Hľa, aké prekvapenie!
Možné je to azda?
Je to prelud? Skutočnosť?
Faust

i

ŠTEFAN PORUBSKÝ, Bratislava

História i. V období renesancie matematici v Európe (a nielen oni) po prvýkrát prekročili hranice vedomostí, ktoré boli vymedzené znalosťami starých Grékov a východných národov. Menovite, v tomto období bol víťazne zavŕšený rozhodujúci boj za zavedenie desatinnej pozičnej aritmetiky. Ďalej sa položili základy aritmetickej a algebraickej symbolike, bez ktorej je veľmi ťažké predstaviť si rozvoj týchto dvoch disciplín. Zaviedli sa racionálne a záporné exponenty. Úspešne sa vyriešil problém riešenia algebraických rovníc tretieho a štvrtého stupňa pomocou radikálov, t. j. problém, pred ktorým „zastali" matematici v islamských krajinách. Riešenie tohto problému prinieslo na svet imaginárne čísla. Vzápätí F. VIET zaviedol v algebre symbolický počet tým, že začal používať špeciálne označenia pomocou písmen pre neznáme a pre koeficienty mnohočlena a tiež rozšíril symboliku algebraických operácií. Mohli by sme takto ešte pokračovať vo vymenúvaní úspechov, ktoré matematika v období renesancie dosiahla.

Predchádzajúce riadky nám napovedajú, že najväčšie úspechy v Európe v 15. a 16. storočí sa v matematike dosiahli v oblasti algebry. Najväčším európskym algebraistom 15. storočia bol Talian LUCA PACCIOLI (1445?—1515). Paccioliho najdôležitejšie dielo je *Summa de arithmetica, geometria, proportioni et proportionalita*, ktoré bolo vydané v Benátkach v r. 1494. Tú časť *Summy*, ktorá je venovaná algebraickým rovniciam, končí Paccioli úvahou o riešiteľnosti kubických rovníc typu $x^3 + ax = b$ a $x^3 + b = ax$ (a, b sa predpokladajú kladné): *„umenie algebry nám ešte nedalo metódu, práve tak, ako ešte nemáme metódu na kvadratúru kruhu"*. A práve tieto Paccioliho slová sa stali východiskom pre prácu vynikajúcich talianskych algebraistov v oblasti riešenia kubických rovníc pomocou radikálov.

Prvý, komu sa podarilo rozriešiť jeden z typov kubickej rovnice $x^3 + ax = b$ (a, $b > 0$), bol profesor boloňskej univerzity SCIPIO DEL FERRO (1456?—1526). No tak, ako to bolo zvykom v tom období, DEL FERRO nepublikoval svoje výsledky, ale ich poskytol svojmu žiakovi A. M. FIOROVI, ktorý tieto s úspechom používal na vtedy veľmi obľúbených matematických turnajoch. Na jednom

takomto turnaji dňa 12. 2. 1535 sa FIOR stretol so samoukom NICCOLOM TARTAGLIOM (1500?—1557). Tartaglia pred turnajom nezávisle odvodil del Ferrove výsledky, čo mu umožnilo vyriešiť všetky úlohy postavené Fiorom, ktorý na druhej strane bol natoľko zarazený, že nebol schopný vyriešiť jediný príklad predložený Tartagliom. Deň po turnaji Tartaglia úspešne rozriešil aj rovnicu $x^3 = ax + b$. V r. 1539 si vyžiadal od Tartaglia tieto riešenia HIERONIMO CARDANO (1501—1576) s tým, že ich nebude publikovať (dokonca sa zaprisahal). Tartaglia mu oznámil svoje pravidlo vo forme 25-riadkovej básne. Po preformulovaní nie vždy jasných a jednoznačných tartagliových formulácií a po dokázaní tohto pravidla sa Cardano cítil oprávnený ho publikovať v r. 1545 v *Ars magna sive de regulis algebraicis*, pričom spomenul Tartagliovu prioritu. Napriek tomu tieto pravidlá dodnes nesú prívlastok „Cardanove". Po tomto publikovaní nasledoval celý rad rozhorčených dopisov (na potešenie historikov, lebo obsahovali hodne údajov) medzi Tartagliom a Cardanom. V *Ars magna* CARDANO publikoval aj riešenie rovníc štvrtého stupňa, ktoré pochádzalo od jeho žiaka L. FERRARIHO (1522—1565). Takto sa v *Ars magne* po prvýkrát stretávame s novými matematickými objektmi — s imaginárnymi veličinami. No sám Cardano ich považoval za bezcenné a zbytočné. Prvým matematikom, ktorý správne ocenil použitie imaginárnych veličín, bol RAFAEL BOMBELLI (1530?—1572?). Pri analýze predchádzajúcich prác Tartagliho, Cardana a Ferrariho sa mu práve použitím imaginárnych veličín podarilo objasniť casus irreducibilis. Prínos Bombelliho spočíva aj v tom, že vo svojom diele *L'algebra parte maggiore dell' arithmetica*, Bologna 1572, položil základy teórie komplexných čísiel tým, že zaviedol násobenie imaginárnych a reálnych veličín, napr. v dnešnej symbolike: $(\pm 1)i = \pm i$, $(-i) \cdot (+i) = +1$ atď. Bombelli bol posledný z tejto plejády vynikajúcich talianskych algebraikov.

