PRIRODNI I CELI BROJEVI

Prvo matematičko znanje koje stičemo je znanje o prirodnim brojevima. U toku školovanja, u osnovnoj i srednjoj školi, stečeno znanje ne podvrgavamo kritici. Radimo sa nekim konkretnim prirodnim brojevima, ispitujemo svojstva koja imaju i pripisujemo ih svim prirodnim brojevima. Uvereni smo da možemo sabrati i pomnožiti bilo koja dva prirodna broja, da za sabiranje i množenje važe komutativni i asocijativni zakon i slično. Nedostatak koji imaju prirodni brojevi, da jednačina $a + x = b$ nije rešiva u ovom skupu za $b \leq a$, otklanjamo uvođenjem skupa celih brojeva. Slično, kao u slučaju prirodnih brojeva, prihvatamo da postoji zbir i proizvod svaka dva cela broja, a sabiranje i množenje celih brojeva učimo preko pravila.

Ovim predavanjem će biti dat prikaz aksiomatske postavke skupa prirodnih brojeva i konstrukcije celih brojeva, koji će fiksirati našu intuiciju o brojevima i omogućiti rešavanje zadataka poput ovog i njemu sličnih:

Dokazati:

(**1**) $\mathbf{2+2=4}$, $\mathbf{3+5=5+3}$, $\mathbf{3+(-7)=-4}$, $\mathbf{(-2)\cdot(-5)=10}$, $\mathbf{(-2)\cdot 5=-10}$.

(**2**) **Za svaka dva cela broja** x **i** y **važi** $x+y=y+x$**.**

(**3**) **Za svaki ceo broj** x **važi** $x^2 \geq 0$**.**

Za razliku od (elementarne) geometrije, koja je aksiomatski zasnovana još u drevnoj Grčkoj (Euklid i drugi), aksiomatske postavke raznih vrsta brojeva su stare stotinak godina. Intuicija prirodnog broja bila je dovoljno čvrsta osnova aritmetike. Aksiomatizacijom aritmetike nije poljuljana sigurnost intuitivnog shvatanja broja. Zadatak aksiomatizacije aritmetike je njeno logičko oblikovanje: izdvajanje osnovnih aritmetičkih pojmova (određivanjem njihovih osnovnih svojstava) dovoljnih za izgradnju deduktivnog sistema aritmetike. Aksiomatizacija je izvršena u toku druge polovine 19. veka, a poznata je kao Peanova[1] aksiomatika. Dva su izvora Peanove aksiomatike. On sam kaže da je aksiome preuzeo od Dedekinda, i da se izgrađujući deduktivni aritmetički sistem temeljen na tim aksiomama obilato služio Grassmannovim radom. Peano ih je formulisao u svom radu "*O pojmu broja*", publikovanom 1891. godine.

1. Prirodni brojevi

Svi se pisci razmatranja o brojevima slažu da su prirodni brojevi bili prvi apstraktni pojmovi kod ljudi. Brojanje istovrsnih predmeta, kao i dodavanje još jednog primerka zbirci istovrsnih primeraka, čini sigurnu osnovu za apstrakciju prirodnog broja. Prvi zapis o prelasku sa konkretnog brojanja na apstraktno datira iz 3001. godine p.n.e. Na jednoj sumerskoj glinenoj pločici prikazan je broj 33 pomoću tri kružića (desetice) i tri zareza (jedinice), zapisanih ispod kružića. Zajedno sa znakom za ćup, koji se nalazi pored, ceo zapis bi se mogao pročitati kao 33 ćupa ulja.

Prirodni brojevi su poznat objekat $\mathbb{N} = \{1, 2, 3, \ldots\}$. Intuitivno se podrazumeva da iza svakog broja sledi broj, te da se nabrajanje može odvijati bez ograničenja. Oznaka $\mathbb{N}$ za skup prirodnih brojeva je prvo slovo latinske reči *naturalis*=prirodno.

Radi jednostavnijeg dokazivanja potrebno je preciznije fiksirati našu intuiciju o brojevima. To ćemo učiniti koristeći Peanovu aksiomatiku. *Peanova aksiomatika temelji deduktivni aritmetički sistem na trima osnovnim pojmovima: prirodan broj, sledbenik, 1.*

[1] Giuseppe Peano, 1858-1932.

Aksiomatika prirodnih brojeva, koja se danas izlaže, se po formi donekle razlikuje od izvorne.

Strukturu prirodnih brojeva uvodimo kao uređenu trojku $(\mathbb{N}, ', 1)$, gde $\mathbb{N}$ je neprazan skup, $'$ (prim) je operacija dužine jedan i 1 je konstanta iz $\mathbb{N}$, tako da važi:

(P1) $(\forall x)(1 \neq x')$.
(1 nije sledbenik nijednog prirodnog broja.)
(P2) $(\forall x, y)(x' = y' \Rightarrow x = y)$
(Ako su sledbenici dva broja jednaki, onda su ta dva broja jednaka.)
(P3) (**Aksioma indukcije.**) Ako je $M \subseteq \mathbb{N}$, koji zadovoljava uslove:
(1) $1 \in M$ i
(2) $(\forall x)(x \in M \Rightarrow x' \in M)$,
onda je $M = \mathbb{N}$.

