B: Nyní již vím, jaká jsou to čísla.
Víte to i vy?

Napišme si tabulku se dvěma sloupci, do které budeme do levého sloupce psát možné součty $a+b$ a do pravého sloupce možné hodnoty a^2+b^2 při daném součtu. Na konci ukážeme, že se můžeme omezit jen na prvních 17 řádků.Po první odpovědi .3 můžeme vyškrtnout ty hodnoty, které se v pravém sloupci vyskytnou jen jednou, takže nám zbyde tato tabulka:

8	50
9	65
10	50
11	65, 85
13	85, 125, 145
14	130, 170
15	125
16	130, 200
17	145, 185, 205
...	...

Čísla 50, 65, 85, 125 a 145 se na dalších řádcích už v pravém sloupci nevyskytnou. Po první informaci od A můžeme vyškrtnout řádky, na kterých je vpravo jen jedno číslo, tedy součty 8, 9, 10 a 15. Druhé tvrzení B vyloučí číslo 65 (součet 11) a 125 (součet 13) – tato čísla už zbyla napravo jen jednou. Druhé tvrzení A vyloučí součet 11. Po třetím výroku B vyškrtneme 85 z řádku se součtem 13 a třetí odpověď A vyloučí tento řádek úplně. Čtvrté tvrzení B ukazuje, že součet je 17, součet čtverců je 145 a hledaná čísla jsou 8 a 9.

Aby byly úvahy korektní, je potřeba ještě ukázat, že i po provedených úpravách budou na řádcích počínaje osmnáctým v pravém sloupci vždy alespoň dvě čísla. Pro součet 18 to plyne z rovnosti $11^2 + 7^2 = 13^2 + 1^2$ (na řádku 14 nám 170 zbyla). Pro součet 19 to plyne z rovnosti $8^2+11^2 = 4^2+13^2$ (na řádku 17 nám 185 zůstalo). Pro součet 20 to plyne z rovnosti $10^2 + 10^2 = 2^2 + 14^2$ (200 na řádku 16 zbyla), pro 21 z rovnosti $16^2 + 7^2 = 4^2 + 17^2$ (305 na řádku 22 jsme neškrtli – po odpovědi B proto, že 305 se pořád vpravo vyskytuje aspoň dvakrát, po odpovědi A proto, že na řádku jsou pořád aspoň dvě čísla). Druhá čísla do těchto řádků a obě do řádků se součtem aspoň 22 dostaneme použitím identity $(a+2b)^2+(2a-b)^2 = (a-2b)^2+(2a+b)^2$ pro $a \geq 7$, $b = 1, 2, 3$ a podobné úvahy (rozmyslete si detaily).

Komentáře k 6. sérii

1. úloha Dokažte, že neprázdná množina $A \subset \mathbb{Z}$ je ideálem právě tehdy, když jsou splněny následující podmínky

(i) $a, b \in A \Rightarrow a + b \in A$
(ii) $a \in A, c \in \mathbb{Z} \Rightarrow ca \in \mathbb{Z}$.

Do zadání se opět vloudila chybička. V podmínce (ii) má samozřejmě správně být $ca \in A$. To, že každý ideál splňuje podmínky (i) a (ii), není potřeba moc rozebírat. Jádro tvrzení je

tedy v opačné implikaci.

Pokud $A = \{0\}$, je zjevně $A = 0\mathbb{Z}$. Předpokládejme, že A obsahuje nějaké nenulové číslo. Kdyby bylo záporné, můžeme použít (ii) s $n = -1$; A tedy určitě obsahuje aspoň jedno kladné číslo. Označme n nejmenší takové. Snadno z (ii) odhalíme, že $n\mathbb{Z} \subseteq A$. Mějme nyní libovolné $k \in A$. Podle (ii) je $-n \in A$ a podle (i) jsou v A i všechna čísla typu $k + nj$ kde $j \in \mathbb{Z}$. Jedno z nich ale musí ležet v $\{0, 1, \ldots, n-1\}$ (zbytek k po dělení n). Protože n byl nejmenší kladný prvek A, musí to být nula. Tedy k je násobkem n, což jsme chtěli dokázat.

Úmluva: Pokud v následujícím textu řeknu "generátor ideálu A", myslím tím pro $A = \{0\}$ nulu, jinak nejmenší kladný prvek.

2. úloha Nechť $A \subset \mathbb{Z}$, $B \subset \mathbb{Z}$ jsou ideály. Potom $A+B$, $A \cdot B$ a $A \cap B$ jsou ideály. Dokažte a zjistěte, kterými celými čísly jsou tyto ideály generovány.

Je-li např. $A = \{0\}$, je $A+B = B$, analogicky pro $B = \{0\}$. Omezme se tedy na případ, kdy A a B jsou nenulové. Nechť $A = a\mathbb{Z}$, $B = b\mathbb{Z}$ a označme (a, b) největšího společného dělitele čísel a, b. Pak pro $r \in A + B$ existují $p \in A$, $q \in B$ tak, že $p + q = r$; p je násobkem a, q je násobkem b, obě jsou tedy násobkem (a, b); pak ale musí být násobkem (a, b) i jejich součet, proto $A+B \subseteq (a, b)\mathbb{Z}$. Na druhou stranu snadno ukážeme, že $A+B$ splňuje podmínky (i) a (ii) z první úlohy a například z Eukleidova algoritmu dostaneme existenci $s, t \in \mathbb{Z}$ takových, že $(a, b) = sa + tb$, dohromady dostaneme $(a, b) \in A + B$, a odtud aplikací (ii) i $(a, b)\mathbb{Z} \subseteq A + B$.

Je-li $c \in A \cdot B$, můžeme ho zapsat ve tvaru $c = (pa) \cdot (qb) = (pq)(ab) \in (ab)\mathbb{Z}$. Naopak pro $r \in (ab)\mathbb{Z}$ je $r = (a) \cdot (rb) \in A \cdot B$.

Pomocí podmínek z první úlohy snadno zjistíme, že $A \cap B$ je ideál: je-li $p, q \in A \cap B$, pak určitě $p + q \in A$ (protože p i q jsou v A) a stejně tak i $p + q \in B$, tedy $p + q \in A \cap B$; je-li $p \in A \cap B$, $k \in \mathbb{Z}$, je $kp \in A$ ($p \in A$) a $kp \in B$ ($p \in B$), tedy $kp \in A \cap B$. Je tedy podle tvrzení první úlohy $A \cap B$ ideál. Nahlédneme-li do důkazu, zjistíme, že je generovaný svým nejmenším kladným prvkem ($A \cap B = \{0\}$ právě tehdy, když $A = \{0\}$ nebo $B = \{0\}$, jinak $0 \neq ab \in A \cap B$, dále se budeme zabývat případem, kdy $a \neq 0 \neq B$). Z definice $A \cap B$ vidíme, že obsahuje právě ta čísla, která jsou násobky a i b; nejmenší takové kladné číslo je jejich nejmenší společný násobek.

3. úloha Definujme nyní podíl ideálu $A \subset \mathbb{Z}$ a celého čísla k:

$$A : k = \{l \in \mathbb{Z} : lk \in A\}.$$

a radikál ideálu

$$\sqrt{A} := \{l \in \mathbb{Z} : \text{ existuje } k \in \mathbb{N} \text{ tak, že } l^k \in A\}.$$

Dokažte, že právě definované množiny jsou ideály. Zjistěte, čím jsou generovány.

Zřejmě $\{0\} : k = \{0\}$, $A : 0 = \mathbb{Z}$ a $\sqrt{\{0\}} = \{0\}$; dále si uvědomme, že $(-n)\mathbb{Z} = n\mathbb{Z}$ a $A : (-k) = A : k$. Omezme se tedy na případ $k > 0$ a $A = a\mathbb{Z}$, $a > 0$. Mějme $k = p_1^{k_1} p_2^{k_2} p_3^{k_3} \ldots$, $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \ldots$ prvočíselné rozklady čísel k a a. Číslo $b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \ldots$ je pak prvkem A právě tehdy, když $b_i \geq a_i$ pro každé $i \in \mathbb{N}$. Prvočíselný rozklad čísla bk,

kde $b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \dots$ je $p_1^{b_1+k_1} p_2^{b_2+k_2} \dots$. Odtud už snadno nahlédneme, že $b \in A : k$ právě tehdy, když $b_i \geq c_i = \max(a_i - k_i, 0)$, tedy $A : k = c\mathbb{Z}$, kde $c = p_1^{c_1} p_2^{c_2} p_3^{c_3} \dots$.

Mějme $a = q_1^{a_1} q_2^{a_2} \dots q_r^{a_r}$, $a_i > 0$ prvočíselný rozklad a a označme $c = q_1 q_2 \dots q_r$. m označme největší z čísel a_i. Mějme $l \in c\mathbb{Z}$; exponenty u všech prvočísel q_i v prvočíselném rozkladu l budou kladné, příslušné exponenty v rozkladu l^m budou tedy aspoň m, tedy větší nebo rovné exponentům u a. Bude tedy $l \in \sqrt{A}$. Naopak, pokud by l nebylo dělitelné $c = q_1 q_2 \dots q_r$, pak není l dělitelné některým q_j; potom ale tímto prvočíslem nebude dělitelná ani žádná jeho mocnina. Je tedy $\sqrt{A} = c\mathbb{Z}$.

