Horní Lysečiny

Sborník, podzim 2013

Martin Čech
Filip Hlásek
David Hruška
Jakub „Roman“ Klemsa
Bára Kociánová
Anh Dung „Tonda“ Le
Vít „Vejtek“ Musil
Tomáš „Šavlík“ Pavlík
Alča Skálová
Štěpán Šimsa
Pepa Tkadlec
Martina Vaváčková
Lukáš Zavřel

Autoři: Martin Čech, Filip Hlásek, David Hruška, Jakub „Roman“ Klemsa, Bára Kociánová, Anh Dung „Tonda“ Le, Vít „Vejtek“ Musil, Tomáš „Šavlík“ Pavlík, Alča Skálová, Štěpán Šimsa, Pepa Tkadlec, Martina Vaváčková, Lukáš Zavřel
Editor: Vít „Vejtek“ Musil
vydání druhé, elektronická edice
listopad 2013
Díky za pomoc všem, kterým je za co děkovat.

Cifry a ciferné součty

Martin Čech

Abstrakt. Přednáška z teorie čísel zaměřená na řešení úloh, v nichž se vyskytují cifry a ciferné součty čísel. Ukážeme si několik nejobvyklejších metod řešení a na konci se dostaneme i k obtížnějším příkladům, na něž tyto obvyklé postupy nestačí.

Dekadický zápis

Každé přirozené číslo n lze zapsat ve tvaru

$$n = \sum_{i=0}^{k} a_i \cdot 10^i,$$

kde $a_i \in \{0, 1, \ldots, 9\}$ a $a_k \neq 0$. Navíc platí, že $10^k \leq n < 10^{k+1}$. Tomuto zápisu budeme říkat *dekadický zápis čísla* n, popř. zápis čísla n v *desítkové soustavě*. Čísla a_i nazýváme *ciframi* čísla n. Někdy také používáme zápis $n = \overline{a_k a_{k-1} \ldots a_1 a_0}$. U mnohých úloh stačí vyjádřit si čísla v dekadickém zápisu a poté vyřešit diofantické rovnice.

Příklad 1. Najděte všechna dvojciferná čísla n s následující vlastností: když sečteme n s číslem vzniklým prohozením jeho cifer, dostaneme čtverec přirozeného čísla.

Příklad 2. Najděte všechna přirozená čísla, která se zdvojnásobí po přesunutí své první cifry na konec.

Příklad 3. Dokažte, že pokud čísla 2^n a 5^n začínají stejnou číslicí, pak začínají číslicí 3.

Ciferné součty

Zapíšeme-li přirozené číslo n v desítkové soustavě jako

$$n = \sum_{i=0}^{k} a_i \cdot 10^i,$$

číslo $s(n) = a_0 + a_1 + \cdots + a_k$ nazveme *ciferným součtem* čísla n. Zřejmě platí, že $s(n) \leq 9(k+1)$. Důležitější je ale následující tvrzení:

Tvrzení. *Pro každé přirozené číslo n dává $s(n)$ po dělení 9 stejný zbytek jako n, neboli*

$$s(n) \equiv n \pmod 9.$$

Vybaveni tímto tvrzením se můžeme pustit do řešení následujících úloh:

Příklad 4. Najděte všechna přirozená čísla n, která končí cifrou a a která splňují:

$$n = s(n) + a^2.$$

Příklad 5. Dvě přirozená čísla nazveme *podobná*, jestliže ve svém dekadickém zápisu obsahují stejný počet stejných číslic. Dokažte, že dvě různé mocniny dvojky nikdy nejsou podobné. (MKS 31–3–7)

Příklad 6. Dokažte, že pro každé přirozené číslo m existuje n takové, že $m = s(n) + n$ nebo $m + 1 = s(n) + n$.

Příklad 7. Existuje přirozené číslo n takové, že $s(n) = 1000$ a $s(n^2) = 1000^2$?

Soustavy jiné než desítkové

V desítkové soustavě jsme každé přirozené číslo n vyjadřovali pomocí mocnin desítky. Číslo deset však není ničím speciální a není důvod, proč bychom nemohli čísla zapisovat i v jiných soustavách. Každé přirozené číslo n lze vyjádřit v soustavě o přirozeném základu $b \neq 1$ jako

$$n = \sum_{i=0}^{k} a_i \cdot b^i,$$

přičemž platí, že $a_i \in \{0, 1, \ldots, b-1\}$ a $a_k \neq 0$. Čísla $a_0, a_1 \ldots, a_k$ jsou takto určena jednoznačně a tento zápis nazýváme *ciferný zápis čísla n v soustavě o základu b*. Budeme ho značit $(a_k a_{k-1} \ldots a_0)_b$.

Příklad 8. Najděte všechna a taková, že číslo 2013 zapsané v soustavě o základu a končí cifrou 3.

Příklad 9. Odvoďte vzorec pro součet geometrické posloupnosti.

Příklad 10. Najděte všechna přirozená $b > 6$ taková, že číslo $(5654)_b$ je mocninou prvočísla. (TR*i*KS, 2. série)

Nyní si uvedeme tvrzení, jenž nám pomůže určit, kolik má které číslo cifer. Použijeme ho v následných úlohách.

Tvrzení. (o počtu cifer) *Číslo n zapsané v soustavě o základu b má $\lfloor \log_b n \rfloor + 1$ cifer.*[1]

Příklad 11. Kolik z prvních 2013 mocnin dvojky

(i) začíná cifrou 1?
(ii) začíná cifrou 4?

Čísla se zajímavým ciferným zápisem

Oblíbené jsou úlohy, ve kterých vystupují čísla se zajímavými ciferými zápisy, například tvořenými jedinou opakující se číslicí. Zkusíme si nyní vyřešit pár takových úloh.

Příklad 12. Dokažte, že $3^n \mid \underbrace{\overline{aaa\ldots a}}_{3^n}$ pro každé přirozené číslo n a každou nenulovou cifru a. (MKS 30–2–4)

Příklad 13. Dokažte, že $\underbrace{\overline{111\ldots1}}_{k} \mid \underbrace{\overline{111\ldots1}}_{n}$, právě když $k \mid n$.

Příklad 14. Dokažte, že pro každé liché m, které není násobkem pěti, existuje přirozené n takové, že $m \mid \underbrace{\overline{111\ldots1}}_{n}$.

Příklad 15. Dokažte, že číslo $\overline{4\underbrace{44\ldots4}_{n}\underbrace{88\ldots8}_{n}9}$ pro celé nezáporné číslo n je čtverec přirozeného čísla.

Příklad 16. Dokažte, že číslo zapsané pomocí $2n$ jedniček zmenšené o číslo zapsané pomocí n dvojek je čtvercem přirozeného čísla.

Těžší příklady

Následující úlohy jsou trochu obtížnější a je potřeba přijít na nějakou rafinovanější metodu, jak je vyřešit.

Příklad 17. Přirozené číslo N je šestnácticiferné. Dokažte, že součin některých jeho po sobě jdoucích cifer je čtverec přirozeného čísla. (MKS 28–5–7)

Příklad 18. Dokažte, že pro každé přirozené číslo n existuje n-ciferné číslo, které je dělitelné 2^n a jehož cifry jsou pouze jedničky a dvojky. (MKS 26–4–6)

Příklad 19. Zjistěte, zda je číslo $\lfloor (1+\sqrt{2})^{2010!} \rfloor$ liché, nebo sudé. (MKS 30–1–7)

[1] Symbol $\lfloor x \rfloor$ znamená dolní celou část čísla x, tedy největší celé číslo, které není větší než x.

Příklad 20. Mějme číslo 2^{2013}. V každém kroku vymažeme poslední číslici a přičteme k nově vzniklému číslu, takto pokračujeme, dokud nezískáme deseticiferné číslo. Dokažte, že toto číslo má alespoň dvě cifry stejné.

Příklad 21. Dokažte, že pro každou posloupnost číslic $a_1, a_2, \dots, a_n$ existuje přirozené k takové, že k^2 začíná $\overline{a_1 a_2 \dots a_n \dots}$.

Příklad 22. Najděte dvě podobná čísla (viz příklad 5), která mají stejnou množinu prvočíselných dělitelů. (ARO 2004)

Tatrankové úlohy

A úplně na závěr dvě těžké úlohy, jejichž vyřešením si ode mě vysloužíte tatranku! Tak směle do toho:

Příklad 23. Dokažte, že pro libovolná přirozená čísla a, b existuje nějaký přirozený násobek a, jehož zápis v soustavě o základu b obsahuje všechny cifry $0, 1, \dots, b-1$.

Příklad 24. Existuje rostoucí aritmetická posloupnost mající 10 000 členů taková, že ciferné součty jejích členů také tvoří rostoucí aritmetickou posloupnost?

Návody

1. Jak vypadá zápis dvojciferného čísla v desítkové soustavě? A jak zápis čísla vzniklého prohozením jeho cifer?

2. Nějak si označte původní číslo bez první cifry, sestavte rovnici a dokažte, že žádné takové neexistuje.

3. Vyjádřete, kolik mají čísla 2^n, 5^n cifer a vynásobte příslušné nerovnosti.

4. Odhadněte levou a pravou stranu pomocí nerovnosti, abyste omezili počet cifer (všimněte si, že pro velká čísla je pravá strana menší než levá), poté vyřešte příslušné rovnice.

5. Přečtěte si název této kapitoly, dejte jej do souvislosti s podobnými čísly a použijte tvrzení.

6. O kolik se zvětší m, pokud zvětšíme n o 1?

7. Takové číslo existuje, skládá se ze samých nul a jedniček „správně daleko“ od sebe.

8. Sestavte rovnici.

9. Chcete vlastně zjistit hodnotu čísla $(111\dots1)_q$, kde q je kvocient. Co dostanete, když toto číslo vynásobíte $q-1$ a přičtete jedničku?

10. Vyjádřete rovnicí. Nejdřív zkoumejte, jaké to může být prvočíslo, poté rozložte na součin.

11. Kdy začíná mocnina dvojky jedničkou? Ve druhé části podle podobného kritéria rozdělte mocniny dvojky na skupiny a všimněte si, co mají společného ty skupiny, kde nějaká mocnina dvojky začíná čtyřkou.

12. Indukcí dokažte, že $3 \mid \underbrace{\overline{111\ldots1}}_{3^n}$.

13. Uvědomte si, že když $\underbrace{\overline{111\ldots1}}_{k} \mid \underbrace{\overline{111\ldots1}}_{n}$, musí $\underbrace{\overline{111\ldots1}}_{k} \mid \underbrace{\overline{111\ldots1}}_{n-k}$.

14. Vezměte si čísla $1, 11, \ldots, \underbrace{\overline{11\ldots1}}_{m+1}$.

15. Buď dokažte, že to je $\overline{\underbrace{6\ldots6}_{n}7}$, nebo si jej vyjádřete jako $4\cdot\underbrace{\overline{1\ldots11}}_{2n+2}+4\cdot\underbrace{\overline{1\ldots11}}_{n+1}+1$ a využijte vzorec pro součet geometrické posloupnosti.

16. Vyjádřete si obě čísla pomocí vzorce pro součet geom. posloupnosti a upravte pomocí vzorce $a^2 + 2ab + b^2 = (a + b)^2$

17. Vezměte si součin prvních i cifer pro všechna i od jedné do šestnácti, použijte rozklad na prvočísla a Dirichletův princip.

18. Indukcí takové číslo zkonstruujte.

19. Přičtěte vhodné jiné číslo, jehož paritu znáte, tak, abyste mohli jednoduše zjistit paritu součtu (pomocí binomické věty).

20. Ukažte, že žádný krok nezmění zbytek po dělení devíti.

21. Použijte tuto úvahu: dva po sobě jdoucí čtverce, které mají hodně číslic, se od sebe liší pouze na těch číslicích vzadu.

22. Využijte vlastností čísel $\overline{31\cdot111\ldots1}$, $\overline{13\cdot111\ldots1}$ a výsledku příkladu 14.

Literatura

[1] Andreescu, Dospinescu: *Problems From the Book*, XYZ Press, 2008.
[2] Herman, Kučera, Šimša: *Metody řešení matematických úloh I*, Brno, 2001.
[3] *http://www.artofproblemsolving.com.*

Algoritmy z teorie čísel

Filip Hlásek

Abstrakt. Příspěvek shrnuje základní matematické metody především z teorie čísel, které je možné využít k návrhu velice efektivních algoritmů. K vyřešení samotných úloh musíme často přidat i špetku důvtipu.

Úmluva. Všechna čísla v celém příspěvku jsou celá.

Důležité poznatky z teorie čísel

Tvrzení. (Bézoutova rovnost) *Pro každá dvě přirozená čísla a, b existují celá čísla α, β taková, že $\gcd(a, b) = \alpha \cdot a + \beta \cdot b$, kde $\gcd(a, b)$ značí největšího společného dělitele čísel a, b.*

Poznámka. Později tvrzení dokážeme tím, že vyhovující α a β přímo nalezneme.

Tvrzení. (Malá Fermatova věta) *Pro každé prvočíslo p a každé celé číslo a takové, že $\gcd(p, a) = 1$, dává a^{p-1} po dělení p zbytek roven jedné (neboli $a^{p-1} \equiv 1 \pmod p$).*

Tvrzení. (Čínská věta o zbytcích) *Mějme $m_1, m_2, \ldots, m_r$ po dvou nesoudělná přirozená čísla a $0 \leq a_1 < m_1, 0 \leq a_2 < m_2, \ldots, 0 \leq a_r < m_r$ libovolná. Potom existuje právě jedno $0 \leq x < m_1 \cdot m_2 \cdots m_r$ takové, že dává zbytek a_i po dělení m_i pro všechna $i = 1, 2, \ldots, r$.*

Tvrzení. (Multiplikativní inverz) *Buď p prvočíslo a $0 < a < p$. Pak existuje právě jedno $0 < b < p$ takové, že ab dává po dělení p zbytek jedna (neboli $ab \equiv 1 \pmod p$).*

Samotné algoritmy

Algoritmus je postup, jak něco vyřešit. Obvykle je popsán posloupností kroků, které jsou jednoznačné a vedou ke správnému výsledku. Několik takových algoritmů si zkusíme navrhnout na tradičních úlohách, které se nám později budou hodit.

Příklad. (Eratosthenovo síto) Pro dané N nalezněte všechna prvočísla, která jsou menší nebo rovna N.

Příklad. (Rozšířený Eukleidův algoritmus) K zadaným přirozeným číslům a, b nalezněte α, β splňující Bézoutovu rovnost $\gcd(a, b) = a \cdot \alpha + b \cdot \beta$.

Příklad. (Rychlé mocnění) Mějme přirozená čísla b, N a M. Navrhněte algoritmus, který spočítá zbytek b^N po dělení číslem M. Zajímá nás především efektivita algoritmu vzhledem k N.

Definice. (Kombinační číslo) Pro $0 \leq K \leq N$ budeme symbolem $\binom{N}{K}$ (čteme *„kombinační číslo N nad K“* nebo jen *„N nad K“*) značit počet způsobů, jak z N-prvkové množiny vybrat K-prvkovou podmnožinu.

Cvičení. (Násobení a sčítání modulo) Pokud nás zajímá zbytek součtu po dělení nějakým přirozeným číslem, stačí nejprve „vymodulit“ jednotlivé sčítance, poté zbytky sečíst a na závěr opět „vymodulit“. Analogicky to platí také pro násobení. Dokažte.

Příklad. (Kombinační číslo modulo prvočíslo) Pro zadaná $0 \leq K \leq N \leq M$ (M je prvočíslo) spočítejte zbytek po dělení $\binom{N}{K}$ číslem M. Vylepšete algoritmus tak, aby si nejprve něco předpočítal a poté odpovídal na kombinační čísla efektivně.

Příklad. (Fibonacciho čísla) Spočtěte zbytek N-tého členu Fibonacciho posloupnosti[1] po dělení zadaným přirozeným číslem M.

Ostré úlohy

Příklad 1. Jsou dány rozměry mřížky $1 \leq M, N \leq 100\,000$. Dále je zadáno $1 \leq K \leq 100$ mřížových bodů, na kterých leží kámen. Navrhněte algoritmus, který spočítá počet cest po mřížce z levého horního do pravého dolního rohu, které jdou pouze doprava nebo dolů a které neprocházejí přes políčka s kameny. Vypište pouze zbytek po dělení číslem $10^9 + 9$. (MO 59–P–III–4)

Příklad 2. Nalezněte počet neprázdných podmnožin množiny

$$\{1^1, 2^2, 3^3, \ldots, 250\,250^{250\,250}\}$$

takových, že součet jejich prvků je dělitelný číslem 250. Zajímá nás pouze posledních 16 cifer odpovědi. (Project Euler [1] – úloha 250)

Příklad 3. Je dána mřížka $M \times N$, které chybí pravý horní roh o rozměrech $m \times n$. Kolik existuje různých cest z levého horního do pravého dolního rohu, které jdou po mřížce vždy jen doprava nebo dolů? Vypište zbytek po dělení výsledku číslem $10^9 + 7$. (Codechef [2] – December Challenge 2012 – problem CNTWAYS)

[1] Fibonacciho posloupnost je definována následujícím předpisem: $F_0 = 0$, $F_1 = 1$ a $F_{i+2} = F_{i+1} + F_i$ pro nezáporné celé i.

Příklad 4. Monča má dřevěnou šachovnici o rozměrech $R \times C$ a N kovových krychlí takových, že délky jejich hran jsou stejné jako délka strany jednoho čtverečku šachovnice. Můžete předpokládat, že $1 \leq R, C \leq 10$ a $1 \leq N \leq 100\,000$. Chce z nich na šachovnici postavit takové věže, aby bylo co nejvíce stěn nepřiléhajících k jiné stěně (krychle smí umísťovat jen do imaginární trojrozměrné mřížky určené šachovnicí). Navrhněte algoritmus, který spočítá počet rozložení maximalizujících počet viditelných stěn a vypište zbytek výsledku po dělení prvočíslem $10^9 + 9$.

(Rýchlostné programovanie [3] – úloha seecubes2)

Příklad 5. V nově vybudované obytné čtvrti stojí v řadě N obydlí. Chceme uspořádat večírek a seznámit tak zejména co nejvíce lidí, kteří doposud neměli příležitost k setkání. Kolika různými způsoby můžeme pozvat lidi z jednotlivých domů tak, aby nebyli pozváni obyvatelé tří po sobě jdoucích domů? Jinými slovy, kolik podmnožin domů neobsahuje tři po sobě jdoucí domy (včetně prázdné podmnožiny)? Pro $1 \leq N \leq 10^{15}$ vypište výsledek modulo $10^9 + 7$.

(Codechef [2] – September Challenge 2012 – problem CROWD)

Příklad 6. Je zadáno $1 \leq M \leq 10^{18}$ a $1 \leq N \leq 8$. Kolika způsoby je možné vyskládat mřížku $M \times N$ dominovými kostkami?[2] Vypište výsledek modulo $10^9 + 9$.

(variace MO 60–P–I–1)

Odkazy

[1] *http://projecteuler.net/*
[2] *http://www.codechef.com/*
[3] *http://people.ksp.sk/~acm*
[4] *http://www.cse.iitd.ernet.in/~sak/courses/ant/notes/ant.pdf*
[5] *http://www.math.leidenuniv.nl/~psh/ANTproc/02buhler.pdf*
[6] *http://mj.ucw.cz/papers/numth.pdf*

[2]Dominové kostky jsou tvaru 2×1 a v tomto případě na sebe nemusí navazovat tak, jak je tomu v původní hře.

Polynomy kvadratické a jiné

David Hruška

Začneme zlehka dobře známou kvadratickou rovnicí a potom se podíváme obecněji na polynomy. Nebudeme se moc zdržovat teorií, hlavně budeme řešit úlohy. K těm neřešeným jsou na konci příspěvku hinty. Tak pojďme na to!

Kvadratická rovnice

Tuhle legraci asi znáte ze školy, připomeňme si tedy základní vlastnosti.

Tvrzení. *Rovnice (kvadratická s koeficienty a, b, c; $a \neq 0$) tvaru $ax^2 + bx + c = 0$ má řešení (kořeny)*

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Pokud je výraz pod odmocninou (tzv. diskriminant) záporný, žádná reálná řešení rovnice nemá, pokud je roven nule, je řešení jedno a pokud je kladný, jsou řešení dvě. Rovnici potom také můžeme napsat jako $a(x - x_1)(x - x_2) = 0$.

Porovnáním dostáváme vztahy (Viètovy)

$$x_1 + x_2 = -\frac{b}{a} \quad \text{a} \quad x_1 x_2 = \frac{c}{a}.$$

Toto tvrzení projde zatěžkávací zkouškou v následujícím příkladu:

Příklad 1. Nechť a, b, c jsou různá reálná čísla. Podívejme se na rovnici

$$\frac{(x-a)(x-b)}{(c-a)(c-b)} + \frac{(x-b)(x-c)}{(a-b)(a-c)} + \frac{(x-a)(x-c)}{(b-c)(b-a)} = 1.$$

Rovnice vypadá velmi kvadraticky, přesto všechna tři (různá) čísla a, b, c jsou jejím řešením, o čemž se snadno přesvědčíme. Jak je to možné?

Tvrzení. *Grafem kvadratické funkce $f(x) = ax^2 + bx + c$ je parabola s vrcholem o souřadnicích $[-\frac{b}{2a}, -\frac{b^2}{4a} + c]$. Pro kladné a je vrchol minimem funkčních hodnot, pro záporné je maximem.*

Znalosti o kvadratické rovnici můžeme (možná trošku překvapivě) velmi dobře využít pro řešení (kvadratických) nerovností.

Příklad 2. Pro $x, y \in \mathbb{R}$ dokažte nerovnost $x^2 + y^2 + 1 \geq xy + x + y$.

Řešení. Na nerovnost se podíváme jako na nerovnici s neznámou x a upravíme ji na tvar kvadratické rovnice: $x^2 + x(-y-1) + y^2 - y + 1 \geq 0$. Koeficient kvadratického členu je kladný, takže levá strana je záporná pouze pro hodnoty mezi kořeny. Chtěli bychom tedy ukázat, že (nezávisle na y) má nejvýše jeden (tzv. dvojný) kořen (z geometrického hlediska chceme dokázat, že graf naší funkce je celý nad osou x). Diskriminant je roven: $D = (-y-1)^2 - 4(y^2 - y + 1) = -3(y-1)^2 \leq 0$. Nerovnice tedy platí pro všechna x nezávisle na y, z čehož již plyne dokazovaná nerovnost. Našli jsme i jediný případ rovnosti (pro nulový diskriminant se parabola dotýká osy x, čili $y = 1$, a tedy $x = \frac{1+1}{2} = 1$).

Příklad 3. Pro všechna reálná x, y dokažte následující nerovnosti.

$$x^2 + y^2 + 2y + 4 \geq xy + 2x$$
$$2x^2 + 2y^2 + 1 \geq x + y + 2xy$$

Podívejme se na něco trochu těžšího.

Příklad 4. Jsou dána různá reálná čísla a, b, c. Dokažte, že alespoň dvě z rovnic

$$(x-a)(x-b) = x - c$$
$$(x-b)(x-c) = x - a$$
$$(x-c)(x-a) = x - b$$

mají reálný kořen. (Rusko 2013)

Příklad 5. Nechť $P(x)$ a $Q(x)$ jsou kvadratické trojčleny, pro které platí, že rovnice $P\big(Q(x)\big) = 0$ má kořeny -22, 7, 13. Jaká čísla mohou být čtvrtým kořenem?

Příklad 6. Reálná čísla a, b mají následující vlastnost: kvadratická rovnice $x^2 + ax + b + 1 = 0$ má v množině reálných čísel dva různé kořeny, jejichž rozdíl je kladným kořenem rovnice $x^2 + ax + b + 1 = 0$.

(i) Dokažte nerovnost $b > 3$.
(ii) Vyjádřete kořeny obou rovnic pomocí b.

(MO 59–B–I)

Příklad 7. Buďte $f(x)$ a $g(x)$ kvadratické trojčleny s koeficientem 1 u kvadratického členu. Dokažte, že pokud rovnice $f\big(g(x)\big) = 0$, $g\big(f(x)\big) = 0$ nemají reálné kořeny, pak alespoň jedna z rovnic $f\big(f(x)\big) = 0$, $g\big(g(x)\big) = 0$ nemá reálné kořeny. (Rusko 2007)

Příklad 8. Kvadratický trojčlen $P(x) = x^2 + ax + b$ sdílí kořen s polynomem $P\Big(P\big(P(x)\big)\Big)$. Dokažte, že $P(0) \cdot P(1) = 0$. (Rusko 2011)

Příklad 9. (Těžší) Nechť $f(x) = x^2 + ax + b$ je kvadratický trojčlen takový, že rovnice $f\big(f(x)\big) = 0$ má čtyři reálné kořeny (počítáno včetně násobnosti), přičemž součet nějakých dvou z nich je roven -1. Dokažte, že $b \le -\frac{1}{4}$.

(Mecz Domaslav 2010)

Polynomy

Definice. Polynom stupně n je výraz tvaru

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

přičemž $a_n \neq 0$. Čísla $a_i \in \mathbb{R}$ jsou koeficienty polynomu a x je proměnná.

Poznámka. Podmínka $a_i \in \mathbb{R}$ není nutná, polynomy se definují i v jiných oborech, my se však budeme zabývat těmi reálnými.

Tvrzení. *Pokud $q \in \mathbb{R}$ je kořen $P(x)$, tak $(x - q) \mid P(x)$.*

Tvrzení. *Každý polynom stupně n má nejvýše n reálných kořenů.*

Důsledek. *Pokud se dva polynomy stupně n shodují v alespoň $n + 1$ různých hodnotách, jsou identické.*

Důsledek. (Viètovy vztahy) *Má-li polynom $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ n reálných kořenů $t_1, \ldots, t_n$, pak $P(x) = (x - t_1)(x - t_2) \cdots (x - t_n)$. Porovnáním koeficientů tak dostáváme*

$$a_i = (-1)^{n-i} \sum_{j_1 < \cdots < j_i} t_{j_1} \cdots t_{j_i} \qquad j_i \in \{1, \ldots, n\}.$$

Speciálně $a_0 = (-1)^n t_1 \cdots t_n$ a $a_{n-1} = -(t_1 + \cdots + t_n)$.

Lehčí příklady

Příklad 10. Vyřešte rovnice:

$$2x^5 + x^4 + 2x + 1 = 0,$$
$$x^6 + 2x^5 + 2x^4 + 2x^3 + 3x^2 + 4x + 2 = 0.$$

Příklad 11. Polynom $P(x)$ stupně 2012 pro $k = 1, \ldots, 2013$ splňuje $P(k) = \frac{1}{k}$. Určete $P(2014)$.

(MKS 29–1–8)

Příklad 12. Určete koeficienty polynomu $p(x) = x^4 + ax^2 + bx + c$, pokud znáte tři jeho kořeny 2, -3, 5.

Příklad 13. Nechť jsou a, b, c reálná čísla taková, že

$$\begin{aligned} a+b+c &> 0,\\ ab+ac+bc &> 0,\\ abc &> 0. \end{aligned}$$

Dokažte, že $a, b, c > 0$.

Příklad 14. Nechť a, b, c jsou kořeny polynomu x^3+5x^2+3. Spočtěte $\frac{1}{a}+\frac{1}{b}+\frac{1}{c}$ a $a^4+b^4+c^4$.

Těžší příklady

Příklad 15. Nechť $P(x)$ a $Q(x)$ jsou monické polynomy stupně 10 (tj. koeficient u x^{10} je 1). Dokažte, že pokud rovnice $P(x)=Q(x)$ nemá žádné reálné řešení, pak rovnice $P(x+1)=Q(x-1)$ reálné řešení má.

Příklad 16. Dokažte, že polynom $P(x)=(x-a_1)(x-a_2)\cdots(x-a_n)-1$, kde $a_i \in \mathbb{Z}$ jsou po dvou různá, nelze zapsat jako součin dvou polynomů stupně alespoň 1 s celočíselnými koeficienty.

(MKS 28–3–8)

Příklad 17. Polynom $P(x)$ stupně n má tu vlastnost, že $P(k) \in \mathbb{Z}$ pro všechna $k \in \{0,1,\ldots,n\}$. Dokažte, že potom už $P(x) \in \mathbb{Z}$ pro každé celé x.

Příklad 18. (Těžký) Pepa měl dvě stotice různých reálných čísel $(a_1, a_2, \ldots, a_{100})$, $(b_1, b_2, \ldots, b_{100})$. Políčka tabulky 100×100 vyplnil tak, že do políčka o souřadnicích $[i, j]$ napsal číslo $a_i + b_j$. Všiml si, že součin čísel v každém sloupci je 1. Dokažte, že součin čísel v každém řádku je -1.

Návody

1. Co kdyby rovnice ve skutečnosti kvadratická nebyla? Upravte ji.

3. Postupujte stejně jako v řešeném příkladu.

4. Pro spor předpokládejte, že dvě konkrétní rovnice (jsou cyklické) nemají reálné řešení, potom povolejte diskriminant.

5. Uvědomte si, co znamená, že je nějaké číslo kořenem $P\big(Q(x)\big)$. Představte si graf $Q(x)$.

6. Použijte Viètovy vztahy. A pak znovu. Prostě pořád.

7. Kde musí mít trojčlen $f(x)$ kořeny, aby $f(g(x))$ kořen neměl?

8. Dokažte, že $P(0)$ je společný kořen.

9. Nakreslete si obrázek. Z toho, že má $f\big(f(x)\big)$ čtyři řešení, odvoďte $4b \le a^2 - 2a$. Rozeberte dva případy podle toho, které dva kořeny dávají součet -1.

10. Rozložte. Uhádněte kořen.

11. Jak to vypadá s kořeny polynomu $Q(x) = xP(x) - 1$?

12. Koeficient u kubického členu je nula. Co nám potom říkají Viètovy vztahy?

13. Nepřipadají vám ty výrazy nějak povědomé?

14. Opět Viètovy vztahy a potom chytře vyjádřit, co je třeba, pomocí toho, co už známe.

15. Zamyslete se nad stupni polynomů $P(x) - Q(x)$ a $P(x+1) - Q(x-1)$.

16. Postupujte sporem. Polynomy z předpokládaného rozkladu sečtěte a něco vhodného do nich dosaďte.

17. Nejprve dokažte, že $P(x)$ má racionální koeficienty. Potom dokažte, že společný jmenovatel koeficientů jakožto zlomků nedělí moc velká prvočísla.

18. Ze zadání vyrobte polynom(y) a pak překlápějte podle osy y.

Literatura a zdroje

[1] Vít Musil, *Triky s kvadratickou rovnicí*, Sborník MKS, Dobrá Voda, 2010.
[2] Michal Szabados, *Triky s polynómami*, Sborník MKS, Staré Město, 2009.
[3] *http://www.artofproblemsolving.com.*

Rozlouskneme RSA?

Jakub „Roman“ Klemsa

Abstrakt. RSA je moderní (1977) asymetrická šifrovací metoda, na které je postavena většina dnešních šifrovacích systémů. Nejprve si ukážeme princip fungování na základě Eulerovy věty, poté si vyzkoušíme něco zašifrovat. Předvedeme si i několik jak teoretických, tak praktických způsobů prolomení této šifry, taktéž na příkladech.

Eukleidův algoritmus

Připomeneme si Eukleidův algoritmus. BÚNO předpokládejme $a > b$ a postupujme takto, dokud jsou oba členy NSD nezáporné:

$$\mathrm{NSD}(a,b) = \mathrm{NSD}(a-b,b) = \ldots = \mathrm{NSD}(a-k_1b,b).$$

Označíme $r_1 := a - k_1b = a \mod b$ a víme, že $0 \leq r_1 < b$. Pokud $r_1 = 0$, algoritmus končí s hodnotou b, pokud ne, opakujeme algoritmus pro dvojici b, r_1:

$$\mathrm{NSD}(a,b) = \mathrm{NSD}(r_1,b) = \mathrm{NSD}(r_1,b-k_2r_1) = \mathrm{NSD}(r_1,r_2),$$

kde $r_2 = b \mod r_1$. Rekurzivně opakujeme, dokud nedojdeme k $\mathrm{NSD}(r_k,0) = r_k$.

Tvrzení. *Zpětným postupem dokážeme z Eukleidova algoritmu najít celá čísla x_0, y_0 taková, že $\mathrm{NSD}(a,b) = ax_0 + by_0$. Protože $k(ab - ba) = 0$ a každé z čísel a, b je dělitelné $\mathrm{NSD}(a,b)$, najdeme zbývající řešení pomocí*

$$\mathrm{NSD}(a,b) = k\left(a\frac{b}{\mathrm{NSD}(a,b)} - b\frac{a}{\mathrm{NSD}(a,b)}\right) + ax_0 + by_0$$

ve tvaru $x = x_0 + k\frac{b}{\mathrm{NSD}(a,b)}$, $y = y_0 - k\frac{a}{\mathrm{NSD}(a,b)}$, kde $k \in \mathbb{Z}$. Ukazuje se, že toto jsou již všechna řešení rovnice $ax + by = \mathrm{NSD}(a,b)$.

Cvičení. Pomocí Eukleidova algoritmu najděte $\mathrm{NSD}(432,234)$ a dvě „nejbližší“ dvojice celých čísel x, y, aby platilo $\mathrm{NSD}(432,234) = 432x - 234y$.

Asymetrická šifra RSA

Šifru RSA navrhli roku 1977 matematici Rivest, Shamir a Adleman. Jde o šifru s jedním veřejným šifrovacím klíčem a jedním soukromým, dešifrovacím.

Pro šifrování pomocí RSA budeme potřebovat dvě velká (ale opravdu velká) prvočísla p a q, jejich vynásobením dostaneme tzv. modulus $n = pq$. Odtud známe i hodnotu Eulerovy funkce $\varphi(n) = (p-1)(q-1)$. Dále vygenerujeme veřejný exponent (klíč) e takový, aby platilo $e \perp \varphi(n)$, $1 < e < \varphi(n)$. Nesoudělnost ověříme Eukleidovým algoritmem, odkud zjistíme i koeficienty d a k takové, že $ed - k\varphi(n) = 1$. Najdeme d takové, že $1 < d < \varphi(n)$. Toto d bude náš soukromý exponent.

Dvojici (n, e) uveřejníme jako veřejný klíč, dvojici (n, d) uchováme jako soukromý klíč, prvočísel p, q společně s hodnotou $\varphi(n)$ se bezpečně zbavíme.

Postup šifrování (Alice $\to$ Bob):

(i) Alice si nechá poslat od Boba jeho veřejný klíč (n, e),
(ii) tajnou zprávu (číslo $m < n$) Alice zašifruje jako $c = m^e \mod n$,
(iii) Bob dešifruje c svým soukromým klíčem (n, d) nápodobně: $m = c^d \mod n$.

Tvrzení. *Pro m, e, d, n splňující požadavky RSA platí*

$$c^d \equiv m^{ed} \equiv m \pmod{n}.$$

Poznámka. Na tomto stojí funkčnost RSA. Její bezpečnost jsme tím neukázali.

Rozlousknutí RSA: faktorizace

RSA bychom zlomili, pokud bychom uměli vyřešit alespoň jeden z následujících problémů v polynomiálním čase:

(i) najít prvočíselný rozklad velkého čísla (factorization problem),
(ii) spočítat d ze znalosti (n, e),
(iii) vypočítat e-tou odmocninu modulo n (tzv. RSA problem).

Nejslibnější přístup se zdá být faktorizace n, zbytek lze už snadno dopočítat. Bohužel, nebo spíše naštěstí, není znám polynomiální algoritmus pro faktorizaci velkých čísel.[1] Zároveň ale nebylo dokázáno, že neexistuje.

O mnoho větší problém by nastal, pokud by se skutečně podařilo sestavit kvantový počítač a „naučit“ ho faktorizovat. Peter Shor v roce 1994 ukázal, že kvantový počítač k tomuto účelu postavený by byl schopen faktorizovat v polynomiálním čase!

[1] Stačí číslo n o několik cifer prodloužit a nepříteli bude trvat násobně déle rozklad najít. To činí RSA tak bezpečnou.

Fermatova metoda

Tato metoda předpokládá malý rozdíl p a q, prakticky $p - q < 2n^{\frac{1}{4}}$. Označme $D := \frac{p-q}{2}$. Všimneme si, že

$$n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2,$$

odtud $n + D^2 = \left(\frac{p+q}{2}\right)^2$. Pro malá D testujeme, jestli je číslo $n + D^2$ čtverec (krok lze volit i větší než 1). Jakmile takové D najdeme, dopočteme p a q ze soustavy rovnic

$$p, q = \sqrt{n + D^2} \pm D.$$

Cvičení. Faktorizujte 437 Fermatovou metodou.

Pollardova $p - 1$ metoda

Pollardova $p - 1$ metoda předpokládá, že alespoň pro jeden faktor n (ozn. p) má číslo $p - 1$ všechny své faktory relativně malé (omezené nějakým b). Nyní můžeme odhadnout[2] například $k = b!$ jako násobek $p-1$, neboli $p-1 \mid k$. Dle Fermatovy věty pro dané a nesoudělné s p (což není problém najít, např. $a = 2$) platí

$$a^{p-1} \equiv 1 \pmod{p}.$$

Protože $p - 1 \mid k$, můžeme tuto kongruenci umocnit do tvaru

$$a^k \equiv 1 \pmod{p}.$$

Odtud $p \mid \mathrm{NSD}(a^k - 1, n)$, neboli můžeme předpokládat, že $p = \mathrm{NSD}(a^k - 1, n)$. Pokud vyjde 1, náš odhad k nebyl násobkem $p - 1$ ani $q - 1$, pokud vyjde n, odhad k byl násobkem obou. Podle toho zlepšujeme odhad k. Pro silná p, q je toto hádání velmi obtížné, protože dokud nenatipujeme všechny faktory $p - 1$, dostáváme jako NSD 1 a o $p - 1$ nadále nic nevíme. A pokud ano, je dost pravděpodobné, že máme i všechny faktory $q - 1$ a dostaneme jako NSD n.

Cvičení. Faktorizujte 377 Pollardovou $p - 1$ metodou.

[2]Lze provést i jiný odhad čísla, které by mohlo být násobkem $p - 1$.

Wienerův útok

Tvrzení. (Wiener) *Nechť pro prvočíselnou dvojici platí $q < p < 2q$ a nechť dále soukromý klíč splňuje $d < \frac{1}{3}n^{\frac{1}{4}}$. Potom lze z veřejného klíče (n, e) efektivně získat soukromý klíč d včetně faktorizace $n = p \cdot q$.*

Postup je následující:

$$ed = k(p-1)(q-1) + 1,$$
$$\frac{e}{pq} = \frac{k}{d}\left(1 - \frac{p+q-1-\frac{1}{k}}{pq}\right) = \frac{k}{d}(1-\delta).$$

Výraz na levé straně známe, podíl $\frac{k}{d}$ je „o málo" větší. Snažíme se tedy získat postupné horní odhady – od nejhrubšího (tvaru $\frac{1}{l}$) až po samotný $\frac{e}{pq}$. K tomu poslouží zápis řetězovým zlomkem. Předvedeme příklad.

Příklad. Veřejný klíč budiž $(n, e) = (90\,581, 17\,993)$, cílem je získat klíč soukromý. Řetězový zlomek vyjde

$$\frac{17\,993}{90\,581} = \cfrac{1}{5 + \cfrac{1}{29 + \cfrac{1}{\ddots + \cfrac{1}{3}}}} = [0; 5, 29, 4, 1, 3, 2, 4, 3].$$

Odtud získáváme posloupnost odhadů

$$\frac{k}{d} = 0, \frac{1}{5}, \frac{29}{146}, \frac{117}{589}, \ldots, \frac{17\,993}{90\,581}.$$

Spočteme hodnotu Eulerovy funkce pro první smysluplný odhad $\frac{1}{5}$, tedy $k = 1$ a $d = 5$, a ověříme správnost:

$$\varphi(n) = \frac{ed-1}{k} = 89\,964,$$
$$x^2 - \big(n - \varphi(n) + 1\big)x + n = 0,$$

dostaneme kořeny $x_{1,2} = 379,\ 239$. Opravdu, $90\,581 = 379 \cdot 239$. Všimneme si, že dle Wienerova teorému bude útok fungovat, pokud $d < \frac{1}{3} \cdot N^{\frac{1}{4}} \doteq 5{,}7828$.

Rozlousknutí RSA: využití chyb(y) při šifrování

Generování prvočísel

Probíhá tak, že se vygeneruje náhodné číslo p, to se poté otestuje prvočíselnými testy.[3] Že je p skutečně prvočíslo není zaručené, je to jen extrémně nepravděpodobné. Úplně největší chybou je použít p dvakrát s různými q_i! Součiny $n_{1,2} = p \cdot q_{1,2}$ jsou veřejné, kdokoliv může okamžitě spočítat jejich NSD a tím zjistit p.

Slabiny zpráv

Každého napadne, že pokud je malé e i m, může se stát, že $m^e < n$. Takovou zprávu stačí jednoduše odmocnit, nedošlo totiž k modulení n. Myšlenka je doplnit zprávu zepředu náhodnými znaky. Ani zde není situace jednoduchá, původní verze standardu doplňování PKCS#1 dokonce měla slabinu.

Velkou chybu uděláme, pokud stejnou zprávu pošleme e nebo více příjemcům, kteří používají stejné e, ale různá p, q. Poté zprávu snadno rozluštíme pomocí Čínské zbytkové věty.

Chybou, kterou nejspíše neuděláme, je dešifrování protivníkem podvržené zprávy. Pokud k dešifrování předloží $c \cdot r^e \mod n$ pro zvolené r, dostane zpět $m \cdot r \mod n$.

Podepisování zpráv

Zatím jsme neřešili jednoduchou otázku: jak Bob zjistí, že mu zprávu poslala právě Alice, že se nejedná o podvrh? Zprávu následujícím způsobem „podepíše“.

Bob má dvojici klíčů (e_b, d_b), Alice chce poslat zprávu m majíc klíče (e_a, d_a). Zprávu m zašifruje Bobovým veřejným klíčem e_b, vypočte heš zprávy a zašifruje ji svým soukromým klíčem d_a. Bob dešifruje zprávu svým soukromým klíčem d_b, heš pomocí e_a. Heš dešifrované zprávy pak musí odpovídat dešifrované heši. Zprávu mohl poslat jedině ten, kdo zná klíč d_a.

[3] Popis těchto testů přesahuje rámec přednášky.

Obarvování

Bára Kociánová

Jak na to?

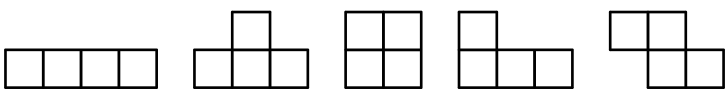
Obarvování je opravdu elegantní a účinný způsob, jak vyřešit některé kombinatorické úlohy. V principu rozdělíme množinu na konečný počet podmnožin a pro lepší představu pak jednotlivé části obarvíme různými barvami. V typických úlohách se často objevuje černobílá šachovnice, ale mnohdy je potřeba využít barev více.

Řešení problému obarvováním je v podstatě třífázové – nejdříve si musíme uvědomit, že je to obarvovací úloha, dále vymyslet vhodné rozdělení na části a pak už zbývá jen okomentovat, proč něco je, případně není možné.

Příklad 1. Obyčejné šachovnici 8×8 uřežeme dva protější rohy. Kolika způsoby je pak možné ji pokrýt dominovými kostkami?

Řešení. Každá dominová kostka zakrývá právě jedno políčko od každé barvy. Dohromady tedy 31 kostek potřebných k pokrytí šachovnice pokrývá 31 bílých a 31 černých polí. Na šachovnice bez dvou protějších rohů je ale polí jedné barvy 32 a druhé jen 30. Proto takovou šachovnici dominem nemůžeme pokrýt.

Příklad 2. Je možné vytvořit obdélník z pěti různých tetromin? Konkrétně z rovného, T-tetromina, čtvercového, L-tetromina a šikmého (postupně na obrázku).



Příklad 3. Můžeme pokrýt šachovnici o rozměrech 8×8 patnácti T-tetrominy a jedním čtvercovým?

Příklad 4. Ukažte, že šachovnici 10×10 nemůžeme vyplnit rovnými tetrominy.

Příklad 5. Na každém poli šachovnice $n \times n$ sedí beruška. Po zaznění výstřelu se každá přesune na pole, které hranou sousedí s jejím původním místem. Pro která n mohou být znovu obsazená všechna políčka?

Příklad 6. Potřebujeme zabalit 53 kostek $1 \times 1 \times 4$ a máme jen krabici $6 \times 6 \times 6$. Bude nám stačit, nebo musíme koupit větší?

Příklad 7. Obdélníková podlaha koupelny je pokrytá kachličkami 2×2 a 1×4. Jedna dlaždička se rozbila a od toho druhu už žádné další nejsou. Dokažte, že pomocí druhého typu nejde podlaha opravit, ať kachličky jakkoli přeskládáme.

Příklad 8. Uřezali jsme jeden roh šachovnice $(2n+1) \times (2n+1)$. Pro která n můžeme plochu pokrýt dominovými kostkami tak, aby polovina z nich byla umístěna horizontálně?

Příklad 9. Dokažte, že obdélník $a \times b$ můžeme pokrýt obdélníky $1 \times n$ právě tehdy, když $n \mid a$ nebo $n \mid b$.

Příklad 10. Na ledové ploše trénuje hokejista. Má tři puky a pokaždé jeden z nich odpálí tak, že proletí mezi zbylými dvěma. Umí hokejista 1001. odpalem vrátit puky do původní pozice?

Příklad 11. Do tabulky 5×5 napíšeme do jednoho čtverečku -1 a do zbývajících 24 míst $+1$. V jednom tahu můžeme vybrat nějaký čtverec $a \times a$ (pro $a > 1$) a změnit v něm všechna znaménka. Na kterém místě musí být na začátku -1, abychom mohli získat tabulku plnou $+1$?

Příklad 12. V mřížce vyberme body $A = (0,0)$, $B = (0,1)$, $C = (1,0)$. V jednom tahu můžeme zobrazit bod ve středové souměrnosti podle jiného už označeného bodu. Můžeme se dostat k poslednímu bodu čtverce $D = (1,1)$?

Příklad 13. Galerie má tvar n-úhelníku. Najděte nejmenší počet dozorců, kteří dokážou ohlídat všechny obrazy, ať je tvar místnosti jakkoli složitý.

Příklad 14. Čtvercový dort o rozměrech 6×6 chceme shora pokrýt kousky čokolády 2×1. Ukažte, že ať plochu vyplníme jakkoli, vždy můžeme dort rozkrojit, aniž bychom krájeli dvojdílek čokolády.

Příklad 15. Ukažte, že šachový kůň nemůže skočit právě jednou na všechna pole šachovnice $4 \times n$ a znovu se vrátit na původní.

Návody

2. Obarvení šachovnice.

3. Počet černých polí pokrytých T-tetrominem.

4. Hrubší šachovnice.

5. Šachovnice.

6. Hrubá šachovnice do prostoru.

7. Děravá šachovnice.

8. Sloupce.

9. Obarvení n sloupců n barvami.

10. Orientace trojúhelníku.

11. Bílý sloupec uprostřed a rotace.

12. Obarvení bodů podle parity souřadnic.

13. Rozdělení na trojúhelníky.

14. Počet možných řezů a počet dvojdílků čokolády.

15. Čtyři barvy.

Literatura

[1] Arthur Engel, *Problem-Solving Strategies*, Springer, UK, 1998.

Složená čísla

ANH DUNG „TONDA“ LE

ABSTRAKT. Příspěvek se zabývá složenými čísly a souvisejícími pojmy. Podíváme se na různé typy úloh a na některé postupy, jak přijít na řešení, která mohou na první pohled vypadat triková a nepřirozená.

Úmluva. Všechny proměnné v dalším textu jsou z oboru celých čísel, nebude-li řečeno jinak.

Tvrzení. (Malá Fermatova věta) *Pro prvočíslo p a přirozené číslo a takové, že $p \nmid a$, platí*

$$a^{p-1} \equiv 1 \pmod p.$$

Malá Fermatova věta se často kombinuje s následujícím užitečným tvrzením.

Tvrzení. („Krácení exponentů“) *Pro přirozená čísla a, b, m, n taková, že a, b jsou nesoudělná s prvočíslem p, platí následující tvrzení. Pokud*

$$\begin{aligned} a^m &\equiv b^m \pmod p, \\ a^n &\equiv b^n \pmod p, \end{aligned}$$

potom

$$a^{\mathrm{NSD}(m,n)} \equiv b^{\mathrm{NSD}(m,n)} \pmod p.$$

Příklad 1. Dokažte, že pro přirozená čísla x, y, z platí:

(i) $x + y + z$ dělí $x^3 + y^3 + z^3 - 3xyz$.

(ii) Pokud $2z^2 = 3xy$, pak $x + y - z$ dělí $x^3 + y^3 + z^3$.

Příklad 2. Dokažte, že $4^{125} + 125^4$ a $4^{245} + 245^4$ jsou složená čísla.

Příklad 3. Dokažte, že 104 060 401 je složené číslo.
(MM, Problem Q614, Rod Cooper)

Příklad 4. Dokažte, že 1 280 000 401 je složené číslo. (Estonsko TST 2004)

Příklad 5. Pomocí příkladu 1 (i) dokažte, že $512^3 + 675^3 + 720^3$ je složené číslo.

Příklad 6. Pomocí příkladu 1 (ii) najděte dělitele čísla $2^{33} - 2^{19} - 2^{17} - 1$ v intervalu od 1 000 do 5 000. (MM, Problem Q684, Noam Elkies)

Příklad 7. Dokažte, že $\frac{5^{125}-1}{5^{25}-1}$ je složené číslo. (IMO shortlist 1992, P16)

Příklad 8. Najděte nejmenší složené číslo n, pro které platí $n \mid 3^{n-1} - 2^{n-1}$.

Příklad 9. Nechť a, b, c, d jsou přirozená čísla splňující $a^2 + b^2 + ab = c^2 + d^2 + cd$. Dokažte, že $a + b + c + d$ je složené číslo.

Příklad 10. Dokažte, že existuje přirozené číslo k takové, že $k2^n + 1$ je složené číslo pro každé přirozené n. (USAMO 1982)

Příklad 11. Nechť x, y jsou celá čísla taková, že $2 \leq x, y \leq 100$. Dokažte, že $x^{2^n} + y^{2^n}$ je složené číslo pro nějaké přirozené číslo n.

Příklad 12. Dokažte, že pro každé přirozené číslo k a celočíselný nekonstantní polynom P existuje k po sobě jdoucích čísel takových, že funkční hodnoty polynomu P ve všech těchto číslech jsou složená čísla.

Příklad 13. Uvažme celá čísla $a > b > c > d > 0$ splňující

$$ac + bd = (b + d + a - c)(b + d - a + c).$$

Dokažte, že $ab + cd$ je složené číslo. (IMO 2001, 6)

Příklad 14. Dokažte, že $n^n + (n + 1)^{n+1}$ je složené pro nekonečně mnoho přirozených n.

Příklad 15. Dokažte, že pro každé přirozené číslo $k > 1$ existuje nekonečně mnoho přirozených čísel n takových, že $k2^{2^n} + 1$ je složené číslo.

Příklad 16. Dokažte, že existuje přirozené číslo N takové, že pro každé přirozené číslo $n > N$ existuje $2n$ po sobě jdoucích složených čísel menších než $n!$.

Literatura a zdroje

[1] *http://www.mathlinks.ro.*
[2] Hojoo Lee, *Problems in Elementary Number Theory.*

Rozklad výrazů obsahujících $a-b$, $b-c$, $c-a$

Vít „Vejtek“ Musil

Abstrakt. Příspěvek obsahuje sadu logicky navazujících příkladů, jejichž cílem je ukázat jednoduchost a sílu několika elementárních algebraických obratů.

Fundamentální vlastností čísel $a-b$, $b-c$ a $c-a$ je to, že jejich součet je nula:

$$(a-b)+(b-c)+(c-a)=0.$$

Stejně tak platí, že pokud nějaká reálná čísla x, y, z dávají součet nula, můžeme najít čísla a, b a c splňující

$$x=a-b \quad y=b-c \quad z=c-a.$$

Vskutku, stačí vzít $a=0$, $b=-x$ a $c=z$. Jistě však čísla a, b, c nejsou určena jednoznačně – přičteme-li ke každému z nich stejnou konstantu, nová trojice splňuje tytéž rovnosti jako a, b a c.

Často se lze setkat s výrazy typu

$$(a-b)P(a,b,c)+(b-c)Q(a,b,c)+(c-a)R(a,b,c),$$

kde P, Q, R jsou polynomy nebo racionální funkce, a nezřídka mají tyto výrazy zajímavé rozklady na součin. Metoda pro jejich získání je velmi snadná, prostě položíme $c-a=-(a-b)-(b-c)$ a vytkneme členy obsahující zvlášť $a-b$ a $b-c$.

Následující příklad by nás měl přesvědčit, že jde o nástroj značně univerzální.

Příklad. Rozložte $a^2(b-c)+b^2(c-a)+c^2(a-b)$ a najděte nutnou a postačující podmínku pro a, b, c, aby platilo

$$a^2b+b^2c+c^2a=ab^2+bc^2+ca^2.$$

Řešení. Nahraďme $c-a$ výrazem $-(a-b)-(b-c)$. Dostáváme

$$\begin{aligned} a^2(b-c)+b^2(c-a)+c^2(a-b) &= a^2(b-c)+c^2(a-b)+b^2\big(-(a-b)-(b-c)\big) \\ &= (a-b)(c^2-b^2)+(b-c)(a^2-b^2) \\ &= (a-b)(c-b)(c+b)+(b-c)(a-b)(a+b) \\ &= (a-b)(c-b)\big(c+b-(a+b)\big) \\ &= -(a-b)(b-c)(c-a). \end{aligned}$$

Odtud speciálně plyne, že $a^2b+b^2c+c^2a=ab^2+bc^2+ca^2$ právě tehdy, když jsou dvě z čísel a, b, c stejná.

Není-li řečeno jinak, jsou a, b, c vždy reálná čísla.

Příklad 1. Rozložte $a^4(b-c)+b^4(c-a)+c^4(a-b)$ a najděte všechny trojice a, b, c, pro které je tento výraz nulový.

Příklad 2. Rozložte

$$(a-b)(a^2+b^2-c^2)c^2+(b-c)(b^2+c^2-a^2)a^2+(c-a)(c^2+a^2-b^2)b^2.$$

Příklad 3. Dokažte, že pro všechna reálná čísla a, b, c splňující $(a+b)(b+c)(c+a)\neq 0$ platí

$$\frac{a-b}{a+b}+\frac{b-c}{b+c}+\frac{c-a}{c+a}=-\frac{a-b}{a+b}\cdot\frac{b-c}{b+c}\cdot\frac{c-a}{c+a}.$$

Příklad 4. Dokažte, že pro všechna po dvou různá reálná čísla a, b, c platí

$$\frac{a+b}{a-b}\cdot\frac{a+c}{a-c}+\frac{b+c}{b-c}\cdot\frac{b+a}{b-a}+\frac{c+a}{c-a}\cdot\frac{c+b}{c-b}=1.$$

Příklad 5. Dokažte, že pro všechna po dvou různá reálná čísla a, b, c platí

$$\frac{bc}{(a-b)(a-c)}+\frac{ca}{(b-c)(b-a)}+\frac{ab}{(c-a)(c-b)}=1.$$

Příklad 6. Dokažte pro všechna po dvou různá reálná čísla a, b, c nerovnost

$$\frac{a^2}{(b-c)^2}+\frac{b^2}{(c-a)^2}+\frac{c^2}{(a-b)^2}\geq 2.$$

Příklad 7. Dokažte, že pro všechna po dvou různá reálná čísla a, b, c platí

$$\frac{a-b}{1+ab}+\frac{b-c}{1+bc}+\frac{c-a}{1+ca}\neq 0.$$

Příklad 8. Dokažte pro všechna čísla a, b, c rovnost

$$(a-b)^5+(b-c)^5+(c-a)^5=5(a-b)(b-c)(c-a)(a^2+b^2+c^2-ab-bc-ca).$$

Příklad 9. Rozložte $a^3(b-c)^3+b^3(c-a)^3+c^3(a-b)^3$ a najděte všechny trojice a, b, c, pro které je tento výraz nulový.

Příklad 10. Reálná čísla a, b, c splňují

$$(b-c)\sqrt[3]{1-a^3}+(c-a)\sqrt[3]{1-b^3}+(a-b)\sqrt[3]{1-c^3}=0.$$

Dokažte, že

$$(1-a^3)(1-b^3)(1-c^3)=(1-abc)^3.$$

Příklad 11. Kladná reálná čísla a, b, c splňují

$$\frac{a(b-c)}{b+c}+\frac{b(c-a)}{c+a}+\frac{c(a-b)}{a+b}=0.$$

Dokažte, že $(a-b)(b-c)(c-a)=0$.

Příklad 12. Dokažte, že pro všechna po dvou různá reálná čísla a, b, c platí

$$a^2\frac{(a+b)(a+c)}{(a-b)(a-c)}+b^2\frac{(b+c)(b+a)}{(b-c)(b-a)}+c^2\frac{(c+a)(c+b)}{(c-a)(c-b)}=(a+b+c)^2.$$

Příklad 13. Dokažte, že pro všechna kladná reálná čísla a, b, c platí

$$a^2\frac{b+c}{b^2+c^2}+b^2\frac{c+a}{c^2+a^2}+c^2\frac{a+b}{a^2+b^2}\geq a+b+c.$$

Literatura

[1] Titu Andreescu, *105 Algebra Problems From the AwesomeMath Summer Program*, XYZ Press, 2013.

Může být číslo skoro racionální?

Vít „Vejtek“ Musil

Entrée

Pepa: Hej Vejte, umím dokázat, že $\sqrt{2}$ je iracionální.
Vejtek: Však to je hračka: Vezmu kalkulačku, zmáčknu $\sqrt{\ }$, pak dvojku a mrkneme se na odmocninu ze dvou na displeji. Je jasné, že je iracionální:

$$1.\ 4\ 1\ 4\ 2\ 1\ 3\ 5\ 6\ 2$$

Pepa: Co je to za kecy? Co kdyby měla periodický desetinný rozvoj s periodou delší než délka displeje? Když si namačkáš na kalkulačku třeba 25 děleno 17, taky dostaneš divokou posloupnost číslic:

$$1.\ 4\ 7\ 0\ 5\ 8\ 8\ 2\ 3\ 5$$

A přitom je to číslo racionální.
Vejtek: Na tom něco bude, nicméně pro čísla kolem nás moje metoda dává uspokojivé výsledky. Takže se mohu spolehnout, že moje kalkulačka mi pomůže odhalit, která čísla jsou racionální. Pravděpodobnost chyby bude mizivá.
Pepa: S tím nesouhlasím.

Kdo má pravdu?

Zkuste se kohokoliv zeptat a každý řekne, že Pepa. Když známe devět (nebo devadesát či devět milionů) číslic z desetinného rozvoje nějakého čísla, nemůžeme říct, zda je racionální nebo ne. Existuje nekonečně mnoho racionálních a iracionálních čísel se stejným počátečním úsekem desetinného rozvoje.

Stejně však se čísla z předchozího odstavce, jakkoliv se mohou zdát podobná, v něčem zásadním liší. Druhé je velmi blízko racionálnímu číslu $\frac{25}{17}$, rozdíl mezi $\frac{25}{17}$ a $1.470\,588\,235$ je zhruba $3 \cdot 10^{-10}$. Naproti tomu k číslu $1.414\,213\,562$ neexistuje tak blízký zlomek s dvouciferným jmenovatelem. Nejblíže je číslo $\frac{99}{70}$, a to s chybou okolo $7 \cdot 10^{-5}$. Nejkratší zlomek aproximující $\sqrt{2}$ s chybou $3 \cdot 10^{-10}$ je $\frac{47\,321}{33\,461}$, což je o dost delší zlomek než $\frac{25}{17}$. Podstatné je, že tuto vlastnost, pouhým okem nerozeznatelnou, lze snadno odhalit jednoduchými výpočty na kapesním kalkulátoru.

Trik

Budeme potřebovat kalkulačku, která zvládne sčítat, odčítat, násobit a dělit. Někdo nám dá dvě čísla mezi 0.5 a 1, například

$$0.635\,149\,023 \quad \text{a} \quad 0.728\,101\,457.$$

Jedno z těchto čísel by mělo vzniknout jako podíl dvou čísel, kde dělitel je menší než 1000, druhé by mělo být náhodné. Tvrdíme, že s pomocí kalkulačky dokážeme během minuty zjistit, které z předložených čísel je onen podíl, a dokonce najdeme vyjádření ve tvaru zlomku.

Jak na to?

Podstata triku bude obsahem přednášky. Zjednodušeně řečeno, jedno z výše zmíněných čísel je *skoro racionální*, zatím co to druhé ne — ať už to znamená cokoliv.

Co je dobrá aproximace?

Buď α iracionální číslo. Na základě čeho usoudíme, že zlomek $\frac{p}{q}$ (kterýžto uvažujeme v základním tvaru) je dobrou aproximací čísla α? Jednak nám záleží na velikosti chyby $\left|\alpha - \frac{p}{q}\right|$, která by měla být malá, dále chceme, aby čísla p a q nebyla moc velká. Čitatel p závisí na α a ne na přesnosti aproximace. Chceme tedy minimalizovat chybu $\left|\alpha - \frac{p}{q}\right|$ a jmenovatele q. Zřejmě zmenšování chyby vede k růstu jmenovatele a naopak. Přirozeně tedy můžeme tyto požadavky nakombinovat do *ukazatele kvality* $q\left|\alpha - \frac{p}{q}\right|$. O aproximaci bychom pak řekli, že je *dobrá*, pokud je $q\left|\alpha - \frac{p}{q}\right|$ malé. K naší smůle však platí následující věta.

Věta 1. *Pro libovolné reálné číslo α a každé $\varepsilon > 0$ existuje nekonečně mnoho zlomků $\frac{p}{q}$ takových, že platí*

$$q\left|\alpha - \frac{p}{q}\right| < \varepsilon.$$

Ta říká, že všechna čísla jsou stejně *dobrá* a nedává nám tedy žádnou metodu, jak rozlišovat mezi čísly, která mají dobré racionální aproximace a která ne.

Jako zlepšovák můžeme zkusit použít jiný ukazatel kvality, který bude klást větší váhu na velikost jmenovatele q. Říkejme tedy, že aproximace $\frac{p}{q}$ je „dobrá“, pokud je součin $q^2\left|\alpha - \frac{p}{q}\right|$ malý. Následující věta říká, že tento výběr už je opodstatněný.

Věta 2.

(a) *Pro libovolné reálné číslo α existuje nekonečně mnoho zlomků $\frac{p}{q}$ takových, že platí*

$$q^2\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}}.$$

(b) *Existuje iracionální číslo α takové, že pro každé $\lambda > \sqrt{5}$ existuje pouze konečně mnoho zlomků $\frac{p}{q}$ splňujících*

$$q^2\left|\alpha - \frac{p}{q}\right| < \frac{1}{\lambda}.$$

Které že je to číslo α z tvrzení (b)? Jaké je nejiracionálnější ze všech iracionálních čísel, nejvíce se vyhýbající racionálním aproximacím? Překvapivě jde o číslo milované generacemi malířů, sochařů a architektů, zlatý řez[1] $\frac{1+\sqrt{5}}{2}$.

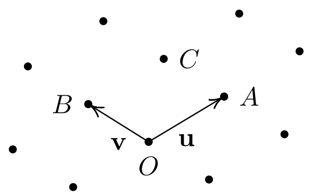
Geometrie čísel

Abychom odkryli pravdu skrývající se za těmito a mnoha dalšími pozoruhodnými tvrzeními, budeme používat čistě geometrické argumenty. Žádné upocené počty, žádné kanóny z teorie čísel, jen elementární hříčky s obrázky, které vystihují pravou podstatu problému.

Mřížka

Jedinou, a to základní, ingrediencí pro nás bude *mřížka*. Buď O bod v rovině (říkejme mu počátek) a $\mathbf{u} = \overrightarrow{OA}$, $\mathbf{v} = \overrightarrow{OB}$ dvě nekolineární šipky[2] (body O, A a B neleží v přímce). Šipka je svým koncovým bodem dána jednoznačně, často proto budeme tento bod a šipku zaměňovat. Šipky lze přirozeně sčítat i násobit reálným číslem. Za součet šipek $\mathbf{u}$ a $\mathbf{v}$ označíme šipku $\mathbf{u}+\mathbf{v}$, která je určena bodem, kam ukáže šipka $\mathbf{u}$ pokud ji posuneme o šipku $\mathbf{v}$, c-násobkem šipky $\mathbf{u}$ myslíme šipku $c\mathbf{u}$, která vznikne natažením šipky $\mathbf{u}$ c-krát.

Mřížkou (generovanou $\mathbf{u}$ a $\mathbf{v}$) rozumíme všechny možné součty $a\mathbf{u} + b\mathbf{v}$, kde a a b jsou celá čísla. Mřížku tak vlastně tvoří všechny body, kam se lze dostat pomocí skládání šipek.



Snadno se nahlédne, že je-li $KLMN$ rovnoběžník takový, že body K, L, M jsou body mřížky, pak též N je bodem mřížky.

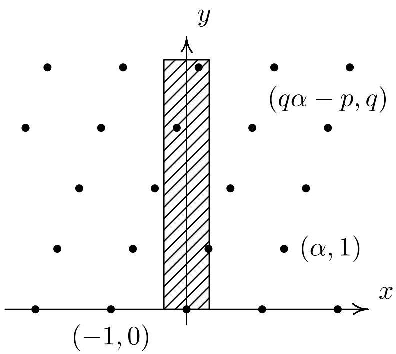
[1] Toto číslo není unikátní, existují další čísla v jistém smyslu podobná zlatému řezu, která jsou stejně „špatná“.

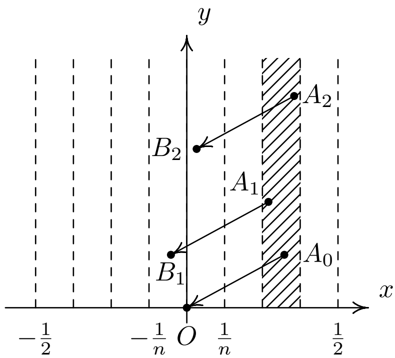
[2] Většinou se šipkám říká vektory.

Význam mřížky vyplyne z následující úvahy. Volme za šipky **u** a **v** postupně $(-1,0)$ a $(\alpha,1)$, kde α je obecně reálné číslo. Pro celá čísla p a q (výše to byla čísla a a b) náleží body

$$p(-1,0)+q(\alpha,1)=(q\alpha-p,q)=\left(q\left(\alpha-\frac{p}{q}\right),q\right)$$

mřížce. Náš ukazatel kvality je pak vzdálenost tohoto mřížového bodu od osy y. Abychom dokázali Větu 1, musíme najít nekonečně mnoho bodů této mřížky libovolně blízko ose y. To nahlédneme z následujících obrázků.





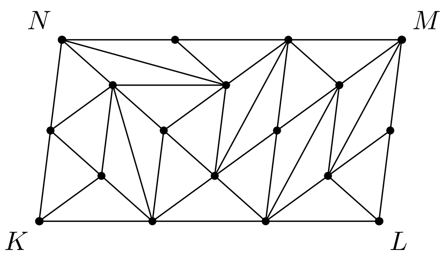
Jak vidno, tato mřížka byla zvolena lišácky na míru našemu ukazateli kvality.

Označme si dále písmenkem s obsah (tzv. základního) rovnoběžníku $OACB$, kde $C=A+B$. Platí následující.

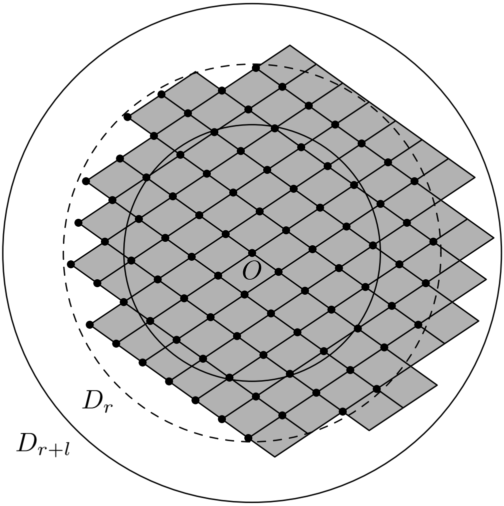
Tvrzení 3. *Buď $KLMN$ rovnoběžník z mřížových bodů. Pak platí následující.*

(a) *Obsah $KLMN$ je roven ns, kde n je přirozené číslo.*
(b) *Pokud rovnoběžník $KLMN$ neobsahuje žádné mřížové body uvnitř ani na hranici, pak je jeho obsah roven s.*

Myšlenku důkazu (a) lze najít v obrázku.



Důkazu (b) pak v obrázku.



Konstrukce čísel

Chceme-li objevit ty skutečně dobré aproximace, musíme si osvojit práci s řetězovými zlomky a s Euklidovým algoritmem. Pak si uvědomíme příslušné souvislosti a vypěstujeme si patřičný náhled, pochopitelně geometrický.

Řetězové zlomky

Konečný *řetězový zlomek* je výraz tvaru

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}},$$

kde a_0 je celé číslo, a_1 až a_n jsou kladná celá a $a_n > 1$. Snadno si rozmyslíme, že každé racionální číslo lze zapsat jako konečný řetězový zlomek. Okamžitě také přijdeme na algoritmus, jak ze zadaného racionálního čísla r čísla a_i dostávat. Prostě

$$a_0 = [r], \quad a_1 = \left[\frac{1}{r - a_0}\right], \quad a_2 = \left[\frac{1}{\frac{1}{r-a_0} - a_1}\right], \ldots$$

Nic nám však nebrání použít tento algoritmus i pro iracionální číslo α. Dostaneme pak nekonečně mnoho čísel $a_0, a_1, a_2, \dots$ Formálně píšeme

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}}.$$

Čísla $a_0, a_1, a_2, \dots$ nazýváme *neúplnými podíly* čísla α, číslo

$$r_n = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

pak pojmenujeme *n-tým aproximantem* čísla α. Zřejmě platí

$$r_0 < r_2 < r_4 < \dots < \alpha < \dots r_5 < r_3 < r_1.$$

Zaveďme si ještě úspornější značení $[a_0; a_1, a_2, \dots, a_n]$ pro konečný řetězový zlomek s neúplnými podíly $a_0, a_1, a_2, \dots a_n$ a $[a_0; a_1, a_2, \dots]$ pro nekonečný řetězový zlomek.

Vyjdeme-li naopak z neúplných podílů, můžeme počítat čitatele a jmenovatele čísla $r_n = \frac{p_n}{q_n}$.

$$r_0 = \frac{a_0}{1}, \quad r_1 = \frac{a_0 a_1 + 1}{a_1}, \quad r_2 = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1}, \dots$$

a rychle objevíme následující rekurentní vztahy.

Tvrzení 4. *Platí*

(a) $p_n = a_n p_{n-1} + p_{n-2}$ *($n \geq 2$),*
(b) $q_n = a_n q_{n-1} + q_{n-2}$ *($n \geq 2$),*
(c) $p_{n-1} q_n - p_n q_{n-1} = (-1)^n$, *($n \geq 1$).*

Euklidův algoritmus

Euklidův algoritmus většinou používáme k nalezení největšího společného dělitele. Připomeňme, že pro daná kladná celá čísla M a N ($N > M$) stále opakujeme dělení se zbytkem podle schématu

$$\begin{aligned} N &= a_0 M + b_0 \\ M &= a_1 b_0 + b_1 \\ b_0 &= a_2 b_1 + b_2 \\ &\vdots \\ b_{n-2} &= a_n b_{n-1}, \end{aligned}$$

kde a_i a b_i jsou kladná celá čísla a

$$0 < b_{n-1} < b_{n-2} < \cdots < b_0 < M.$$

Číslo b_{n-1} je největší společný dělitel čísel M a N.

Souvislost s řetězovými zlomky je nasnadě.

Tvrzení 5.

(a) *Čísla* $a_0, a_1, a_2, \ldots, a_n$ *jsou neúplné podíly čísla* $\frac{N}{M}$,

$$\frac{N}{M} = [a_0; a_1, a_2, \ldots, a_n].$$

(b) *Pro i-tý aproximant* $\frac{p_i}{q_i}$ *platí*

$$b_i = (-1)^i (Nq_i - Mp_i).$$

Kdybychom čísla N a M nahradili obecně reálnými čísly β a γ, dostaneme nekonečnou posloupnost rovnic (pokud je podíl $\frac{\beta}{\gamma}$ iracionální)

$$\begin{aligned}
\beta &= a_0\gamma + b_0\\
\gamma &= a_1 b_0 + b_1\\
b_0 &= a_2 b_1 + b_2\\
&\ \vdots
\end{aligned}$$

a Tvrzení 5 bude stále platit (se zjevnou modifikací, tj. $\frac{\beta}{\gamma} = [a_0; a_1, a_2, \ldots])$.

Geometrická reprezentace Euklidova algoritmu

Buď O bod v rovině a ℓ buď přímka tímto bodem procházející (v obrázku svislá). Zvolme body A_{-2} a A_{-1} ve vzdálenosti β a γ od přímky ℓ, oba horizontálně nad bodem O, A_{-2} vpravo a A_{-1} vlevo.

Přičtěme vektor $\overrightarrow{OA_{-1}}$ k A_{-2} co nejvícekrát, aby výsledek neprotnul přímku ℓ. Koncový bod označme jako A_0. V druhém kroku přičteme podobně vektor $\overrightarrow{OA_0}$ k bodu A_1 co nejvícekrát bez protnutí přímky ℓ. Dostaneme bod A_1. Ve třetím přičteme $\overrightarrow{0A_1}$ k A_0, dostaneme A_3 a tak dále. Celkem jsme vyrobili dvě lomené čáry $A_{-2}A_0A_2A_4\ldots$ a $A_{-1}A_1A_3A_5\ldots$ přimykající se k přímce ℓ.

Příslušné celočíselné násobky si budeme značit a_i, platí tedy

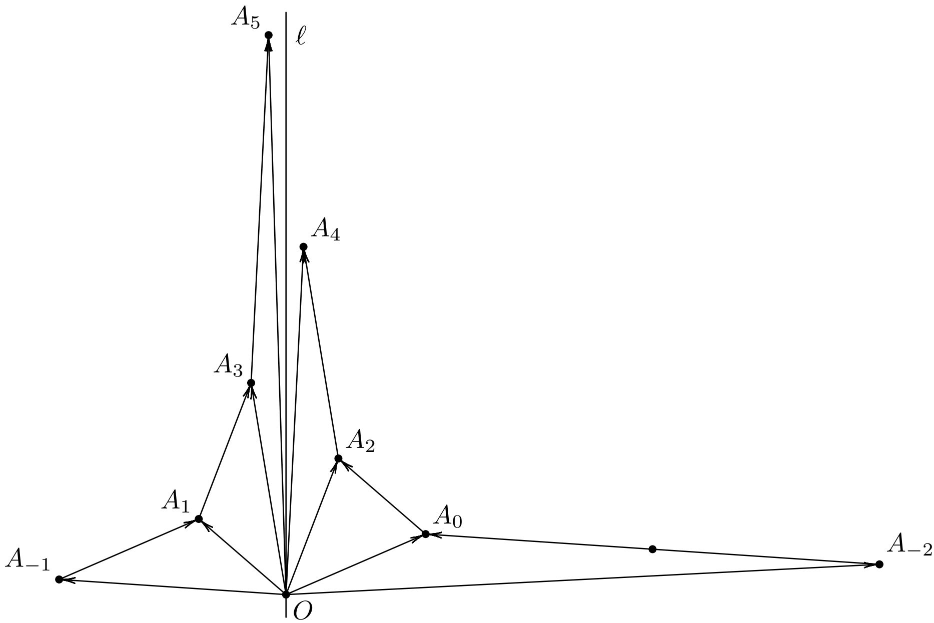
$$\begin{aligned}
\overrightarrow{A_{-2}A_0} &= a_0\overrightarrow{OA_{-1}}\\
\overrightarrow{A_{-1}A_1} &= a_1\overrightarrow{OA_0}\\
\overrightarrow{A_0A_2} &= a_2\overrightarrow{OA_1}\\
&\ \vdots
\end{aligned}$$

Dále si označme vzdálenosti bodů A_i od přímky ℓ postupně β, γ, b_0, b_1 a tak dále. Z konstrukce výše můžeme postupně vypočítávat tyto vztahy

$$\begin{aligned} \beta &= a_0\gamma + b_0 \\ \gamma &= a_1 b_0 + b_1 \\ b_0 &= a_2 b_1 + b_2 \\ &\vdots \end{aligned}$$

a tedy jest $\frac{\beta}{\gamma} = [a_0; a_1, a_2, \dots]$.

Poznamenejme, že pokud některý z bodů A_n leží na přímce ℓ, je podíl $\frac{\beta}{\gamma}$ racionální a platí $\frac{\beta}{\gamma} = [a_0; a_1, a_2, \dots, a_n]$.



Pojďme učinit další klíčové pozorování. Uvažujme mřížku generovanou vektory $\overrightarrow{OA_{-2}}$ a $\overrightarrow{OA_{-1}}$. Potom všechny body A_i jsou body této mřížky. Z Tvrzení 3 vydedukujeme následující.

