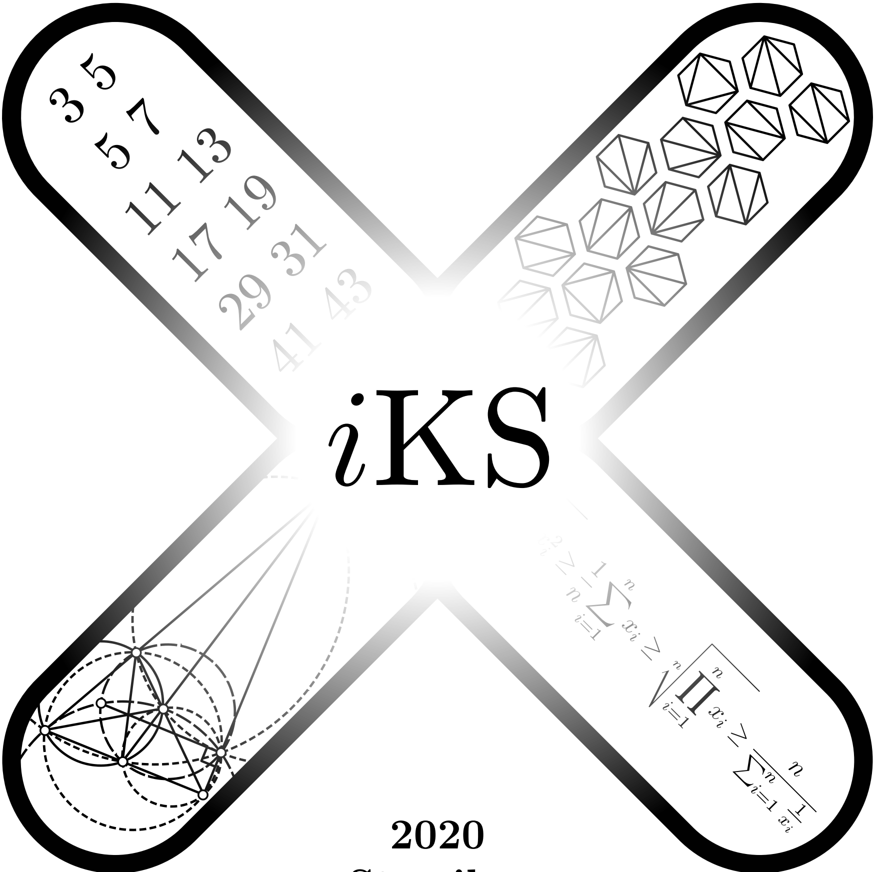

2020
Strmilov

Matěj Doležálek
Pavel Hudec
Jakub Löwit
Josef Minařík
Radek Olšák
Tomáš Sásik
Michal Staník
Ákos Záhorský

Diskrétní logaritmus

Matěj Doležálek

Abstrakt. Jak se chová násobení a mocnění mod n? S pomocí primitivního prvku si zadefinujeme diskrétní logaritmus a ukážeme, jak skrze grupy nahlížet na řády, kvadratické zbytky a další.

Bleskový úvod do grup

Definice. *Grupou* rozumíme množinu G s binární operací $\circ$ takovou, že

(i) G je uzavřená na $\circ$,
(ii) existuje takové $e \in G$, že $e \circ a = a \circ e = a$ pro každé $a \in G$,
(iii) pro každé $a \in G$ existuje a' takové, že $a \circ a' = a' \circ a = e$,
(iv) operace $\circ$ je asociativní.

Definice. Řekneme, že H je *podgrupou* grupy G, pokud $H \subseteq G$ a zároveň tvoří H grupu se stejnou operací jako G. Řekneme, že prvky $a_1, \ldots, a_n \in G$ *generují* H, pokud je H nejmenší podgrupa G splňující $\{a_1, \ldots, a_n\} \subseteq H$. Tuto skutečnost značíme $\langle a_1, \ldots, a_n \rangle = H$.

