Теория на числата

$\mathbb{Z} \supset \mathbb{N}$ - дефинират се на принципа на индукцията (0 обикновено не се брои)

В $\mathbb{N}$ $a+b$ и $a.b$ са дефинирани за всяко естествено число и дават естествено число. В $\mathbb{N}$ не са дефинирани - и :.

Свойства на + и . : $(a+b)+c = a+(b+c)$

$(ab).c = a(bc)$

$a+b = b+a$

$ab = ba$

Естествените числа са наредими, т.е. $a,b \in \mathbb{N} \Rightarrow a>b, a=b$ или $a<b$

Т Теорема на Безу за деление с частно и остатък

$a,b \in \mathbb{Z}, b \neq 0 \Rightarrow \exists$ единствени $q,r \in \mathbb{Z}$: $a = bq+r$, където q наричаме частно, а r - остатък, $0 \leq r < |b|$.

Доказателство:

множество: $M = \{a-bs \mid s \in \mathbb{Z}\} \to M^+ = \{x \in M \mid x \geq 0\}$

r - най-малкото число в M^+; $r-|b|<0 \Rightarrow \underbrace{0 \leq r}_{r \in M^+} < b$.

$a-bs_1 = r \Rightarrow a = bs_1 + r \Rightarrow$ доказахме съществуването.

Доказателство на единствеността.

Нека имаме 2 числа:

$$\left.\begin{array}{l} a = bq_1 + r_1 \\ a = bq_2 + r_2 \end{array}\right\} |b| > r_i \geq 0$$

$$\Rightarrow b(q_1 - q_2) = r_1 - r_2$$

$0 \leq |r_2 - r_1| < b$. Ако $q_2 - q_1 \neq 0 \Rightarrow |b(q_2 - q_1)| \geq |b|$

$\Rightarrow$ т.к. $|r_2 - r_1| < b$ $\lightning \Rightarrow q_2 - q_1 = 0 \Rightarrow r_2 - r_1 = 0 \Rightarrow q_1 = q_2$ и $r_1 = r_2$

Сл 1 Нека $b>1, b \in \mathbb{Z}$, a - произволно, положително, цяло $\Rightarrow$

$\Rightarrow \exists\, q_0, q_1 \ldots q_n : a = q_0 + q_1 b + \ldots + q_e b^e$, $|b| > q_i \geq 0$; $q_e \neq 0$

Ист. $a = q_0 + ba_1$

IIст. $a_1 = q_1 + ba_2, 0 \leq q_i < 0$

$\vdots$

Докато $a_k < b$

Сл.2 | Опр.: Казване, че $b|a$, когато $a=b.q$.

Свойства на делимостта:

1.) $\pm 1 | a, \forall a$

2.) $a | \pm a, \forall a \neq 0$

3.) $a|0, \forall a \neq 0$

4.) $a|b$ и $b|c \Rightarrow a|c \ \forall a,b,c; a,b \neq 0$

5.) $a|b \Rightarrow a|b.q$

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

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

Опр: НОД (най-голям общ делител) $(a,b)=d$:

опр1) $d|a, d|b, d$ е максималното такова число.

опр2) 1. $d|a$ и $d|b$

2. Ако $d_1|a$ и $d_1|b \Rightarrow d_1|d$

Получава се не само d, но и $-d$.

→ По-удобна за употреба при полиномите.

→ ± 1 са единствените обратими елементи в $\mathbb{Z}$.

Т | $a,b \in \mathbb{Z}$; $a \neq 0$ или $b \neq 0 \Rightarrow \exists (a,b)=d$ и $d=ua+vb; u,v \in \mathbb{Z}$

Тъждество на Безу

Доказателство:

$M=\{as+bt \mid s,t \in \mathbb{Z}\} \rightarrow M^+=\{x \in M \mid x \geq 0\} \rightarrow d$ е мин. число в $M^+ \Rightarrow$

$\Rightarrow d>0; d=au+vb$

$x \in M$

$x=dq+r \Rightarrow \exists! q,r: x=dq+r, 0 \leq r < d$

$x \in M \Rightarrow x=as_1+bt_1=(au+bv)q+r \Rightarrow r=(s_1-uq)a+(t_1-vq)b$

$\Rightarrow r \in M$

$0 \leq r < d, d=\min M^+ \Rightarrow r=0 \Rightarrow x=dq \Rightarrow d|x, \forall x \in M \Rightarrow d|a$ и $d|b$.