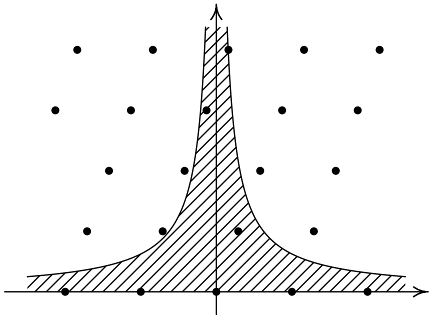
Tvrzení 6. *Neexistuje mřížový bod mezi lomenými čárami $A_{-2}A_0A_2A_4\dots$ a $A_{-1}A_1A_3A_5\dots$.*

Nejlepší racionální aproximace

Uvažujme opět mřížku generovanou šipkami $(-1,0)$ a $(\alpha,1)$, tj. body o souřadnicích

$$p(-1,0)+q(\alpha,1)=(q\alpha-p,q)=\left(q\left(\alpha-\frac{p}{q}\right),q\right).$$

Nový ukazatel kvality $q^2\left|\alpha-\frac{p}{q}\right|$ je pak absolutní hodnota součinu souřadnic mřížových bodů. Otázka počtu aproximací $\frac{p}{q}$ čísla α, pro které je tento ukazatel menší než ε, je ekvivalentní otázce počtu mřížových bodů pod grafem „hyperbolického kříže“ $|xy|<\varepsilon$.



Aplikujme předchozí konstrukci Euklidova algoritmu pro $A_{-2}=(\alpha,1)$ a $A_{-1}=(-1,0)$. Význam bodů A_0, A_1, $A_2\dots$ objasňuje následující věta.

Věta 7. *Buď $n\geq 0$. Pak $A_n=(q_n\alpha-p_n,q_n)$, kde p_n a q_n jsou nesoudělné čitatele a jmenovatele n-tých aproximantů čísla α.*

Věta 7 společně s Tvrzením 6 říká, že právě tyto aproximanty tvoří prvky nejlepší aproximace. Formálně si shrňme tento poznatek do věty.

Věta 8. *Buď $\varepsilon>0$. Pokud existuje jen konečně mnoho zlomků $\frac{p_n}{q_n}$ takových, že $q_n^2\left|\alpha-\frac{p_n}{q_n}\right|<\varepsilon$, pak množina všech zlomků $\frac{p}{q}$ splňujících $q^2\left|\alpha-\frac{p}{q}\right|<\varepsilon$ je konečná.*

Již víme, které zlomky jsou číslu α nejblíže, nyní zaměříme svou pozornost na odhad chyby. Fascinující je, že hodnotu ukazatele kvality umíme určit přesně.

Věta 9. *Buď $\frac{p_n}{q_n}$ ireducibilní n-tý aproximant reálného čísla $\alpha=[a_0;a_1,a_2,\dots]$. Pak*

$$q_n^2\left|\alpha-\frac{p_n}{q_n}\right|=\frac{1}{\lambda_n},$$

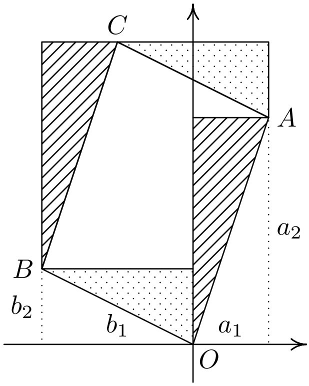
kde

$$\lambda_n=a_{n+1}+\cfrac{1}{a_{n+2}+\cfrac{1}{a_{n+3}+\cfrac{1}{\ddots}}}+\cfrac{1}{a_n+\cfrac{1}{a_{n-1}+\cfrac{1}{\ddots+\cfrac{1}{a_1}}}}.$$

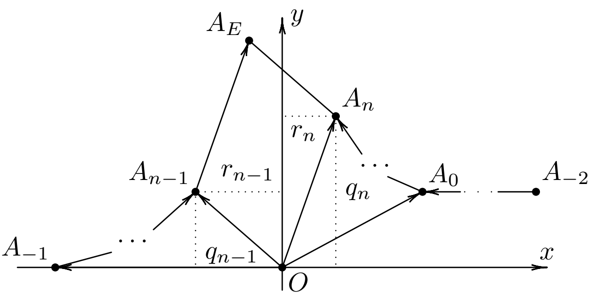
K důkazu této věty budeme potřebovat jedno snadné lemma.

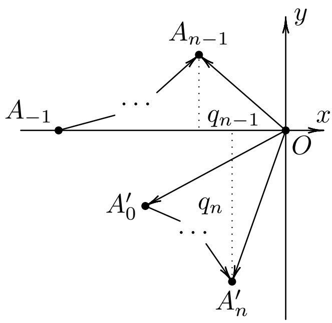
Lemma 10. *Mějme v rovině s počátkem O body A a B o souřadnicích (a_1, a_2) a $(-b_1, b_2)$, kde a_1, a_2, b_1, b_2 jsou kladná reálná čísla. Označme si $C = A + B$. Pak obsah rovnoběžníku $OACB$ je roven $a_1b_2 + a_2b_1$.*

Důkaz lemmatu se nahlédne posunutím dvou trojúhelníků.



K důkazu Věty 9 použijeme podobný obrázek jako dříve, navíc jednu větev z Euklidovy konstrukce zobrazíme středově podle počátku. To se bude jistě hodit.





Vybaveni těmito nástroji už můžeme dokázat Větu 2 nebo objasnit podstatu triku a Vejtkova „důkazu“.

Zpět k triku

Na začátku jsme obdrželi dvě devíticiferná desetinná čísla, z nichž jedno vzniklo jako podíl dvou čísel s nejvýše tříciferným jmenovatelem a druhé bylo libovolné. Chceme poznat, které je které.

Je-li číslo α devíticiferná aproximace čísla $\frac{p}{q}$ s tříciferným jmenovatelem, pak

$$q^2\left|\alpha - \frac{p}{q}\right| < \frac{1}{10^9} = \frac{1}{1000 \cdot (1000^2)} < \frac{1}{1000q^2}.$$

To znamená, že jedno z čísel λ_n je alespoň tisíc. Triviálně platí, že $a_{n+1} < \lambda_n < a_{n+1} + 2$, takže a_{n+1} musí být více než tisíc a odpovídající q_n menší než tisíc. Otázka je, jak velké může být n?

Protože platí $q_n = a_n q_{n-1} + q_{n-2}$, čísla q_n rostou alespoň jako Fibonacciho čísla F_n. Jelikož $F_{15} = 987$, může být n nejvýše patnáct.

Nyní zbývá jen převést ona dvě zadaná čísla na řetězové zlomky a podívat se nejvýše na prvních 15 z nich.

$$0.635\,149\,023 = [0; 1, 1, 1, 2, 1, 6, 13, 1204, 1, \dots]$$
$$0.728\,101\,457 = [0; 1, 2, 1, 2, 9, 1, 1, 1, 1, 3, 1, 15, 1, 59, 7, 1, 39, \dots]$$

Zřejmě první z těchto čísel má dobrou racionální aproximaci, konkrétně je to racionální číslo $[0; 1, 1, 1, 2, 1, 6, 13]$. Snadno již dopočítáme čitatele i jmenovatele.

Závěr: První číslo je racionální, a to $\frac{618}{973}$.

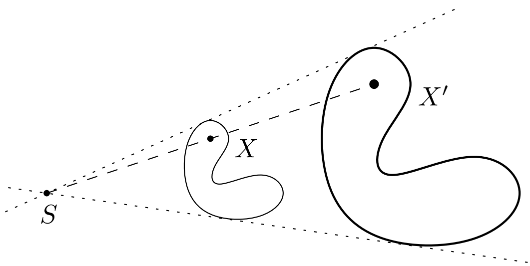
Literatura

[1] Dmitry Fuchs, Sergej Tabachnikov, *Mathematical Omnibus*, AMS, 2007.

Stejnolehlost

Tomáš „Šavlík“ Pavlík

Geometrická zobrazení tvoří nedílnou součást výuky geometrie. Na stejnolehlost však obvykle nebývá kladen takový důraz. A přitom právě stejnolehlost je nejúčinnějším nástrojem pro využívání faktu, že při zvětšování objektů se nemění jejich tvar, ale jen jejich velikost.



Definice. (Stejnolehlost) Je dán bod S a reálné číslo k, $k \neq 0$. *Stejnolehlost se středem S a koeficientem k* je zobrazení $\mathrm{H}(S,k)$, které přiřazuje:

(i) každému bodu $X \neq S$ bod X' tak, že platí $|SX'| = |k| \cdot |SX|$ (přitom pro $k > 0$ leží bod X' na polopřímce SX a pro $k < 0$ je bod X' bodem polopřímky opačné),
(ii) bodu S bod $S' = S$.

Příklady k procvičení

Nyní si zkusíme pár příkladů. Většina geometrických úloh už v zadání napovídá, kterou metodou půjde vyřešit. U příkladů na stejnolehlost jsou typické tyto znaky:

(i) dvě nebo více kružnic se dotýkají,
(ii) kružnice mají společné tečny,
(iii) dokazujeme, že tři body leží v přímce,
(iv) dokazujeme, že se tři přímky protínají v jednom bodě,
(v) množina hledaných bodů je kružnice.

Příklad 1. Kružnice k, l mají vnitřní dotyk v bodě T. Na l zvolíme body A, B tak, že AB se dotýká k v bodě S. Dokažte, že TS je osou úhlu ATB.

Příklad 2. Nechť $ABCD$ je lichoběžník s rovnoběžnými stranami AB a CD, jeho průsečík úhlopříček označme E. Najdeme body F a G tak, aby trojúhelníky ABF a CDG byly rovnostranné a zároveň byly vně $ABCD$. Dokažte, že E, F a G leží na jedné přímce.

Příklad 3. (Eulerova přímka) Je dán trojúhelník ABC. Body H, G a O jsou postupně ortocentrum, těžiště a opsiště. Dokažte, že tyto tři body leží na jedné přímce a zároveň platí $|GH| = 2 \cdot |GO|$.

Příklad 4. Je dán trojúhelník ABC. Body dotyků úsečky BC s kružnicí vepsanou a připsanou označme postupně D a E. Přímka AE protne kružnici vepsanou blíže bodu A v bodě F. Dokažte, že DF je kolmá na BC.

Příklad 5. Mějme přímku p a dvě kružnice k_1, k_2, které se dotýkají p ze stejné strany postupně v bodech T a U. Kružnice k neprotíná p a dotýká se zvnějšku k_1 a k_2 postupně v bodech K a L. Dokažte, že KT, LU a k mají společný bod.

Příklad 6. Kružnice k, l mají vnější dotyk v bodě T. Navíc se obě vnitřně dotýkají kružnice m postupně v bodech R, S. Druhý průsečík přímky RT s kružnicí m označme Q. Dokažte, že $|\sphericalangle TSQ| = 90°$.

Příklad 7. V trojúhelníku ABC zvolme body D a E na straně BC tak, že $|BD| = |EC|$. Střed úsečky AD označme M. Dokažte, že ME prochází jedním pevným bodem nezávisle na volbě bodů D a E.

Příklad 8. Jsou dány dvě kružnice k_1 a k_2, které se zvenčí dotýkají v bodě T. Dokažte, že pro každé dva body A na k_1 a B na k_2 takové, že platí $|\sphericalangle ATB| = 90°$, prochází přímka AB pevným bodem.

Příklad 9. Je dána pevná kružnice k se středem O a bod A mimo ni. Po k se hýbe bod X tak, že O, A a X nejsou v přímce. Nejděte množinu průsečíků AX s osou úhlu AOX.

Příklad 10. Nechť ABC je trojúhelník a nechť D je průsečík tečny ke kružnici opsané trojúhelníku ABC v bodě A a přímky BC. Nechť E je průsečík kolmice na BC v B a osy strany BA. Analogicky nechť F je průsečík kolmice na BC v bodě C a osy strany CA. Dokažte, že D, E, F leží v přímce.

Skládání stejnolehlostí

V některých případech si nevystačíme s jednou stejnolehlostí, ale budeme jich potřebovat více. K řešení pak budeme používat následující, velmi užitečné, lemma.

Lemma 11. *Nechť* $\mathrm{H}_1(S_1, k_1)$ *a* $\mathrm{H}_2(S_2, k_2)$ *jsou stejnolehlosti takové, že* $S_1 \neq S_2$ *a* $k_1 \cdot k_2 \neq 1$. *Pak jejich složením je opět stejnolehlost, a to se středem na přímce* S_1S_2.

Příklad 12. V trojúhelníku ABC označme k kružnici jemu opsanou. Najdeme kružnici k_a, která se dotýká přímek AB a AC a navíc se vnitřně dotýká k v bodě A'. Obdobně najdeme k_b, k_c a body B' a C'. Dokažte, že AA', BB' a CC' procházejí jedním bodem.

Příklad 13. V rovině jsou dány dvě neprotínající se kružnice k, l, přičemž k leží uvnitř l. Buď m kružnice, která má s k vnější dotyk v bodě K a s l vnitřní dotyk v bodě L. Dokažte, že KL prochází pevným bodem X nezávislým na volbě m.

Příklad 14. Jsou dány kružnice k_1, k_2 a k_3 takové, že žádná neleží uvnitř jiné. Kružnice l s nimi má vnitřní dotyk v bodech A_1, A_2 a A_3 a kružnice m s nimi má vnější dotyk v bodech B_1, B_2 a B_3. Dokažte, že přímky A_1B_1, A_2B_2 a A_3B_3 procházejí jedním bodem.

Příklad 15. Do kružnice k je vepsán rovnoramenný trojúhelník ABC, kde $|AB| = |AC|$. Dále vepíšeme kružnice k_b a k_c do úsečí kružnice k, které jsou určené tětivami AC a AB. Ty se dotknou kružnice k postupně v bodech B' a C'. Společná vnější tečna kružnic k_b a k_c protne AC v bodě P a AB v bodě Q. Dokažte, že se přímky $C'Q$ a $B'P$ protnou na ose úhlu BAC. (Polsko 2012)

Těžké úlohy

Příklad 16. Jsou dány dvě kružnice, jejich středy jsou vzdálené 10 jednotek a mají poloměry 1 jednotku a 3 jednotky. Najděte množinu středů úseček XY, kde X leží na jedné kružnici a Y na druhé. (Putnam 1996)

Příklad 17. Kružnice k a l mají vnější dotyk v bodě T. Navíc mají vnitřní dotyk s kružnicí m v bodech A a B. Společná tečna k a l v bodě T protne m v bodě P. AP protne k podruhé v bodě X, BP protne l podruhé v bodě Y. Dokažte, že XY je společná tečna kružnic k a l.

Příklad 18. Body A, B a C leží v přímce v tomto pořadí. Navíc platí $|AB| \neq |BC|$. Najděte množinu bodů X takových, že $|\sphericalangle AXB| = |\sphericalangle BXC|$.

Příklad 19. Buď $ABCD$ konvexní čtyřúhelník a P bod na straně AB takový, že kružnice vepsaná trojúhelníku CPD mající střed v I se dotýká kružnic vepsaných trojúhelníkům APD, PBC postupně v bodech K, L. Označme $E = AC \cap BD$ a $F = AK \cap BL$. Dokažte, že body E, I, F leží v přímce.

Příklad 20. V trojúhelníku ABC platí $|AC| + |BC| = 3 \cdot |AB|$. Kružnice vepsaná se středem I se dotkne stran BC, AC postupně v bodech D, E. Nechť body K a L jsou obrazy bodů D a E ve středové symetrii se středem v I. Dokažte, že body A, B, K a L leží na jedné kružnici. (IMO 2005 shortlist)

Příklad 21. Nechť $ABCD$ je konvexní čtyřúhelník, ve kterém $|BA| \neq |BC|$. Označme postupně k_1 a k_2 kružnice vepsané trojúhelníkům ABC, ADC. Předpokládejme, že existuje kružnice k, která se dotýká polopřímky BA za bodem A, polopřímky BC za bodem C a přímek AD, CD. Dokažte, že společné vnější tečny kružnic k_1 a k_2 se protnou na kružnici k. (IMO 2008)

Návody

1. Zobrazení bodu S na kružnici l se středem T. Stačí říci, ze tento obraz leží uprostřed oblouku AB.

2. Stejnolehlost podle bodu P taková, že AB přejde na DC.

3. Zobrazíme vrcholy podle bodu G s koeficientem $-\frac{1}{2}$. Pak výšky přejdou na osy stran.

4. Zobrazíme připsanou na vepsanou podle bodu A.

5. Dokreslíme bod X na k co nejdále od p a dokážeme, že K, T, X a L, U, X leží na přímkách.

6. Označme P bod, kde ST protne m. Stačí dokázat, že PQ je průměr m.

7. Nejdříve ve stejnolehlosti z A, kdy E přejde na M, zobrazíme bod B na bod X. $|XM|/|EC|$ je konstantní, a tedy střed stejnolehlosti, kdy jedna úsečka přejde na druhou, je pevně vzdálen od BC a zároveň leží na XC.

8. Dokážeme, že body jsou na stejném místě v rámci své kružnice.

9. Označme onen průsečík Y. Stačí použít známý fakt, že $\frac{|OX|}{|OA|} = \frac{|XY|}{|YA|}$.

10. Vedeme rovnoběžku bodem B s AC, stačí dokázat, že E je střed kružnice opsané nově vzniklého trojúhelníku.

12. Je to střed (kladné) stejnolehlosti, v níž kružnice opsaná přejde na kružnici vepsanou.

13. Je to střed stejnolehlosti mezi k a l.

14. Je to střed stejnolehlosti, kdy m přejde na l.

15. Dokreslíme kružnici vepsanou trojúhelníku APQ.

16. Nejdříve zafixujeme Y a zobrazíme X ve stejnolehlosti se středem Y a $k = \frac{1}{2}$. Pak sledujeme, jak se hýbe střed této kružnice, když se Y mění.

17. Mocnost z bodu X.

18. Najdeme střed stejnolehlosti, kdy AB přejde na BC, a zobrazíme podle ní bod X.

19. Dokažte, že $CDPA$ a $CDBP$ jsou tečnové, a dokreslete kružnici, která se dotýká DA, AB a BC.

20. Dokažte, že $|AB| = |CD|$, a pak, že $ABKI$ je tětivový.

21. Dokažte, že body dotyků kružnic s AC jsou symetrické podle středu úsečky. Nakreslete si obrázek tak, že AC je vodorovně. Vzpomeňte si na minulé úlohy.

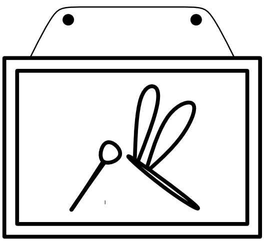
Literatura

[1] Pepa Tkadlec, *Stejnolehlost a kružnice*, Sborník MKS, Staré Město, 2009.
[2] Andreescu, Rolínek, Tkadlec, *107 Geometry Problems*, XYZ Press, 2013.

Jak (ne)věšet obrazy na zeď

Alča Skálová

Představme si, že máme doma opravdu nepěkný obraz komára, který nám už notně pije krev. Rovnou ho sundat ze zdi sice nechceme, ale rádi bychom provázek kolem obou hřebíků, na nichž je obraz zavěšen, omotali tak, že kdyby „náhodou“ jeden z hřebíků zmizel, celý obraz by spadl. Dokážete to?



Co kdyby obraz původně visel na k hřebících? Dal by se i v tomto případě přemotat provázek tak, aby po odebrání libovolného hřebíku obraz spadl? A existuje lepší metoda než jen „pokus – omyl“?