Definice. *Homomorfismem* mezi grupami G, H po řadě s operacemi $\circ$, $*$ rozumíme zobrazení $f : G \to H$ splňující

$$f(a \circ b) = f(a) * f(b)$$

pro každá $a, b \in G$. *Izomorfismem* rozumíme homomorfismus, který je zároveň bijekcí. Skutečnost, že G, H jsou izomorfní, značíme $G \simeq H$.

Definice. *Direktním součinem* grup G, H rozumíme grupu $G \times H$ uspořádaných dvojic (g, h), $g \in G$, $h \in H$, v níž binární operaci provádíme po složkách: v první složce operaci z G, v druhé z H.

Definice. Budiž n přirozené číslo. Znakem $\mathbb{Z}_n$ miňme množinu zbytkových tříd mod n, resp. jejich grupu se sčítáním. Znakem $\mathbb{Z}_n^*$ miňme množinu těch zbytkových tříd mod n, které jsou nesoudělné s n, resp. jejich grupu s násobením. Označme $\varphi(n) = |\mathbb{Z}_n^*|$.

Cvičení. Najdi všechny podgrupy $\mathbb{Z}_n$.

Mocnění v $\mathbb{Z}_n^*$

Definice. *Řádem* prvku $a \in \mathbb{Z}_n^*$ rozumíme mohutnost podgrupy, kterou a generuje v $\mathbb{Z}_n^*$. Značíme $\mathrm{ord}_n(a) = |\langle a \rangle|$.

Cvičení. Nejmenší přirozené k takové, že $a^k \equiv 1 \pmod{n}$, je $k = \mathrm{ord}_n(a)$.

Důsledek. Platí $a^x \equiv a^y \pmod{n}$, právě pokud $x \equiv y \pmod{\mathrm{ord}_n(a)}$.

Věta (Euler, malý Fermat). Pro $a \in \mathbb{Z}_n^*$ platí $a^{\varphi(n)} \equiv 1 \pmod{n}$. Pro prvočíslo p pak speciálně $a^{p-1} \equiv 1 \pmod{p}$.

Důsledek. Pro každé $a \in \mathbb{Z}_n^*$ platí $\mathrm{ord}_n(a) \mid \varphi(n)$. Díky tomu můžeme s exponenty ve výrazu mod n nakládat jako s prvky $\mathbb{Z}_{\varphi(n)}$.

Primitivní prvek

Definice. *Primitivním prvkem* rozumíme takové $g \in \mathbb{Z}_n^*$, že $\mathrm{ord}_n(g) = \varphi(n)$, neboli $\langle g \rangle = \mathbb{Z}_n^*$.

Lemma. Nechť $a \in \mathbb{Z}_n^*$ a $k \mid \mathrm{ord}_n(a)$. Pak v $\mathbb{Z}_n^*$ existuje prvek řádu k.

Lemma. Nechť $a, b \in \mathbb{Z}_n^*$, $\alpha = \mathrm{ord}_n(a)$, $\beta = \mathrm{ord}_n(b)$. Potom pokud jsou α, β nesoudělná, pak $\mathrm{ord}_n(ab) = \alpha\beta$.

Věta (Lagrange). Nechť je f polynom s celočíselnými koeficienty, z nichž ne všechny jsou násobky p. Pak má f nejvýše $\deg f$ různých kořenů mod p.

Věta. Pro liché prvočíslo p existuje primitivní prvek mod p.

Lemma. Pro liché prvočíslo p a přirozené $k \geq 2$ platí $\mathrm{ord}_{p^k}(1+p) = p^{k-1}$.

Věta. Primitivní prvek mod n existuje, právě pokud je n rovno 2, 4, p^k nebo $2p^k$ pro liché prvočíslo p a $k \in \mathbb{N}$.

