Елементи от Теория на числата

Нека в цялото въпрос ще разбираме под число = цяло число $\in \mathbb{Z}$.

Деф Нека $a, b \neq 0$, $a, b \in \mathbb{Z}$. Казваме че "b дели a" и означаваме $b \mid a$, $b \mid a$,

ако $\exists c \in \mathbb{Z}$: $a = bc$.

Свой. 1) $a \mid a$

2) $a \mid b$ и $b \mid a \Rightarrow |a| = |b|$

3) $a \mid b$ и $b \mid c \Rightarrow a \mid c$

4) $a \mid b_i, i = \overline{1,k} \Rightarrow a \mid c_1 b_1 + c_2 b_2 + \dots + c_k b_k$

5) $a \mid b+c \Rightarrow a \mid c$
$a \mid b$

Забел: $a \mid b+c=0$
$a \mid b$ $\Rightarrow a \mid c$ ∎

Th (деление с частно и остатък в $\mathbb{Z}$):

$\forall a, b \neq 0, a, b \in \mathbb{Z}$ $\exists!$ q (частно) и r (остатък),

$a = bq + r$, $0 \leq r < |b|$.

Деф. Нека $a, b \in \mathbb{Z}$ $b \neq 0$. Най-голям общ делител на a и b наричаме число d и означаваме $d = (a, b) = НОД(a, b)$) ако за d са изпълнени следните две свойства:

1) $d \mid a$ и $d \mid b$

2) $d_1 \mid a$ и $d_1 \mid b \Rightarrow d_1 \mid d$.

Th (алгоритъм на Евклид) $\forall a, b \neq 0$, $\exists!$ (с точност до знак $d = (a, b) > 0$) като

$d = (a, b) = ua + vb$, където $\exists u, v \in \mathbb{Z}$

$d = au + bv$ – представяне на Безу

$a = bq + r, \quad 0 \le r < |b|$

Ако $r = 0 \Rightarrow d = (a,b) = b$

Ако $r \neq 0$

$b = rq_1 + r_1, \quad 0 \le r_1 < r$

$r = r_1 q_2 + r_2, \quad 0 \le r_2 < r_1$

$r_{j-1} = r_j q_{j+1} + r_{j+1} \Rightarrow d \mid d$

$r_j = r_{j+1} q_{j+2} + r_{j+2}, \quad r_{j+2} = 0$

$\Rightarrow d$

Последният ненулев остатък $r_{j+1} = d = (a,b)$

$d = r_{j-1} - r_j q_{j+1} = \dots$

$= (u)a + (v)b$

Обратно на Безу

Деф.: a и b са взаимно прости цели числа, ако $(a,b) = 1$.

Забел.: $d = (a,b) \Rightarrow \exists u, v : au + bv = d$

$(a,b) = 1 \Leftrightarrow \exists! u, v : au + bv = 1$

Свва: 1) $a \mid bc \Rightarrow a \mid c$
(a,b) $(a,b)=1$

2) $(a,b)=1$ и $a \mid c$, $b \mid c \Rightarrow ab \mid c$

3) $(a,b)=1$, $(a,c)=1 \Rightarrow (a,bc)=1$

Деф: Нека $a,b \in \mathbb{Z}$, $a \neq 0, b \neq 0$ и казваме, че m е НОК(a,b) и означаваме $m=[a,b]$, ако m удовлетворява следните две условия:

1) $a \mid m$ и $b \mid m$

2) $a \mid m_1$ и $b \mid m_1 \Rightarrow m \mid m_1$

Th $a,b \in \mathbb{Z}$, $a \neq 0, b \neq 0 \Rightarrow$
$(a,b)[a,b]=ab$

$\square$

Нека $p \in \mathbb{N}$ $(\mathbb{Z})$ е

Казваме, че p е просто число, ако единствените делители на p са $\pm 1, \pm p$.

Забл: 1) 1 не е просто число.

2) p прост, $a \in \mathbb{Z}$: $p \nmid a \iff (p,a)=1$

"p не дели a"

Тв: Ако p е прост и $a,b \in \mathbb{Z}$ и $p \mid ab \Rightarrow p \mid a$ или $p \mid b$, т.е. p дели поне едно от a и b.

Тл (основна Тл на аритметиката): $\forall n \in \mathbb{N}$, $\exists!$ с точност до реда на множителите разлагане в произведение от прости делители.

а) $\forall a \in \mathbb{Z}$, $|a| > 1$ има поне един прост делител;

б) (Евклид) $\exists \infty$ много прости числа.

Дв-во: Да допуснем, че $\exists$ краен брой прости числа $p_1, \dots, p_k$ са всички. Образуваме

$N = p_1 \cdot \dots \cdot p_k + 1$ и ще покажем, че

N е следващото просто число, т.е. са ∞ много прости числа.

$N = p_1 \cdot \dots \cdot p_k + 1$

$p_i \mid N$ и $p_i \mid N \Rightarrow p_i \mid 1$

p_i дел. N $\quad$ p_i дел. N $\quad$ $p_i \mid 1$

$\Rightarrow \Leftarrow$

p, q – прости числа $\Rightarrow (p,q) = 1 \Rightarrow pq$

$\Rightarrow \Leftarrow$

осн. $\Rightarrow$ $n = p_1 p_2 \cdot \dots \cdot p_k \Rightarrow$

теор. аритм.

$\forall n \in \mathbb{N} \Rightarrow n = p_1^{k_1} p_2^{k_2} \sim p_s^{k_s}$,

2 е единственото четно просто число

p – просто число $p \geq 3$ е нечетно

Където $p_1, \sim p_s$ са $\neq$ прости делители на т. n и $(p_i, p_j) = 1$, $i \neq j$.

$n = p_1^{k_1} p_2^{k_2} \sim p_s^{k_s}$ – каноничното разлагане на всяко т. n

$k_i > 0$

$a = p_1^{k_1} p_2^{k_2} \sim p_s^{k_s}$, $k_i \geq 0$

$b = p_1^{l_1} p_2^{l_2} \sim p_s^{l_s}$, $l_i \geq 0$

$(a,b) = p_1^{d_1} p_2^{d_2} \sim p_s^{d_s}$, $d_i = \max(k_i, l_i)$

$[a,b] = p_1^{m_1} p_2^{m_2} \sim p_s^{m_s}$, $m_i = \max(k_i, l_i)$