Сабирање природних бројева : $a+b$ $\qquad +: \mathbb{N}^2 \to \mathbb{N}$, $(a,b) \mapsto a+b$

- $a + 0 := a$
- $a + S(b) := S(a+b)$

Особине: (1) $(a+b)+c = a+(b+c)$

доказ: $P(c)$: $(a+b)+c = a+(b+c)$; $a, b \in \mathbb{N}$ фикс.

циљ: $(\forall c \in \mathbb{N})\ P(c)$; инд. по c

$P(0)$: $$\underbrace{(a+b)+0}_{=\, a+b} = a + \underbrace{(b+0)}_{:=\, b} = a+b \quad ✓$$

$P(c) \to P(S(c))$: (ИХ) $P(c)$: $(a+b)+c = a+(b+c)$

циљ: $P(S(c))$: $(a+b)+S(c) = a+(b+S(c))$

$$\begin{aligned}(a+b)+S(c) &:= S((a+b)+c)\\ &= S(a+(b+c)) \quad \text{по ИХ } P(c)\\ &=: a+S(b+c)\\ &=: a+(b+S(c)) \quad \blacksquare\end{aligned}$$

(2) $0+a = a$

(3) $1+a = S(a) = a+1$ $\quad$ сабирање са 1

(4) $a+b = b+a$

(5) $a+b=0 \leftrightarrow a=0 \wedge b=0$

(6) $a+c = b+c \leftrightarrow a=b$

Задатак: доказати (2)–(6).

Напомена: • Ако $a \geq b$, онда $(\exists_1 c)\ a = b+c$ и јединствено c тд је $a=b+c$ означавамо са $c =: a-b$ и зове се разлика a и b.

• Ако $a<b$, онда $\neg(\exists c)\ a=b+c$, па $a-b$ није дефинисано (у $\mathbb{N}$).

Множење природних бројева: $a \cdot b$ $\qquad \cdot : \mathbb{N}^2 \to \mathbb{N}$, $(a,b) \mapsto a \cdot b$

- $a \cdot 0 := 0$
- $a \cdot S(b) := ab + a$

Особине: (1) $(xy)z = x(yz)$

(2) $0 \cdot a = 0$

(3) $1 \cdot x = x = x \cdot 1$

(4) $xy = yx$

(5) $x(y+z) = xy + xz$

(6) $(x+y)z = xz + yz$

(7) $xy = 0 \iff x = 0 \lor y = 0$

(8) $xy = 1 \iff x = 1 \land y = 1$

Степеновање природних бројева: a^b $\qquad \wedge : \mathbb{N}^2 \to \mathbb{N}$, $(a,b) \mapsto a^b$

$a^0 := 1$ (спец; $0^0 := 1$)

$a^{S(b)} := a^b \cdot a$

Особине: (1) $a^{bc} = (a^b)^c$

(2) $a^{b+c} = a^b \cdot a^c$

(3) $0^b = 0$ за $b > 0$ и $0^0 := 1$

(4) $1^b = 1$; $a^1 = a$.

ДЕЉИВОСТ

Дефиниција: $a \mid b :\equiv (\exists k)\ b = a \cdot k$

Сетимо се: $\mid$ је поредак на $\mathbb{N}$, 1 је минимум, 0 је максимум

Особине: (1) $a \mid b \land a \mid c \to a \mid b+c$

доказ: $b = a \cdot k$, $c = a \cdot l$

$b + c = a \cdot k + a \cdot l = a(k+l)$, па $a \mid b+c$ ∎

(2) $a \mid b \vee a \mid c \rightarrow a \mid b \cdot c$

(3) $a \mid b \rightarrow a \mid b^n$ за све $n>0$

<u>Тврђење (дијељење са остатком)</u>: Нека $a, b \in \mathbb{N}$, $b \neq 0$. Тада $(\exists_1 q, r \in \mathbb{N})(a = bq + r \wedge 0 \leq r < b)$.

<u>доказ:</u> уочимо $S = \{x \in \mathbb{N} \mid (\exists q)\ x = a - bq\} \subseteq \mathbb{N}$

- <u>$S \neq \emptyset$</u>: $a \in S$ јер $a = a - b \cdot 0$

По принципу минимума, S има минимум r. Како $r \in S$, имамо и q тд $r = a - bq$, тј. $\boxed{a = bq + r}$

- <u>$0 \leq r < b$</u>: (ртс) $r \geq b$, тада узмимо $r_1 := r - b < r$, $r = r_1 + b$

$a = bq + r = bq + b + r_1 = b(q+1) + r_1$, тј.