Elemente skupa $\mathbb{N}$ zovemo *prirodni brojevi* i, na osnovu gornjeg, su to $1, 1', (1')'$ ili $1''$, itd. U dekadnoj notaciji njihove oznake su redom $1, 2, 3$, itd.

Od posebnog je značaja uslov (P3), Aksioma indukcije. Na osnovu njega se dokazuje sledeće tvrđenje, poznato kao **Princip matematičke indukcije**.

Tvrđenje 1 *Neka je $\varphi(n)$ tvrđenje koje zavisi od prirodnog broja n tako da važi:*
(i) $\varphi(1)$ je tačno tvrđenje.
(ii) Za svako n ako je $\varphi(n)$ tačno, onda je i $\varphi(n')$ tačno tvrđenje.
Tada, $\varphi(n)$ je tačno tvrđenje za svaki prirodan broj n.

Dokaz. Neka je M skup svih prirodnih brojeva za koje $\varphi(n)$ je tačno tvrđenje. Tada, skup M zadovoljava pretpostavke u (P3) pa je, prema (P3), $M = \mathbb{N}$. ■

U nastavku dajemo osnovna svojstva strukture prirodnih brojeva, koja proizilaze iz navedenih uslova.

Tvrđenje 2 *Nijedan prirodni broj nije jednak svom sledbeniku.*

Dokaz. Pretpostavimo da za neko $p \in \mathbb{N}$ važi $p = p'$. Uočimo skup $M = \mathbb{N} \setminus \{p\}$. Pokazujemo da je narušen uslov $(P3)$. Zbog $(P1)$, $p \neq 1$, pa važi $1 \in M$. Dalje, ako je $x \in M$, onda je $x \neq p$, pa je i $x' \neq p' = p$, dakle, $x' \in M$. Sledi da su ispunjene pretpostavke uslova (P3), pa je $M = \mathbb{N}$ što je, s obzirom na izbor skupa M, netačno. ■

Tvrđenje 3 *Broj 1 je jedini elemenat skupa $\mathbb{N}$ koji nije sledbenik nijednog prirodnog broja.*

Dokaz. Pretpostavimo da osim 1 postoji i prirodni broj q koji nije sledbenik nijednog prirodnog broja, tj. $q \neq x'$ za svaki $x \in \mathbb{N}$. Pokazaćemo da skup $P = \mathbb{N} \setminus \{q\}$ ne zadovoljava uslov (P3). Zaista, $1 \in P$, a iz $x \in P$, očigledno, sledi $x' \in P$. Dakle, skup P zadovoljava pretpostavke uslova (P3), ali je $P \neq \mathbb{N}$. ■

U strukturi $(\mathbb{N}, ', 1)$ definišu se binarne operacije *sabiranja* $(+)$ i *množenja* $(\cdot)$ na sledeći način.

$$\begin{array}{ll} x + 1 := x' & x \cdot 1 := x \\ x + y' := (x + y)' & x \cdot y' := (x \cdot y) + x \end{array}$$

Tvrđenje 4 *Za svaka dva prirodna broja m i n, zbir $m + n$ i proizvod $m \cdot n$ su jedinstveno određeni prirodni brojevi.*

Dokaz. Dokazaćemo tvrđenje indukcijom po n. Neka je m proizvoljan prirodni broj. Neka je, zatim, $M = \{n \in \mathbb{N} \mid P(n)\}$, gde je $P(n)$ svojstvo *"m+n je jedinstveno određen prirodni broj"*, i $S = \{n \in \mathbb{N} \mid Q(n)\}$, gde $Q(n)$ je svojstvo *"$m \cdot n$ je jedinstveno određen prirodni broj"*.

Za $n = 1$, prema definiciji zbira (proizvoda), je $m + 1 = m'$ ($m \cdot 1 = m$), pa $1 \in M$ ($1 \in S$). Pretpostavimo da $n \in M$ ($n \in S$). Dakle, $m + n$ ($m \cdot n$) je jedinstveno određen prirodni broj. Tada je i $(m+n)'$ jedinstven, jer je $'$ funkcija. Odatle je zbog $m + n' = (m + n)'$ i $m + n'$ jedinstven, pa $n' \in M$. Dakle, $M = \mathbb{N}$. Iz $m \cdot n' = (m \cdot n) + m$, pretpostavke da je $m \cdot n$ jedinstveno određen i, upravo dokazane, činjenice da je zbir svaka dva prirodna broja jedinstveno određen, sledi da $m \cdot n'$ je jedinstveno određen, pa $n' \in S$. Dakle, i $S = \mathbb{N}$. ■

Tvrđenje 5 *Za svaka tri prirodna broja x, y i z važi:*

(**1**) $x \cdot 1 = 1 \cdot x = x$
(**2**) $x + (y + z) = (x + y) + z$
(**3**) $x + y = y + x$
(**4**) $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
(**5**) $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$
(**6**) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
(**7**) $x \cdot y = y \cdot x$.

Dokaz. Sve jednakosti se dokazuju indukcijom po jednoj od promenljivih. Slede dokazi za (**1**), (**2**) i (**4**).

(**1**) Prema definiciji proizvoda je $x \cdot 1 = x$.

Jednakost $1 \cdot x = x$ dokazujemo indukcijom po x. Za $x = 1$ je, prema definiciji, $1 \cdot 1 = 1$. Neka je $1 \cdot x = x$. Tada je $1 \cdot x' = 1 \cdot x + 1 = x + 1 = x'$.

