PRESEK
List za mlade matematike, fizike, astronome in računalnikarje

ISSN 0351-6652
Letnik **19** (1991/1992)
Številka 1
Strani 50–53

Borut Zalar:

KOMPLEKSNA CELA ŠTEVILA

Ključne besede: matematika, algebra, teorija števil, kompleksno celo število, kompleksno praštevilo.

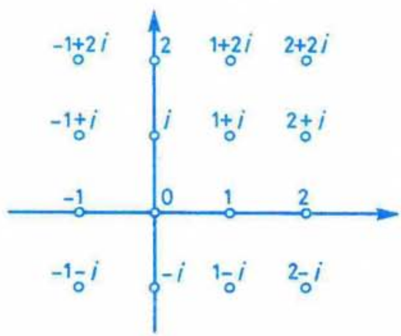
Elektronska verzija: http://www.presek.si/19/1075-Zalar.pdf

KOMPLEKSNA CELA ŠTEVILA

Ogledali si bomo eno od možnosti posplošitve pojma celega števila. Z imenom cela števila mislimo množico $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$. Cela števila si lahko predstavljamo kot ogrlico na številski osi.

Osnovo za uvedbo pojma kompleksnega števila predstavlja enačba $x^2 = -1$. Ta enačba nima rešitve v celih številih, pa tudi v realnih številih ne. Da bi to in podobne enačbe lahko reševali, so matematiki uvedli pojem imaginarne enote. To je število $\mathbf{i}$, ki reši zgornjo enačbo, torej $\mathbf{i}^2 = -1$. Besedo imaginaren navadno slovenimo kot izmišljen ali navidezen. Število $\mathbf{i}$ naj bi torej ne obstajao v resnici, ampak naj bi bilo izmišljotina matematikov. Toda razvoj matematike in tehnike v zadnjem stoletju je pokazal, da je število $\mathbf{i}$ zelo uporabno pri čisto praktičnih problemih in torej ni tako za lase privlečeno, kot bi se komu zdelo.

Zdaj definirajmo kompleksna cela števila. Vzemimo dve celi števili a, b, zapišimo $z = a + b\mathbf{i}$ in ta formalni zapis imenujmo kompleksno celo število. Zapisa $a_1 + b_1\mathbf{i}$ in $a_2 + b_2\mathbf{i}$ predstavljata isto kompleksno število natanko takrat, kadar je $a_1 = a_2$ in $b_1 = b_2$.



Seštevanje in množenje kompleksnih celih števil definiramo takole: naj bodo a, b, c, d cela števila. Potem je

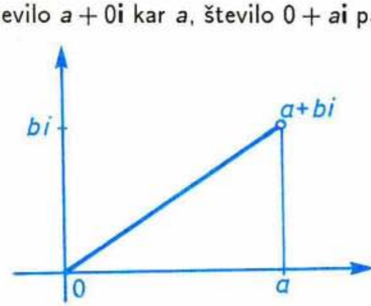
$$(a + b\mathbf{i}) + (c + d\mathbf{i}) = (a + c) + (b + d)\mathbf{i}$$
$$(a + b\mathbf{i})(c + d\mathbf{i}) = (ac - bd) + (bc + ad)\mathbf{i}$$

Zgled:

$$(1 + 2\mathbf{i}) + (3 - 5\mathbf{i}) = (1 + 3) + (2 - 5)\mathbf{i} = 4 - 3\mathbf{i}$$
$$(1 + 2\mathbf{i})(3 - 5\mathbf{i}) = 1 \cdot 3 + 2 \cdot 3 \cdot \mathbf{i} - 1 \cdot 5 \cdot \mathbf{i} - 2 \cdot 5 \cdot \mathbf{i}^2 =$$
$$= 3 + 6\mathbf{i} - 5\mathbf{i} - 10 \cdot (-1) = 13 + \mathbf{i}$$

Zaradi poenostavitve, zapišemo število $a + 0\mathbf{i}$ kar a, število $0 + a\mathbf{i}$ pa $a\mathbf{i}$.

Vsakemu kompleksnemu celemu številu $z = a + bi$ bomo priredili še pozitivno število $N(z) = a^2 + b^2$, ki ga imenujemo *norma* števila z. Če kompleksna cela števila predstavimo kot mrežo, potem je zaradi Pitagorovega izreka $N(z)$ ravno kvadrat dolžine hipotenuze v spodnjem trikotniku.



Najpomembnejša lastnost norme je izražena v naslednji trditvi:

Trditev 1. Naj bosta $z_1 = a + b\mathbf{i}$ ter $z_2 = c + d\mathbf{i}$ dve kompleksni celi števili. Potem velja $N(z_1 z_2) = N(z_1)N(z_2)$.