Komplexné čísla sa ešte dlho potom „zmietali" v boji o uznanie, až nakoniec po prácach Eulera, Gaussa a Lagrangea sa stali neodmysliteľnou súčasťou matematiky. Stojí za zmienku, že historicky zavedenie komplexných čísiel súviselo s riešením algebraických rovníc tretieho stupňa a nie s riešením kvadratických rovníc, t. j. so stanoviskom, ktoré dnes považujeme za najprirodzenejšie (opäť príklad kľukatej cestičky vývoja).

Komplexné čísla. Je mimoriadne ťažké zachytiť čo len najdôležitejšie prínosy zavedenia komplexných čísiel pre matematiku. Spomeňme si len ich kľúčové postavenie v mnohých disciplínach, ako napr. teória čísiel, teória funkcií s komplexnou premennou, alebo v tých vedných disciplínach, ktoré hodne využívajú matematický aparát ako fyzika, elektrotechnika a pod.

Upustíme od opakovania definícií všeobecne známych pojmov z oblasti komplexných čísiel a nebudeme sa zaoberať algebraickým zdôvodnením konštrukcie telesa komplexných čísiel. Našim cieľom je krátko sa zastaviť pri niektorých

dôležitých výsledkoch, ktoré ovplyvnili ďalší vývoj, alebo pri výsledkoch, ktoré (podľa pamäti autora) nie sú natoľko známe na úrovni strednej školy.

Jedným z najprekvapivejších výsledkov L. EULERA (od ktorého pochádza aj označenie i) bolo, že našiel tesné vnútorné súvislosti v oblasti komplexnej premennej medzi funkciami sínus a kosínus na jednej strane a exponenciálnou funkciou na strane druhej, menovite nájdenie vzťahu

$$\cos x + i \sin x = e^{ix}$$

Je príznačné (a aj prirodzené) pre obdobie, v ktorom Euler žil, že metódy dôkazov zďaleka neznesú dnešné prísne kritériá a mnohokrát by ich dnešní pedagógovia považovali za nesprávne. No vzhľadom na fantastickú Eulerovu intuíciu, väčšina jeho výsledkov zostala správna, okrem iného aj práve uvedený. Tento Eulerov výsledok umožňuje zapísať každé komplexné číslo z v *Eulerovom tvare*

$$z = |z| \cdot e^{i \cdot \mathrm{Arg}\, z}$$

kde Arg z je amplitúda (alebo argument) komplexného čísla z. Z tohto vzťahu napr. okamžite vyplýva *de Moivrova veta* o násobení, resp. mocnine komplexných čísiel. Moivrova veta je v stredoškolskej matematike obyčajne prostriedkom na odvodenie niektorých identít, napr. vyjadrenie cos nx alebo sin nx pomocou cos x a sin x, alebo na výpočet súčtov

$$\sum_{k=1}^{n} \cos kx \qquad a \qquad \sum_{k=1}^{n} \sin kx$$

atď.

Základná veta algebry. Prvá formulácia základnej vety algebry je od A. GIRARDA z r. 1629. Neskôr ju môžeme nájsť aj u DESCARTESA, v jeho *Geometrii* (presnejšie v jej tretej knihe), ktorá vyšla r. 1637. No na dôkaz tvrdenia, že *každý polynóm n-tého stupňa s reálnymi koeficientmi má práve n koreňov*, museli matematici čakať ešte veľmi dlho. Prvý ho „dokázal" D'ALEMBERT r. 1746 (a preto vo francúzskej literatúre nájdeme pomenovanie d'Alembertova veta). D'Alembert (a mnoho ďalších matematikov) v dôkaze a priori predpokladal, že každý polynóm možno rozložiť na lineárne (koreňové) faktory. Pri tomto prístupe zostalo len dokázať, že všetky korene majú tvar $a + bi$. Prvý skutočný dôkaz je až od GAUSSA z r. 1799. Gauss dokázal tvrdenie, že každý polynóm n-tého stupňa s reálnymi koeficientmi má v množine komplexných čísiel aspoň jeden koreň. Z tohto tvrdenia možno potom ľahko dokázať aj základnú vetu algebry.

Dnes poznáme viac ako 100 rôznych dôkazov základnej vety algebry, ale každý z nich využíva nejaký nealgebraický argument (čo sa často používa na dokumentáciu jednoty matematických disciplín). Zdá sa, že základná veta algebry je založená na spojitosti polynómu ako funkcie s komplexnou premennou, a preto je potrebné použiť aj nealgebraické argumenty. Sám Gauss podal štyri dôkazy, a to v r. 1799, 1815, 1816 a 1849. V dôkaze z r. 1815 sa snažil Gauss obmedziť na minimum použitie analýzy. Na tento dôkaz potom o 60 rokov neskôr nadviazal KRONECKER pri konštrukcii *telesa rozkladu polynómu*, t. j. minimálneho telesa, v ktorom sa dá daný polynóm rozložiť na lineárne faktory. Takto dostala *základná veta* tento tvar: *teleso rozkladu ľubovoľného polynómu s reálnymi alebo komplexnými koeficientmi je (až na izomorfizmus) podteleso telesa komplexných čísiel.* Inými slovami, *teleso komplexných čísiel je algebraicky uzavreté.* Označenie základná veta pochádza ešte z čias, keď pod algebrou sa rozumelo štúdium polynómov s komplexnými koeficientmi.

Gauss nielen dôkazom základnej vety algebry, ale aj prácami v ostatných oblastiach matematiky a fyziky ukázal, aký prínos znamená zavedenie komplexných čísiel. Gauss si zrejme od začiatku uvedomoval rovnocennosť imaginárnych čísiel s reálnymi, výhody komplexných čísiel a vo svojich prácach, ktoré často predstihli dobu, ukázal ako majstrovsky vedel s nimi narábať. Gauss bol vôbec prvý matematik, ktorý začal systematicky vedecky používať komplexné čísla. Je samozrejmé (a z predchádzajúcich riadkov by to malo aj vyplynúť), že imaginárne veličiny sa čoraz častejšie používali aj pred Gaussom, no ich podstata zostala až do polovice 19. storočia v podstate neobjasnená. A práve Gaussove práce v podstatnej miere prispeli k objasneniu aj tejto skutočnosti. Boli to predovšetkým práce, v ktorých vystúpili tzv. Gaussove celé čísla a interpretácia komplexných čísiel ako bodov v rovine (aj keď autorom tejto interpretácie nebol Gauss). Pretože aritmetika Gaussových celých čísiel sa podobá aritmetike celých čísiel a interpretácia komplexných čísiel ako bodov v rovine sa dnes už široko používa, pohovoríme si v posledných dvoch častiach o týchto faktoch trochu podrobnejšie. Záverom len poznamenajme, že pomenovanie *komplexné číslo* pochádza tiež od Gaussa.

Aritmetika Gaussových celých čísiel. V tejto časti naším cieľom bude ukázať, že základnú vetu aritmetiky, podľa ktorej *každé prirodzené číslo* > 1 *sa dá jednoznačne napísať ako súčin prvočísiel,* možno celkom prirodzene preniesť aj na Gaussove celé čísla.

Aby nedošlo v ďalšej terminológii k nedorozumeniam, budeme tak, ako je to bežné v teórii algebraických čísiel, používať označenie *racionálne celé číslo* a *racionálne prvočíslo* pre obvyklé celé čísla a prvočísla. Množinu (racionálnych) celých čísiel budeme označovať Z.

Pod množinou $Z[i]$ *Gaussových celých čísiel* budeme rozumieť všetky komplexné čísla v tvare

$$a + bi,\ a, b \text{ racionálne celé čísla}$$

Zrejme *každé racionálne celé číslo je aj Gaussovým celým číslom.* Pomenovanie Gaussovo celé číslo sa historicky traduje odvtedy, čo ich použil Gauss v jednej svojej práci, ktorá sa týkala niektorých problémov teórie čísiel.

Vzhľadom na obvyklé sčítanie a násobenie komplexných čísiel je $Z[i]$ *komutatívny obor integrity* (podobne ako Z). Z tohto dôvodu môžeme v $Z[i]$ definovať pojem *deliteľnosti*. Ak $\alpha, \beta \neq 0$ sú dve Gaussove celé čísla, tak hovoríme, že β delí α, ak existuje Gaussovo celé číslo γ, pre ktoré $\alpha = \beta\gamma$. Ďalej GAUSS postrehol, že v okruhu $Z[i]$ možno prirodzene definovať pojem *prvočísla*, a že platí veta o jednoznačnosti rozkladu Gaussových celých čísiel na tieto prvočísla. Pritom niektoré racionálne prvočísla, napr. 3, 7, zostanú prvočíslami aj v $Z[i]$, zatiaľ čo napr. 5, 13 už nie.