(**2**) Indukcijom po z.

Za $z = 1$, jednakost postaje $x + (y + 1) = (x + y) + 1$, a ovo je tačno po definiciji sabiranja, tj. zbog $x + y' = (x + y)'$.

Iz indukcijske pretpostavke $x + (y + z) = (x + y) + z$ i definicije sabiranja sledi

$x + (y + z') = x + (y + z)' = (x + (y + z))' = ((x + y) + z)' = (x + y) + z'$,

pa jednakost pod (2) važi.

(**4**) Indukcijom po z.

Za $z = 1$, imamo $x \cdot (y + 1) = x \cdot y' = (x \cdot y) + x = (x \cdot y) + (x \cdot 1)$.

Pretpostavimo da je $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$. Tada je

$x \cdot (y + z') = x \cdot (y + (z + 1)) = x \cdot ((y + z) + 1) = x \cdot (y + z)' = (x \cdot (y + z)) + x =$

$((x \cdot y) + (x \cdot z)) + x = (x \cdot y) + ((x \cdot z) + x) = (x \cdot y) + (x \cdot z')$,

čime je jednakost pod (4) dokazana. ■

Tvrđenje 6 *Dokazati da za svaka tri prirodna broja x, y i z važi:*

(1) $x + z = y + z \Rightarrow x = y$ *i* **(2)** $x \cdot z = y \cdot z \Rightarrow x = y$.

Dokaz **(1)** Dokaz se izvodi matematičkom indukcijom po z. Za $z = 1$ iz $x + 1 = y + 1$, odnosno, $x' = y'$ sledi, prema (P2), da je $x = y$.

Pretpostavimo da iz $x+z = y+z$ sledi $x = y$, i da je $x+z' = y+z'$, tj. $x+(z+1) = y+(z+1)$. Dakle, $(x + z) + 1 = (y + z) + 1$, odnosno $(x + z)' = (y + z)'$, odakle, takođe, prema (P2) važi $x + z = y + z$, pa je prema induktivnoj pretpostavci $x = y$.

(2) Dokazujemo matematičkom indukcijom po x. Za $x = 1$, treba da dokažemo da iz $1 \cdot z = y \cdot z$ sledi $y = 1$. Pretpostavimo suprotno, da je $y \neq 1$. Prema Tvrđenju 3, sledi da je y sledbenik nekog prirodnog broja. Neka je to broj u. Dakle, $1 \cdot z = (u+1) \cdot z$, pa je $z = u \cdot z + z$. Iz jednakosti gornjih brojeva sledi i jednakost njihovih sledbenika, pa je $z + 1 = u \cdot z + z + 1$. Iz komutativnosti i kancelacije za sabiranje (dokazane pod **(1)**) je $1 = u \cdot z + 1$. Dobijena je kontradikcija jer 1 nije sledbenik nijednog prirodnog broja. Zato je $y = 1$.

Pretpostavimo da tvrđenje važi za x, tj. da za svako y i z iz $x \cdot z = y \cdot z$ sledi $x = y$.

Neka je $(x + 1) \cdot z = y \cdot z$. Da je $y = 1$ bilo bi $x + 1 = 1$, slično kao u prvom koraku indukcije, što vodi do kontradikcije. Dakle, $y \neq 1$, pa je y sledbenik nekog broja, recimo u. Dakle, $(x + 1) \cdot z = (u + 1) \cdot z$. Odavde sledi $x \cdot z + z = u \cdot z + z$, odnosno $x \cdot z = u \cdot z$, i prema induktivnoj pretpostavci $x = u$, odakle je $x + 1 = u + 1 = y$. ■

Primetimo da je skup prirodnih brojeva *beskonačan*, tj. da se može bijektivno preslikati na neke od svojih pravih podskupova. Na primer, lako se proverava da je takvo preslikavanje $n \mapsto 2n$, koje $\mathbb{N}$ preslikava na podskup parnih brojeva. Za skup koji je u bijekciji sa $\mathbb{N}$, pa dakle i za sam skup $\mathbb{N}$, kažemo da je *prebrojivo beskonačan*.

Poredak na N

Na skupu $\mathbb{N}$ definiše se uređenje (poredak) $\leq$, kao što sledi. Najpre, se definiše relacija $<$ (*manje*):

$x < y$ ako i samo $(\exists z)(x + z = y)$.

Relacija $\leq$ (*manje ili jednako*) se, zatim, definiše na sledeći način:

$x \leq y$ ako i samo ako $x = y \vee x < y$.

Tvrđenje 7 *Relacija $\leq$ je relacija uređenja na skupu $\mathbb{N}$.*

Dokaz. Treba pokazati da je relacija $\leq$ refleksivna, antisimetrična i tranzitivna.

Refleksivnost ($(\forall x)(x \leq x)$): Po definiciji je $x \leq x$, jer za svako $x \in \mathbb{N}$ važi $x = x$.

Antisimetričnost ($x \leq y \wedge y \leq x \Rightarrow x = y$): Neka je $x \leq y$ i $y \leq x$. Tada su mogući sledeći slučajevi:

(1) $x = y$ i $y = x$;

(2) $x = y$ i $y + v = x$, za neko $v \in \mathbb{N}$;

(3) $x + u = y$, za neko $u \in \mathbb{N}$ i $y = x$;

(4) $x + u = y$ i $y + v = x$, za neke $u, v \in \mathbb{N}$.