$r_1 = a - b(q+1)$, па $r_1 \in S$, па $r_1 \geq r$ јер је r минимум од S ↯

- <u>јединственост q и r</u>: $a = bq' + r' \wedge 0 \leq r' < b$

тада $r' = a - b \cdot q'$, па $r' \in S$, па $r' \geq r$ јер је r минимум скупа S

$0 \leq r' - r < b - r \leq b$

$(a - b \cdot q') - (a - bq) = b(q - q')$

тј. $0 \leq b(q - q') < b$, па $b(q - q') = 0$

па $q - q' = 0$ јер $b \neq 0$, тј. $\boxed{q = q'}$

$r' - r = b(q - q') = 0$, па $\boxed{r' = r}$ ■

<u>напомена:</u> • $\mid$ дефинише се и на $\mathbb{Z}$

$a \mid b :\equiv (\exists k \in \mathbb{Z})\ b = ak$

$\mid$ није поредак на $\mathbb{Z}$ ($5 \mid -5$, $-5 \mid 5$, али $5 \neq -5$)

- за $a, b \in \mathbb{Z}$, $b \neq 0$, $(\exists_1 q, r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)$

доказ: 1° $a, b \in \mathbb{N}$, применимо претх. теорему

2° $a \in \mathbb{N}$, $b \notin \mathbb{N}$, -//- на $a' := a$ и $b' := -b$

3° $a \notin \mathbb{N}$, $b \in \mathbb{N}$, -//- на $a' := -a$ и $b' := b$

4° $a, b \notin \mathbb{N}$, -//- на $a' := -a$ и $b' := -b$. ... $\boxed{\checkmark}$

дефиниција (НЗД и НЗС): Нека $a, b \in \mathbb{N}$.

(1) $D(a,b) = \{d \mid d|a \wedge d|b\}$ - скуп заједничких делилаца од a и b

$НЗД(a,b) := \max(D(a,b))$ (видећемо да постоји)

Другим речима, $d = НЗД(a,b)$ ако:

$d|a \wedge d|b \wedge (\forall e)[e|a \wedge e|b \rightarrow e|d]$

Још једнана ознака је $(a,b) := НЗД(a,b)$.

(2) $S(a,b) = \{s \mid a|s \wedge b|s\}$ - скуп заједничких садржалаца од a и b

$НЗС(a,b) := \min(S(a,b))$ (видећемо да постоји)

Другим речима, $s = НЗС(a,b)$ ако:

$a|s \wedge b|s \wedge (\forall t)[a|t \wedge b|t \rightarrow s|t]$

Још једна ознака је $[a,b] := НЗС(a,b)$.

запажање: Ако $a|b$, онда $(a,b) = a$.

доказ: Ако $a|b$, тада $a \in D(a,b)$.

Нека $d \in D(a,b)$; онд. $d|a$, па $a = \max(D(a,b))$ $\boxed{\checkmark}$

лема: (1) Ако $a = bq + r$, онда $D(a,b) = D(b,r)$.

(2) Ако $a = bq + r$, онда $(a,b) = (b,r)$ (ако макс. постоји)

доказ: (2) следи из (1)

(1) $\boxed{\subseteq}$ Нека $d|a$, $d|b$, тада $d \mid a - b \cdot q = r$

$\boxed{\supseteq}$ Нека $d|b$, $d|r$, тада $d \mid bq + r = a$ $\boxed{\checkmark}$

Еуклидов алгоритам: Нека $a, b \in \mathbb{N}$, $b \neq 0$.

$$
\begin{array}{llll}
(1) & a = b \cdot q_1 + r_1 & & 0 < r_1 < b \\
(2) & b = r_1 \cdot q_2 + r_2 & & 0 < r_2 < r_1 \\
(3) & r_1 = r_2 \cdot q_3 + r_3 & & 0 < r_3 < r_2 \\
(4) & r_2 = r_3 \, q_4 + r_4 & & 0 < r_4 < r_3 \\
 & \dots & & \\
(n-2) & r_{n-4} = r_{n-3} \, q_{n-2} + r_{n-2} & & 0 < r_{n-2} < r_{n-3} \\
(n-1) & r_{n-3} = r_{n-2} \, q_{n-1} + r_{n-1} & & 0 < r_{n-1} < r_{n-2} \\
(n) & r_{n-2} = r_{n-1} \, q_n & &
\end{array}
$$

Како $b > r_1 > r_2 > r_3 > \dots$ овај алгоритам се завршава у највише b корака. ($n \leq b$).

Теорема: Нека $a, b \in \mathbb{N}$, $b \neq 0$. Последњи ненула остатак (r_{n-1}) је НЗД(a,b).

