mid n : 1 < d < n \to 1 < \frac{n}{d} < n$

$\Rightarrow$ от инд. доп. $d = p_1 \ldots p_s$; $\frac{n}{d} = q_1 \ldots q_t$

$\Rightarrow n = p_1 \ldots p_s q_1 \ldots q_t$

(единственность) Пусть $n = p_1 \ldots p_k = q_1 \ldots q_s$

(p_i, q_i - простые, >0)

$p_k \mid n = q_1 \ldots q_s \Rightarrow \exists i : p_k \mid q_i$; б.о.о. $i = s$, т.е. $p_k \mid q_s$

$(p_k, q_s) = p_k \neq 1 \to p_k = q_s$

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

перенумеруем $p_i = q_i$

Зам. • $n \in \mathbb{Z}$ $n = \pm p_1 \ldots p_k$; в единственном разложении
$\pm p_i = \varepsilon p_i$, $\varepsilon \in \mathbb{Z}^*$

• $n = \varepsilon p_1 \ldots p_k$, $\varepsilon = \pm 1$

• $n = \varepsilon p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ — каноническая запись

• $d \mid n \to d = \varepsilon p_1^{\beta_1} \ldots p_k^{\beta_k}$ и $\forall i$ $\beta_i \le \alpha_i$
всего их (>0) к $(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1)$

• $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ $\quad \alpha_i \geq 0$

$b = p_1^{\beta_1} \dots p_k^{\beta_k}$ $\quad \beta_i \geq 0$

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

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

X – множество

$R \subset X^2 = X \times X = \{(x,y) \mid x,y \in X\}$ – релация

(може $R \subset X \times Y$ – гр. $f: X \to Y$ $\quad R_f = \{(x, f(x)) \mid x \in X\}$

$(\forall x \exists y : (x,y) \in R_f;\ (x,y_1),(x,y_2) \in R_f \Rightarrow y_1 = y_2)$

Св-ва (с имена)

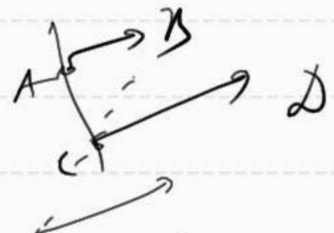
- R е рефлексивна, ако $\forall x \in X$ $(x,x) \in R$
- R е симетрична, ако от $(x,y) \in R \Rightarrow (y,x) \in R$
- R е транзитивна, ако от $(x,y),(y,z) \in R \Rightarrow (x,z) \in R$

Ако R е рефл., симетр. и транзит. се нарича релация на еквивалентност (РЕ); $(a,b)\in R \to a \overset{R}{\sim} b$

Пр. 1) $=$ е РЕ

2) $\leq$ – рефл. и транзитивна; не е симетр.

3) $\overrightarrow{AB} \sim \overrightarrow{CD} \iff AB = CD,\ AB \parallel CD$, еднопосочни



– $A = C,\ B = D$

– $A \neq C$

$[\overrightarrow{AB}] = \vec{a} \ni \overrightarrow{AB}$

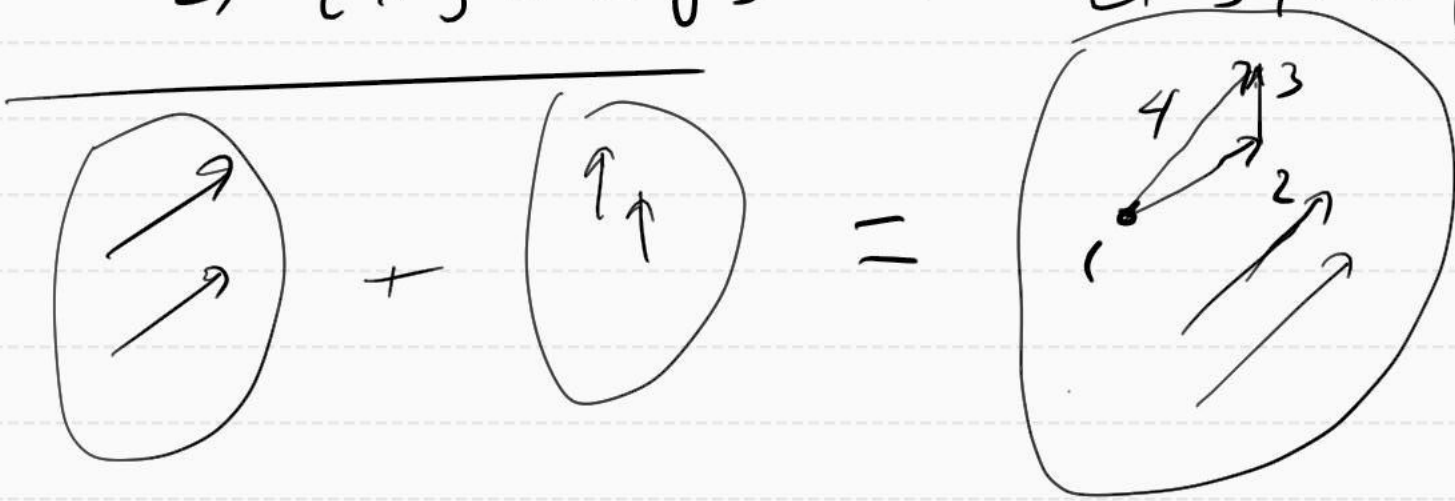
$\sim$ е РЕ

$\sim$ е РЕ в X с $[x] = \{y \in X \mid x \sim y\}$ $\forall x \in X$

клас на еквивалентност

<u>Тв.</u> 1) $X = \bigcup\limits_{x \in X} [x]$

2) $[x] = [y]$ или $[x] \cap [y] = \varnothing$



„корректность“ опр +

<u>Д-во</u> 1) $x \in [x]$ (рефл.) $\to X = \bigcup\limits_{x \in X} [x]$

2) Пусть $[x] \cap [y] \neq \varnothing \Rightarrow \exists z \in [x] \cap [y]$

$\Rightarrow x \sim z,\ y \sim z$

$\overset{\text{симм.}}{z \sim y} \to \underline{x \sim y}$ (тр.)