U slučaju (1), antisimetričnost je zadovoljena. Ako važi (2), onda je $x + v = x$, odnosno $x + v' = x'$, pa je $v' = 1$, što je netačno. Dakle, slučaj (2) je nemoguć. Slično se isključuju i (3) i (4). Sledi da je $\leq$ antisimetrična relacija.

Tranzitivnost ($x \leq y \wedge y \leq z \Rightarrow x \leq z$): Ako je $x \leq y$ i $y \leq z$, onda je moguće:

(1) $x = y$ i $y = z$;

(2) $x = y$ i $y + v = z$, za neko $v \in \mathbb{N}$;

(3) $x + u = y$, za neko $u \in \mathbb{N}$ i $y = z$;

(4) $x + u = y$ i $y + v = z$, za neke $u, v \in \mathbb{N}$.

Ako važi (1), onda je tranzitivnost ispunjena, jer je $x = z$. U slučaju (2) (slično i (3)) je $x + v = z$, pa je $x \leq z$. U slučaju (4) je $x + (u + v) = z$, dakle, $x \leq z$. Time je dokazano da je relacija $\leq$ uređenje na $\mathbb{N}$. ■

Tvrđenje 8 *Skup* $\mathbb{N}$ *je relacijom* $\leq$ *potpuno uređen.*

Dokaz. Dokazaćemo, indukcijom po x, da za svaka dva prirodna broja x i y važi uslov $x \leq y \vee y \leq x$.

Za $x = 1$ uslov se svodi na $1 \leq y \vee y \leq 1$. Ova formula je tačna, jer za $y = 1$ imamo $1 = 1$, a za $y \neq 1$ postoji z čiji je y sledbenik, tj. $z' = z + 1 = 1 + z = y$ i zato $1 \leq y$.

Pretpostavimo da važi $x \leq y \vee y \leq x$. Dakle, postoje tri mogućnosti:

(1) $x + u = y$, za neko $u \in \mathbb{N}$; (2) $y + v = x$, za neko $v \in \mathbb{N}$ i (3) $x = y$.

U slučaju (1), ako je $u = 1$, onda je $x' = y$, pa je $x' \leq y$. Ako je $u \neq 1$, onda je $u = w'$, pa je $x + w' = y$, odnosno $x + v + 1 = y$, tj. $x' + v = y$ i zato $x' \leq y$. Ako važi (3), (slično za (2)) onda je $y = x \leq x + 1 = x'$, pa je u svim slučajevima i x' uporediv sa y. ■

Tvrđenje 9 *Poredak* $\leq$ *je saglasan sa operacijama u* $\mathbb{N}$*, tj. za svaki* $z \in \mathbb{N}$*, iz* $x \leq y$ *sledi* $x + z \leq y + z$ *i* $x \cdot z \leq y \cdot z$. ■

Poredak $\leq$ definisan je preko operacije sabiranja. Analogno se pomoću operacije množenja definiše drugi fundamentalni poredak na $\mathbb{N}$, u oznaci $\mid$ (*deli, je delitelj*):

$x \mid y$ ako i samo ako $(\exists z)(x \cdot z = y)$.

Tvrđenje 10 *Relacija* $\mid$ *je poredak na* $\mathbb{N}$.

Dokaz. Refleksivnost: $x \mid x$ jer je $x \cdot 1 = x$.

Antisimetričnost: Iz $x \mid y$ i $y \mid x$ sledi $x \cdot u = y$ i $y \cdot v = x$, za neke $u, v \in \mathbb{N}$. Sledi $x \cdot u \cdot v = x = x \cdot 1$, pa je po kancelaciji $u \cdot v = 1$, odakle je $u = v = 1$ (dokaz se ostavlja slušaocima), tj. $x = y$.

Tranzitivnost: Neka $x \mid y$ i $y \mid z$. Sledi $x \cdot u = y$ i $y \cdot v = z$, za neke $u, v \in \mathbb{N}$. Tada je $(x \cdot u) \cdot v = x \cdot (u \cdot v) = z$, pa važi $x \mid z$. ■

Za razliku od relacije $\leq$, poredak $\mid$ na $\mathbb{N}$ nije linearan, jer nisu svaka dva prirodna broja uporediva ovom relacijom. Takođe, ovaj poredak saglasan je sa množenjem, jer iz $x \mid y$ sledi $x \cdot z \mid y \cdot z$, ali ne i sa sabiranjem: važi na pr. $3 \mid 6$, ali nije tačno da $3 + 1$ deli $6 + 1$.

Najzad, slušalac može, kao vežbu, dokazati da iz $x \mid y$ sledi $x \leq y$.

2. Celi brojevi

Celi brojevi su poznat objekat: $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$. Do njih se dolazi pomoću prirodnih brojeva, posebnom konstrukcijom koju opisujemo u nastavku.

Simbol za nulu "0" pojavio se u Indiji u 9. veku. Na jednom natpisu u Gwalioru iz 876. brojevi 50 i 270 napisani su sa nulom. Poreklo samog znaka je neizvesno. Moguće je da je nastao kao asocijacija na prazan krug, ali je mnogo verovatnije da potiče od grčkog slova *omikron* "O" koje predstavlja inicijal grčke reči *oúδén* (*ouden*), što znači "ništa".