Základná veta aritmetiky tak, ako sme ju citovali v úvode tejto časti, je tvrdením o prirodzených číslach, lenže pojem prirodzeného čísla v podstatnej miere závisí od usporiadania množiny (racionálnych) celých čísiel. Na druhej strane, množinu komplexných čísiel nevieme „slušne" usporiadať, a preto sa pokúsime preformulovať základnú vetu aritmetiky iným spôsobom, hoci *každé (racionálne) celé číslo rôzne od* 0 *a* ± 1 *môžeme napísať ako súčin prvočísiel jednoznačne, až na znamienko pri jednotlivých činiteľoch*, napr. $-6 = -2 \cdot 3 = 2 \cdot (-3)$. Poslednú prekážku, ktorú potrebujeme odstrániť, je pojem znamienka v poslednom tvrdení. K tomu nám pomôže nasledujúci pojem. Dva prvky a, b nejakého číselného systému nazývame *asociované*, ak súčasne a delí b a b delí a. Nie je ťažké dokázať, že relácia „byť asociovaný" je reláciou ekvivalencie a k tomu, aby sme určili triedu prvkov asociovaných s daným prvkom, nám stačí zistiť všetky tzv. jednotky (nestotožňovať ich s jednotkovým prvkom z teórie okruhov alebo grúp). Pod *jednotkou* rozumieme taký prvok, ktorý delí všetky ostatné prvky uvažovaného systému. Menovite platí (dokážte): *prvky* a, b *sú asociované práve vtedy, ak* $a = \varepsilon b$, *kde* ε *je jednotka.* Pretože v okruhu racionálnych celých čísiel jedinými jednotkami sú čísla $+1$ a -1, môžeme základnú vetu aritmetiky konečne preformulovať do pre nás použiteľnej formy: *každé racionálne celé číslo rôzne od* 0 *a* ± 1 *môžeme až na asociovanosť jednoznačne vyjadriť ako súčin racionálnych prvočísiel.*

Obráťme teraz našu pozornosť ku *Gaussovým celým číslam.* Veľmi dôležitým pojmom v teórii Gaussových celých čísiel (a vôbec v teórii algebraických čísiel) je pojem normy. Názov norma pochádza tiež od Gaussa. Pod *normou* $N(\alpha)$ čísla

$\alpha \in Z[i]$ rozumieme racionálne celé číslo $N(\alpha) = \alpha \,.\, \bar{\alpha} = |\alpha|^2$. Norma má dôležitú vlastnosť, je *multiplikatívna*, t. j. $N(\alpha \,.\, \beta) = N(\alpha) \,.\, N(\beta)$. Analogicky ako v prípade racionálnych celých čísiel, za jednotky prehlásime tie $\varepsilon \in Z[i]$, pre ktoré $\varepsilon | \alpha$ pre každé $\alpha \in Z[i]$. Vzhľadom na spomínanú multiplikatívnosť normy ľahko dokážeme, že: *norma jednotky je 1 a každé* $\alpha \in Z[i]$, *pre ktoré* $N(\alpha) = 1$, *je jednotka.* Odtiaľ hneď dostávame, že jednotkami v $Z[i]$ sú práve tieto štyri čísla: $1, -1, i, -i$.

Pod *prvočíslom* v $Z[i]$ budeme rozumieť číslo π, ktoré nie je 0 ani jednotka a ktorého jedinými deliteľmi sú čísla asociované s ním samým a s 1, t. j. ktorého všetky delitele v $Z[i]$ sú

