Komentáře k 5. sérii

1. úloha Nechť $m \in \mathbb{M}$, $n \in \mathbb{M}$. Potom $m \cdot n \in \mathbb{M}$.

Je-li $m = a^2 + b^2$, $n = c^2 + d^2$, můžeme psát součin mn ve tvaru

$$mn = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 = (ac + bd)^2 + |ad - bc|^2 .$$

2. úloha Nechť $m \in \mathbb{M}$, $n \in \mathbb{M}$ a nechť $\frac{m}{n} \in \mathbb{N}$. Potom $\frac{m}{n} \in \mathbb{M}$.

3. úloha Nechť $m \in \mathbb{M}$, $n \in \mathbb{M}$. Potom $\mathrm{NSD}(m,n) \in \mathbb{M}$ a $\mathrm{NSN}(m,n) \in \mathbb{M}$

Z euforie nad jednoduchostí 1. úlohy většina řešitelů prohlásila, že tvrzení 2. úlohy plyne z identity

$$\frac{a^2+b^2}{c^2+d^2} = \left(\frac{ac-bd}{c^2+d^2}\right)^2 + \left(\frac{ad+bc}{c^2+d^2}\right)^2 .$$

Jenže např. pro $a = 3$, $b = 4$, $c = 0$, $d = 5$ je zlomek v první závorce roven $-\frac{4}{5}$, což není celé číslo. Pro správné vyřešení druhé a třetí úlohy je třeba získat lepší znalost struktury množiny $\mathbb{M}$. Rozdělme prvočísla podle toho, zda leží v množině $\mathbb{M}$ na prvočísla prvního a druhého druhu. Dá se ukázat, že prvočísla prvního druhu jsou dvojka a prvočísla tvaru $4k+1$, zatímco druhého druhu jsou prvočísla tvaru $4k+3$, a že existuje nekonečně mnoho prvočísel obou druhů. Nebudeme to však potřebovat k řešení; postačí nám následující věta:

Věta. *Přirozené číslo m leží v množině $\mathbb{M}$ právě tehdy, když se v jeho prvočíselném rozkladu vyskytují prvočísla druhého druhu pouze v sudých mocninách.*

Pokud je nějaké prvočíslo v sudé mocnině v rozkladu čísel m a n, potom je také v sudé mocnině v rozkladu čísel $\frac{m}{n}$, $\mathrm{NSD}(m,n)$ a $\mathrm{NSN}(m,n)$. Odtud již ihned plyne tvrzení druhé a třetí úlohy. K důkazu věty užijeme následující lemma:

Lemma. *Buď p prvočíslo a x, y celá čísla taková, že $p \mid (x^2 + y^2)$ a $p \nmid x$. Potom p je prvočíslo prvního druhu.*

Důkaz: $p \nmid x$, tedy existuje prvek x^{-1} takový, že $xx^{-1} \equiv 1 \pmod p$ (je to vlastně ukázáno v řešení čtvrté a páté úlohy šesté série). Položme $a = yx^{-1}$. Potom $p \mid x^2 + (ax)^2$, tedy $p \mid a^2 + 1$. Uvažujme nyní čísla ia pro $0 \le i < \sqrt{p}$. Těchto čísel je více než $\sqrt{p}$, tedy podle Dirichletova principu musí být zbytek rozdílu některých dvou z nich modulo p menší než $\sqrt{p}$. Nechť $(ia - ja) \bmod p < \sqrt{p}$. Položme $\tilde{x} = i - j$, $\tilde{y} = (ia - ja) \bmod p = a\tilde{x} \bmod p$. Potom $p \mid \tilde{x}^2 + \tilde{y}^2$ a $0 < |\tilde{x}|, |\tilde{y}| < \sqrt{p}$, tedy $0 < \tilde{x}^2 + \tilde{y}^2 < 2p$, tedy $\tilde{x}^2 + \tilde{y}^2 = p$ a $p \in \mathbb{M}$.

Důkaz věty: Pokud prvočíselný rozklad m obsahuje prvočísla druhého druhu pouze v sudých mocninách, dostaneme $m \in \mathbb{M}$ z toho, že prvočísla prvního druhu a čtverce prvočísel druhého druhu jsou v $\mathbb{M}$ a z tvrzení první úlohy.