Pojam **negativnih brojeva** javlja se po prvi put u kineskoj matematici. Naime, u starokineskoj knjizi *K'iu-ch'ang Suan-shu* (*Devet knjiga o matematičkoj veštini*, oko 200. p.n.e. ali

možda i mnogo ranije, pre 1000. p.n.e.) iz perioda dinastije Han (202 p.n.e. – 211 n.e.) negativni brojevi su zapisivani crnom bojom dok su pozitivni brojevi pisani crvenom bojom.

Prvi napredak u razmatranju negativnih brojeva načinio je **Fibonacci** koji je interpretirao negativno rešenje u finansijskim problemima kao gubitak umesto zarade. Međutim, prvi koji je tretirao negativne brojeve na pravi način bio je italijanski matematičar **Girolamo Cardan** (1501–1576). On je formulisao jednostavne zakone sa negativnim brojevima u svojoj knjizi *Ars Magna* (1545). Usvojio je simbol za negativan broj "m :" (m je od latinskog *meno* – minus) tako da je pisao "$m : 5$" za -5, dok je njegov kolega **Raphael Bombelli** koristio oznaku "$m.$".

Kao što smo pokazali u strukturi prirodnih brojeva $(\mathbb{N}, +, \cdot)$, za svaka tri prirodna broja x, y i z važi:

(**1**) $x \cdot 1 = 1 \cdot x = x$
$x + (y + z) = (x + y) + z$
$x + y = y + x$
$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
$(x + y) \cdot z = (x \cdot z) + (y \cdot z)$
$x \cdot (y \cdot z) = (x \cdot y) \cdot z$
$x \cdot y = y \cdot x.$

Takođe, za $a < b$ jednačina

(**2**) $a + x = b$

ima rešenje u $\mathbb{N}$. Ali, ova struktura ima i sledeći nedostatak: Jednačina (2) nije rešiva u $\mathbb{N}$ za prirodne brojeve a i b takve da je $b \leq a$. Da bismo otklonili ovaj nedostatak, očigledno, neophodno je proširiti skup prirodnih brojeva, odnosno proširiti strukturu $(\mathbb{N}, +, \cdot)$.

O čemu treba voditi računa?

1. Svaka tri elementa x, y i z nove strukture zadovoljavaju **(1)**.
2. Nedostatak **(2)** je otklonjen.
3. Konstruisana struktura je najmanja.

Šta treba uraditi? Praktično, treba "izmisliti nove brojeve" koji su rešenja jednačine $a+x = b$. Neka je rešenje jednačine predstavljeno uređenim parom (a, b). Primetimo: U skupu $\mathbb{N}$ jednačine $2 + x = 5$ i $n + (2 + x) = n + 5$ za proizvoljno $n \in \mathbb{N}$ imaju isto rešenje $x = 3$. Dakle, hoćemo da i u tom širem skupu jednačine $a + x = b$ i $n + a + x = n + b$ imaju isto rešenje, tj. da je $x = (a, b) = (n + a, n + b)$. Neka jednačine $a + x = b$ i $c + x = d$ imaju isto rešenje. Tada, prema prethodnom, i jednačine $c + a + x = c + b$ i $a + c + x = a + d$ imaju isto rešenje. Iz $c + a = a + c$ sledi $c + b = a + d$. Prema tome, u skupu $\mathbb{N}^2$ smatraćemo jednakim parove (a, b) i (c, d) za koje važi: $a + d = b + c$.

Upravo ovo će poslužiti za definiciju relacije $\sim$ na $\mathbb{N}^2$:

$$(a, b) \sim (c, d) \Longleftrightarrow a + d = b + c.$$

Naredno tvrđenje dokazuje se direktno na osnovu ove definicije.

Tvrđenje 11 *$\sim$ je relacija ekvivalencije na skupu $\mathbb{N}^2$.* ■

Klase ekvivalencije su opisane u definiciji relacije $\sim$: *jednu klasu čine uređeni parovi sa istim zbirovima unutrašnjih i spoljašnjih članova.* Klasu uređenog para (a, b) označavaćemo sa $C_{(a\,,\,b)}$.

Na količničkom skupu $\mathbb{N}^2/\!\sim$ definišemo operacije $+$ i $\cdot$:

$C_{(a\,,\,b)} + C_{(c\,,\,d)} := C_{(a+c\,,\,b+d)}$ i

$C_{(a\,,\,b)} \cdot C_{(c\,,\,d)} := C_{(ad+bc\,,\,ac+bd)}$.

Intuitivno obrazloženje za ove definicije je sledeće: zbir rešenja jednačina $a+x = b$ i $c+x = d$

je rešenje jednačine $a+c+x=b+d$, a proizvod je rešenje jednačine $ad+bc+x=ac+bd$. Ovo se neposredno proverava.