Diskrétní logaritmus

Definice. Nechť je n jedno z čísel z předchozí věty. Pevně zvolme primitivní prvek g mod n. Potom *diskrétním logaritmem* prvku $a \in \mathbb{Z}_n^*$ míníme ten prvek $b \in \mathbb{Z}_{\varphi(n)}$, který splňuje $g^b \equiv a \pmod{n}$, a značíme jej $\log a$.

Cvičení. Nahlédni, že pro $x, y \in \mathbb{Z}_n^*$, $a \in \mathbb{Z}_{\varphi(n)}$ platí

$$\log(xy) \equiv \log x + \log y \pmod{\varphi(n)}, \qquad \log(x^a) \equiv a \log x \pmod{\varphi(n)}.$$

Pozorování. Diskrétní logaritmus je izomorfismem ze $\mathbb{Z}_n^*$ do $\mathbb{Z}_{\varphi(n)}$.

Cvičení (Wilsonova věta). Kongruence $(p-1)! \equiv -1 \pmod{p}$ platí právě tehdy, když je p prvočíslo.

Cvičení. Pokud existuje primitivní prvek mod n, pak už existuje přesně $\varphi(\varphi(n))$ navzájem nekongruentních primitivních prvků mod n.

Cvičení. Pokud $n > 2$ a existuje primitivní prvek, pak $\log(-1) \equiv \frac{\varphi(n)}{2} \pmod{\varphi(n)}$.

Cvičení. Nechť existuje primitivní prvek mod n. Potom:

(i) Kongruence $x^m \equiv 1 \pmod{n}$ má právě $\gcd(m, \varphi(n))$ řešení.
(ii) Výraz $x^m \pmod{n}$ nabývá právě $\frac{\varphi(n)}{\gcd(m,\varphi(n))}$ různých hodnot.

Cvičení. Budiž p prvočíslo a nechť je $H \neq \{1\}$ podgrupou $\mathbb{Z}_p^*$. Potom nutně platí $\sum\limits_{a \in H} a \equiv 0 \pmod{p}$.

Co složené moduly?

Cvičení. Pro nesoudělná a, b platí $\varphi(ab) = \varphi(a)\varphi(b)$. Následně

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

kde součin jde přes prvočísla p, která dělí n.

Věta (Čínská zbytková). Nechť jsou a, b nesoudělná přirozená čísla. Potom platí

$$\mathbb{Z}_{ab} \simeq \mathbb{Z}_a \times \mathbb{Z}_b, \qquad \mathbb{Z}_{ab}^* \simeq \mathbb{Z}_a^* \times \mathbb{Z}_b^*.$$

Cvičení. Pro $k \geq 2$ je $\mathbb{Z}_{2^k}^*$ izomorfní direktnímu součinu $\mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$.

Věta (Dirichlet). Nechť $a \in \mathbb{Z}_n^*$. Potom existuje nekonečně mnoho prvočísel p splňujících $p \equiv a \pmod{n}$.

Kvadratické zbytky

Definice. Prvek $a \in \mathbb{Z}_n^*$ nazvěme *kvadratickým zbytkem*, pokud $x^2 \equiv a \pmod{n}$ má řešení. V opačném případě jej zvěme *kvadratickým nezbytkem.*

Pozorování. Nenulové kvadratické zbytky mod p jsou právě prvky se sudým diskrétním logaritmem.

Důsledek. Pro liché prvočíslo p leží v $\mathbb{Z}_p^*$ právě $\frac{p-1}{2}$ kvadratických zbytků a $\frac{p-1}{2}$ kvadratických nezbytků.

Cvičení. Nechť je p prvočíslo a n přirozené číslo. Charakterizuj v $\mathbb{Z}_p^*$ zbytky tvaru x^n pomocí diskrétního logaritmu.

Cvičení. Pokud má n dva různé liché prvočíselné dělitele, pak neexistuje primitivní prvek mod n.

