

# Teorie nejen čísel 1

1. SERIÁLOVÁ SÉRIE

TERMÍN ODESLÁNÍ: 7. PROSINCE 2020

*V úlohách lze používat všechna tvrzení (i cvičení) ze seriálu. K využití nějaké vlastnosti některého okruhu, která v seriálu nebyla ukázána, je třeba ji dokázat.*

ÚLOHA 1. (5 BODŮ)

Najděte všechny dvojice prvočísel  $p, q$ , které splňují  $p^4 + p^2 + 1 = q^3$ .

ÚLOHA 2. (5 BODŮ)

Najděte všechna celočíselná řešení rovnice  $x^2 + x = y^3 - 3$ .

ÚLOHA 3. (5 BODŮ)

Je dáno přirozené číslo  $n$ . Dokažte, že přirozená čísla  $x, y$  splňující

$$x(x + 1) + y(y + 1) = n(n + 1)$$

existují právě tehdy, když je  $2n^2 + 2n + 1$  složené číslo.

# Teorie nejen čísel 1

1. SERIÁLOVÁ SÉRIE

VZOROVÉ ŘEŠENÍ

## Úloha 1.

Najděte všechny dvojice prvočísel  $p, q$ , které splňují  $p^4 + p^2 + 1 = q^3$ . (Filip Čermák)

ŘEŠENÍ MODULEM 3:

Díky sudým mocninám na levé straně se nic nezmění, když budeme místo  $p$  uvažovat  $-p$ , takže BÚNO hledejme  $p$  kladné. Dále je  $p^4 + p^2 + 1 \geq 1$ , tudíž  $q > 0$ . Podívejme se na prvočíslo  $p$  modulo 3. Pokud je  $p$  dělitelné třemi, pak musí z prvočíselnosti být  $p = 3$ . Po dosazení dostáváme  $91 = 3^4 + 3^2 + 1 = q^3$ . Avšak 91 není třetí mocninou žádného celého čísla, takže tento případ nemá žádné řešení.

Dále uvažme případ, kdy je trojka nesoudělná s  $p$ . To v jazyku kongruencí znamená, že  $p \equiv \pm 1 \pmod{3}$ . Pokud jej umocníme na druhou a na čtvrtou jako na levé straně v zadání, dostaneme, že  $p^4 \equiv p^2 \equiv 1 \pmod{3}$ . Nyní už se stačí podívat na celou rovnici modulo 3. Tím dostaneme

$$q^3 = p^4 + p^2 + 1 \equiv 1 + 1 + 1 \equiv 3 \equiv 0 \pmod{3}.$$

To ovšem znamená, že číslo  $q^3$  je dělitelné třemi, a tedy i samotné  $q$  je dělitelné třemi. Proto už se jakožto prvočíslo opět rovná 3. Zpětným dosazením dostáváme, že  $p^4 + p^2 + 1 = 27$  neboli  $p^2(p^2 + 1) = 2 \cdot 13$ . Nyní si buď stačí říct, že  $p^2$  nedělí 26 pro žádné prvočíslo  $p$ , nebo vyzkoušet malá  $p$  a říct, že výraz na levé straně roste.

ŘEŠENÍ NESOUDELNÝM ROZKLADEM:

Upravme levou stranu do tvaru

$$p^4 + p^2 + 1 = p^4 + 2p^2 + 1 - p^2 = (p^2 + 1)^2 - p^2 = (p^2 + 1 - p)(p^2 + 1 + p).$$

První úprava vznikla přičtením a odečtením  $p^2$ , abychom dostali rozdíl dvou čtverců a na něj pak mohli aplikovat známý rozklad  $a^2 - b^2 = (a - b)(a + b)$ .

Nyní by bylo hezké říct, že jsou obě závorky nesoudělné. Z Eukleidova algoritmu víme, že  $\text{NSD}(p^2 + 1 + p, p^2 + 1 - p) = \text{NSD}(p^2 + 1 + p, p^2 + 1 + p - (p^2 + 1 - p)) = \text{NSD}(p^2 + p + 1, 2p)$ , takže nás zajímají dělitelé  $p^2 + p + 1$  soudělní s 2 či s  $p$ .