Tvrđenje 12 *Operacije* $+$ *i* $\cdot$ *na* $\mathbb{N}^2/\sim$ *su dobro definisane.*

Dokaz. Za svake dve klase $C_{(a\,,\,b)}$ i $C_{(c\,,\,d)}$ postoji zbir, klasa $C_{(a+c\,,\,b+d)}$, jer uvek postoje odgovarajući zbirovi $a+c$, $b+d$. Ta klasa je jedinstvena. Ako se uzmu drugi predstavnici, $(a_1,b_1)\in C_{(a\,,\,b)}$ i $(c_1,d_1)\in C_{(c\,,\,d)}$, onda je $a_1+b=b_1+a$ i $c_1+d=c+d_1$, pa je $(a_1+c_1\ ,\ b_1+d_1)\sim(a+c,b+d)$. Zato je $C_{(a_1+c_1\,,\,b_1+d_1)}=C_{(a+c\,,\,b+d)}$.

Analogno zaključivanje važi i za proizvod klasa. Za $C_{(a\,,\,b)}$ i $C_{(c\,,\,d)}$ postoji klasa $C_{(ad+bc\,,\,ac+bd)}$ koja je po definiciji njihov proizvod. Dokazujemo njenu jedinstvenost. Za $(a_1,b_1)\in C_{(a\,,\,b)}$ i $(c_1,d_1)\in C_{(c\,,\,d)}$, iz $a_1+b=b_1+a$ i $c_1+d=d_1+c$ sledi $a_1d_1+b_1c_1+ac+bd=a_1c_1+b_1d_1+ad+bc$, pa je $C_{(a_1d_1+b_1c_1\,,\,a_1c_1+b_1d_1)}=C_{(ad+bc\,,\,ac+bd)}$. Bez obzira na izbor predstavnika, dobija se ista klasa kao proizvod. ■

Tvrđenje 13 *Za svaka tri elementa* $C_{(a\,,\,b)},C_{(c\,,\,d)},C_{(e\,,\,f)}\in\mathbb{N}^2/\sim$ *važi:*

(1) $C_{(a\,,\,b)}+(C_{(c\,,\,d)}+C_{(e\,,\,f)})=(C_{(a\,,\,b)}+C_{(c\,,\,d)})+C_{(e\,,\,f)}$

(2) $C_{(a\,,\,b)}+C_{(c\,,\,d)}=C_{(c\,,\,d)}+C_{(a\,,\,b)}$

(3) $C_{(a\,,\,b)}+C_{(1\,,\,1)}=C_{(1\,,\,1)}+C_{(a\,,\,b)}=C_{(a\,,\,b)}$

(4) $C_{(a\,,\,b)}\cdot(C_{(c\,,\,d)}\cdot C_{(e\,,\,f)})=(C_{(a\,,\,b)}\cdot C_{(c\,,\,d)})\cdot C_{(e\,,\,f)}$

(5) $C_{(a\,,\,b)}\cdot C_{(c\,,\,d)}=C_{(c\,,\,d)}\cdot C_{(a\,,\,b)}$

(6) $C_{(a\,,\,b)}\cdot C_{(1,2)}=C_{(1\,,\,2)}\cdot C_{(a\,,\,b)}=C_{(a\,,\,b)}$.

(7) $C_{(a\,,\,b)}\cdot(C_{(c\,,\,d)}+C_{(e\,,\,f)})=(C_{(a\,,\,b)}\cdot C_{(c\,,\,d)})+(C_{(a\,,\,b)}\cdot C_{(e\,,\,f)})$

(8) $(C_{(a\,,\,b)}+C_{(c\,,\,d)})\cdot C_{(e\,,\,f)}=(C_{(a\,,\,b)}\cdot C_{(e,f)})+(C_{(c\,,\,d)}\cdot C_{(e\,,\,f)})$.

Dokaz. **(2)** $C_{(a\,,\,b)}+C_{(c\,,\,d)}=C_{(a+c\,,\,b+d)}=C_{(c+a\,,\,d+b)}=C_{(c\,,\,d)}+C_{(a\,,\,b)}$, jer je sabiranje komutativno u $\mathbb{N}$. Sličnim rezonovanjem dokazuju se i $(1),(4),(5),(7)$ i (8). Direktnom proverom se dokazuju (3) i (6).

Klasa $C_{(1\,,\,1)}$ je neutralni elemenat za sabiranje, a klasa $C_{(1\,,\,2)}$ je neutralni elemenat za množenje. Element $C_{(b\,,\,a)}$ je suprotni elemenat za klasu $C_{(a\,,\,b)}$. ■

Uočimo u skupu $\mathbb{N}^2/\sim$ podskup

$\mathbb{N}^*=\{C_{(1\,,\,1+a)}\mid a\in\mathbb{N}\}$.

Jednostavno se proverava da je zbir i proizvod svaka dva elementa iz $\mathbb{N}^*$, takođe, element ovog skupa. Dobijamo:

$C_{(1\,,\,1+a)}+C_{(1\,,\,1+b)}=C_{(1\,,\,1+a+b)}$ i

$C_{(1\,,\,1+a)}\cdot C_{(1\,,\,1+b)}=C_{(1\,,\,1+ab)}$.

Neka je $h:\mathbb{N}\to\mathbb{N}^*$ preslikavanje definisano sa: $h(a)=C_{(1\,,\,1+a)}$. Ono je 1–1 jer različitim prirodnim brojevima odgovaraju različite klase (sledi iz definicije klase). h je *na* jer se u $C_{(1\,,\,1+a)}$ preslikava prirodni broj a.