$$1, -1, i, -i, \pi, -\pi, i\pi, -i\pi$$

Zrejme, ak π je prvočíslo v $Z[i]$, tak aj všetky s ním asociované čísla v $Z[i]$ sú prvočísla. Dôležité je nasledujúce jednoduché tvrdenie, ktorého dôkaz prenechávame čitateľovi: *Gaussove celé číslo, ktorého norma je racionálne prvočíslo, je prvočíslo.* Takto napr. $N(2+i) = 5$, a teda $2+i$ je prvočíslo v $Z[i]$, z čoho okamžite (vzhľadom na definíciu normy) dostávame, že 5 nie je prvočíslo v $Z[i]$. Pretože norma je nezáporné celé číslo, tak indukciou, podobne ako v prípade racionálnych celých čísiel, môžeme dokázať, že každé Gaussovo celé číslo je deliteľné aspoň jedným prvočíslom zo $Z[i]$. Okamžitý dôsledok tohto tvrdenia je skutočnosť, že *každé Gaussove celé číslo sa dá napísať ako súčin prvočísiel* (dokážte). K tomu, aby sme boli schopní dokázať základnú vetu aritmetiky Gaussových celých čísiel, nám už chýba len jediný krok, nájsť a dokázať analóg *algoritmu o delení*, ktorý je podstatou Euklidovho algoritmu (porovnaj Znám, Š.: *Kapitoly z teórie čísiel.* Mat. obzory 3, 4). Čitateľ už iste tuší jeho tvar: *ku každým dvom číslam* $\alpha, \beta \in Z[i]$, $\beta \neq 0$, *existujú* $\gamma, \delta \in Z[i]$ *tak, že*

$$\alpha = \gamma\beta + \delta, \text{ pričom } N(\delta) < N(\beta)$$

Načrtnime dôkaz. Pretože $\beta \neq 0$, tak $\frac{\alpha}{\beta} = a + bi$ (a, b racionálne čísla). Nech x, y sú racionálne celé čísla, pre ktoré $|a - x| \leqq \frac{1}{2}$, $|b - y| \leqq \frac{1}{2}$. Potom

$$\left|\frac{\alpha}{\beta} - (x + iy)\right| = \left|(a - x) + i(b - y)\right| = \{(a - x)^2 + (b - y)^2\}^{\frac{1}{2}} \leqq \frac{1}{\sqrt{2}}$$

Nakoniec položme $\gamma = x + iy$ a $\delta = \alpha - \gamma\beta$. Potom $|\alpha - \gamma\beta| \leqq \frac{1}{\sqrt{2}} |\beta|$ a po umocnení na druhú máme $N(\delta) = \leqq \frac{1}{2} N(\beta) < N(\beta)$.

Z tohto algoritmu o delení dostaneme analóg *Euklidovho algoritmu: Pre každé dve čísla* $\gamma, \gamma_1 \in Z[i]$, $\gamma_1 \neq 0$, *máme*

$$\gamma = \alpha\gamma_1 + \gamma_2, \qquad N(\gamma_2) < N(\gamma_1).$$

Ak $\gamma_2 \neq 0$, *tak ďalej*

$$\gamma_1 = \alpha_1\gamma_2 + \gamma_3, \qquad N(\gamma_3) < N(\gamma_2)$$

atď. Pretože $N(\gamma_1), N(\gamma_2), \ldots$ je klesajúca postupnosť nezáporných celých čísiel, tak musí existovať n, pre ktoré $N(\gamma_{n+1}) = 0$, t. j.

$$\gamma_{n-2} = \alpha_{n-2}\gamma_{n-1} + \gamma_n, \qquad N(\gamma_n) < N(\gamma_{n-1})$$
$$\gamma_{n-1} = \alpha_{n-1}\gamma_n$$

Podobne ako v prípade racionálnych celých čísiel sa môžeme presvedčiť, že γ_n delí aj γ aj γ_1, a že každý spoločný deliteľ čísiel γ, γ_1 delí aj γ_n. V okruhu racionálnych celých čísiel vieme, že posledný nenulový zvyšok v Euklidovom algoritme je najväčší spoločný deliteľ (n. s. d.) východiskových čísiel. V okruhu racionálnych celých čísiel je najväčší spoločný deliteľ definovaný ako najväčší zo spoločných deliteľov daných čísiel. Touto cestou by sme mohli postupovať aj v $Z[i]$, t. j. za n. s. d. čísiel α, β prehlásiť toho ich spoločného deliteľa, ktorý má najväčšiu normu. No pre ďalšie zovšeobecnenia je vhodnejšia nasledujúca definícia, ktorá je ekvivalentná so spomínanou v prípade Z a $Z[i]$: *pod n. s. d. čísiel* α, $\beta \in Z[i]$ *rozumieme také číslo* (α, β) *zo* $Z[i]$, *pre ktoré*

$$(\alpha, \beta) | \alpha, \qquad (\alpha, \beta) | \beta$$

a

$$ak\ \delta | \alpha, \delta | \beta, tak\ \delta | (\alpha, \beta)$$

Nie v každom okruhu môžeme zabezpečiť ku každým dvom prvkom n. s. d. Ale zo skutočnosti, že v $Z[i]$ možno uskutočniť Euklidov algoritmus, dostaneme, že v $Z[i]$ ku každým dvom prvkom existuje ich n. s. d., menovite $(\gamma, \gamma_1) = \gamma_n$. Opäť prenecháme čitateľovi dokázať, že *v* $Z[i]$ *je n. s. d. určený až na asociovanosť jednoznačne*. V tomto momente, úplne tým istým postupom ako v prípade