Definice. Nechť je p liché prvočíslo. Pak pro $a \in \mathbb{Z}_p^*$ definujeme *Legendreův symbol* jako

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{pokud je } a \text{ kvadratický zbytek,} \\ -1, & \text{pokud je } a \text{ kvadratický nezbytek.} \end{cases}$$

Tvrzení (Eulerovo kritérium). Platí $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.

Důsledek. Legendreův symbol je úplně multiplikativní – pro $a, b \in \mathbb{Z}_p^*$ platí

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Věta (Zákon kvadratické reciprocity). Nechť jsou p, q různá lichá prvočísla. Potom platí

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} = \begin{cases} \text{-1}, & \text{pokud } p \equiv q \equiv 3 \pmod 4, \\ 1, & \text{jinak.} \end{cases}$$

Věta (Druhý suplement). Pro liché prvočíslo p platí

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{pokud } p \equiv \pm 1 \pmod 8, \\ \text{-1}, & \text{pokud } p \equiv \pm 3 \pmod 8. \end{cases}$$

Počítáme

Příklad 1. Jsou dána různá prvočísla p, q. Dokaž $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Příklad 2. Jsou dána prvočísla p, q splňující $q \mid 2^p - 1$. Dokaž, že $p \mid q - 1$.

Příklad 3. Najdi všechna přirozená čísla nesoudělná se všemi členy nekonečné posloupnosti $a_n = 2^n + 3^n + 6^n - 1$. (IMO 2005, 4)

Příklad 4. Nechť je p prvočíslo a b celé číslo. Dokaž, že $b^{p^2-1} \equiv 1 \pmod{p^2}$, právě pokud $b^{p-1} \equiv 1 \pmod{p^2}$. (MKS 28–9–4)

Příklad 5. Nechť je $p > 3$ prvočíslo a $n = \frac{2^{2p}-1}{3}$. Dokaž, že $n \mid 2^n - 2$. (*i*KS 1, N4)

Příklad 6. Najdi všechny trojice prvočísel p, q, r splňující soustavu dělitelností

$$p \mid q^r + 1, \qquad q \mid r^p + 1, \qquad r \mid p^q + 1.$$

(USA TST 2003)

Příklad 7. Dokaž, že pro $n > 4$ je součin všech primitivních prvků mod n kongruentní 1.

Příklad 8. Nechť je p prvočíslo tvaru $3k+2$. Ukaž, že pokud $p \mid a^2+ab+b^2$, pak $p \mid a, b$.

Příklad 9. Nechť je p prvočíslo tvaru 2^k+1. Potom je každý kvadratický nezbytek mod p primitivním prvkem.

Příklad 10. Pro liché prvočíslo p urči součet všech kvadratických zbytků a součet všech kvadratických nezbytků mod p.

Příklad 11. Rozhodni, zda existuje nekonečná rostoucí posloupnost čtverců celých čísel $a_1, a_2, \dots$ taková, že $13^n \mid a_n+1$ pro každé $n \in \mathbb{N}$. (ELMO SL 2014)

Příklad 12. Ukaž, že 2 je primitivní prvek mod 3^n.

Příklad 13. Pro $n \in \mathbb{N}$ nemá 2^n+1 žádné prvočíselné dělitele tvaru $8k-1$. (Vietnam TST 2004)

Příklad 14. Dokaž, že neexistuje přirozené číslo a takové, že všechna tři 2^a-1, $2^{2a+1}-1$, $2^{4a+3}-1$ jsou prvočísla.

Příklad 15. Je dáno liché prvočíslo p, přirozené m, n a celé nezáporné s tak, že $p \mid m^{2^s}+n^{2^s}$. Dokaž, že $p \equiv 1 \pmod{2^{s+1}}$.

Příklad 16. Pro každé $a \in \mathbb{N}$, které není čtverec, existuje nekonečně mnoho prvočísel p takových, že $\left(\frac{a}{p}\right) = -1$.