Dokazujemo i da za svaka dva prirodna broja važi:

♢ slika zbira je zbir slika;

♢ slika proizvoda je proizvod slika.

$h(a+b)=C_{(1\,,\,1+a+b)}=C_{(1\,,\,1+a)}+C_{(1\,,\,1+b)}=h(a)+h(b)$;

$h(a\cdot b)=C_{(1\,,\,1+a\cdot b)}=C_{(1\,,\,1+a)}\cdot C_{(1\,,\,1+b)}=h(a)\cdot h(b)$.

Šta nam ovo govori?

- Svaki prirodni broj ima jedinstvenog predstavnika u $\mathbb{N}^*$.
- Svaki element iz $\mathbb{N}^*$ je predstavnik jednog i samo jednog prirodnog broja.

• Element iz $\mathbb{N}^*$ koji je predstavnik zbira (proizvoda) ma koja dva prirodna broja je zbir (proizvod) njihovih predstavnika.

Dakle, možemo identifikovati strukture $(\mathbb{N},+,\cdot)$ i $(\mathbb{N}^*,+,\cdot)$ i, u tom smislu, smatrati $(\mathbb{N},+,\cdot)$ delom strukture $(\mathbb{N}^2/\!\sim,+,\cdot)$.

Pokazaćemo da je $(\mathbb{N}^2/\!\sim,+,\cdot)$ najmanja struktura koja sadrži $(\mathbb{N},+,\cdot)$ i zadovoljava uslove (1). Neka je $\mathbf{R}$ proizvoljna struktura koja zadovoljava uslove (1) i sadrži $\mathbb{N}^*$. Pokazaćemo da R sadrži $\mathbb{N}^2/\!\sim$, tj. da je svaki $C_{(a\,,\,b)} \in \mathbb{N}^2/\!\sim$ sadržan u R. Primetimo

$$C_{(a\,,\,b)} = C_{(1+a\,,\,1)} + C_{(1\,,\,1+b)}.$$

$C_{(1\,,\,1+b)} \in R$ jer R sadrži $\mathbb{N}^*$, ali i $C_{(1+a\,,\,1)} \in R$, kao suprotan element za $C_{(1\,,\,1+a)}$, pa je i njihov zbir u R, tj. $C_{(a\,,\,b)} \in R$.

I na kraju uvodimo sledeće oznake:

♣ $\mathbb{N}^2/\!\sim = \mathbb{Z}$, i $\mathbb{Z}$ zovemo skupom celih brojeva.

♣ $\mathbf{C_{(1\,,\,1+a)} = a},\ \mathbf{C_{(1+a\,,\,1)} = -a},\ \mathbf{C_{(1\,,\,1)} = 0},\ \mathbf{C_{(a\,,\,b)} = b - a},$

$(C_{(a\,,\,b)} = (-a) + b = b + (-a).)$

Posmatrajmo zbir i proizvod u $\mathbb{Z}$ u svetlu novih oznaka:

$\mathbf{(-a)+b},\ \mathbf{(-a)+(-b)},\ \mathbf{(-a)\cdot b},\ \mathbf{(-a)\cdot(-b)},\ \mathbf{a,b} \in \mathbb{N}.$

1. $\mathbf{(-a)+b}$

1.1. $a + k = b,\ k \in \mathbb{N}$

$(-a) + b = C_{(1+a\,,\,1)} + C_{(1\,,\,1+b)} = C_{(1+a\,,\,1)} + C_{(1\,,\,1+a+k)} = C_{(1+a+1\,,\,1+1+a+k)} = C_{(1\,,\,1+k)} = k;$

1.2. $a = b$

$(-a) + b = C_{(1+a\,,\,1)} + C_{(1\,,\,1+a)} = C_{(1+a+1\,,\,1+1+a)} = C_{(1\,,\,1)} = 0;$

1.3. $a = b + k,\ k \in \mathbb{N}$

$(-a) + b = C_{(1+a\,,\,1)} + C_{(1\,,\,1+b)} = C_{(1+b+k\,,\,1)} + C_{(1\,,\,1+b)} = C_{(1+b+k+1\,,\,1+1+b)} = C_{(1+k\,,\,1)} = -k.$

2. $\mathbf{(-a)+(-b)}$

$(-a) + (-b) = C_{(1+a\,,\,1)} + C_{(1+b\,,\,1)} = C_{(1+a+1+b\,,\,1+1)} = C_{(1+a+b\,,\,1)} = -(a+b);$

3. $\mathbf{(-a)\cdot b}$

$(-a)\cdot b = C_{(1+a\,,\,1)} \cdot C_{(1\,,\,1+b)} = C_{(1+a+b+ab+1\,,\,1+a+1+b)} = C_{(1+ab\,,\,1)} = -(ab).$

4. $\mathbf{(-a)\cdot(-b)}$

$(-a)\cdot(-b) = C_{(1+a\,,\,1)} \cdot C_{(1+b\,,\,1)} = C_{(1+a+1+b\,,\,1+a+b+ab+1)} = C_{(1\,,\,1+ab)} = ab.$

Tvrđenje 14 *U skupu $\mathbb{Z}$ za svaki $a,b,c,d \in \mathbb{Z}$ i $d \neq 0$ važi:.*

(**1**) $a + c = b + c \Rightarrow a = b$;

(**2**) $a \cdot d = b \cdot d \Rightarrow a = b$.