4. úloha Ideál A se nazývá maximální, jestliže platí: je-li B ideál takový, že $A \subseteq B$, pak buď $B = A$ nebo $B = \mathbb{Z}$. Nalezněte všechny maximální ideály.

Zřejmě $\{0\}$ není maximální ideál a $\mathbb{Z}$ je. Podobně jako u minulé úlohy se omezíme na situaci $A = a\mathbb{Z}$, $a > 1$. Je-li a složené, je pro jeho vlastního dělitele b určitě $A \subseteq b\mathbb{Z}$, $A \neq b\mathbb{Z}$ (např. $b \notin A$) a protože $b > 1$, je také $b \neq \mathbb{Z}$.

Naopak, buď $A = a\mathbb{Z}$ ideál, který není maximální, $a > 1$; B buď takový ideál, že $A \subseteq B$, $A \neq B \neq \mathbb{Z}$, b buď kladný generátor B. Pak zřejmě $b \mid a$, $b \neq a$, $b \neq 1$ (to je přepis jednotlivých podmínek na B). Závěr: maximální ideály jsou právě ideály generované prvočísly a $\mathbb{Z}$.

5. úloha Nechť A je ideál. Dokažte, že následující čtyři podmínky jsou ekvivalentní.

(i) A je maximální ideál.
(ii) $\forall a, b \in \mathbb{Z} : ab \in A \implies a \in A$ nebo $b \in A$.
(iii) $\forall a, b \in \mathbb{Z} : (\{a\} + A) \cdot (\{b\} + A) = A) \implies (\{a\} + A = A$ nebo $\{b\} + A = A)$.
(iv) $\forall a \in \mathbb{Z} \setminus A : \exists b \in \mathbb{Z} \setminus A : ((\{a\} + A) \cdot (\{b\} + A)) = \{1\} + A$.

V této úloze se sešly celkem tři chyby v zadání, takže výsledkem bylo, že nakonec nebyly spolu ekvivalentní žádné dvě podmínky. Ideál $\{0\}$ je protipříkladem na (ii) $\implies$ (i), (iii) $\implies$ (i), (ii) $\implies$ (iv) a (iii) $\implies$ (iv). Pro $A = 5\mathbb{Z}$, $a = 2$ jsou určitě 1 prvkem pravé strany v (iv), ale všechny prvky $\{a\} + A$ má všechny prvky různé od ± 1, takže pro žádné b není jednička prvkem levé strany; podle výsledku čtvrté úlohy je ale $5\mathbb{Z}$ maximální, neplatí tedy (i) $\implies$ (iv). Podmínka (iii) je splněna pro každý ideál: je-li $(\{a\} + A) \cdot (\{b\} + B) = A$, musí tento součin obsahovat nulu; pak ji ale obsahuje aspoň jedna ze závorek, a tedy buď $a \in A$ nebo $b \in A$, což je ekvivalentní s pravou stranou. Protože např. $6\mathbb{Z}$ nesplňuje (ii), neplatí ani (iii) $\implies$ (ii).

Pro jistotu ještě uvedu, jak měla úloha znít a jak by vypadalo její řešení.

5. úloha Buď A ideál různý od $\{0\}$. Pak jsou následující čtyři podmínky ekvivalentní:

(i) A je maximální,
(ii) $\forall a, b \in \mathbb{Z} : (ab \in A) \implies (a \in A) \vee (b \in A)$,
(iii) $\forall a, b \in \mathbb{Z} : ((\{a\} + A) \cdot (\{b\} + A) \subseteq A) \implies ((\{a\} + A \subseteq A) \vee (\{b\} + A \subseteq A)$,
(iv) $\forall a \in \mathbb{Z} \setminus A : \exists b \in \mathbb{Z} \setminus A : (\{a\} + A) \cdot (\{b\} + A) \subseteq \{1\} + A$.

(ii) $\implies$ (i): Buď $A \subseteq B$, B ideál. Označme a generátor A, b generátor B. Protože $a \in A \subseteq B$, je a násobkem b, tedy existuje c tak, že $a = bc$, tedy $bc \in A$ a buď b nebo c leží v A. Pokud

