OKRUH S NEJEDNOZNAČNÝM ROZKLADOM

ZOLTÁN ZALABAI, Nitra

Žiaci stredných škôl poznajú vetu o rozklade prirodzeného čísla $n \geqq 2$ na súčin prvočísel. Je im známe, že ak prvočíslo delí súčin, potom delí aspoň jedného činiteľa. Vedia vypočítať najväčšieho deliteľa dvoch prirodzených čísel.

S podobnou problematikou a s podobnými výsledkami sa stretávame napr. v okruhu $(Z, +, \cdot)$ celých čísel, v okruhu $R[x]$ (okruh polynómov s reálnymi koeficientmi) a v okruhu tzv. Gaussových celých čísel (množina všetkých čísel tvaru $a + bi$, kde $a, b \in Z$, spolu s operáciou sčítania a násobenia komplexných čísel). Túto problematiku žiak strednej školy je schopný naštudovať. Výsledky v uvedených okruhoch sú však v podstate rovnaké. Žiakom sa preto toto všetko bude zdať samozrejmým. „Nič nového. Všade platia rovnaké vety."

Preto je veľmi poučné študovať okruhy, ktoré spomínané vlastnosti nemajú.

Uvediem štyri príklady. Z nich prvé tri dajú v podstate rovnaké výsledky. Okruh v príklade 4 však už takéto vlastnosti nemá. Príklad 4 tvorí vlastne jadro tohto článku. Chcem tu ukázať, že rozklad na súčin tzv. ireducibilných prvkov nemusí byť jednoznačný; ak ireducibilný prvok delí súčin, nemusí deliť ani jedného činiteľa; ďalej, dva prvky okruhu, ktoré majú spoločných deliteľov, nemusia mať najväčšieho spoločného deliteľa.

V príkladoch 1, 2, 3 chcem zvýrazniť základný význam Euklidovho algoritmu postupného delenia.

Teraz ešte uvediem definície tých pojmov, ktoré sú v ďalších úvahách osobitne dôležité.

Hovoríme, že prvok a okruhu A *delí* prvok $b \in A$, ak existuje také $c \in A$, že $b = c \cdot a$. (Označenie: $a|b$.) Hovoríme tiež, že prvok a je *deliteľom* b.

V tomto zmysle chápeme aj delitele jednotky.

Prvok a okruhu A nazývame *asociovaným* k prvku $b \in A$, ak platí $b = a \cdot \varepsilon$, kde ε je deliteľ jednotky.

Prvok $a \neq 0$ okruhu A nazývame *ireducibilným prvkom*, keď nie je deliteľom jednotky a keď každý jeho deliteľ je s ním alebo asociovaný, alebo je deliteľom jednotky.

Prvok d okruhu A je *najväčším spoločným deliteľom* prvkov $a, b \in A$, ak:

1. $d|a \wedge d|b$ (d je spoločným deliteľom prvkov a, b).
2. $(d'|a \wedge d'|b / \Rightarrow d'|d$. (Ak d' je spoločný deliteľ prvkov a, b, potom $d'|d$. Označenie: $d = (a, b)$).

1. príklad. Uvažujme o okruhu $(Z, +, \cdot)$ celých čísel. Najväčší spoločný deliteľ čísel a, b (stačí sa obmedziť na prirodzené čísla) vypočítame napr. pomocou Euklidovho algoritmu postupného delenia. Dostaneme konečnú sústavu rovností. Na ilustráciu uveďme prípad, keď sa sústava skladá zo štyroch rovností:

$$\begin{aligned} a &= b \cdot q_0 + r_0 \\ b &= r_0 \cdot q_1 + r_1 \\ r_0 &= r_1 \cdot q_2 + r_2 \\ r_1 &= r_2 \cdot q_3 \end{aligned} \tag{1}$$

Najväčší spoločný deliteľ d čísel a, b je posledný nenulový zvyšok. Zapíšme to v tvare $d = (a, b) = r_2$. Čísla r_0, r_1, r_2 sú prirodzené a platí: $a > b > r_0 > r_1 > r_2$. Tvoria klesajúcu postupnosť.

Zo sústavy (1) môžeme vyjadriť $r_2 (= d)$ pomocou čísel a, b.

Dostaneme teda takýto výsledok

$$ax + by = d \quad (x, y \in Z) \tag{2}$$

Ak napr. $(a, b) = 1$ — čísla sú nesúdeliteľné, potom

$$ax + by = 1 \quad (x, y \in Z) \tag{3}$$

V ďalšom uvedieme niekoľko základných viet.