(**3**) $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$. ■

Poredak na $\mathbb{Z}$

Kao i na strukturi $(\mathbb{N},+,\cdot)$, na strukturi $(\mathbb{Z},+,\cdot)$ uvodi se relacija $<$ (*manje*):

$x < y$ ako i samo ako $(\exists n \in \mathbb{N})(x + n = y)$.

• *Za svaki prirodan broj n važi $0 < n$.* Zaista, $0 + n = n$, $n \in \mathbb{N}$.

Relacija $<$ ima i sledeća svojstva.

Tvrđenje 15 *Za svako $x \in \mathbb{Z}$ važi:*

(**a**) *ako je $0 < x$, onda je $-x < 0$;* (**b**) *ako je $x < 0$, onda je $0 < -x$.*

Dokaz. (**a**) Ako je $0 < x$, onda je na osnovu definicije $0 + n = x$, za neki $n \in \mathbb{N}$, pa je $(-x) + 0 + n = (-x) + x$, tj. $(-x) + n = 0$, dakle, $-x < 0$.

(b) Slično kao pod (a). ■

U odnosu na relaciju $<$, sve cele brojeve možemo podeliti u tri disjunktne klase:
klasu $\mathbb{Z}^+$ koju čine prirodni ili *pozitivni celi brojevi*, skup $\{0\}$ i klasu *negativnih celih brojeva* $\mathbb{Z}^- = \{x \mid -x \in \mathbb{N}\}$.

Relaciju $\leq$ definišemo sa:

$x \leq y$ ako i samo ako $x = y \vee x < y$.

Tvrđenje 16 *Relacija $\leq$ je poredak na $\mathbb{Z}$.*

Dokaz. Za svaki $x \in \mathbb{Z}$ važi $x \leq x$, jer je $x = x$, pa je $\leq$ refleksivna relacija.

Da bismo dokazali antisimetričnost, pretpostavimo da je $x \leq y$ i $y \leq x$. Pokazaćemo da od slučajeva : $x = y$, $x = y \wedge x < y$, $x = y \wedge y < x$ i $x < y \wedge y < x$ jedini moguć je $x = y$. Posmatrajmo slučaj $x < y$ i $y < x$ (prethodna dva se analiziraju slično). Dakle, neka je $x+u = y$ i $y + v = x$, za neke $u, v \in \mathbb{N}$. Sledi $x = x + u + v$, tj. $x + 1 = x + u + v + 1$, pa je na osnovu kraćenja, $1 = u + v + 1 = (u + v)'$, što je netačno.

Tranzitivnost se dokazuje na isti način kao u $\mathbb{N}$. ■

Tvrđenje 17 *Poredak $\leq$ na $\mathbb{Z}$ je:*

(**1**) *Potpun, tj. za sve $x, y, z \in \mathbb{Z}$, $x \leq y$ ili $y \leq x$;*

(**2**) *Saglasan sa operacijama tj. iz $x \leq y$ sledi $x + z \leq y + z$ i iz $x \leq y$ i $0 \leq t$ sledi $x \cdot t \leq y \cdot t$.* ■

Dokaz. (**1**) S obzirom da je jednačina $x + u = y$ rešiva u $\mathbb{Z}$ za svaki $x, y \in \mathbb{Z}$, to postoji $z \in \mathbb{Z}$ takav da je $x+z = y$. Ako je $z = 0$, onda je $x = y$. Ako je $0 < z$, onda je, po definiciji relacije $<$, $x < y$. Ako je $z < 0$, onda je $0 < -z$, pa s obzirom da iz $x+z = y$ sledi $x+z+(-z) = y+(-z)$, tj. $x = y + (-z)$, to je $y < x$.

(2) Dokaz se ostavlja slušaocima. ■

Sa $\geq$ (veće ili jednako) označava se poredak dualan relaciji $\leq$: $x \geq y$ ako i samo ako $y \leq x$. Odatle i oznaka $x > y$, kao zamena za $x \geq y \wedge x \neq y$.

Tvrđenje 18 *Za svaka dva cela broja x i y važi:*

$x \cdot y > 0$ *ako i samo ako* $(x > 0 \wedge y > 0) \vee (x < 0 \wedge y < 0)$.

Dokaz. Ako je $x \cdot y > 0$, onda je $xy \neq 0$, pa je $x \neq 0$ i $y \neq 0$. Neka su x i y u različitim klasama, recimo, $x < 0$ i $y > 0$. Tada je $-x > 0$, pa je $(-x) \cdot y = -(x \cdot y) > 0$, odnosno, $x \cdot y < 0$, što je netačno.

Obratno, ako je $x > 0$ i $y > 0$, onda je na osnovu prethodnog tvrđenja, $x \cdot y > x \cdot 0$, tj. $x \cdot y > 0$. Ako je $x < 0$ i $y < 0$, onda je $-x > 0$ i $-y > 0$, pa je $(-x) \cdot (-y) > 0$. Odavde, i iz $(-x) \cdot (-y) = x \cdot y$ sledi $x \cdot y > 0$. ■

- *Za svaki ceo broj x važi $x^2 \geq 0$.*

dr Snežana Ilić, prof. PMF-a u Nišu