Podívejme se tedy na číslo  $p^2 + p + 1 = p(p + 1) + 1$ . Můžeme snadno vidět, že  $p(p + 1)$  je vždy součin sudého a lichého čísla, tedy číslo sudé. Po přičtení jedničky se tak stane číslem lichým, a proto nemůže být dělitelné dvěma.

Soudělnost s  $p$  lze také hned vyloučit, jelikož  $p(p + 1)$  je násobkem  $p$ , takže  $p(p + 1) + 1$  dává zbytek jedna po dělení  $p$ , a proto není násobkem  $p$ . Z toho už ovšem plyne, že  $\text{NSD}(p^2 + p + 1, 2p) = 1$ .

Už víme, že závorky v rozkladu  $q^3 = (p^2 + 1 - p)(p^2 + 1 + p)$  jsou nesoudělné. Jelikož má jejich součinem být třetí mocnina prvočísla, musí se ta menší z nich rovnat 1 a ta větší z nich  $q^3$ . Pohybujeme se však v přirozených číslech, takže první závorka je určitě menší než ta druhá. Z toho už nutně plyne  $p^2 + 1 - p = 1$  neboli  $p^2 - p = p(p - 1) = 0$ . Vidíme, že jedinými řešeními této rovnice jsou  $p = 0$  a  $p = 1$ , což rozhodně nejsou prvočísla, a tudíž zadaná rovnice žádná prvočíselná řešení nemá.

POZNÁMKY:

Zhruba polovina řešení šla cestou prvního a polovina cestou druhého řešení. Občas se stávaly numerické chyby, takže byl stržen nějaký ten bod. Vesměs všechna, co se vydala správnou cestou, to dotáhla až do konce a nebyly zde žádné velké problémy. K této úloze nebylo nutné použít žádnou z vět ze seriálu, ale občas řešení používala tvrzení o rozkladu na nesoudělné mocniny, což byl tedy trochu kanon na vrabce, ale proč ne.

**Úloha 2.**

Najděte všechna celočíselná řešení rovnice  $x^2 + x = y^3 - 3$ . (Matěj Doležálek)

ŘEŠENÍ:

Ukážeme, že rovnice nemá řešení. Rovnici nejprve upravíme na  $x^2 + x + 3 = y^3$ . Nyní budeme chtít levou stranu rozložit na součin ve vhodném oboru a následně použít tvrzení o mocninách a nesoudělnosti. Nechť je  $\alpha = \frac{1+\sqrt{-11}}{2}$ , toto komplexní číslo pak splňuje  $\alpha^2 = \alpha - 3$ . Dále také  $\alpha + \bar{\alpha} = 1, \alpha \cdot \bar{\alpha} = 3$ . S jeho pomocí levou stranu rovnice rozložíme jako  $(x + \alpha)(x + \bar{\alpha}) = y^3$ . Mohli bychom také volit  $\alpha$  tak, aby bylo kořenem  $x^2 + x + 3 = 0$ , další postup by pak byl téměř stejný, jen bychom na některých místech obrátili znaménka.

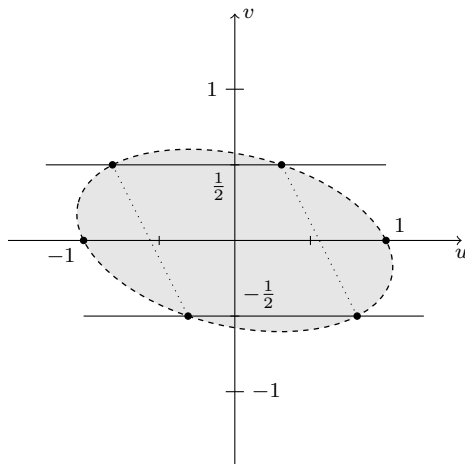
Zkoumejme tedy obor  $\mathbb{Z}[\alpha] = \{a + b\alpha : a, b \in \mathbb{Z}\}$ . Že se jedná o obor integrity, je zjevné: je to podmnožina komplexních čísel, takže stačí ověřit, že je uzavřený na sčítání a násobení. Sčítání je zřejmé, uzavřenost na násobení pak máme skrze

$$(a_1 + b_1\alpha)(a_2 + b_2\alpha) = a_1a_2 + a_1b_2\alpha + a_2b_1\alpha + b_1b_2\alpha^2 = (a_1a_2 - 3b_1b_2) + (a_1b_2 + a_2b_1 + b_1b_2)\alpha.$$