Dokaz nam da naslednji račun:

$$\begin{aligned}
N(z_1 z_2) = N((ac - bd) + (ad + bc)\mathbf{i}) &= (ac - bd)^2 + (ad + bc)^2 = \\
&= a^2c^2 + b^2d^2 - 2acbd + a^2d^2 + b^2c^2 + 2adbc = \\
&= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 = \\
&= (a^2 + b^2)(c^2 + d^2) = N(z_1)N(z_2)
\end{aligned}$$

Poglejmo si nekoliko pobliže deljivost kompleksnih celih števil. Definiramo jo enako kot pri celih številih, torej z_1 *deli* z_2, če obstaja tako kompleksno celo število w, da je $wz_1 = z_2$.

Najprej si oglejmo zgled:

$$1 \cdot \mathbf{i} = \mathbf{i}$$
$$\mathbf{i} \cdot (-\mathbf{i}) = -\mathbf{i}^2 = -(-1) = 1$$

Torej 1 deli $\mathbf{i}$ in tudi $\mathbf{i}$ deli 1. Pri naravnih številih je takšno medsebojno deljenje nemogoče, zato si moramo ta fenomen pobliže ogledati.

Trditev 2. Naj bosta z_1 in z_2 dve neničelni kompleksni celi števili in naj z_1 deli z_2 ter z_2 deli z_1. Tedaj imamo štiri možnosti:

$$z_1 = z_2, \quad z_1 = -z_2, \quad z_1 = \mathbf{i}z_2, \quad \text{ali} \quad z_1 = -\mathbf{i}z_2$$

Dokaz: Iz danih pogojev za števili z_1 ter z_2 sledi, da obstajata dve taki kompleksni celi števili x, y da velja:

$$z_1 = xz_2 \quad \text{in} \quad z_2 = yz_1$$

Z uporabo trditve 1 dobimo

$$N(z_1) = N(x)N(z_2)$$
$$N(z_2) = N(y)N(z_1) = N(y)N(x)N(z_2)$$

Ker je $z_1 \neq 0, z_2 \neq 0$, so norme pozitivne in zato mora biti $N(x) = N(y) = 1$. Pišemo $x = a + b\mathbf{i}$ in dobimo $a^2 + b^2 = 1$. Od tod očitno sledi, da je $a = 0$ in $b^2 = 1$ ali pa $a^2 = 1$ in $b = 0$, torej je x eno od števil $1, -1$, $\mathbf{i}$ in -$\mathbf{i}$.

To pomeni, da ima vsako kompleksno celo število z vsaj osem deliteljev. To so $1, -1$, $\mathbf{i}$, -$\mathbf{i}$, $z, -z$, $\mathbf{i}z$, $-\mathbf{i}z$. Število, ki ima samo teh osem deljiteljev, bomo imenovali kompleksno praštevilo. Naj bo p naravno število. Kdaj je p kompleksno praštevilo? Očitno je, da mora biti p praštevilo v običajnem smislu. Da to še ne zadošča, kaže naslednji zgled:

$$(1 + \mathbf{i})(1 - \mathbf{i}) = 1 + \mathbf{i} - \mathbf{i} - \mathbf{i}^2 = 2$$

število $1 + \mathbf{i}$ deli 2, zato 2 ni kompleksno praštevilo.Delni odgovor na naše vprašanje daje:

Trditev 3. Naj bo p praštevilo, ki ima pri deljenju s 4 ostanek 3. Tedaj je p tudi kompleksno praštevilo.

Dokaz: Denimo, da je p mogoče zapisati kot produkt

$$p = (a + b\mathbf{i})(c + d\mathbf{i})$$

in da sta števili $a + b\mathbf{i}$, $c + d\mathbf{i}$ različni od števil $1, -1$, $\mathbf{i}$, -$\mathbf{i}$, $p, -p$, $\mathbf{i}p$, -$\mathbf{i}p$. Tedaj dobimo $N(p) = p^2 = N(a + bi)N(c + di)$.

Ker število p^2 nima drugih naravnih deliteljev kot $1, p$ in p^2 in ker $N(a + b\mathbf{i}), N(c + d\mathbf{i}) \neq 1$, dobimo $N(a + b\mathbf{i}) = p = a^2 + b^2$. Število p je liho, zato mora biti eno izmed števil a, b sodo, eno pa liho. Kvadrat sodega števila je deljiv s 4, kvadrat lihega števila pa pri deljenju s 4 da ostanek 1 (Dokaži!). Zato vsota $p = a^2 + b^2$ pri deljenju s 4 da ostanek 1, kar pa po predpostavki ni res. Torej je p kompleksno praštevilo.

Pripomnimo še, da tista praštevila, ki pri deljenju s 4 dajo ostanek 1, niso kompleksna praštevila, vendar to ni tako enostavno dokazati.

Za konec pa nekaj nalog: