1. Делимост в пръстена числа. Най-голям общ делител, съществуване на Безу. Прости числа и основна теорема на аритметиката

Операции: $a+b=b+a$

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

$ab=ba$

$(ab)c=a(bc)$ наредба: $a>b$ и $a=b$ и $a<b$

Th за делене с частно и остатък:

Ако $a,b\in\mathbb{N}$ и $b\neq 0 \Rightarrow \exists!\, q,r\in\mathbb{Z}$: $a=qb+r$, където $0\leq r<|b|$ q - частно, r - остатък.

Док-во:

Нека мн-во $M=\{a-b\cdot s \mid s\in\mathbb{Z}\}$ (в M има и >0 и <0 числа. Интересуваме се от >0)

I) $\exists$ (съществуване) $M^+=\{x\in M \mid x\geq 0\}$

Нека $r=\min M^+ \Rightarrow r-|b|\leq 0 \Rightarrow r<|b|$

$0\leq r<|b|$, $a-b\cdot s_1=r \Rightarrow a=b\cdot s_1+r$

II) ! (единственост) $\left.\begin{aligned} a&=b\cdot q_1+r_1\\ a&=b\cdot q_2+r_2\end{aligned}\right\} \Rightarrow b(q_1-q_2)=\underbrace{r_2-r_1}_{0\leq r_i<|b|}$

$0\leq |r_2-r_1|<b$

$\Rightarrow$ ако $q_1-q_2\neq 0 \Rightarrow |b(q_1-q_2)|\geq |b|$

от където следва, че $|r_1-r_2|<|b| \Rightarrow q_1-q_2=0 \Rightarrow q_1=q_2$, $r_1=r_2$

Следствие 1: (представяне на числата в q-ична бр. система)

$b>1$, $b\in\mathbb{N}$ и $a>0$, $a\in\mathbb{N} \Rightarrow \exists!\ q_0,q_1,\dots q_k$:

$a=q_0b^0+q_1\cdot b^1+\dots+q_cb^c$ и $q_c\neq 0$ $\quad 0\leq q_i<b$

Док-во: $a=q_0+b\cdot a_1$ - i

$a_1=q_1+b\cdot a_2$ - i $\quad 0\leq q_i<b$

$\vdots$

$a\dots a_0<b$ $\rightarrow$ продължаваме докато a със нарастващ индекс стане $<b$

Опред: Казваме, че b дели a, $(b\mid a)$ когато $a=b\cdot q$ $b\neq 0$

св-ва на делимостта:

1) $\pm 1\mid a$, $\forall a$

2) $a\mid \pm a$, $\forall a\neq 0$

3) $a\mid 0$, $\forall a\neq 0$

4) ако $a\mid b$ и $b\mid c \Rightarrow a\mid c$

5) $a\mid b \Rightarrow a\mid b\cdot u$

6) $a\mid b_1$ и $a\mid b_2 \Rightarrow a\mid(b_1u_1+b_2u_2)$

7) $a\mid b$ и $b\neq 0 \Rightarrow |a|\leq|b|$

Деф 1: НОД $(a,b) = (a,b)$ d - max: $d \mid a$ и $d \mid b$

Деф 2: $d = (a,b)$

1) $d \mid a$, $d \mid b$

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

Тоя 2-та деф. се получава като d_1 така и $= d$ (за 2 и 6 и ее други 2и-2)

1 - удача с обратима и що само не е друг ост. число ($1^{-1} = 1$, $-1^{-1} = -1$)

(Тъждество на Безу)

Тв: Ако $a, b \in \mathbb{Z}$ поне едното е различно от 0, то $\exists (a,b) = d$ и $\exists x, y \in \mathbb{Z}$: $d = xa + yb$

Док-во: Нека $M = \{ as + bt \mid s, t \in \mathbb{Z} \}$ тъй, като в M имаме както > 0, така и < 0 числа $M^+ = \{ x \in M \mid x > 0 \}$

Взимаме $d = \min$ число в $M^+ \Rightarrow$ 1) $d > 0$ 2) $d = ax + by$

Нека $x \in M$ По ТИ: $x = dq + r \Rightarrow \exists! q, r$, $0 \le r \le d$

$x = as_1 + bt_1 = (ax + by)q + r \Rightarrow$

$\Rightarrow r = (s_1 - xq) \cdot a + (t_1 - yq) b \Rightarrow r \in M$

но $r < d$, а $d = \min M^+$ и $0 \le r \Rightarrow r = 0$

Тогава $x = d \cdot q = d \mid x$, $\forall x \in M \Rightarrow d \mid a$ и $d \mid b$