Literatura

[1] David Ploog, *The best way how not to hang pictures on walls – topology in school.*

[2] Leland McInnes, *Picture Hanging Problem*, 2003.

Počítání dvěma způsoby

Štěpán Šimsa

Abstrakt. Seznámíme se s metodou *počítání dvěma způsoby*, která vychází z triviálního pozorování, že spočítáme-li dvakrát to samé, dostaneme stejný výsledek. Začneme několika motivačními příklady. Poté se vrhneme na kombinatorické identity. V další části se budeme zabývat různorodějšími úlohami na tuto metodu, například grafovými.

Úmluva. Všechna čísla $n, k, r, \ldots$ budeme chápat jako přirozená, nebude-li řečeno jinak.

Motivační příklady

Příklad 1. Každý člen komise je zároveň členem právě tří podkomisí, přičemž každá podkomise má právě tři členy. Dokažte, že počet členů je stejný jako počet podkomisí.

Řešení. Označme si počet členů komise n a počet podkomisí k. Kolik je celkem dvojic podkomise a jeden člověk, který v ní je? Podkomisí je k a v každé jsou tři členové komise, takže je těchto dvojic $3k$. Ale každý člen komise je ve třech podkomisích, takže jich je $3n$. Přitom jsme spočítali dvakrát odpověď na jednu a tu samou otázku, takže $3n = 3k$, neboli $n = k$.

Příklad 2. Mějme tabulku $m \times n$ vyplněnou reálnými čísly. Ke každému řádku si napíšeme součet všech čísel v tomto řádku. Tomuto součtu budeme říkat řádkový. Podobně si ke každému sloupci napíšeme jeho sloupcový součet. Dokažte, že součet řádkových součtů je stejný jako součet sloupcových součtů.

Definice. *Kombinační číslo* $\binom{n}{k}$ vyjadřuje počet možností, jak vybrat k objektů z n.

Příklad 3. Dokažte

$$\binom{n}{k} = \binom{n}{n-k}.$$

Příklad 4. Dokažte
$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

Příklad 5. Dokažte
$$k\binom{n}{k} = n\binom{n-1}{k-1}.$$

Příklad 6. Dokažte
$$\binom{n}{k} + \binom{n-1}{k} + \cdots + \binom{k}{k} = \binom{n+1}{k+1}.$$

Interpretace kombinatorických pojmů

Při počítání dvěma způsoby je klíčové si osvojit ještě jednu schopnost. Když dostaneme nějaký počet možností, potřebujeme vymyslet příklad, kterému by tento počet odpovídal. Pojďme si to zkusit na několik příkladech.

Příklad 7. Určete, co vyjadřuje výraz $n! = n \cdot (n-1) \cdot (n-2) \cdots 1$.

Řešení. Vidíme, že výraz je závislý na n, uvažujme tedy nějakých n objektů, pro lepší představu lidí. Nejdříve n nám představuje počet možností, jak z nich vybrat jednoho. Potom $n-1$ může vyjadřovat počet možností, jak vybrat jednoho už jen z $n-1$ zbylých. Potom vybereme dalšího z $n-2$ zbylých lidí atd. Tím jsme vlastně našich n lidí vybrali v nějakém pořadí, jinak řečeno, nějak jsme je uspořádali. Tedy $n!$ odpovídá počtu způsobů, jak uspořádat n lidí. Tato uspořádání objektů nazýváme *permutace.*

Příklad 8. Interpretujte kombinatoricky m^n.

Příklad 9. Interpretujte
$$\binom{n}{m} \cdot 2^m.$$

Příklad 10. Interpretujte
$$\frac{n(n-1)\cdots(n-k+1)}{k!}.$$

Kombinatorické identity

Příklad 11. (lehký) Dokažte

(i)

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n,$$

(ii)

$$\binom{n}{r}\binom{r}{k} = \binom{n}{k}\binom{n-k}{r-k}.$$

Příklad 12. (Vandermondova identita)

$$\sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k} = \binom{m+n}{r}.$$

Příklad 13. (střední) Dokažte

(i)

$$\sum_{k=1}^{n} k\binom{n}{k} = n \cdot 2^{n-1},$$

(ii)

$$\binom{2n}{2} = 2\binom{n}{2} + n^2,$$

(iii)

$$\sum_{k=0}^{n} 2^k \binom{n}{k} = 3^n.$$

Příklad 14. (těžký) Dokažte

(i)

$$\sum_{k=1}^{n} k^2\binom{n}{k} = n(n+1)2^{n-2},$$

(ii)

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n},$$

(iii)

$$\sum_{i=0}^{m} \binom{n}{i}\binom{n-i}{m-i} = \binom{n}{m}2^m,$$

(iv)
$$\sum_{k=0}^{m} \binom{n+k}{k} = \binom{n+m+1}{m}.$$

Grafy

Definice. Graf je množina vrcholů V a hran E, přičemž hrana je dvojice vrcholů. Graf může být orientovaný (což znamená, že má každá hrana ještě svůj směr) nebo neorientovaný.

Definice. Výstupní stupeň vrcholu v je počet vrcholů, do kterých vede z v hrana, a značíme ho $\mathrm{out}(v)$. Podobně vstupní stupeň vrcholu v je počet vrcholů, ze kterých vede do v hrana, a značíme ho $\mathrm{in}(v)$. Pro neorientované grafy je $\mathrm{out}(v) = \mathrm{in}(v) = \deg(v)$.

Příklad 15. Dokažte, že součet stupňů vrcholů v neorientovaném grafu je sudý.

Definice. Graf je *rovinný*, pokud jej lze nakreslit do roviny tak, aby se jednotlivé hrany nekřížily. Graf je *souvislý*, pokud se z každého vrcholu dá dostat po hranách do libovolného jiného vrcholu.

Tvrzení. (Eulerův vzorec) *Mějme souvislý rovinný graf s n vrcholy, h hranami a s stěnami. Pak*
$$n - h + s = 2.$$

Toto tvrzení si nebudeme dokazovat (přestože jde o celkem jednoduché cvičení na matematickou indukci), bude se nám ale hodit pro následující tvrzení.

Tvrzení. *Rovinný graf s n vrcholy má maximálně $3n - 6$ hran.*

Příklad 16. Předchozí tvrzení si dokažte.

Příklad 17. Mějme pravidelný n-úhelník a spojme každé dva vrcholy úsečkou. Spočítejte, kolik je takových dvojic úseček, že se protínají (myslíme jinak, než svými krajními body).

Příklad 18. Na oslavě zná každý (včetně Pavla) přesně sedm chlapců a přesně deset děvčat („znání se“ je vzájemné, sám sebe nikdo nezná). Kolik nejméně lidí se na oslavě mohlo sejít? (Náboj 2011, 45)

Příklad 19. Na Alčině večírku se sešla velmi zajímavá společnost. Posuďte sami:

(i) každý na večírku zná právě 22 lidí,
(ii) pokud se dva lidé znají, nemají na večírku žádné společné známé,
(iii) pokud se dva lidé neznají, pak mají na večírku právě šest společných známých.

Určete, kolik lidí bylo na večírku. (MKS 30–5–7)

Definice. Turnaj je takový orientovaný graf, kde jsou každé dva různé vrcholy spojené hranou. Graf je tedy záznamem výsledků turnaje, kde hrál každý s každým.

Příklad 20. (lehký) Dokažte, že v každém orientovaném grafu je součet vstupních stupňů vrcholů stejný jako součet výstupních stupňů vrcholů, tedy

$$\sum_{v\in V} \mathrm{in}(v) = \sum_{v\in V} \mathrm{out}(v).$$

Příklad 21. Dokažte, že v turnaji navíc platí

$$\sum_{v\in V} (\mathrm{in}(v))^2 = \sum_{v\in V} (\mathrm{out}(v))^2.$$

Další příklady

Příklad 22. Matematické soutěže, která se skládala ze šesti úloh, se zúčastnilo 200 řešitelů. Je známo, že každou úlohu vyřešilo aspoň 120 řešitelů. Dokažte, že existují dva řešitelé takoví, že každou zadanou úlohu vyřešil aspoň jeden z nich.

Příklad 23. V tabulce $n \times n$ je v každém políčku napsáno číslo, v kolika pravoúhelnících se vyskytuje. Dokažte, že součet těchto čísel je druhá mocnina celého čísla. (MKS 29–3–7)

Příklad 24. Ukažte, že existuje přirozené číslo, které se dá alespoň 100 způsoby zapsat jakou součet 2012 čísel, z nichž každé je 2011-tou mocninou přirozeného čísla. Zápisy, které se liší jen pořadím sčítanců, považujeme za stejné. (MKS 31–8–3)

Příklad 25. Uvažujme $2n$ různých přirozených čísel $a_1, a_2, \ldots, a_{2n}$, která jsou menší než n^2+1 $(n > 2)$. Dokažte, že nějaké tři z rozdílů $a_i - a_j$ (pro všechny možné $i \neq j$) jsou stejné. (KMS 12 2003)

Příklad 26. V poslanecké sněmovně je 200 poslanců, kteří postupně hlasují o n zákonech (poslanec může být buď *pro* schválení zákona, nebo *proti* jeho schválení, nebo se může *zdržet* hlasování). Je známo, že pro každá dvě hlasování existuje poslanec, který v jednom z nich hlasoval pro a v jednom proti. Označme z_i počet poslanců, kteří se zdrželi hlasování o i-tém zákonu. Dokažte, že

$$\sum_{i=1}^{n} 2^{z_i} \leq 2^{200}.$$

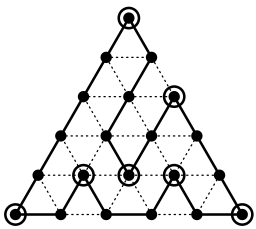
(MKS 32–8–7)

Příklad 27. Osm zpěváků se zúčastnilo hudebního festivalu, kde vystoupili s m písněmi $(m > 0)$. Každou píseň zpívali čtyři z nich a každá dvojice zpívala ve stejném počtu písní, jako libovolná jiná dvojice. Jaké je nejmenší m, pro které je to možné? (KMS 7 2005)

Příklad 28. V obdélníkové tabulce $m \times n$ jsou nezáporná reálná čísla, přičemž každý řádek a každý sloupec obsahuje alespoň jedno kladné číslo. Pokud se navíc řádek a sloupec protínají v políčku, kde je kladné číslo, tak je jejich součet stejný. Dokažte $m = n$. (Kanada 2006)

Příklad 29. Ve škole je 2007 holek a 2007 kluků. Každý student je členem nejvýše 100 klubů. Víme, že každí dva studenti opačného pohlaví jsou oba členové alespoň jednoho společného klubu. Dokažte, že existuje klub, ve kterém je alespoň 11 holek a alespoň 11 kluků. (CHKMO 2007)

Příklad 30. Rovnostranný trojúhelník o straně délky n je vyplněný jednotkovou trojúhelníčkovou mřížkou. Uzavřená lomená čára vede podél této mřížky a každý vrchol mřížky potká právě jednou. Dokažte, že tato čára alespoň $(n+1)$-krát zahne do ostrého úhlu. (iKS 3–C3)



Návody

2. Počítejte dvěma způsoby součet všech čísel v tabulce.

3. Počítejte, jak vybrat k lidí z n, a poté tyto možnosti spočítejte pomocí lidí, které nevyberete.

4. Vybírejte $k+1$ lidí z $n+1$ a rozeberte, zda prvního vyberete nebo ne.

5. Počítejte, jak vybrat k lidí z n a ještě z nich vybrat jednoho kapitána.

6. Vybírejte $k+1$ lidí z $n+1$ a rozeberte, který bude první vybraný člověk.

8. Rozepište $m^n = m \cdot m \cdots m$ a rozmyslete si, že stačí jen něco vhodného opakovat n-krát.

9. Vyberte m lidí z n a u každého se rozhodněte pro některou ze dvou možností.

10. Vybírejte po jednom k lidí z n a stavte je do řady. Poté si rozmyslete, kolikrát jste započítali každou k-tici lidí (pokud je nechcete uspořádaně).

11.

(i) Počítejte, jak vybrat nějaký počet lidí z n.

(ii) Vyberte r lidí z n a z nich ještě k výjimečných. Potom je vybírejte v opačném pořadí.

12. Rozdělte si $m+n$ lidí na skupinky s m a n lidmi.

13.

(i) Počítejte, jak vybrat nějaký počet lidí z n a z nich jednoho kapitána.
(ii) Rozdělte si $2n$ lidí na dvě skupinky po n.
(iii) Vyberte několik lidí z n a každého z nich dejte buď do první nebo druhé skupiny.

14.

(i) Vyberte několik lidí z n a z nich vyberte jednoho kapitána a jednoho nejlepšího hráče (může a nemusí jít o stejného člověka).
(ii) Rozdělte si $2n$ lidí na dvě skupinky po n a vzpomeňte si na vztah $\binom{n}{k} = \binom{n}{n-k}$.
(iii) Viz Návod 9.
(iv) Rozeberte, kolik lidí ze začátku vyberete.

15. Počítejte jednou pomocí vrcholů a podruhé pomocí hran, kolik je dvojic vrchol a hrana, která z něj vychází.

16. S kolika hranami sousedí stěna a s kolika stěnami sousedí hrana?

17. Vezměte si libovolné čtyři body a spočítejte, kolik je tam protínajících se dvojic úseček.

18. Kolik vede hran mezi kluky a holkami? Kolik je holek minimálně?

19. Kolik je trojic lidí takových, že jeden zná zbylé dva (a ti se tedy neznají)? Počítejte jednou přes člověka, co zná zbylé dva, a jednou přes chybějící hranu.

20. Počítejte počet hran dvěma směry.

21. Počítejte, kolik se v grafu vyskytuje trojic vrcholů takových, že z prvního vede hrana do zbylých dvou (jednou přes toho, který porazil zbylé dva, a jednou přes toho, který proti zbylým dvěma prohrál).

22. Sporem – z každé dvojice nějakou úlohu nevyřešil ani jeden. Kolik je pro každou úlohu dvojic řešitelů, kteří ji ani jeden nevyřešili?

23. Spočítejte součet políček přes počet obdélníků a nějaké políčko, které obsahují. Na výběr je, kam umístit levou a pravou hranu obdélníku a v jakém sloupci bude políčko. Podobně pro vertikální směr.

24. Počítejte, kolika způsoby se dají zapsat čísla menší než $2012n^{2011}$, pokud sčítáme jen 2011-té mocniny čísel $1, 2, \ldots, n$.

25. Čísla si uspořádejte a koukejte na rozdíly $a_{i+1} - a_i$. Jaký je součet těchto rozdílů?

26. Každému poslanci, který se zdržel, domyslete, jak mohl hlasovat. Porovnejte s počtem všech možných hlasování.

27. Spočítejte počet písní pomocí toho, kolikrát každá dvojice zpívala v nějaké písni spolu (a kolik dvojic zpěváků zpívalo každou píseň).

28. Vezměte si všechny řádky se součtem r, k nim odpovídající sloupce, které musejí mít stejný součet, a tabulku rozdělte na dvě podtabulky.

29. Postupujte sporem. Počítejte počet trojic holka, kluk a klub, jehož členové oba jsou.

30. Zabarvěte si na černo trojúhelníčky otočené špičkou nahoru. Jak dlouhá je lomená čára? Jednou spočítejte pomocí počtu bodů v mřížce a podruhé pomocí počtu černých trojúhelníčků, kde čára vede podél jedné/dvou z jejich stran.

Literatura a zdroje

[1] πtr Korcsok, *Kombinatorické identity*, Sborník MKS, Hojsova Stráž, 2011.
[2] Zuzka Safernová, *Dvojí počítání*, Sborník MKS, Staré Město, 2009.
[3] Sbírka úloh KMS, *http://www.kms.sk/zbierka*.

Dokreslování

Pepa Tkadlec

Abstrakt. Příspěvek obsahuje přes čtyřicet geometrických úloh, v jejichž řešení se dokreslují body nebo přímky, které v zadání původně nebyly. Úlohy jsou seskupeny podle myšlenek, které dotyčná dokreslení motivují. Na konci příspěvku jsou k úlohám uvedeny návody.

Při řešení geometrických úloh se zpravidla snažíme obrázek zjednodušovat, jak jen je to možné (typicky tím, že úlohu přeformulujeme na ekvivalentní úlohu na méně bodech). Občas ale stojí za to naopak nějaké body nebo přímky dokreslit. Poznat, kdy je k tomu vhodná příležitost, vyžaduje notnou dávku intuice. Ta se ale dá získat :).

Protahujeme čáry

Přímka je přirozenějším geometrickým objektem než úsečka či polopřímka. Pokud tedy narazíme na jednu z posledně dvou jmenovaných, její protažení stojí za zvážení. Obzvláště tehdy, získáme-li tím druhý průsečík s kružnicí. Jindy protahujeme čáry proto, abychom na ně mohli nanést úsečky a tím „narovnat“ lomenou čáru.

Příklad 1. Pětiúhelník $ABCDE$ má všechny vnitřní úhly stejné velikosti. Dokažte, že osa strany AB, osa strany CD a osa úhlu DEA procházejí jedním bodem. (Polsko 2010)

Příklad 2. Ve čtyřúhelníku $ABCD$ platí $|AB| = 2$, $|BC| = \sqrt{2}$, $|CD| = 3$ a $|\sphericalangle ABC| = |\sphericalangle BCD| = 135°$. Určete $|AD|$. (MKS 31–6–3)

Příklad 3. Na průměru AB půlkružnice τ jsou dány body X, Y tak, že $|AX| = |BY|$. Rovnoběžné paprsky vedoucí z X a Y zasáhnou τ v P a Q. Dokažte, že hodnota součinu $|XP| \cdot |YQ|$ nezávisí na volbě směru paprsků.

Příklad 4. V trojúhelníku ABC s vepsištěm I platí $|BC| = |AC| + |AI|$. Dokažte, že $\alpha = 2\beta$. (TR*i*KS 2013)

Příklad 5. Uvnitř trojúhelníka ABC je dán bod P tak, že platí

$$|\sphericalangle APB| = |\sphericalangle PCA| = \frac{1}{3}(\beta + \gamma).$$

Ukažte, že
$$\frac{|AB|}{|AC|} = \frac{|AC| + |PB|}{|AB| + |PC|}.$$

(Polsko 1997)

Příklad 6. Je dán pravoúhlý trojúhelník ABC s pravým úhlem u vrcholu C. Označme D patu výšky z bodu C. Nechť X je bod uvnitř úsečky CD. Označme K ten bod na úsečce AX, pro který $|BK| = |BC|$. Podobně označme L ten bod na úsečce BX, pro který $|AL| = |AC|$. Dále nechť M je průsečík úseček AL a BK. Ukažte, že $|MK| = |ML|$. (IMO 2012, 5)

Příklad 7. Je dán trojúhelník ABC. Osy vnitřních úhlů u vrcholů A, B protnou protější strany v bodech P, Q. Platí-li $\alpha = 60°$ a $|AB|+|BP| = |AQ|+|QC|$, určete velikosti zbylých vnitřních úhlů v $\triangle ABC$. (IMO 2001, 5)

Poznáváme známou konfiguraci

Často dokreslujeme body tak, aby vznikla známá konfigurace – například trojúhelník s kolmištěm a kružnicí devíti bodů, nebo třeba trojúhelník se Švrčkovými body či připsišti. Nezřídka se totiž úloha jen snaží maskovat známé tvrzení ze známého obrázku.

Příklad 8. Uvnitř trojúhelníka ABC je dán bod P tak, že platí $|\sphericalangle ABP| = 30°$, $|\sphericalangle PBC| = 40°$, $|\sphericalangle BCP| = 20°$ a $|\sphericalangle PCA| = 30°$. Ukažte, že $AP \perp BC$.