Ukážeme, že obor  $\mathbb{Z}[\alpha]$  je eukleidovský, čímž pak budeme mít zaručeno, že je i gaussovský, a budeme tak moci použít tvrzení o nesoudělnosti a mocninách. Jako eukleidovskou funkci použijeme normu definovanou předpisem  $N(a + b\alpha) = (a + b\alpha)(a + b\bar{\alpha}) = a^2 + ab + 3b^2$ . Nechť jsou dána  $\beta, \gamma \in \mathbb{Z}[\alpha]$ ,  $\gamma \neq 0$  a najdeme  $\delta \in \mathbb{Z}[\alpha]$  takové, že  $N(\beta - \delta\gamma) < N(\gamma)$ . Podobně jako jsme to dělali v seriálu, vydělíme  $\frac{\beta}{\gamma} = \frac{\beta\bar{\gamma}}{N(\gamma)} = u + v\alpha$  pro nějaká  $u, v \in \mathbb{Q}$ , a potřebujeme následně zvolit  $\delta$  tak, aby

$$N(\gamma) \cdot N\left(\frac{\beta}{\gamma} - \delta\right) = N(\beta - \delta\gamma) < N(\gamma),$$
$$N((u + v\alpha) - \delta) < 1.$$

Na to nahlédneme geometricky. Nerovnice  $N(u + v\alpha) = u^2 + uv + 3v^2 < 1$  určuje v rovině se souřadnicemi  $u, v$  vnitřek elipsy.



Průsečíky přímkou  $v = \frac{1}{2}$  s touto elipsou jsou  $u_{1,2} = \frac{-\frac{1}{2} \pm \sqrt{\frac{1}{4} + 4 \cdot \frac{1}{4}}}{2}$ , takže jsou od sebe vzdáleny  $\sqrt{\frac{5}{4}} > 1$ . Spolu s dvěma středově souměrnými průsečíky s přímkou  $v = -\frac{1}{2}$  tak můžeme vytvořit rovnoběžník s výškou 1 a šířkou větší než 1 tím, že o něco málo posuneme vrcholy vytvořené z průsečíků dovnitř elipsy. Odečítáním celých čísel od souřadnic  $u, v$  skrze volbu složek čísla  $\delta$  se pak dovedeme trefit dovnitř tohoto rovnoběžníku: nejprve zvolíme složku  $v$  tak, abychom se trefili do pásu  $-\frac{1}{2} \leq v \leq \frac{1}{2}$ , a následně nám postačí trefit se složkou  $u$  dovnitř rovnoběžníku, který má ale šířku větší než 1, takže to vždycky půjde.

V souhrnu tak dovedeme  $\delta$  zvolit tak, aby  $N((u + v\alpha) - \delta) < 1$ , jelikož vnitřek elipsy odpovídá přesně těm číslům, co mají normu ostře menší než 1. To znamená, že v  $\mathbb{Z}[\alpha]$  dovedeme dělit se zbytkem, takže je to eukleidovský obor, jak jsme chtěli.

Nyní se můžeme vrátit na rovnici  $(x + \alpha)(x + \bar{\alpha}) = y^3$ . Ukažme, že aby  $x, y$  řešily rovnici, musí  $x + \alpha$  a  $x + \bar{\alpha}$  být nesoudělné v  $\mathbb{Z}[\alpha]$ . Každý jejich společný dělitel bude muset dělit i

$$(x + \alpha) - (x + \bar{\alpha}) = \alpha - \bar{\alpha} = \frac{1 + \sqrt{-11}}{2} - \frac{1 - \sqrt{-11}}{2} = \sqrt{-11}.$$