racionálnych celých čísiel, môžeme dokázať: ak π je prvočíslo v $Z[i]$ a $\pi|\alpha\beta$, tak buď $\pi|\alpha$, alebo $\pi|\beta$. V dôsledku posledného tvrdenia je dôkaz jednoznačnosti v základnej vete aritmetiky Gaussových celých čísiel jednoduchou záležitosťou: *každé Gaussove celé číslo rôzne od nuly a jednotiek sa dá až na asociovanosť jednoznačne napísať ako súčin prvočísiel.*

Zaujímavá je aj otázka, ktoré čísla v $Z[i]$ sú prvočísla. Prirodzene, ak nejaké racionálne celé číslo je prvočíslo v $Z[i]$, tak je prvočíslo aj v Z. Na druhej strane, *každé prvočíslo π v $Z[i]$ je deliteľom práve jedného racionálneho prvočísla.* Toto vyplýva z toho, že každé π delí aspoň jedno prirodzené číslo, menovite svoju normu a najmenšie prirodzené číslo s touto vlastnosťou je hľadané racionálne prvočíslo. Z práve uvedeného tvrdenia vyplýva, že *všetky prvočísla v $Z[i]$ dostaneme faktorizáciou racionálnych prvočísiel.* Bez dôkazu uvedieme toto tvrdenie o prvočíslach v $Z[i]$. *Prvočísla v $Z[i]$ sú:*

a) $1+i$ *a s ním asociované čísla,*

b) *racionálne prvočísla v tvare* $4n+3$ *a čísla s nimi asociované,*

c) *všetky faktory* $a+bi$ *racionálnych prvočísiel v tvare* $4n+1$.

Ako vedľajší produkt dôkazu posledného tvrdenia sa obyčajne uvádza toto zaujímavé konštatovanie: *každé racionálne prvočíslo tvaru* $4n+1$ *sa dá napísať ako súčet dvoch štvorcov.* Dôkazy posledných tvrdení sú jednoduché a čitateľ ich môže nájsť napr. v monografii HARDY — WRIGHT: *An introduction to the theory of numbers.*

Dnes už poznáme asymptotický zákon rozloženia prvočísiel v $Z[i]$ a mnohé iné výsledky, ktoré boli motivované pozoruhodnými podobnosťami medzi Z a $Z[i]$. Niektoré problémy v Z sa dajú previesť na problémy v $Z[i]$; tak napr. nevieme, či existuje nekonečne veľa racionálnych prvočísiel tvaru n^2+1. Zrejme toto je ekvivalentné s tým, či existuje nekonečne veľa Gaussových prvočísiel v tvare $n+i$.

Už podľa Gaussa zavedenie Gaussových celých čísiel „nekonečne" rozšírilo oblasť teórie čísiel. V skutočnosti boli v tejto myšlienke utajené zárodky teórie číselných telies, ktorá sa potom začala rozvíjať v druhej polovici 19. storočia najmä v prácach Dirichleta a Kummera, z ktorej niektorých výsledkov sa dožil ešte sám Gauss.

Na záver len pripomeňme, že uvedené analógie medzi Z a $Z[i]$ nie sú celkom náhodné. Ich spoločné korene treba hľadať v skutočnosti, že ako v Z, aj v $Z[i]$ môžeme použiť Euklidov algoritmus. *Každý okruh, v ktorom možno použiť Euklidov algoritmus, je okruh hlavných ideálov a v každom okruhu hlavných ideálov platí veta o jednoznačnosti rozkladu na prvočinitele.*

Komplexné čísla v elementárnej geometrii. Rozvoj teórie komplexných čísiel sa v podstatnej miere spájal s využitím interpretácie komplexných čísiel ako bodov

v rovine. Túto interpretáciu nachádzame prvýkrát u dánskeho zememerača G. WESSELA.