(MKS 32–8–4a)

Příklad 9. V rovině jsou dány body A, B, C, D tak, že platí $|\sphericalangle ACB| = 20°$, $|\sphericalangle ADB| = |\sphericalangle ABC| = 40°$ a $|\sphericalangle ADC| = 80°$. Určete $|\sphericalangle ABD|$. (KMS 2008)

Příklad 10. Čtyřúhelník $ABCD$ je vepsán do půlkružnice s průměrem AB. Tečny k půlkružnici vedené body C, D se protnou v E a úhlopříčky AC, BD v bodě F. Označme M průsečík EF a AB. Dokažte, že body E, C, M, D leží na jedné kružnici.

(China West 2010)

Příklad 11. V tětivovém čtyřúhelníku $ABCD$ označme I, J postupně vepsiště trojúhelníků ABD, ABC. Dále označme K průsečík kolmic vedených z bodů I, J po řadě na přímky BD, AC. Dokažte, že trojúhelník IJK je rovnoramenný.

(MO 56–A–III–2)

Příklad 12. V ostroúhlém různostranném trojúhelníku ABC označme P patu A-výšky, H kolmiště, O opsiště, D průsečík AO a BC a konečně M střed úsečky AD. Dokažte, že přímka PM prochází středem úsečky OH. (MO 60–A–III–5)

Příklad 13. V trojúhelníku ABC označme M střed strany BC, I vepsiště a N střed oblouku BC kružnice opsané obsahujícího bod A. Dokažte, že $|\sphericalangle INA| = |\sphericalangle IMB|$. (ARO 2005)

Středy a body v poměru

Samostatnou přednášku by zasloužilo zacházení se středy úseček. Obecně lze říci, že máme-li v obrázku středy alespoň dva, snažíme se dokreslit další, abychom využili vlastností středních příček. Je-li přítomen střed jeden, můžeme s výhodou použít středovou souměrnost (dokreslit rovnoběžník). Na závěr ještě zmiňme, že ačkoliv středy obecně nemají dobré úhlové vlastnosti, středy přepon pravoúhlých trojúhelníků jsou (jakožto středy opsaných kružnic) „úhlově“ příjemné.

Příklad 14. Ve čtyřúhelníku $ABCD$ svírá spojnice středů stran BC a AD stejné úhly s oběma úhlopříčkami. Dokažte, že tyto úhlopříčky jsou stejně dlouhé.
(ARO 1990)

Příklad 15. Uvnitř trojúhelníka ABC na jeho těžnici AM je dán bod K tak, že $|CK| = |AB|$. Označme L průsečík přímek CK a AB. Dokažte, že trojúhelník AKL je rovnoramenný.

Příklad 16. Je dán trojúhelník ABC vepsaný do kružnice k. Tečna k vedená bodem A protne přímku BC v bodě P. Označme M střed AP a Q druhý průsečík MB a k. Ukažte, že $|\sphericalangle PQA| = |\sphericalangle AQC|$. (Alex Zhai)

Příklad 17. Na straně BC ostroúhlého trojúhelníka ABC s kolmištěm H je dán bod D. Kolmice na DH vedená bodem H protne strany AB, AC v bodech F, E. Dokažte, že

$$\frac{|BD|}{|DC|} = \frac{|FH|}{|HE|}.$$

(Polsko)

Příklad 18. Na stranách BC, CA, AB trojúhelníka ABC jsou dány body P, Q, R tak, že

$$\frac{|BP|}{|PC|} = \frac{|CQ|}{|QA|} = \frac{|AR|}{|RB|}.$$

Navíc platí $|\sphericalangle ABC| = |\sphericalangle PRQ|$. Dokažte, že trojúhelníky ABC a PRQ jsou podobné.
(ARO 1989)

Příklad 19. Úhlopříčky tětivového čtyřúhelníka $ABCD$ se protínají v bodě P. Označme K, L paty kolmic z P na AB, CD a dále buď M střed strany AD. Dokažte, že $|MK| = |ML|$. (USA TST 2000)

Stříhání a přelepování

Dokreslování hojně využíváme tehdy, je-li obrázek svázaný nezvyklými podmínkami. V takovém případě se ho snažíme přeorganizovat tak, aby podmínky začaly dávat lepší geometrický smysl.

Příklad 20. V konvexním čtyřúhelníku $ABCD$ platí $|\sphericalangle ADB| + |\sphericalangle ACB| = 90°$ a $|\sphericalangle DBC| + 2 \cdot |\sphericalangle DBA| = 180°$. Navíc $|AD| = 6$ a $|DB| + |BC| = 10$. Určete $|AC|$.
(MKS 26–6–7)

Příklad 21. V obdélníku $ABCD$ jsou dány body E, F tak, že $EF \parallel AB$, $AE \parallel FC$ a AE protíná stranu CD. Navíc $|AB| = 9$, $|BC| = 8$, $|AE| = 4$ a $|FC| = 6$. Určete $|EF|$.
(AIME 2011)

Příklad 22. Uvnitř úhlu BAC je dán bod P. Na ramenech AB, AC najdeme body X, Y tak, aby $|AX| = |AY|$ a délka lomené čáry XPY byla nejkratší možná, Dokažte, že $|\sphericalangle APX| = |\sphericalangle APY|$.
(Polsko 2008)

Příklad 23. V rovnoběžníku $ABCD$ je dán bod P tak, že $|\sphericalangle APB| + |\sphericalangle CPD| = 180°$. Dokažte, že $|\sphericalangle ABP| = |\sphericalangle ADP|$.
(ruský folklór)

Příklad 24. Na stranách AB, AC trojúhelníka ABC s opsištěm O jsou dány body M, N tak, že $|\sphericalangle MON| = \alpha$. Dokažte, že obvod trojúhelníka MAN není menší než $|BC|$.
(ARO 2002)

Příklad 25. Bod M uvnitř konvexního čtyřúhelníka $ABCD$ splňuje $|MA| = |MC|$,

$$|\sphericalangle AMB| = |\sphericalangle MAD| + |\sphericalangle MCD| \qquad \text{a} \qquad |\sphericalangle CMD| = |\sphericalangle MCB| + |\sphericalangle MAB|.$$

Dokažte, že $|AB| \cdot |CM| = |BC| \cdot |MD|$ a $|BM| \cdot |AD| = |MA| \cdot |CD|$.
(IMO shortlist 1999, G7)

Vždy rovnostranný trojúhelník!

V úlohách s konkrétně zadanými velikostmi úhlů se snad vždy snažíme vyrobit rovnostranný trojúhelník – tím namnožíme úsečky jedné pevné délky a získáme rovnoramenné trojúhelníky či dokonce kružnice. Dalším opakujícím se motivem je používání opsiště střídavě jako bodu stejně vzdáleného od tří jiných a bodu, u nějž jsou dvojnásobné (totiž středové) úhly.

Příklad 26. V konvexním čtyřúhelníku $ABCD$ platí $|AB| = |BC| = |CD|$. Dále $|\sphericalangle ABC| = 150°$ a $|\sphericalangle BCD| = 90°$. Určete $|\sphericalangle ADB|$.

Příklad 27. Uvnitř rovnoramenného trojúhelníka ABC splňujícího $|AB| = |AC|$ a $|\sphericalangle BAC| = 99{,}4°$ je dán bod D tak, že $|AD| = |DB|$ a $|\sphericalangle BAD| = 19{,}7°$. Určete $|\sphericalangle ACD|$.
(Náboj 2013, 54)

Příklad 28. V A-rovnoramenném trojúhelníku ABC s vnitřním úhlem $\alpha = 80°$ je dán bod P tak, že $|\sphericalangle PAC| = 10°$ a $|\sphericalangle PCA| = 20°$. Určete $|\sphericalangle PBC|$.

Příklad 29. Ve čtyřúhelníku $ABCD$ platí $|AB| = |AC|$, $|AD| = |CD|$, $|\sphericalangle BAC| = 20°$ a $|\sphericalangle ADC| = 100°$. Dokažte, že $|AB| = |BC| + |CD|$.

Příklad 30. Uvnitř trojúhelníka ABC splňujícího $\beta = 2\gamma$ je dán bod P tak, že $|PB| = |PC|$ a $|AB| = |AP|$. Dokažte, že $|\sphericalangle PAC| = 2 \cdot |\sphericalangle PAB|$.

Příklad 31. Je dán trojúhelník ABC splňující $\beta = \gamma = 50°$. Na jeho stranách BC, CA jsou dány body P, Q tak, že $|\sphericalangle BAP| = 50°$ a $|\sphericalangle QBA| = 30°$. Určete $|\sphericalangle BQP|$.

Příklad 32. Je dán trojúhelník ABC splňující $\beta = \gamma = 80°$. Na straně AB najdeme bod P tak, aby $|AP| = |BC|$. Určete $|\sphericalangle ACP|$.

Příklad 33. Na straně AD kosočtverce $ABCD$ splňujícího $|\sphericalangle DAB| = 40°$ je dán bod M tak, že $|\sphericalangle DBM| = 30°$. Určete $|\sphericalangle DCM|$.

Magie

Ať se nám to líbí, či ne, je potřeba se smířit s tím, že stále budou existovat úlohy, které tak úplně nespadají do žádné z výše uvedených kategorií. Pak je potřeba vhodné dokreslení prostě vymyslet :). Nebojte se experimentovat!

Příklad 34. Je dán konvexní šestiúhelník $ABCDEF$ splňující $|AB| = |BC|$, $|CD| = |DE|$ a $|EF| = |FA|$. Dokažte, že osy úhlů ABC, CDE a EFA procházejí jedním bodem.

Je to tak.

Příklad 35. V rovnoramenném trojúhelníku ABC se základnou BC označme M střed těžnice AD a P patu kolmice z D na BM. Dokažte, že $|\sphericalangle APC| = 90°$.

(Rumunsko 2006)

Příklad 36. Body X, Y, Z jsou dány na výškách AD, BE, CF trojúhelníka ABC tak, že

$$[ABZ] + [BCX] + [CAY] = [ABC]$$

(kde symbolem $[PQR]$ značíme obsah trojúhelníka PQR). Označme H kolmiště trojúhelníka ABC. Dokažte, že body X, Y, Z, H leží na jedné kružnici.

Příklad 37. Je dán ostroúhlý trojúhelník ABC vepsaný do kružnice k se středem O. Ať AA' je její průměr. Tečna ke k vedená bodem A' protne přímku BC v bodě P. Přímka PO vytne na trojúhelníku ABC úsečku. Dokažte, že O je jejím středem.

(Výběrko 2007)

Příklad 38. Je dán čtyřúhelník $ABCD$ splňující $a + c = b + d$. Nad všemi jeho stranami jako nad průměry jsou sestrojeny kružnice. Dokažte, že existuje kružnice, která se jich všech dotýká. (Polsko 2013)

Příklad 39. Je dán konvexní čtyřúhelník $PIVO$. Osy stran PI a VO se protínají v bodě Y. Bod X uvnitř $PIVO$ splňuje

$$|\sphericalangle XVI| = |\sphericalangle XOP| < 90° \qquad \text{a} \qquad |\sphericalangle XIV| = |\sphericalangle XPO| < 90°.$$

Ukažte, že $|\sphericalangle VYO| = 2 \cdot |\sphericalangle XIV|$. (IMO shortlist 2000, G6)

Příklad 40. Kružnice vepsaná trojúhelníku ABC se dotýká jeho stran AB, AC v bodech Z, Y. Zkonstruujme body R, S tak, aby $BCYR$ a $BCSZ$ byly rovnoběžníky, a označme G průsečík přímek BY a CZ. Dokažte $|GR| = |GS|$.

(IMO shortlist 2009, G3)

Příklad 41. (Brianchonova věta) Lze-li šestiúhelníku $ABCDEF$ vepsat kružnici, pak úhlopříčky AD, BE, CF procházejí jedním bodem.

Návody

1. V rovnoramenném trojúhelníku splývá osa strany s osou úhlu.

2. Je to pravoúhlý trojúhelník s ustřihnutým rohem.

3. Dokreslete druhou polovinu obrázku a využijte středové souměrnosti.

4. Překlopte A podle osy úhlu u C (nebo narovnejte AI na CA) a najděte tětivový čtyřúhelník.

5. Po protažení úseček najděte podobné trojúhelníky.

6. Nakreslete vhodné kružnice se středy A, B, protněte je podruhé, protáhněte úsečky a najděte tětivový čtyřúhelník.

7. „Narovnejte“ lomené čáry na přímky AB, AC. Poúhlete a dokažte, že jelikož P není A-připsiště v $\triangle ABQ$, musí být $|QB| = |QT|$.

8. Poznejte kolmiště.

9. Dokažte, že bod D je opsiště $\triangle ABC$.

10. Protáhněte ramena a poznejte obrázek s kolmištěm a kružnicí devíti bodů.

11. Dokreslete tzv. „Švrčkův bod“ – střed oblouku AB kružnice opsané čtyřúhelníku $ABCD$.

12. Obraz H podle strany BC padne na kružnici opsanou.

13. Dokreslete B- a C-připsiště a uvědomte si, že N je jejich středem.

14. Dokreslete střed AB.

15. „Navažte“ na sebe shodné úsečky dokreslením rovnoběžníka $BKCX$.

16. Dokreslete současně rovnoběžník $PBAX$ a tětivový čtyřúhelník $PQAX$.

17. Na polopřímku BH naneste X, aby $|BH|/|HX| = |BD|/|DC|$, a odhalte kolmiště.

18. Dokreslete průsečík BC a rovnoběžky s AB skrz Q.

19. Středy PA a PD, jakožto středy přepon pravoúhlých trojúhelníků, vůbec nejsou špatné body.

20. Obrázek vznikl přehnutím podle AB (proto v něm není CD). Narovnejte ho.

21. Vystřihněte pásek skrz E a F.

22. Rozstřihněte $AXPY$ podle AP a přelepte.

23. Přelepte $\triangle ABP$ na $\triangle DCX$, aby vznikl tětivový čtyřúhelník.

24. Využijte toho, že $|OA| = |OB| = |OC|$, a přerovnejte obvod $\triangle MAN$ do lomené čáry s konci B a C.

25. Rozstříhejte $ABCD$ podle M na 4 trojúhelníky a přeskládejte je (po případném nafukování) na rovnoběžník.

26. Dokreslete současně čtverec $BCDE$ a rovnostranný trojúhelník ABE.

28. Zobrazte P podle BC.

29. Naneste na AB úsečku délky $|AD|$ nebo přelepte BCD na DEC.

30. Dokreslete rovnoramenný lichoběžník.

31. Zobrazte P podle AC na P' a uvědomte si, že P' leží na BQ (kružnice se středem P).

32. Překlopte C přes AB do X a B přes AC do Y. Najděte tvar ACP na bodech B, C, X, Y.

33. Zobrazte M podle BD na N a všimněte si, že N je opsiště $\triangle MBC$.

34. Dokreslete trojúhelník ACE.

35. Dokreslete obdélník $ADMX$.

36. Veďte body X, Y, Z rovnoběžky s příslušnými stranami.

37. Ať M je střed BC.

38. Střed úhlopříčky!

39. Na osu VO dokreslete body K, L tak, aby $\triangle VKL \sim \triangle VXB$ a $\triangle OKL \sim \triangle OXP$. Vyjde $|LP| = |LI|$.

40. Dokažte, že B a Y leží na chordále R a A-připsané.

41. Dokreslete tři kružnice tak, aby úhlopříčky AD, BE, CF byly jejich chordálami.

Literatura

[1] Andreescu, Rolínek, Tkadlec, *107 Geometry Problems*, XYZ Press, 2013.
[2] Archivy olympiád na *mathlinks.ro*.

Hlavolamy v hlavě

Martina Vaváčková

Abstrakt. Mechanické hlavolamy rozvíjí tvůrčí myšlení a prostorovou představivost. Řešíme-li je zpaměti, procvičíme tyto dvě dovednosti ještě důkladněji, neboť eliminujeme vliv náhody. Příspěvek obsahuje množství úloh – hlavolamů určených k řešení zpaměti.

Hlavolamem máme na mysli hlavolam mechanický, tedy takový, který si zpravidla můžeme vzít do ruky a v němž je cílem oddělit nebo přesunout nějakou součástku. Přitom samozřejmě není dovoleno stříhat, řezat či používat hrubou sílu.

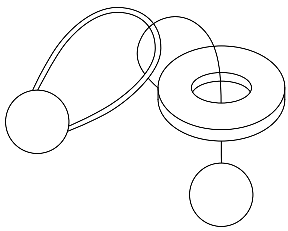
Proč je dobré si hlavolamy představovat?

Řešíme-li hlavolam, který držíme v ruce, mnohdy s ním manipulujeme, aniž bychom se nad tím hlouběji zamysleli. Když máme nějaký nápad, prostě jej vyzkoušíme. Někdy se nám pak stane, že dojdeme k řešení zcela náhodou.

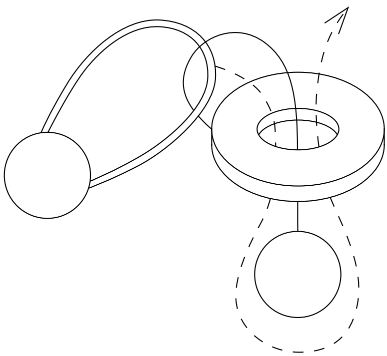
Jakmile si však na hlavolam nemůžeme sáhnout, musíme každý nápad domyslet do konce. Je zapotřebí si jednotlivé kroky představit, případně si je vhodně nakreslit. Tyto dvě věci se zejména v matematice velmi hodí.

Motivační příklady

Příklad 1. Mějme hlavolam, který sestává z kroužku a dvou kuliček spojených provázkem jako na obrázku. Kroužek i kulička projdou skrz očko s kuličkou, ale kulička neprojde skrz kroužek. Oddělte očko s kuličkou.

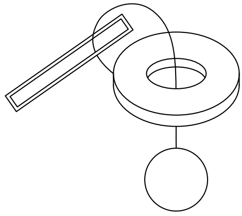


Řešení. Provlečeme očko skrz kroužek a následně kuličku skrz očko – a máme vyhráno.



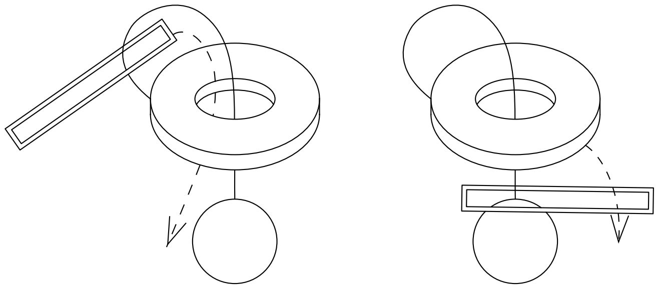
Výborně. A nyní si představme, že místo modrého očka s kuličkou máme kovový obdélník.

Příklad 2. Mějme hlavolam, který sestává z kroužku, kuličky a kovového obdélníku spojených provázkem jako na obrázku. Kroužek projde skrz obdélník, kulička nikoliv. Obdélník projde skrz kroužek. Oddělte kovový obdélník.



Řešení. Postup z předchozího příkladu použít nemůžeme, neboť kulička neprojde skrz obdélník. Můžeme však využít toho, že obdélník lze provléknout skrz kroužek.

Pokud tak učiníme, stačí již jen provléknout kroužek skrz obdélník.



Tipy

Předchozí dva příklady byly spíše ilustrační. Než se pustíme do opravdových hlavolamů, řekneme si několik tipů, které nám mohou pomoct při jejich řešení.