Ако $d_1 \mid a$ и $d_1 \mid b \Rightarrow d_1 \mid \underbrace{xa + yb}_{d} \Rightarrow d_1 \mid d$

1) $d \mid a$, $d \mid b$

2) ако $d_1 \mid a$ и $d_1 \mid b \Rightarrow d_1 \mid d \Rightarrow d = НОД(a,b)$

Опр: a, b - взаимно прости когато $(a,b) = 1$

Св-ва: (следствия от ТИ за Безу)

1) ако $a \mid b_1 b_2$ и $(a, b_1) = 1 \Rightarrow a \mid b_2$

2) ако $a_1 \mid b$ и $a_2 \mid b$ и $(a_1, a_2) = 1 \Rightarrow a_1 \cdot a_2 \mid b$

Д-во: 1) $a \mid b_1 b_2$ и $(a, b_1) = 1$

$\Rightarrow 1 = ax + b_1 y / b_2 \Rightarrow b_2 = \underbrace{ab_2 \cdot x}_{a \mid} + \underbrace{b_1 b_2 \cdot y}_{a \mid} \Rightarrow a \mid b_2$

Д-во: 2) $a_1 \mid b \Rightarrow b = a_1 \cdot s$ но $a_2 \mid b$ т.е. $a_2 \mid a_1 \cdot s$

Т.к. a_1 и a_2 са взаимно прости $(a_1, a_2) = 1 \Rightarrow a_2 \mid s \Rightarrow s = a_2 \cdot t \Rightarrow$

$\Rightarrow b = a_1 a_2 t \Rightarrow a_1 a_2 \mid b$

Опр. Числото $p \in \mathbb{Z}$ е просто, ако p се дели само на ± 1 и $\pm p$

(Т6) Простите числа са безкраен брой.

Д-во: Допускаме, че са краен брой $p_1, \dots p_n$.

$\Rightarrow A = p_1 \dots p_n + 1$ не се дели на нито едно просто число $\Rightarrow$ (ч)

Търсим прости числа чрез решетото на Ератосен.

p - просто, $a \in \mathbb{Z}$

$$(a, p) = \begin{cases} 1, & p \nmid a \\ p, & p \mid a \end{cases}$$

Основна Т на аритметиката:

Всяко естествено число > 1 може да се представи като произведение на прости числа (множители) като това представяне е единствено с точност до реда на множителите.

Д-во:

I) $\exists$ индукция по a

1) $a = 2$, a е просто

2) Нека е вярно за всяко число $< a$

1сл. a - просто $\Rightarrow a = p$

2сл. a - съставно $\Rightarrow \exists p$ - просто : $a = pq$

($\exists b, c, t : a = b \cdot c$ и $b < a$, $c < a$)

прилагаме за b и c $\quad b = p_1 \dots p_r \quad c = q_1 \dots q_s$

p_i, q_j - прости $\Rightarrow a = p_1 \dots p_r q_1 \dots q_s$

II)! Допускаме, че:

$a = p_1 \dots p_k, \quad p_i, q_j$ - прости множители

$a = q_1 \dots q_t$

$p_1 \dots p_k = q_1 \dots q_t \Rightarrow q_t \mid q_1 \dots q_t \Rightarrow q_t \mid p_1 \dots p_k$

но от спомагателно 1! q_t - просто $\Rightarrow q_t$ трябва да дели някое p_i,

но $\forall p_i$ е просто $\Rightarrow \exists$ номер i : $p_i = q_t$. С преномериране на $p_1 \dots p_k$ може да считаме, че $p_k = q_t$. Това означава

$(p_1 \dots p_{k-1}) \underbrace{p_k}_{q_t} = (q_1 \dots q_{t-1}) q_t \Rightarrow p_1 \dots p_{k-1} = q_1 \dots q_{t-1}$

Ако $k > t$, то $p_1 \dots p_{k-t} = 1$ (ч) $\Rightarrow k = t$. Тогава след преномериране на ерната страна, най-сетне ще получим, че $p_i = q_i$, $i = 1 \dots t$.