Přitom  $\sqrt{-11}$  má normu 11, což je prvočíslo, takže je to ireducibilní prvek. Největším společným dělitelem  $x + \alpha$  a  $x + \bar{\alpha}$  je tak buď 1, nebo  $\sqrt{-11}$ . Pro spor nechť je to  $\sqrt{-11}$ . Potom  $\sqrt{-11} \mid x + \alpha$ , z čehož i

$$11 = N(\sqrt{-11}) \mid N(x + \alpha) = x^2 + x + 3 = y^3,$$

takže i  $11 \mid y$ , poněvadž 11 je prvočíslo v  $\mathbb{Z}$ . Původní rovnici dále upravme do tvaru

$$4x^2 + 4x + 12 = 4y^3,$$

$$(2x + 1)^2 + 11 = 4y^3.$$

Kdyby  $11 \mid y$ , tak potom z poslední rovnice i  $11 \mid (2x+1)^2$ , takže  $11 \mid 2x+1$ . Potom ale  $11^2 \mid (2x+1)^2$  a podobně  $11^3 \mid 4y^3$ , z čehož

$$11^2 \mid 4y^3 - (2x + 1)^2 = 11,$$

což je spor. Největším společným dělitelem  $x + \alpha$  a  $x + \bar{\alpha}$  tak nemůže být  $\sqrt{-11}$ , je to tedy 1 a tyto dvě závorky jsou tak nesoudělné.

V rovnici  $(x + \alpha)(x + \bar{\alpha}) = y^3$  tak máme nesoudělné činitele na levé straně. Zároveň si rozmyslíme, že jednotkami v  $\mathbb{Z}[\alpha]$  jsou jen prvky s normou 1, což jsou pouze 1 a  $-1$ . Každá je přitom třetí mocninou sebe samé, takže dovedeme schovat jednotku do mocniny a z tvrzení o nesoudělnosti a mocninách jsou  $x + \alpha$  i  $x + \bar{\alpha}$  třetí mocniny v  $\mathbb{Z}[\alpha]$ . Nechť tedy  $x + \alpha = (a + b\alpha)^3$  pro vhodná  $a, b \in \mathbb{Z}$ . S pomocí  $\alpha^2 = \alpha - 3$  a  $\alpha^3 = \alpha(\alpha - 3) = -2\alpha - 3$  pak rozepíšeme

$$\begin{aligned} x + \alpha &= (a + b\alpha)^3 = a^3 + 3a^2b\alpha + 3ab^2\alpha^2 + b^3\alpha^3 = a^3 + 3a^2b\alpha + 3ab^2(\alpha - 3) + b^3(-2\alpha - 3) = \\ &= (a^3 - 9ab^2 - 3b^3) + (3a^2b + 3ab^2 - 2b^3)\alpha. \end{aligned}$$

Když se nyní podíváme pouze na koeficienty u  $\alpha$ , dostaneme rovnici

$$1 = b \cdot (3a^2 + 3ab - 2b^2).$$

Z toho  $b \mid 1$ , takže  $b = \pm 1$ . Pro  $b = -1$  zbude rovnice  $3a^2 - 3a - 1 = 0$ , což nemá řešení, protože  $3 \nmid 1$ . Pro  $b = 1$  pak zbude  $3a^2 + 3a - 3 = 0$  neboli  $a^2 + a - 1 = 0$ . Tato rovnice už nemá celočíselné řešení, což nahlédneme třeba takto:  $a, a + 1$  jsou po sobě jdoucí čísla, takže jedno z nich je sudé, takže i  $a(a + 1)$  je sudé. Ale přitom má být  $a(a + 1) = 1$  liché, což je spor. Zadaná rovnice tak nemůže mít řešení.

POZNÁMKY:

Všechna správná řešení postupovala zhruba vzorovým způsobem. Některá se zadržla na vyloučení  $\sqrt{-11}$  jako společného dělitele  $x + \alpha$  a  $x + \bar{\alpha}$ . Za netriviální chyby v jinak správném postupu (špatně vyloučené  $\sqrt{-11}$ , špatně dorešená rovnice pro  $a, b$ ) jsem strhával jeden nebo dva body. Za absenci nějakého přímočarého ověření, třeba že  $\{a + b\alpha : a, b \in \mathbb{Z}\}$  je obor, jsem body nestrhával.