To uděláme indukcí podle součtu exponentů u prvočísel druhého druhu. Je-li to nula, není co dokazovat. Nechť tedy $p \mid m = x^2 + y^2$ a p je prvočíslo druhého druhu. Potom podle lemmatu $p \mid x$ a tedy i $p \mid y$. Dostáváme

$$\frac{m}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2,$$

tedy $\frac{m}{p^2}$ leží také v $\mathbb{M}$ a podle indukčního předpokladu má všechna prvočísla druhého druhu ve svém rozkladu v sudé mocnině, tedy i v prvočíselném rozkladu m se prvočísla druhého druhu vyskytují pouze v sudých mocninách.

4. úloha Vyjádření prvků množiny $\mathbb{M}$ jako součtu dvou čtverců zřejmě není jednoznačné: $25 = 0^2 + 5^2 = 3^2 + 4^2$. Dokažte následující tvrzení:

(1) Ke každému $k \in \mathbb{N}$ existuje $m \in \mathbb{M}$ tak, že m lze vyjádřit jako součet dvou čtverců čísel z $\mathbb{N}$ alespoň k různými způsoby.

(2) Existuje nekonečně mnoho prvků v $\mathbb{M}$, pro něž je toto vyjádření (až na pořadí sčítanců) jednoznačné.

(3) Existuje nekonečně mnoho čísel z $\mathbb{N}$, která neleží v $\mathbb{M}$.

(1) Položme $x_0 = 1$, $y_0 = 0$, $x_{n+1} = 3x_n - 4y_n$, $y_{n+1} = 4x_n + 3y_n$. Indukcí se snadno ukáže, že $x_k^2 + y_k^2 = 5^{2k}$ a že čísla x_k a y_k nejsou násobky pěti. Nyní ukážeme matematickou indukcí, že 5^{2k} lze vyjádřit jako součet dvou čtverců aspoň $k+1$ způsoby. Pro $k = 0$ je $1 = 1^2 + 0^2$. Nechť $5^{2k} = a_1^2 + b_1^2 = \cdots = a_{k+1}^2 + b_{k+1}^2$. Potom

$$5^{2k+2} = x_{k+1}^2 + y_{k+1}^2 = (5a_1)^2 + (5b_1)^2 = \cdots = (5a_{k+1})^2 + (5b_{k+1})^2,$$

což (x_{k+1} a y_{k+1} nejsou dělitelná pěti) je vyjádření $k+2$ různými způsoby.

(2) Ukážeme indukcí, že pro čísla typu 2^k je vyjádření ve tvaru součtu čtverců jednoznačné. Rozklady $2^0 = 1 = 1^2 + 0^2$ a $2^1 = 2 = 1^2 + 1^2$ jednoznačné jsou. Dále nechť $k \geq 2$ a $2^k = x^2 + y^2$. Protože čtverce sudých čísel jsou dělitelné čtyřmi a čtverce lichých čísel dávají zbytek jedna, vyplývá z $4 \mid x^2 + y^2$, že x a y jsou sudá. Pak ale můžeme psát $2^{k-2} = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2$ a protože podle předpokladu je toto vyjádření jediné, je jediný i rozklad $2^k = x^2 + y^2$.

(3) Podobnou úvahou jako ve (2) odhalíme, že žádné číslo typu $4k+3$ neleží v $\mathbb{M}$. Rozmyslete si, že dokonce existuje nekonečně mnoho prvočísel tohoto typu (důkaz je obdobou klasického důkazu toho, že existuje nekonečně mnoho prvočísel).

5. úloha Jsou dána dvě čísla $a, b \in \mathbb{N}$. Žák A zná jejich součet, žák B zná součet jejich čtverců. Proběhl tento rozhovor:

B: Nevím, jaká jsou to čísla.
A: Nevím, jaká jsou to čísla.
B: Nevím, jaká jsou to čísla.
A: Nevím, jaká jsou to čísla.
B: Nevím, jaká jsou to čísla.
A: Nevím, jaká jsou to čísla.

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