Ако $d_1|a$ и $d_1|b \Rightarrow d_1|\underbrace{ua+vb}_{d} \Rightarrow d_1|d$

Опр | $(a,b)=1 \Rightarrow a$ и b са взаимно прости числа

Свойства на взаимно простите числа

1) $a|b_1b_2$ и $(a,b_1)=1 \Rightarrow a|b_2$

2) $a_1|b$ и $a_2|b$, и $(a_1,a_2)=1 \Rightarrow a_1a_2|b$

$a|b_1b_2$ и $(a,b_1)=1 \Rightarrow 1=au+b_1v \Rightarrow b_2=ab_2u+b_1b_2v$

$a_1|b \Rightarrow b=a_1s$

$a_2|b \Rightarrow a_2|a_1s \Rightarrow a_2|s \Rightarrow s=a_2.t \Rightarrow b=a_1a_2t \Rightarrow a_1a_2|b$

Прости числа:

в $\mathbb{N}$ $\forall a$: само 1 и $a \mid a$

в $\mathbb{Z}$ $\forall a$: само ± 1 и $\pm a \mid a$

Тв Простите числа са безкраен брой.

Доказателство:

Допускаме, че са краен. $p_1 \dots p_n \Rightarrow A = p_1 \dots p_n + 1$ не се дели на нито едно от тези прости числа.

Решето на Ератостен алгоритъм за намиране на прости числа

~~1~~ ② 3 ~~4~~ 5 ~~6~~ 7 ...

~~1~~ ② ③ ~~4~~ 5 ~~6~~ 7 ...

~~1~~ ② ③ ~~4~~ ⑤ ~~6~~ 7 ...

p - просто, $a \in \mathbb{Z} \Rightarrow (a, p) = \begin{cases} 1 \\ p \end{cases}$

Т Основна теорема на аритметиката

Всяко $\mathbb{N}$ число a по един начин може да се представи като произведение на прости множители (с точност до реда на множителите).

Доказателство:

1) Съществуване - индукция по a

1. $a = 2$ - просто $\Rightarrow$ има само един множител
2. Нека твърдението е в сила за всички числа, по-малки от a:
   1) a - просто $\Rightarrow$ има само един множител
   2) a - съставно $\Rightarrow \exists b, c$ - числа : $b < a, c < a, a = b.c$

   Прилагаме твърдението за b и c:

   $b = p_1 \dots p_r$, p_i - просто

   $c = q_1 \dots q_s$, q_j - просто

   $\Rightarrow a = p_1 \dots p_r q_1 \dots q_s$ - прости множители

2) Единственост

Допускаме: $a = p_1 \dots p_l$; $a = q_1 \dots q_t \Rightarrow p_i, q_j$ - прости

$\Rightarrow p_1 \dots p_l = q_1 \dots q_t$

$q_t \mid q_1 \dots q_t \Rightarrow q_t \mid p_1 \dots p_l$

q_t - просто

Ако $q_t \neq p_i$, $i = \overline{1,l} \Rightarrow$ ↯ $\Rightarrow q_t$ трябва да дели някое $p_i \Rightarrow$

$\Rightarrow q_t = p_i$ за някое i. $\Rightarrow$ С преномериране $p_1 \dots p_l$ може да считаме, че $p_l = q_t \Rightarrow (p_1 \dots p_{l-1}) p_l = (q_1 \dots q_{t-1}) q_t \Rightarrow p_1 \dots p_{l-1} = q_1 \dots q_{t-1}$

Ако $l > t$, ще останат $p_1 \dots p_{l-t} = 1$ ↯ $\Rightarrow l = t \Rightarrow$ След преномериране получаваме $p_i = q_i$