$b \in A$, je $B \subseteq A$ a tedy $A = B$. Pokud $c \in A$, je $a \mid c$, $c \mid a$, tj. $c = a$ (obě čísla jsou kladná) a $b = 1$ tj. $B = \mathbb{Z}$.
(iii) $\Longrightarrow$ (ii): Všimněme si, že je-li A ideál, je pro $x - y \in A$ dokonce $\{x\} + A = \{y\}A$ a pro $x - y \notin A$ je $(\{y\} + A) \cap (\{x\} + A) = \emptyset$. Je-li nyní $ab \in A$, snadno odhalíme, že $(\{a\} + A) \cdot (\{b\} + A) = \{ab + ap + bq + pq : p, q \in A\} \subseteq A$, a použitím (iii) a toho, co bylo řečeno výše, z toho vyplývá $a \in A$ nebo $b \in A$.
(iv) $\Longrightarrow$ (iii) Předpokládejme $(\{a\} + A) \cdot (\{b\} + A) \subseteq A$; stejnou úvahou jako v minulé implikaci z toho odvodíme $ab \in A$. Nechť dále $\{a\} + A \not\subseteq A$ (tj. $a \notin A$); chceme ukázat, že pak už nutně $b \in A$. Z podmínky (iv) najděme k číslu a takové $c \in \mathbb{Z} \setminus a$ tak, aby $ca \in A + 1$ (a tedy $ca - 1 \in A$. Pak ale také $cab - b = (ca - 1)b \in A$ a protože $ab \in a$ (a tedy $cab \in A$), musí být také $b = cab - b \in A$.
(i) $\Longrightarrow$ (iv) Nechť p je generátor A. Pokud $p = 1$, není co řešit (pak zatěžko vybrat nějaké a). Buď tedy p prvočíslo, $A = p\mathbb{Z}$, $a \in \mathbb{Z} \setminus A$. uvažujme množiny $\{ja\} + A$, kde j probíhá $0, 1, \ldots, p-1$. Kdyby např. $\{ia\} + A$ a $\{j\} + A$ měly neprázdný průnik, musely by už (stejnou úvahou jako výše) být nutně stejné a $j - i \in A$, což pro $i \neq j$ z $\{0, \ldots, p-1\}$ nejde. Jsou tedy po dvou disjunktní. Snadno nahlédneme, že každá z uvažovaných množin musí obsahovat některé z čísel $0, \ldots, p-1$ a vzhledem k disjunktnosti každá jiné. Protože máme p množin, musí některá $\{ia\} + A$ obsahovat jedničku. Pak ale $\{ia\} + A = \{1\} + A$, tedy $ia \in \{1\} + A$ a zjevně $i \notin A$. Zbývá si uvědomit, že z $ia \in \{1\} + A$ už plyne $(\{i\} + A) \cdot (\{a\} + A) \subseteq A$.

Komentáře k 7. sérii

1. úloha Řekneme, že konečná množina M bodů roviny je rozptýlená, jestliže platí: jsou-li x, y dva různé body z M, pak mají vzdálenost aspoň 1.
(a) Nalezněte co největší $c > 0$, ke kterému existuje $d > 0$ tak, že pro každé $r > 0$ existuje rozptýlená množina ležící v kruhu o poloměru r, která má aspoň $c(r - d)^2$ prvků.
(b) Nalezněte co nejmenší konstantu $C > 0$, ke které existuje $D > 0$ tak, že platí: kdykoli je M rozptýlená množina ležící v kruhu o poloměru r, potom má M nejvýše $C(r + d)^2$ prvků.
Poznámka: Nemusíte nalézt nejlepší možné hodnoty c a C. Podstatný je důkaz, že hodnoty c, C opravdu splňují podmínky zadání. Na druhou stranu, čím lepší konstanty, tím více bodů.

(a) Bez újmy obecnosti můžeme konstruovat M v kruhu K se středem v počátku a poloměrem R. Označme $A(u, v)$ bod o souřadnicích $(u + \frac{1}{2}v, \frac{\sqrt{3}}{2}v)$. Snadno spočítáme, že čtverec vzdálenosti $A(u_1, v_1)$ a $A(u_2, v_2)$ je

$$(u_2 - u_1)^2 + (u_2 - u_1)(v_2 - v_1) + (v_2 - v_1)^2 = \left((u_2 - u_1) + \tfrac{1}{2}(v_2 - v_1)\right)^2 + \tfrac{3}{4}(v_2 - v_1)^2$$
$$= \left((v_2 - v_1) + \tfrac{1}{2}(u_2 - u_1)\right)^2 + \tfrac{3}{4}(u_2 - u_1)^2.$$

Předpokládejme, že u_i, v_i jsou celá. Z druhého a třetího tvaru vidíme, že pokud je $u_1 \neq u_2$ nebo $v_1 \neq v_2$, je čtverec vzdálenosti aspoň $\frac{3}{4}$. Z prvního tvaru ale vidíme, že je to celé číslo, takže je to aspoň jedna. Množina M těch $A(u, v)$, které leží v kruhu, je tedy rozptýlená. Nyní odhadneme zdola počet jejích prvků. Buď K' kruh se středem v počátku a poloměrem