Příklad 17. Pro $n \in \mathbb{N}$ existuje nekonečně mnoho prvočísel p takových, že každý primitivní prvek mod p je větší než n.

Příklad 18. Najdi všechna $n > 1$, pro která existuje právě jedno $0 < a \le n!$ takové, že $n! \mid a^n+1$. (ISL 2005 N4)

Příklad 19. Nechť je $p \ge 5$ prvočíslo. Dokaž, že existuje $1 \le a < p-1$ takové, že ani $a^{p-1}-1$ ani $(a+1)^{p-1}-1$ není násobkem p^2. (ISL 2001 N4)

Příklad 20. Nechť je p liché prvočíslo. Najdi všechny dvojice (A, B) takové, že A, B jsou různé neprázdné podmnožiny $\mathbb{Z}_p^*$ splňující

(i) $A \cup B = \mathbb{Z}_p^*$,
(ii) pokud $a, b \in A$ nebo $a, b \in B$, pak $ab \in A$,
(iii) pokud $a \in A$, $b \in B$, pak $ab \in B$. (Indická MO)

Příklad 21. Dokaž, že existuje nekonečně mnoho přirozených n takových, že n^4+1 má prvočíselného dělitele většího než $2n$. (MKS 30–2–8)

Příklad 22 (Lifting the exponent lemma – LTE). Nechť je p liché prvočíslo a $x, y \in \mathbb{Z}$ tak, že $p \mid x-y$, $p \nmid x, y$. Potom pro $n \in \mathbb{N}$ platí

$$v_p(x^n - y^n) = v_p(x-y) + v_p(n),$$

kde $v_p(a)$ značí p-valuaci, tj. exponent největší mocniny p, jež dělí a.

Příklad 23. Najdi všechna přirozená n taková, že $n \mid 2^n - 1$.

Příklad 24. Najdi všechna přirozená n taková, že $n^2 \mid 3^n + 1$. (TR*i*KS 69)

Příklad 25. Najdi všechna přirozená n taková, že $n^2 \mid 2^n + 1$.

Příklad 26. Dokaž, že pro $n > 1$ nemůže nastat $n \mid 2^{n-1} + 1$.

Příklad 27. Nechť je p prvočíslo, které dává zbytek 3 nebo 5 mod 8. Nechť navíc platí $p = 2q + 1$, kde q je také prvočíslo. Urči

$$\omega^{2^1} + \omega^{2^2} + \cdots + \omega^{2^{p-1}},$$

kde $\omega \in \mathbb{C}$ splňuje $\omega^p = 1$, $\omega \neq 1$.

Příklad 28. Urči počet všech posloupností $\{a_n\}_{n=0}^{\infty}$ reálných čísel takových, že $a_{m \cdot n} = a_m \cdot a_n$ a zároveň $a_n = a_{n+2011}$ pro každá $m, n \in \mathbb{N}$. (MKS 30–6–8)

Příklad 29. Je dáno liché prvočíslo p. Najdi všechna k taková, že

$$p \mid 1^k + 2^k + \cdots + (p-1)^k.$$

(Hungary-Israel Math Competition 2009)

Příklad 30. Pro liché prvočíslo p definujme

$$F(p) = \sum_{k=1}^{\frac{p-1}{2}} k^{120}, \qquad f(p) = \frac{1}{2} - \left\{ \frac{F(p)}{p} \right\},$$

kde $\{x\} = x - \lfloor x \rfloor$. Urči $f(p)$ pro každé p. (China TST 1993)

Příklad 31. Pro $a \in \mathbb{N}_0$ definujme $n_a = 101a - 100 \cdot 2^a$. Pro $0 \le a, b, c, d \le 99$ ukaž

$$n_a + n_b \equiv n_c + n_d \pmod{10100} \Longrightarrow \{a, b\} = \{c, d\}.$$

(Putnam 1994)