Majme v rovine daný karteziánsky súradnicový systém. Bodu M so súradnicami x, y priraďme komplexné číslo $z = x + iy$. Takto priradené komplexné číslo z budeme nazývať *komplexná súradnica* bodu M. Uvedené priradenie medzi bodmi a komplexnými súradnicami je vzájomne jednoznačné, a preto môžeme bod stotožňovať s jeho komplexnou súradnicou. Prechod od komplexnej súradnice ku karteziánskym súradniciam je daný vzťahmi

$$x = \frac{1}{2}(z - \bar{z}), \qquad y = \frac{1}{2}(\bar{z} - z)$$

Zrejme vzdialenosť dvoch bodov so súradnicami z_1, z_2 je daná absolútnou hodnotou $|z_1 - z_2|$ rozdielu $z_1 - z_2$. Ďalej orientovaný uhol medzi dvoma priamkami, ktoré sa pretínajú v začiatku súradnicového systému a prechádzajú bodmi z_1 *a* z_2, sa rovná

$$\operatorname{Arg} z_1 - \operatorname{Arg} z_2 = \operatorname{Arg} \frac{z_1}{z_2},$$

kde $\operatorname{Arg} z$ označuje amplitúdu komplexného čísla z. V prípade, keď sa tieto priamky pretínajú v bode z_0, rovnobežným posunutím $z - z_0$ prevedieme z_0 do začiatku súradnicového systému. Z predchádzajúcej úvahy dostaneme, že *orientovaný uhol medzi priamkami* z_0z_1 *a* z_0z_2 *je daný vzťahom*

$$\operatorname{Arg} \frac{z_2 - z_0}{z_1 - z_0}$$

Odtiaľto okamžite dostaneme, že *tri body* z_0, z_1, z_2 *ležia na jednej priamke, ak* $\operatorname{Arg} \frac{z_2 - z_0}{z_1 - z_0} = 0$, *alebo* π, alebo inými slovami, *ak* $\frac{z_2 - z_0}{z_1 - z_0}$ *je reálne číslo.* Preto priamka daná bodmi z_1, z_2 je množina bodov z, pre ktoré

$$\frac{z - z_2}{z_1 - z_2} = \overline{\left(\frac{z - z_2}{z_1 - z_2}\right)}$$

Jednoduchými úpravami dostávame

$$(\bar{z}_1 - \bar{z}_2)z - (z_1 - z_2)\bar{z} + (z_1\bar{z}_2 - \bar{z}_1z_2) = 0$$

alebo

$$Bz + \bar{B}\bar{z} + C = 0,\ C \text{ je rýdzoimaginárne číslo.}$$

Naopak, každá rovnica tohto typu je rovnicou nejakej priamky, a to priamky, ktorá prechádza cez body z_1, z_2, pre ktoré $z_1 - z_2 = \bar{B}$ a $z_1\bar{z}_2 - \bar{z}_1 z_2 = C$. Smerový uhol priamky danej predchádzajúcou rovnicou je $\operatorname{Arg} B$ a jej vzdialenosť od začiatku súradnicového systému je $\frac{|C|}{2|B|}$ (dokážte!).

K danej štvorici bodov (alebo čísiel) z_0, z_1, z_2, z_3 priradené číslo

$$W(z_0, z_1, z_2, z_3) = \frac{z_0 - z_2}{z_1 - z_2} : \frac{z_0 - z_3}{z_1 - z_3}$$

budeme nazývať *dvojpomer* týchto bodov (dvojpomer sa obvykle v projektívnej geometrii definuje len pre štyri kolineárne body, no napriek tomu sme si vypožičali tento pojem).

Nájdime teraz rovnicu kružnice, ktorá prechádza tromi bodmi z_0, z_1, z_2. Bod z_3 leží na kružnici určenej bodmi z_0, z_1, z_2, ak rozdiel orientovaných uhlov medzi dvojicami priamok z_0z_2, z_1z_2 a z_0z_3, z_1z_3 je 0 alebo π (prečo?). Tento rozdiel sa rovná

$$\operatorname{Arg}\frac{z_0 - z_2}{z_1 - z_2} - \operatorname{Arg}\frac{z_0 - z_3}{z_1 - z_3} = \operatorname{Arg}\left(\frac{z_0 - z_2}{z_1 - z_2} : \frac{z_0 - z_3}{z_1 - z_3}\right)$$

To znamená, že *štyri body ležia na jednej kružnici, ak ich dvojpomer je reálne číslo.* Preto podobne ako v prípade priamky dostaneme, že rovnica kružnice danej bodmi z_1, z_2, z_3 je

$$W(z, z_1, z_2, z_3) = \overline{W(z, z_1, z_2, z_3)}$$

alebo po úprave

$$Az\bar{z} + Bz - \bar{B}\bar{z} + C = 0$$

kde A, C sú rýdzoimaginárne čísla. (Ak $A = 0$, tak dostaneme rovnicu priamky.) Naopak, každá takáto rovnica, ktorej vyhovuje aspoň jeden bod v rovine, je rovnicou niektorej kružnice.

V nasledujúcich riadkoch ukážeme, ako nám niekedy môže poslúžiť aj ten

jednoduchý aparát, ktorý sme doteraz zaviedli na riešenie mnohých úloh z geometrie.