Veta 1. Ak a, b sú nesúdeliteľné a súčasne $a|bc$ („a delí súčin bc"), potom $a|c$ $(a, b, c \in Z)$.

Stačí rovnosť (3) násobiť číslom c a použiť predpoklad $a|bc$, čiže $bc = az$ $(z \in Z)$.

Veta 2. Ak prvočíslo p delí súčin ab, potom p delí aspoň jedno z čísel a, b $(a, b, p \in Z)$.

V prípade $(p, a) = 1$ ide o dôsledok vety 1. Ak $(p, a) > 1$, potom číslo a musí byť celočíselným násobkom čísla p.

Veta 3. (Fundamentálna veta aritmetiky celých čísel.) Každé zložené číslo sa dá vyjadriť ako súčin konečného počtu ireducibilných prvkov okruhu Z. Ak odhliadneme od poradia a asociovanosti faktorov, je tento rozklad jednoznačný.

K dôkazu sa použije veta 2.

Poznámka 1. Číslo 1 môžeme zapísať v tvare súčinu dvoch celých čísel iba takto: $1 = 1 \cdot 1 = (-1) \cdot (-1)$. Čísla 1 a -1 sú deliteľmi čísla 1 (delitele jednotky). Číslo $\varepsilon \cdot a$, kde ε je deliteľ jednotky, nazývame asociovaným k číslu a. Vzájomne asociované prvky (rôzne) v uvedenom príklade tvoria dvojice: $(2, -2)$, $(6, -6)$ atď. — líšia sa práve znamienkami.

Poznámka 2. Podľa vety 3 rozklady môžu mať napr. takýto tvar:

$$\begin{aligned} a &= 2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 = \\ &= (-2) \cdot 5 \cdot 7 (-13) \cdot 17 = \\ &= 2 \cdot (-5) \cdot 7 \cdot 13 \cdot (-17) = \ldots \end{aligned}$$

Sú to *rovnaké* rozklady, počet rôznych tvarov je konečný. Ak v jednom vystupuje napr. „17", potom v ostatných nájdeme 17 alebo -17.

Poznámka 3. Uvedené vety (1., 2., 3.) majú vlastne svoj *základ* v Euklidovom algoritme [1].

2. príklad. Uvažujme o okruhu $R[x]$ (okruh polynómov s reálnymi koeficientmi).

Euklidov algoritmus postupného delenia dáva v podstate ten istý výsledok, ako v 1. príklade (1). Posledný nenulový zvyšok je najväčší spoločný deliteľ pôvodných daných dvoch polynómov. Namiesto čísel r_0, r_1, r_2 v rovnosti (1) tu dostaneme polynómy, ktorých stupne tvoria klesajúcu postupnosť. Dostaneme teda aj tu konečnú sústavu rovností. Aj tu platia vety, ktoré svojím vnútorným obsahom nám pripomínajú vety 1., 2., 3. Príslušné dôkazy stačí iba vhodne *prepísať*.

Poznámka 4. V tomto okruhu existuje nekonečne veľa deliteľov jednotky. Sú to práve všetky nenulové reálne čísla. K polynómu preto existuje nekonečne veľa asociovaných prvkov.

Poznámka 5. Rovnaké rozklady môžu mať nekonečne veľa rôznych tvarov. Napr.

$$f(x) = (2x+1)(x^2+1) =$$
$$= \left(x + \frac{1}{2}\right)(2x^2+2) =$$
$$= (10x+5)\left(\frac{x^2}{5} + \frac{1}{5}\right) = \ldots$$

Poznámka 6. Základom uvedených výsledkov je aj tu Euklidov algoritmus.

3. príklad. Množina všetkých čísel tvaru $a+bi$ $(a, b \in Z)$ spolu s operáciou sčítania a násobenia komplexných čísel tvorí okruh. Patria sem napr. čísla $2+3i$; $8-7i$; 5 (čiže $5+0i$); $9i$; 0;...

Zavedieme pojem *normy* čísla $\alpha = a+bi$. Je to nezáporné celé číslo $N(\alpha) = a^2+b^2$. Priamym výpočtom zistíme, že $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$.