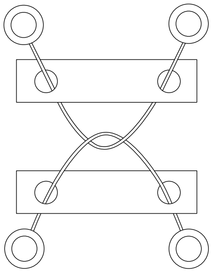
Zaprvé – pohybujme jen vybranými objekty a ostatní si zafixujme. Když budeme pohybovat všemi předměty zároveň, snadno se ve svých představách ztratíme. Zadruhé – nevíme-li, co se stane, když s hlavolamem něco provedeme, namalujme si to! Zatřetí – když nám dochází nápady, zkusme postupovat inverzně. Představme si, že máme hlavolam ve stavu, do kterého jej chceme dostat, a pokusme se jej převést do počátečního stavu.

Úlohy

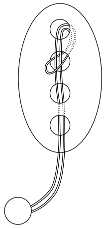
Kdykoliv v následujících úlohách zmíníme některé ze slov dřívko, lodička, kulička, kroužek, tyčka, deska, obdélník nebo kovový objekt, automaticky přidáváme předpoklad, že tyto předměty není možné deformovat. Naproti tomu provázek a smyčka jsou věci ohebné, které se dají provléct skrz libovolný otvor, a to dokonce několikanásobně.

Když řekneme, že provázek je dlouhý, znamená to, že jeho délka nás nelimituje v činnosti – můžeme jej libovolně provlékat a přetahovat přes jiné objekty.

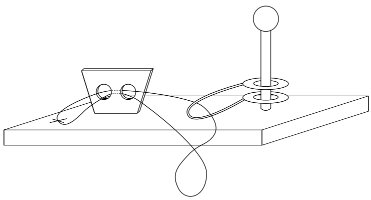
Úloha 1. Dva a dva kroužky jsou spojeny provázkem a provlečeny skrz dvě dřívka s otvory na krajích. Kroužek neprojde skrz otvor. Cílem je rozdělit hlavolam na dva kusy.



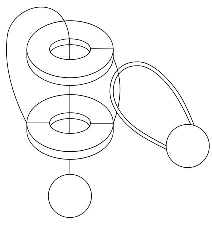
Úloha 2. Skrz oválné dřívko se čtyřmi otvory je provlečena dlouhá smyčka s kuličkou na konci. Kulička neprojde skrz otvor. Cílem je oddělit smyčku s kuličkou na konci.



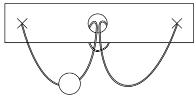
Úloha 3. K desce je připevněna dlouhá smyčka. Skrz ni je provlečen provázek, který je obou na koncích připevněn ke kroužkům. Kroužky jsou navlečeny na tyčce, která je připevněna k desce a na jejímž horním konci se nachází kulička. Kulička neprojde skrz kroužek. Na smyčce je navlečena lodička (ta není připevněna k desce). Cílem je oddělit lodičku.



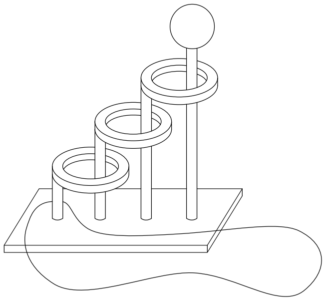
Úloha 4. Oba konce jednoho provázku jsou přivázány ke kroužkům. Druhý provázek je přivázán pouze k jednomu z nich a na jeho druhém konci se nachází kulička. Kulička neprojde skrz kroužek. Za první provázek je zaháknuta smyčka s kuličkou. Kulička i kroužek projdou skrz smyčku. Cílem je oddělit smyčku s kuličkou.



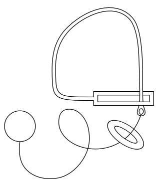
Úloha 5. Ke dřívku s otvorem uprostřed je připevněn dlouhý provázek, na němž je navlečená kulička, která neprojde skrz otvor. Cílem je přesunout kuličku doprava.



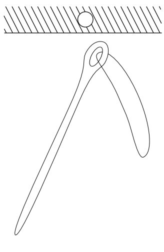
Úloha 6. K desce jsou připevněny tři tyčky s kroužky na koncích a jedna tyčka s kuličkou na konci. Za první tyčku je zaháknuta dlouhá smyčka. Cílem je oddělit smyčku.



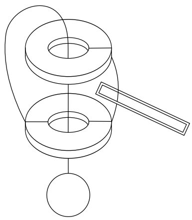
Úloha 7. Ke kovovému objektu je připevněn dlouhý provázek s kuličkou na konci. Na provázku je navlečený kroužek. Kroužek projde skrz otvor, dá se navléct na objekt a „provlékat dokola“, ale neprojde skrz něj kulička. Cílem je oddělit kroužek.



Úloha 8. Tyčka má na konci otvor, skrz který je provlečena smyčka. Tato smyčka je kratší než tyčka samotná. Tyčka projde skrz knoflíkovou dírku. Cílem je zavěsit tyčku do knoflíkové dírky na košili („liščími tlapkami“).



Úloha 9. Oba konce jednoho provázku jsou přivázány ke kroužkům. Druhý provázek je přivázán pouze k jednomu z nich a na jeho druhém konci se nachází kulička. Kulička neprojde skrz kroužek. Za první provázek je zaháknut kovový obdélník. Kroužek projde skrz obdélník, kulička nikoliv. Obdélník projde skrz kroužek. Cílem je oddělit kovový obdélník.



Návody

1. Provlečte spodní provázek skrz otvor v horním dřívku.

2. Proveďte podobný manévr jako v předchozí úloze.

3. Umíme dosáhnout toho, aby byla dlouhá smyčka zaháknutá na tyčce?

4. Smyčku můžete nejen přetahovat přes kroužky, ale i provlékat skrz ně (pouze kulička zůstane stále na stejné straně).

5. Není třeba přetahovat provázek přes dřívko, soustřeďte se na středový otvor.

6. Co by se stalo, kdyby byla smyčka zaháknutá za dvě krajní tyčky?

7. Vyzkoušejte inverzní postup. Představte si, že máte kroužek zvlášť a chcete jej navléct na provázek.

8. Knoflíková dírka je **v látce**.

9. Nejprve provlečte obdélník shora dolů skrz spodní kroužek.

Zdroje

Inspirací pro výše uvedené příklady byly mechanické hlavolamy *Markuse Götze*, jejichž fotografie lze nalézt na webu *http://www.markus-goetz.de/*.

Rekurentní posloupnosti

Martina Vaváčková

Nekonečná reálná posloupnost je formálně funkce $\mathbb{N} \to \mathbb{R}$, která každému přirozenému číslu k přiřadí hodnotu $a_k \in \mathbb{R}$. Místo $a_1, a_2, a_3, \dots$ píšeme často pouze $\{a_n\}_{n=1}^{\infty}$. Podobně zavádíme $\{a_n\}_{n=0}^{\infty}$, $\{a_n\}_{n=1}^{N}$ a další.

Posloupnost můžeme zadat dvěma způsoby – explicitně nebo rekurentně. Explicitní vyjádření nám dává přímý předpis pro n-tý člen, zatímco v případě rekurentního zadání je n-tý člen vyjádřen pomocí n a předchozích členů (prvních několik členů je dáno).

Výhoda explicitního zadání spočívá v tom, že s jeho pomocí můžeme rychle spočítat libovolný člen posloupnosti, na který si vzpomeneme. Rekurentní zadání je však mnohdy snáze zapamatovatelné a na první pohled dává lepší náhled na to, jak ona posloupnost vlastně funguje. To ilustruje následující příklad.

Příklad. Jednou z nejznámějších rekurentních posloupností je *Fibonacciho posloupnost*. Ta je zadaná vztahy $F_0 = 0$, $F_1 = 1$ a $F_n = F_{n-1} + F_{n-2}$ pro $n \geq 2$. Existuje však i její explicitní vyjádření, jímž je

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

Nabízí se otázka, zda umíme explicitní vyjádření nalézt pro libovolnou rekurentně zadanou posloupnost. Odpověď zní: obecně ne, nicméně pokud je rekurence „pěkná“, možné to je. Tím se zde ale zabývat nebudeme a místo toho se vrhneme na úlohy!

Lehčí úlohy

Příklad 1. Posloupnost je zadána rekurentně vztahy $a_1 = 3$, $a_2 = 7$ a $a_{n+1} = a_n - a_{n-1}$ pro $n \geq 3$. Spočtěte a_{100}.

Příklad 2. Buď $\{a_n\}_{n=0}^{\infty}$ posloupnost, v níž je $a_0 = a_1 = 1$ a pro $a \geq 2$ platí $a_{n+1} = a_{n-1}a_n + 1$. Ukažte, že a_{2013} není dělitelné čtyřmi.

Příklad 3. Mějme posloupnost $\{a_n\}_{n=1}^{\infty}$ definovanou rekurentně: $a_1 = 2$, $a_{n+1} = a_n^2 - a_n + 1$. Ukažte, že libovolné dva členy této posloupnosti jsou nesoudělné.

(MKS 22–5–3)

Příklad 4. Posloupnost $\{a_n\}_{n=1}^{\infty}$ reálných čísel splňuje pro $n \geq 2$ vztah $a_n = a_{n-1} + a_{n+2}$. Zjistěte, kolik nejvíce po sobě jdoucích kladných čísel může tato posloupnost obsahovat. (MKS 30–2j–4)

Příklad 5. Buď $\{a_n\}_{n=1}^{\infty}$ posloupnost, v níž je $a_1 = a_2 = 1$ a pro $n \geq 3$ platí $a_n = \frac{a_{n-1}^2+2}{a_{n-2}}$. Ukažte, že pro každé $n \in \mathbb{N}$ je a_n celé číslo.

Příklad 6. Rozhodněte, zda pro každé přirozené číslo n existuje posloupnost prvočísel $\{p_i\}_{i=1}^{n}$ splňující rekurentní formuli $p_i = p_1 p_2 \cdots p_{i-1} + 1$ pro $2 < i \leq n$ (druhý člen je nezávislý na prvním!). (MKS 23–1–3)

Středně těžké úlohy

Příklad 7. Je dána posloupnost: $a_0 = 3$, $a_1 = 4$, $a_2 = 167$, $a_n = 2003a_{n-1} - a_{n-2} + 174$ pro $n \geq 3$. Najděte všechna k taková, že a_k je prvočíslo. (MKS 22–5–4)

Příklad 8. Posloupnost $\{a_n\}_{n=1}^{\infty}$ je dána předpisem $a_1 = 56$, $a_{n+1} = a_n - \frac{1}{a_n}$. Ukažte, že $a_n < 0$ pro nějaké $0 < n < 2013$. (MKS 23–1–4)

Příklad 9. První člen posloupnosti je 99 a každý další je součtem desátých mocnin všech cifer předchozího členu. Může se v takové posloupnosti vyskytnout nějaké číslo přesně dvakrát? (MKS 30–6–5)

Příklad 10. Nechť posloupnost $\{a_n\}_{n=1}^{\infty}$ splňuje vztah $a_{n+1} = a_n + f(a_n)$, kde $f(m)$ značí součin cifer čísla m. Je tato posloupnost omezená pro všechna a_1 přirozená? (MKS 23–1–6)

Příklad 11. Posloupnost má první dva členy $a_1 = 20$ a $a_2 = 11$ a dále je definovaná pomocí vzorce

$$a_{n+2} = a_n - \frac{1}{a_{n+1}},$$

dokud má pravá strana smysl (tj. nedělí se nulou). Určete nejmenší t takové, že $a_t = 0$. (Náboj 2011, 43)

Návody

1. Platí $a_{n+6} = a_n$, řešení je -3.

2. Najděte periodu posloupnosti $\{a_n \mod 4\}_{n=0}^{\infty}$.

3. Ukažte, že pro $i > j$ dává a_i zbytek 1 po dělení a_j.

4. Nanejvýš pět – dokazujte sporem.

5. Odečtěte od sebe rekurentní vztahy pro n-tý a $(n+1)$-tý člen.

6. BÚNO je p_1 sudé. Rozeberte tři případy podle toho, jaký zbytek dává p_2 po dělení třemi. Pro $n \geq 5$ taková posloupnost neexistuje.

7. Ukažte, že členy, jejichž index dává po dělení třemi zbytek $k \in \{0, 1, 2\}$, jsou dělitelné číslem a_k.

8. Nejprve ukažte, že $a_n \neq 0$. Dále předpokládejte, že pro každé n je $a_n > 0$, a použijte vhodné odhady.

9. Ukažte, že každý člen posloupnosti má nejvýše jedenáct cifer.

10. Ano. Rozmyslete si, co se děje, když posloupnost přeskočí na vyšší řád.

11. Co se děje se součiny dvou po sobě jdoucích členů posloupnosti?

Literatura a zdroje

[1] Arthur Engel, *Problem Solving Strategies*, Springer, UK, 1998.
[2] Saša Kazda, *Rekurentní rovnice*, Janova Bouda, 2005.
[3] Miško Szabados, *Rekurentné postupnosti*, Oldřichov, 2009.
[4] Katka Quitnerrová, *Rekurentné postupnosti*, Horní Bradlo, 2004.

Kombinatorická geometrie

Lukáš Zavřel

Postupně si ukážeme, jaké myšlenky se nám budou hodit v řešení těchto netradičních úloh. Často je myšlenka velmi jednoduchá, jen bychom nečekali, že se objeví právě v takových příkladech...

Příklad 1. Vnitřní prostory muzea tvoří mnohoúhelník (ne nutně konvexní) o $3n$ vrcholech. Lze v muzeu rozestavit n hlídačů tak, aby dohromady viděli celý prostor muzea?

Příklad 2. V rovině leží $n \geq 3$ úseček tak, že každé tři mají společný bod. Dokažte, že lze najít bod společný všem těmto úsečkám.

Příklad 3. Na stole leží patnáct časopisů, které jej celý pokrývají. Dokažte, že lze ubrat 7 z nich, aby zbývajících 8 zakrývalo alespoň $\frac{8}{15}$ velikosti stolu.

Příklad 4. Mějme v rovině n modrých a n červených bodů. Dokažte, že je umíme pospojovat n úsečkami tak, že každá úsečka spojuje jeden modrý a jeden červený bod a zároveň se tyto úsečky nekříží.

Příklad 5. V rovině je dáno $n \geq 3$ bodů, které neleží všechny na jedné přímce. Potom lze najít kružnici, která obsahuje alespoň tři z daných bodů, přičemž žádný jiný neleží uvnitř této kružnice. Dokažte.

Příklad 6. Mějme v rovině $3n$ bodů v obecné poloze. Dokažte, že je můžeme pospojovat tak, že vytvoříme n navzájem disjunktních trojúhelníků.

Příklad 7. (Moser spindle) Umístěte do roviny 7 bodů tak, aby libovolný trojúhelník s vrcholy ve třech z těchto sedmi bodů měl alespoň jednu stranu délky 1.

Příklad 8. Na přímce leží n úseček tak, že každé dvě mají společný bod. Dokažte, že lze najít bod společný všem těmto úsečkám.

Příklad 9. Mějme v rovině n mnohoúhelníků takových, že každé dva mají neprázdný průnik. Dokažte, že poté pro libovolný bod roviny A existuje poloměr r takový, že kruh se středem v bodě A a poloměrem r protne každý z těchto mnohoúhelníků. (MKS 28–4–7)

Příklad 10. Uvnitř jednotkového čtverce je rozmístěno několik kružnic, které mají součet obvodů 10. Dokažte, že pak existuje přímka, která protíná alespoň čtyři z těchto kružnic.

Příklad 11. Je dán čtverec a devět přímek. Nechť každá z devíti přímek dělí čtverec na dva čtyřúhelníky, jejichž obsahy jsou v poměru 2 : 3. Dokažte, že alespoň tři z těchto devíti přímek procházejí jedním bodem. (MKS 28–5–5)

Příklad 12. Mějme body v obecné poloze (tj. žádné tři body neleží na přímce, žádné čtyři neleží na kružnici). Kolik poté existuje:

(i) Pro tři body v rovině: Přímek, které mají stejnou vzdálenost od všech tří bodů?
(ii) Pro čtyři body v prostoru: Rovin, které mají stejnou vzdálenost od všech čtyř bodů?
(iii) Pro čtyři body v rovině: Přímek či kružnic, které mají stejnou vzdálenost od všech čtyř bodů?

Příklad 13. Je možné rozdělit rovnostranný trojúhelník na milion konvexních mnohoúhelníků tak, aby jich libovolná přímka protínala nejvýše čtyřicet? (MKS 31–3–8)

Příklad 14. Rozmístění 4027 bodů v rovině nazveme *kolumbijským*, jestliže je z nich 2013 červených, 2014 modrých a žádné tři neleží v přímce. O skupině přímek v rovině řekneme, že je *dobrá* pro dané rozmístění, jestliže:

(i) žádná z přímek neprochází žádným bodem rozmístění,
(ii) žádná z částí, na které je rovina přímkami rozdělena, neobsahuje body různých barev.

Najděte nejmenší k takové, že pro libovolné kolumbijské rozmístění 4027 bodů v rovině v ní existuje skupina k dobrých přímek. (IMO 2013, 2)

Příklad 15. Je dán trojúhelník, který má obsah 1, a v něm pět bodů. Dokažte, že z daných pěti bodů lze vybrat tři různé takové, že jimi určený trojúhelník má obsah nejvýše $\frac{1}{4}$.

Návody

1. Lze. Daný $3n$-úhelník rozdělíme na n čtyřúhelníků, na každý čtyřúhelník stačí jeden hlídač.

2. Vezmeme průsečík dvou úseček. Ten musí ležet na každé další.

3. Ubíráme postupně časopisy po jednom, dokazujeme sporem: Kdyby každý časopis po odebrání odkryl více než $\frac{1}{15}\dots$

4. Extremální princip: Pospojování, které má nejkratší součet délek úseček, podmínku ze zadání splňuje. Pokud se totiž někde dvě úsečky kříží, v daném čtyřúhelníku prohoď úhlopříčky za strany, podle trojúhelníkové nerovnosti bude součet kratší, tedy nastává spor.

5. Začněte s malou kružnicí a nafukujte ji tak dlouho, dokud nenarazíte na tři body.

6. Zvolte směr a jeďte přímkou tohoto směru zleva doprava.

7. Začněte dvěma kosočtverci, které sdílí jeden vrchol, a správně je vůči sobě natočte.

8. Ze všech pravých konců úseček vezměte ten nejvíce vlevo.

9. Za r vezměte nejmenší možnou velikost takovou, že kruh bude obsahovat alespoň jeden celý mnohoúhelník.

10. Hledejte takovou přímku rovnoběžnou s jednou stranou čtverce. Promítněte všechny kružnice na sousední stranu.

11. Ukažte, že dělí-li přímka čtverec na čtyřúhelníky s poměrem obsahů $2 : 3$, pak musí procházet jedním ze čtyř jistých bodů.

12.

(i) Celkem tři, vždy dva body jsou na jedné straně přímky a třetí na straně druhé.

(ii) Dva body na každé straně roviny nebo na jedné straně tři a na druhé jeden, dohromady tedy $3 + 4 = 7$.

(iii) Znovu rozdělíme podle toho, jestli jsou na každé straně přímky/kružnice dva body, či na jedné 1 a na druhé 3. Dohromady $3 + 4 = 7$.

13. Ano. Vytvářejte početné „slupky“ tak, aby každá přímka protťala z každé slupky nejvýše dva mnohoúhelníky.

14. Kolem dvojice stejně barevných bodů jde nakreslit „nanotrubičku“.

Literatura

[1] Libor Barto, *Kombinatorická geometrie*, matematický kroužek.

Obsah