Majme v rovine štyri kružnice K_1, K_2, K_3 a K_4. Nech z_1, w_1 sú priesečníky kružníc K_1 a K_2, z_2, w_2 priesečníky K_2 s K_3, z_3, w_3 kružníc K_3 a K_4 a z_4, w_4 kružníc K_4 a K_1. Ak body z_1, z_2, z_3, z_4 ležia na jednej kružnici (alebo priamke), tak aj w_1, w_2, w_3, w_4 ležia na jednej kružnici (alebo priamke).

Vzhľadom na naše predpoklady, každý z nasledujúcich dvojpomerov je reálne číslo

$$W(z_1, w_2, z_2, w_1), \quad W(z_2, w_3, z_3, w_2), \quad W(z_3, w_4, z_4, w_3), \quad W(z_4, w_1, z_1, w_4).$$

Preto je reálnym číslom aj súčin

$$W(z_1, z_3, z_2, z_4) \cdot W(w_1, w_3, w_2, w_4) =$$

$$= \frac{W(z_1, w_2, z_2, w_1) \cdot W(z_3, w_4, z_4, w_3)}{W(z_2, w_3, z_3, w_2) \cdot W(z_4, w_1, z_1, w_4)}$$

Potom z reálnosti $W(z_1, z_3, z_2, z_4)$ vyplýva, že aj $W(w_1, w_3, w_2, w_4)$ je reálne číslo, čo dokazuje naše tvrdenie.

Ako posledný príklad si dokážeme *vetu o mocnosti bodu ku kružnici.* Nech K je kružnica daná rovnicou

$$Az\bar{z} + Bz - \bar{B}\bar{z} + C = 0, \qquad A, C \text{ sú rýdzoimaginárne}$$

Nech p je priamka, ktorá prechádza začiatkom súradnicového systému O a pretína K v bodoch z_1, z_2. Ukážme, že súčin orientovaných dĺžok úsečiek $\bar{O}z_1$, $\bar{O}z_2$ spĺňa

$$|\overrightarrow{Oz_1}| \cdot |\overrightarrow{Oz_2}| = \frac{C}{A}$$

t. j. je konštantný pre ľubovoľnú polohu priamky p. Body z_1, z_2 ležia na jednej priamke, ktorá prechádza začiatkom súradnicového systému, preto $\operatorname{Arg} z_2 = \operatorname{Arg} z_1$, $\operatorname{Arg} \bar{z}_2 = -\operatorname{Arg} z_1$, ak začiatok súradnicového systému je vonkajším bodom kružnice K; v opačnom prípade máme $\operatorname{Arg} z_2 = \operatorname{Arg} z_1 + \pi$, $\operatorname{Arg} \bar{z}_2 = -\operatorname{Arg} z_1 - \pi$. Súčin $z_1\bar{z}_2$ je v obidvoch prípadoch reálne číslo:

$$z_1\bar{z}_2 = k, \quad \bar{z}_1 z_2 = \overline{z_1\bar{z}_2} = \bar{k} = k$$

Na druhej strane z_1, z_2 sú body kružnice K, a preto

$$Akz_1 + Bz_1z_2 - \bar{B}k + Cz_2 = 0$$

a

$$Akz_2 + Bz_1z_2 - \bar{B}k + Cz_1 = 0$$

Odčítaním dostaneme:

$$Ak(z_1 - z_2) - C(z_1 - z_2) = 0$$

Ak $z_1 \neq z_2$, tak $k = \frac{C}{A}$.

Čitateľ sa už ľahko presvedčí, že súčin $z_1\bar{z}_2$ sa rovná súčinu orientovaných dĺžok $|\overrightarrow{Oz_1}|$ a $|\overrightarrow{Oz_2}|$.

Pred chvíľou sme použili predpoklad, že $z_1 \neq z_2$. No ak $z_1 = z_2$, tak $|\overrightarrow{Oz_1}| \,.\, |\overrightarrow{Oz_2}| = |\overrightarrow{Oz_1}|^2$ a aj $|\overrightarrow{Oz_1}|^2 = \frac{C}{A}$. Poslednú rovnosť dostaneme z toho, že $|\overrightarrow{Oz_1}|^2$ je limita konštantného súčinu $|\overrightarrow{Oz_1}| \,.\, |\overrightarrow{Oz_2}|$, ak z_1 a z_2 sa blížia k dotykovému bodu niektorej z dotyčníc z O ku K.

Prípad, keď bod, ktorého mocnosť ku K vyšetrujeme, nie je začiatkom súradnicového systému, prenechávame ako príklad na riešenie pre čitateľa.