Доказ:

$$
\begin{array}{rll}
r_{n-1} & = (r_{n-1}, r_{n-2}) & \text{због } (n) \text{ и задатака} \\
 & = (r_{n-2}, r_{n-3}) & \text{због } (n-1) \text{ и леме} \\
 & = (r_{n-3}, r_{n-4}) & \text{због } (n-2) \text{ и леме} \\
 & = \dots & \\
 & = (r_3, r_2) & \\
 & = (r_2, r_1) & \text{због } (3) \text{ и леме} \\
 & = (r_1, b) & \text{због } (2) \text{ и леме} \\
 & = (b, a) & \text{због } (1) \text{ и леме} \ \blacksquare
\end{array}
$$

Коментар: Претходни доказ специјално каже да НЗД(a,b) постоји.

Теорема: Ако је $d = (a,b)$, онда постоје $p, q \in \mathbb{Z}$ тд $d = a \cdot p + b \cdot q$.

доказ: Читамо Еуклидов алгоритам уназад:

$$(a,b) = r_{n-1} \overset{(n-1)}{=} r_{n-3} - r_{n-2} q_{n-1}$$
$$\overset{(n-2)}{=} r_{n-3} - (r_{n-4} - r_{n-3} q_{n-2}) \cdot q_{n-1}$$
$$= -r_{n-4} \cdot q_{n-1} + (1 + q_{n-2} q_{n-1}) \cdot r_{n-3}$$
$$\overset{(n-3)}{=} \dots$$
$$= r_{n-5} \cdot \dots + r_{n-4} \cdot \dots$$
$$= \dots$$
$$= r_2 \cdot \dots + r_3 \cdot \dots$$
$$\overset{(3)}{=} r_1 \cdot \dots + r_2 \cdot \dots$$
$$\overset{(2)}{=} b \cdot \dots + r_1 \cdot \dots$$
$$\overset{(1)}{=} a \cdot \underbrace{\dots}_{p} + b \cdot \underbrace{\dots}_{q}$$
◻

Дефиниција: Елементи a и b су узајамно прости ако $(a,b) = 1$.

Тврђење: $a \mid bc \wedge (a,b) = 1 \rightarrow a \mid c$

доказ: из $(a,b)=1$, можемо да запишемо

$$1 = ap + bq \quad \mid \cdot c$$
$$c = \underbrace{acp}_{a \mid} + \underbrace{bcq}_{a \mid \text{ јер } a \mid bc}$$
, па $a \mid c$. ◻

Тврђење: Ако $(a,b) = d$, $a = d \cdot a'$, $b = d \cdot b'$, тада $(a', b') = 1$ (ако бар један од a и $b \neq 0$).

доказ:
$$d = ap + bq \quad \mid : d$$
$$1 = a'p + b'q$$
Нека је $d' = (a', b')$; тада $d' \mid a'p + b'q = 1$ па је $d' = 1$. ◻

Тврђење: Нека $a, b \in \mathbb{N}$, $b \neq 0$. Тада $(\exists_1 s \in \mathbb{N})$ $ab = (a,b) \cdot s$ и то $s = [a,b]$.

<u>Запажање</u>: Следствено, $a \cdot b = (a,b) \cdot [a,b]$.

<u>доказ</u>: Нека $d = (a,b) > 0$ јер $b \neq 0$; $b = b' \cdot d$.

$$ab = a \cdot b' \cdot d = d \cdot \underbrace{(a \cdot b')}_{s}$$

Дакле, $(\exists s \in \mathbb{N})\ ab = ds$.

По теореми о дељивости са остатком имамо

$$\left.\begin{aligned} &(\exists!\, q, r)\,(ab = dq + r \ \wedge \ 0 \le r < d) \\ &ab = ds + 0 \end{aligned}\right\} s \text{ јединствено}$$

<u>$s = [a,b]$</u>: 1° <u>$a, b \mid s$</u>: запишимо $a = a'd$, $b = b'd$

$\cancel{d} s = ab = \cancel{d} a' b \rightarrow s = a'b$, па $b \mid s$

$\cancel{d} s = ab = a \cancel{d} b' \rightarrow \boxed{s = ab'}$ па $a \mid s$.

2° <u>$a, b \mid t \rightarrow s \mid t$</u>: Нека $a \mid t$ и <u>$b \mid t$</u>

запишимо $t = a \cdot x$

како $b \mid t$, то $b \mid a \cdot x$, па $a \cdot x = b \cdot k$

$\cancel{d} a' x = \cancel{d} b' k$

Дакле, $b' \mid a'x$, али $(a', b') = 1$, то $b' \mid x$.