Ak α a $\beta \neq 0$ sú dve ľubovoľné čísla uvažovaného okruhu (dve tzv. G. čísla — Gaussove celé čísla), potom existujú dve také G. čísla μ a ν, že

$$\alpha = \beta \cdot \mu + \nu, \quad \text{kde} \quad N(\nu) < N(\beta)$$

Tieto čísla nájdeme takto: podiel $\alpha : \beta = A + Bi$, kde A, B sú racionálne čísla. Zvolíme si racionálne celé čísla x, y také, aby platilo:

$$|A - x| \leqq \frac{1}{2}$$

$$|B - y| \leqq \frac{1}{2}$$

Potom $\mu = x + iy$, $\nu = \alpha - \mu \cdot \beta$

Z hľadiska Euklidovho algoritmu norma má také postavenie ako *absolútna hodnota celého čísla* v príklade 1 a *stupeň polynómu* v príklade 2. Euklidov algoritmus postupného delenia dáva konečnú sústavu rovností. Platia tu vety analogické k vetám 1, 2, 3.

(Príslušnú kompletnú teóriu nájde čitateľ napr. v knihe [1] na s. 101 až 108).

Poznámka 7. Existujú tu práve štyri delitele jednotky: 1, -1, i, $-i$. Teda asociované prvky (rôzne) tvoria štvorice.

Poznámka 8. Napríklad čísla $1+2i$, $1+i$ sú ireducibilné prvky okruhu. Rovnaké rozklady majú konečný počet rôznych tvarov.

Príklad rozkladu: $=(1+i)(1+2i)=(i-1)(-i+2)=\ldots$

4. príklad. Množina všetkých čísel tvaru $a+b\sqrt{3}i$ $(a, b \in Z)$ spolu s operáciou sčítania a násobenia komplexných čísel tvorí okruh. Zavedieme pojem normy: $N(a+b\sqrt{3}i)=a^2+3b^2$. Platí: $N(\alpha\cdot\beta) = N(\alpha)\cdot N(\beta)$. Môžeme sa o tom presvedčiť priamym výpočtom. Norma je teda nezáporné celé číslo, ale nie všetky nezáporné celé čísla sú normami. Tak napr. neexistuje číslo, ktorého norma je 2. Totiž pre nijaké a, b celé a^2+3b^2 nerovná sa dvom. V uvedenom okruhu existujú práve dva delitele jednotky: 1; -1. Zistíme to napr. takto:

Nech pre α, β platí $1=\alpha\cdot\beta$. Pre príslušné normy dostaneme:

$$N(1)=N(\alpha)\cdot N(\beta), \quad \text{čiže}$$
$$1=N(\alpha)\cdot N(\beta).$$

Normy čísel α, β sa musia rovnať 1. Čísla, ktorých norma je 1, sú práve 1 a -1.

Číslo $1+\sqrt{3}i$ je ireducibilný prvok okruhu.

Skutočne: nech

$$1+\sqrt{3}i=\alpha\cdot\beta.$$

Pre normy platí:

$$N(1+\sqrt{3}i)=N(\alpha)\cdot N(\beta), \quad \text{čiže}$$
$$4=N(\alpha)N(\beta).$$

Dostali sme vlastne rozklad čísla 4 na súčin prirodzených čísel. Súčiny $1\cdot 4$ a $4\cdot 1$ vedú k triviálnym rozkladom čísla $1+\sqrt{3}i$. Prípad $2\cdot 2$ nenastane, pretože neexistuje číslo s normou 2. Teda číslo $1+\sqrt{3}i$ má iba triviálne rozklady, teda i triviálnych deliteľov. Je to skutočne prvok ireducibilný.

Podobne by sme dokázali, že aj čísla $1-\sqrt{3}i$ a 2 sú ireducibilnými prvkami okruhu.

Zrejme platí:

$$4 = \frac{2 \cdot 2}{(1+\sqrt{3}i)(1-\sqrt{3}i)} \tag{4}$$

Ide tu o dva *rôzne rozklady* čísla 4 na súčin ireducibilných prvkov. Činitele nie sú vzájomne asociované. (Vzájomne asociované rôzne prvky tvoria dvojice a líšia sa práve znamienkom.)

Základná veta aritmetiky o jednoznačnosti rozkladu na súčin ireducibilných prvkov tu teda *neplatí.*

Zo vzťahu (4) vyplýva:

$$2 \cdot 2 = (1+\sqrt{3}i)(1-\sqrt{3}i)$$

teda napr. *prvok 2 delí súčin. Nedelí však ani jedného činiteľa.*

Ak by totiž $2|(1+\sqrt{3}i)$, muselo by existovať také číslo $x+y\sqrt{3}i$ $(x, y \in Z)$, že

$$2 \cdot (x+y\sqrt{3}i) = 1+\sqrt{3}i$$

Z tejto rovnosti dvoch komplexných čísel by sme dostali, že $2x = 1$, čiže $x = \frac{1}{2}$. Čo je v rozpore s tým, že $x \in Z$.