$t \in [x] \Rightarrow x \sim t$, $\underset{\substack{\text{т. сим.} \\ x \sim y}}{y \sim x} \Rightarrow y \sim t \Rightarrow t \in [y] \Rightarrow [x] \subseteq [y]$

$t \in [y] \Rightarrow y \sim t$, $x \sim y \Rightarrow x \sim t \Rightarrow t \in [x] \Rightarrow [y] \subseteq [x]$

$\Rightarrow [x] = [y]$

<u>Зад.</u> $[x] = [y] \iff x \sim y$

<u>Зад.</u> X се представя като обединение на непресичащи се класове на еквивалентност (на нееквивалентни <u>ел.</u> - представители на класовете (като <u>елементи</u>))

<u>Зад.</u> $X = \bigcup_{i \in I} X_i$, за $i \neq j$ $X_i \cap X_j = \emptyset$ - разбиване на X

- $\forall$ разбиване ще отговаря РЕ - $a \sim b \overset{def}{\iff} \exists i \in I : a, b \in X_i$

- $a \in X_i \Rightarrow [a] = X_i$

Сравнения

Опр. $a \equiv b \pmod{n}$ („a“ е сравнимо с „b“ по модул „n“),

ако $n \mid a - b$

Св-ва

1) $a \equiv a \pmod{n}$

2) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

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

„$\equiv$“ е РЕ

4) $a \equiv b \ (n) \Rightarrow \exists k \quad a = b + \underline{kn}$

5) $\cancel{a \equiv b \ (n)}$, $a = nq_1 + r_1$, $b = nq_2 + r_2$, $0 \le r_1, r_2 < n$

$a \equiv b \ (n) \Leftrightarrow r_1 = r_2$

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

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

$(a = b + k_1 n,\ c = d + k_2 n \rightarrow ac = bd + n(k_1 d + k_2 b + k_1 k_2 n))$

8) $a \equiv b \Rightarrow a \pm c \equiv b \pm c$, $ac \equiv bc$; $a^n \equiv b^n$

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

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

Зад 1/ $\equiv$ е РЕ

2/ $[a] = \{ b \mid a \equiv b \pmod n \}$; $[a] = [b] \iff a \equiv b \pmod n$

$$\mathbb{Z} = \bigcup_{a \in \mathbb{Z}} [a] = \bigcup_{r=0}^{n-1} [r]$$

- $a = qn + r \rightarrow [a] = [r]$, $a \equiv r$
- $[r_1] = [r_2]$, $0 \leq r_1, r_2 < n \Rightarrow r_1 = r_2$

т.е. $r_1 \neq r_2$ $[r_1] \cap [r_2] = \emptyset$

Опр. $\mathbb{Z}_n = \{ [a] \mid a \in \mathbb{Z} \} = \{ [r] \mid r = 0, 1, \ldots, n-1 \}$ $(|\mathbb{Z}_n| = n)$

$$[a] + [b] := [a+b]$$

$$[a] \cdot [b] := [ab]$$

Тв. $ka \equiv kb \pmod n \Rightarrow a \equiv b \pmod{\frac{n}{(k,n)}}$

Д-во $n \mid ka - kb = k(a-b) \Rightarrow \frac{n}{(k,n)} \mid a - b$

<u>Заб.</u> Операциите в $\mathbb{Z}_n$ са коректно дефинирани:

Ако $[a]=[a']$ и $[b]=[b']$, т.е. $a\equiv a'$, $b\equiv b'$, то

$a+b\equiv a'+b'$ и $ab\equiv a'b'$ $\Rightarrow$ $[a+b]=[a'+b']$ и $[ab]=[a'b']$

<u>Т6.</u> $(\mathbb{Z}_n, +, \cdot)$ комут. пр. с 1

<u>Д-во</u> 0) опер. са коректно деф.

1) $([a]+[b])+[c]=[a+b]+[c]=[(a+b)+c]$

$$\|$$

$[a]+([b]+[c])=[a]+[b+c]=[a+(b+c)]$

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

и т.н. ; $[0]$ – нулев ел.; $[1]$ – ед. ел.; $-[a]=[-a]$

Тв. 1) $\underset{(n\nmid a)}{[a]}$ е делител на $0 \Leftrightarrow (n,a) \neq 1$

$(\exists b : [a][b]=[ab]=0 \Rightarrow n \mid ab \ (n \nmid a, n \nmid b)$; $d \overset{\neq 1}{=} (n,a)$;

$[a]=[d][\frac{a}{d}]$; $[a][\underbrace{\tfrac{n}{d}}_{\neq n}] = [0]$ $)$

2) $[a]$ е обратим $\Leftrightarrow (n,a)=1$

$((\Rightarrow)$ $\exists [b] : [a][b]=1 \Rightarrow ab \equiv 1 \Rightarrow \exists k : ab = 1+kn$

$\Rightarrow (n,a) \mid 1 \Rightarrow (n,a)=1$

$(\Leftarrow)$ Безу: $\exists u,v : nu + av = 1 \Rightarrow av \equiv 1 \Rightarrow [a][v]=[1]$

$\Rightarrow [a]^{-1}=[v])$

Сл. $\forall a$ или $[a]$ е делител на 0, или $[a]$ е обратим