(Matěj Doležálek)

### Úloha 3.

Je dáno přirozené číslo  $n$ . Dokažte, že přirozená čísla  $x, y$  splňující

$$x(x+1) + y(y+1) = n(n+1)$$

existují právě tehdy, když je  $2n^2 + 2n + 1$  složené číslo.

(Matěj Doležálek)

ŘEŠENÍ:

Zkoumanou rovnicí upravme do tvaru

$$\begin{aligned}x^2 + x + y^2 + y &= n^2 + n, \\(4x^2 + 4x + 1) + (4y^2 + 4y + 1) &= 4n^2 + 4n + 2, \\(2x + 1)^2 + (2y + 1)^2 &= (2n + 1)^2 + 1 = 2 \cdot (2n^2 + 2n + 1).\end{aligned}$$

Existence přirozených  $x, y$  splňujících rovnici je nyní ekvivalentní tomu, že existuje  $a + bi \in \mathbb{Z}[i]$  s lichými složkami  $a, b \geq 3$  (jelikož potřebujeme  $x, y \geq 1$ ) takové, že  $N(a + bi) = 2(2n^2 + 2n + 1)$ . S lichostí si nebudeme muset dělat starosti, jelikož modulo čtyři máme  $(2n + 1)^2 + 1 \equiv 1 + 1 \equiv 2$ , takže každé řešení, které najdeme, bude nutně mít  $a, b$  lichá.

Jak je to s  $a, b \geq 3$ ? Jedno řešení je zřejmé:  $a = 2n + 1, b = 1$  plus sedm dalších, která vzniknou prohozením složek a změnami jejich znamének. To však nesplňuje  $b \geq 3$ , takže nám nestačí. Naopak jakékoli jiné řešení (takové, které má úplně jiné absolutní hodnoty svých složek) už jedničku obsahovat nebude:  $a$  a  $b$  vystupují symetricky, takže pokud je jedno z nich  $\pm 1$ , tak už to vynucuje, aby to druhé bylo v absolutní hodnotě  $2n + 1$ . Chceme tedy ukázat, že existuje více než osm čísel  $a + bi$  s normou  $2(2n^2 + 2n + 1)$  právě tehdy, když  $2n^2 + 2n + 1$  není prvočíslo.

K tomu ukážeme, že přenásobení dvojkou nám v podstatě nepřidává nic navíc. Mějme prvek  $a + bi$  s normou  $2(2n^2 + 2n + 1)$ . Jelikož jeho norma je sudá, musí se v rozkladu  $a + bi$  na prvočinitele vyskytovat nějaký prvočinitel s normou 2. Těmi jsou ale pouze  $1 + i, -1 + i, -1 - i$  a  $1 - i$ , což jsou navzájem asociované prvky. Tím pádem kdykoliv má Gaussovo celé číslo sudou normu, pak je násobkem  $1 + i$ . Každému  $a + bi$  s normou  $2(2n^2 + 2n + 1)$  tak můžeme jednoznačně přiřadit číslo  $c + di = \frac{a+bi}{1+i}$  s normou  $2n^2 + 2n + 1$  a dívat se nadále jenom na to, kolik Gaussových celých čísel má normu  $2n^2 + 2n + 1$ .

Když je  $2n^2 + 2n + 1$  prvočíslo, pak má podle *Cvičení 31* v seriálu tuto normu až na prohození složek a změny znamének pouze jedno číslo (zde  $(n + 1) + ni$ ), takže s prohozením složek a změnami znamének je to jen osm čísel. Ukažme, že pokud je naopak  $2n^2 + 2n + 1$  složené, pak získáme více než osm čísel s normou  $2n^2 + 2n + 1$ .

Rozložíme  $2n^2 + 2n + 1$  na součin kladných prvočísel  $p_1^{e_1} \cdots p_r^{e_r}$ , kde jednotlivá  $p_k$  jsou navzájem neasociovaná. Kdyby nějaké prvočíslo  $q \equiv 3 \pmod{4}$  dělilo  $(2n + 1)^2 + 1^2$ , pak by podle *Cvičení 30* muselo  $q$  dělit i obě složky  $(2n + 1) + i$ , tedy  $q \mid 1$ , což je spor. Číslo  $(2n + 1)^2 + 1$  tak má za prvočíselné dělitele pouze dvojkou a prvočísla  $q \equiv 1 \pmod{4}$ , takže všechna  $p_k$  z rozkladu lichého čísla  $2n^2 + 2n + 1$  jsou  $1 \pmod{4}$ . Každé proto k sobě má nějaký prvočinitel  $\pi_k \in \mathbb{Z}[i]$  s normou  $N(\pi_k) = p_k$ , navíc podle *Cvičení 32* nikdy nejsou  $\pi_k$  a  $\overline{\pi_k}$  asociovaná. Pro číslo  $c + di$  s normou  $2n^2 + 2n + 1$  pak můžeme třeba vzít