$t = a \cdot x = \underbrace{a \cdot b'}_{s} \cdot l$, па $s \mid t$. ∎

<u>ДИОФАНТОВЕ ј-не</u>

Диофантова ј-на је алгебарска ј-на са целобројним коефицијентима која се решава у $\mathbb{Z}$.

<u>пример</u>: $2x + 3y = 5$; $x^2 + 1 = 0$; $x^2 + y^2 = z^2$

$x^3 + y^3 = z^3$; $x^4 + y^4 = z^4$.

<u>лин. ј-на са једном непознатом</u>:

$ax = b$, $a, b \in \mathbb{Z}$, $a \neq 0$

$ax = b$ има реш. у $\mathbb{Z}$ акко $a \mid b$ (и решење је $x = \frac{b}{a}$)

Лин. ј-на са две непознате:

$$ax+by=c, \qquad a,b,c\in\mathbb{Z}, \quad a,b\neq 0$$

Теорема: (1) $ax+by=c$ има решење акко $(a,b) \mid c$.

(2) Ако је (x_0,y_0) једно решење, тада су сва решења ј-не $ax+by=c$ дата са:

$$x = x_0 + \frac{b}{(a,b)}\,t$$
$$y = y_0 - \frac{a}{(a,b)}\,t \quad , \quad t\in\mathbb{Z}.$$

Доказ: Нека је $d=(a,b)$, $a=da'$, $b=db'$, $(a',b')=1$

(1) $\boxed{\Rightarrow}$ Ако $ax+by=c$ има решење, онда

$$d \mid ax+by = c$$

$\boxed{\Leftarrow}$ Нека $d \mid c$ и запишимо $1 = a'p+b'q \mid c$

$$c = a'cp + b'cq \quad , \text{ али } \quad c = c'd$$
$$= \underbrace{a'd}\,c'p + \underbrace{b'd}\,c'q$$
$$= a\,\underbrace{c'p}_{x} + b\,\underbrace{c'q}_{y} \quad , \text{ па } (x,y) = (c'p, c'q)$$

је решење.

(2) Нека је (x_0,y_0) једно решење

тј. $ax_0+by_0=c$.

Ако
$$x = x_0 + \frac{b}{(a,b)}\,t$$
$$y = y_0 - \frac{a}{(a,b)}\,t$$
за $t\in\mathbb{Z}$, онда

(x,y) јесте решење:

$$ax+by = ax_0 + \cancel{\frac{ab}{(a,b)}t} + by_0 - \cancel{\frac{ab}{(a,b)}t} =$$
$$= ax_0+by_0 = c.$$

Сва решења су претходног облика:

$$ax_0+by_0=c \qquad |:d$$
$$ax+by=c \qquad |:d$$

$$(*)\quad a'x_0 + b'y_0 = c' \quad -$$
$$(\#)\quad a'x + b'y = c'$$

$$a'(x-x_0) + b'(y-y_0) = 0$$

па $a' \mid b'(y-y_0)$ и $b' \mid a'(x-x_0)$

како $(a',b')=1$ то $a' \mid y-y_0$ и $b' \mid x-x_0$

тј. $x-x_0 = b'\cdot t$; $\quad x = x_0 + b't$

$y-y_0 = a'\cdot s$; $\quad y = y_0 + a's$

У (#): $\cancel{c'} = a'x + b'y = a'x_0 + a'b't + b'y_0 + b'a's \overset{(*)}{=} \cancel{c'} + a'b'(t+s)$

па $a'b'(t+s)=0$ тј. $s=-t$.

Дакле, $x = x_0 + b't = x_0 + \frac{b}{(a,b)}t$

$y = y_0 - a't = y_0 + \frac{a}{(a,b)}t$. ∇

Пример: Решити $2x+3y=5$.

$(2,3)=1 \mid 5$, па $2x+3y=5$ има решења

$1 = 2\cdot p + 3\cdot q$

$2 = 3\cdot 0 + \boxed{2}$

$3 = \boxed{2}\cdot 1 + 1$

$2 = 1\cdot 2 + 0$

$1 = 3 - 2\cdot 1$

$= 2\cdot(-1) + 3\cdot 1$

$p=-1 \quad q=1$

$2\cdot(-1) + 3\cdot 1 = 1 \quad \mid \cdot 5$

$2\cdot(-5) + 3\cdot 5 = 5$ $\quad (-5,5)$ је једно решење

Сва решења су облика: $x = -5 + 3t$

$y = 5 - 2t \quad t\in\mathbb{Z}$

Решење $(10,-5)$ добија се за $t=5$.