V prvých troch príkladoch sme vždy vychádzali z Euklidovho algoritmu postupného delenia. Výsledok bol reprezentovaný konečnou sústavou rovností (pozri (1)). Položme si otázku. Je tu možné *realizovať* Euklidov algoritmus v takom duchu, ako v prvých troch príkladoch? Odpoveď je jednoznačná: nie. Lebo ak by sme mohli napísať takú konečnú sústavu rovností ako (1), potom by sme z toho dokázali aj platnosť vety 2. a vety 3., ktoré však — ako sme to videli — tu neplatia.

Na základe toho, čo sme práve konštatovali, zdá sa, že najväčší spoločný deliteľ dvoch čísel okruhu by nemusel vždy existovať. V príkladoch 1., 2., 3. to bol totiž *posledný nenulový zvyšok.*

Uvažujme o množine všetkých spoločných deliteľov čísel $2+2\sqrt{3}i$ a 4. Najprv treba určiť množiny všetkých deliteľov daných prvkov.

Ak číslo α, resp. β je deliteľom čísla $2+2\sqrt{3}i$, potom

$$2+2\cdot\sqrt{3}i=\alpha\cdot\beta$$

Norma ľavej strany je 16, preto

$$16=N(\alpha)\cdot N(\beta)$$

Číslo 16 môžeme rozložiť na súčiny dvoch prirodzených čísel takto:

$$16=1\cdot 16=16\cdot 1=2\cdot 8=8\cdot 2=4\cdot 4.$$

Normy deliteľov teda sú: 1, 16, 4. Aj norma čísla 4 je 16, deliteľom čísla $2+2\sqrt{3}i$ však zrejme nie je.

(Prípad súčinu $2\cdot 8$ neprichádza do úvahy — norma čísla okruhu sa nemôže rovnať dvom.) Hľadaná množina je táto:

$$\{1,-1,2,-2,2+2\cdot\sqrt{3}i,-2-2\sqrt{3}i,1+\sqrt{3}i,$$
$$1-\sqrt{3}i,-1-\sqrt{3}i,-1+\sqrt{3}i\}$$

Podobným spôsobom nájdeme množinu deliteľov čísla 4. Je to:

$$\{1,-1,2,-2,4,-4,1+\sqrt{3}i,1-\sqrt{3}i,-1-\sqrt{3}i,-1+\sqrt{3}i\}$$

Teda množina všetkých spoločných deliteľov je:

$$\{1,-1,2,-2,1+\sqrt{3}i,1-\sqrt{3}i,-1-\sqrt{3}i,-1+\sqrt{3}i\}$$

Spoločných deliteľov je *veľa*, ale *najväčší spoločný deliteľ neexistuje.* Najväčší spoločný deliteľ d mal by mať túto vlastnosť: každý spoločný deliteľ delí d.

Tak napr. $-1+\sqrt{3}i$ preto nie je najväčší spoločný deliteľ, lebo neexistujú také x, $y\in Z$, aby platilo:

$$2(x+y\sqrt{3}i)=-1+\sqrt{3}i$$

Rovnako neexistujú x, $y\in Z$, aby platilo:

$$(1+\sqrt{3}i)(x+y\sqrt{3}i)=2$$

čo znamená, že ani 2 nie je najväčší spoločný deliteľ. Takisto by sme postupovali aj v ďalších prípadoch.

Poznámka 9. Rozklady $4 = 2 \cdot 2 = (-2)(-2)$ sú rovnaké. Odlišnosť sa prejavuje iba v asociovanosti faktorov.

Poznámka 10. Okruhy v príkladoch 1, 2, 3 sú tzv. euklidovské okruhy.

Literatúra

1. Schwarz, Š.: Algebraické čísla, Praha, JČMF 1950.
2. Znám, Š.: Teória čísel. 1. vyd. Bratislava, Alfa 1977.
3. Znám, Š.: Vybrané kapitoly z elementárnej teórie čísel I. Matematické obzory, 3/1973, Bratislava, Alfa 1973.
4. Znám, Š.: Vybrané kapitoly z elementárnej teórie čísel II. Matematické obzory, 4/1973. Bratislava, Alfa 1973.
5. Legéň, A.: O grupách a okruhoch III. Matematické obzory, 6/1974. Bratislava, Alfa 1974.
6. Szendrei, J.: Algebra és számelmélet. Budapest, Tankönyvkiadó, 1975.
7. Katriňák, T.—Legéň, A.: Algebra (vysokoškolské skriptá). Bratislava, ES Univerzity Komenského v Bratislave, 1977.