$$c + di = \pi_1^{e_1} \cdots \pi_r^{e_r}.$$

Můžeme ale také některá  $\pi_k$  vyměnit za  $\overline{\pi_k}$ . Když tvoříme rozklad  $c + di$ , můžeme za každou mocninu  $p_k^{e_k}$  v rozkladu  $2n^2 + 2n + 1$  použít  $(\overline{\pi_k})^\ell$  pro nějaké  $\ell \in \{0, 1, \dots, e_k\}$  a zbytek exponentu  $\ell$  do  $e_k$  doplnit mocninou  $\pi_k^{e_k - \ell}$ . Jednotlivá čísla  $c + di$ , která takto vyrobíme, budou navzájem neasociovaná, protože budou mít odlišný exponent u nějakého  $\pi_k$  (resp.  $\overline{\pi_k}$ ). Podle *Cvičení 31* jsou vždy  $\pi_k$  a  $\overline{\pi_k}$  navzájem neasociovaní prvočinitelé, takže se všechny rozklady, které vyrobíme, navzájem liší (nejdou na sebe převést tím, že některé prvočinitele přenásobíme jednotkami). Pro každé  $p_k^{e_k}$  takto budeme moci vybírat z  $e_k + 1$  možností a všechny tyto možnosti jsou nezávislé.

Navíc pak ještě každé získané  $c + di$  budeme moci přenásobit jednou ze čtyř jednotek  $1, i, -1, -i$ , takže celkem tímto vyrobíme

$$4 \cdot (e_1 + 1) \cdot (e_2 + 1) \cdots (e_r + 1)$$

možných čísel  $c + di$ . Tento počet už bude více než osm – kdyby to bylo nanejvýš osm, znamenalo by to, že máme jenom jednu závorku  $(e_1 + 1)$ , v níž je navíc  $e_1 = 1$ . Jenže to by potom  $2n^2 + 2n + 1 = p_1^1$  bylo prvočíslo, což není.

V souhrnu tedy: když je  $2n^2 + 2n + 1$  prvočíslo, můžeme  $a + bi$  s normou  $2(2n^2 + 2n + 1)$  získat jen tak, že jedno z  $a, b$  bude jednička, což nám nedá přirozená  $x, y$ . Pokud je  $2n^2 + 2n + 1$  složené, pak už dovedeme prvočinitele do rozkladu  $c + di$ , resp.  $a + bi$  poskládat vícero způsobů, což dá nějaké  $a + bi$ , kde  $a$  ani  $b$  nejsou jednička, takže dostaneme skutečně přirozená  $x, y$ .

POZNÁMKY:

Úloha byla trochu technicky náročná, ale základní úvaha je velmi prostá: upravíme rovnici tak, aby hovořila o součtech čtverců, a díváme se na to, co to chceme součtem čtverců vyjádřit. Už se jen snažíme precizně formulovat, že prvočísla dávají málo prvočinitelů, takže málo způsobů, jak je poskládat dohromady, takže prvočísla mají „jen jeden“ zápis jako součet čtverců, zatímco složená čísla už dovolují namíchat ze svých prvočinitelů mnohem více vyjádření.

Všechna správná řešení postupovala vesměs podobně jako vzorák. Rovnici šlo též upravit do tvaru  $(x - y)^2 + (x + y + 1)^2 = 2n^2 + 2n + 1$  a nezaobírat se tak dvojkou navíc na pravé straně. Postup s vynásobením čtyřmi a úpravou na čtverce je však celkem poučný a často se hodí, protože je ve vzoráku použit. (Matěj Doležálek)