Příklad 32. Najdi všechna přirozená $n > 1$, pro která

$$n \mid 1 + \prod_{a \in \mathbb{Z}_n^*} a.$$

Příklad 33. Buď p prvočíslo a $a_1, \ldots, a_n$ po dvou různá přirozená čísla menší než p. Předpokládejme, že $p \mid a_1^k + \cdots + a_n^k$ pro každé $k \in \{1, \ldots, p-2\}$. Urči $\{a_1, \ldots, a_n\}$. (Mathematical Reflections)

Příklad 34. Budiž q liché prvočíslo. Najdi všechna prvočísla p taková, že existuje celé číslo x splňující

$$x^{q-1} + x^{q-2} + \cdots + x + 1 \equiv p^{q-1} \pmod{p^q}.$$

(ELMO SL 2010)

Příklad 35. Budiž $p > 13$ prvočíslo takové, že $p = 2q+1$ pro nějaké prvočíslo q. Urči, kolik existuje uspořádaných dvojic (m, n) celých čísel takových, že $0 \leq m < n < p-1$ a zároveň

$$3^m + (-12)^m \equiv 3^n + (-12)^n \pmod{p}.$$

(ELMO SL 2011)

Příklad 36. Jsou dána celá čísla a, b taková, že pro všechna přirozená n platí $b^n + n \mid a^n + n$. Dokaž, že $a = b$. (ISL 2005 N6)

Příklad 37. Najdi všechny trojice (a, b, c) přirozených čísel takové, že pro každé přirozené n, které nemá žádného prvočíselného dělitele menšího než 2020, platí

$$n + c \mid a^n + b^n + n.$$

(ELMO SL 2014)

Literatura a zdroje

[1] Štěpán Šimsa; *Řády a primitivní prvek*, Sborník *i*KS, 2016

[2] Filip Bialas, Kuba Löwit; *Teorie grup*, PraSečí seriál, 2017/2018

[3] Filip Bialas; *Kvadratická reciprocita*, Zásada 2017

Hinty

Hint 1. Dívej se zvlášť mod p a mod q.
Hint 2. $\mathrm{ord}_q(2) = p$.
Hint 3. Malý Fermat je tvůj kamarád. $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$.
Hint 4. Kolik může být $\log\left(b^{p-1}\right)$?
Hint 5. Kolik může být $\mathrm{ord}_{q^\alpha}(2)$ pro prvočíselnou mocninu q^α, jež dělí n?
Hint 6. $\mathrm{ord}_p(q) \in \{2, 2r\}$. Pro lichá p, q, r vyvoď spor.
Hint 7. Co je nějak spárovat?
Hint 8. Uprav na $a^3 \equiv b^3 \pmod p$.
Hint 9. Řád dělí $p-1$.
Hint 10. Geometrická řada s pomocí primitivního prvku.
Hint 11. Samozřejmě, že existuje. Rostoucnost nás vůbec neomezuje.
Hint 12. Kvadratické zbytky mod 3 a kubické zbytky mod 9.
Hint 13. Eulerovo kritérium a druhý suplement.
Hint 14. Kvadratické zbytky mod a, $2a+1$, $4a+3$.
Hint 15. -1 je 2^s-tá mocnina něčeho, přitom její diskrétní logaritmus je $\frac{p-1}{2}$.
Hint 16. Navol si správné zbytky modulo prvočinitelé čísla a. Čínská zbytkovka a Dirichlet zařídí zbytek.
Hint 17. Navol si správné zbytky modulo $1, \ldots, n$. Čínská zbytkovka a Dirichlet zařídí zbytek.
Hint 18. Řeš zvlášť v jednotlivých modulech p^α – každé řešení mod $n!$ jednoznačně odpovídá posloupnosti řešení v jednotlivých modulech p^α. Pro složené n najdi spor díky $p^2 \mid n!$ pro prvočíslo $p \mid n$.
Hint 19. Vždy $(-a)^{p-1} \equiv a^{p-1}$. Jak jsou rozmístěna řešení $x^{p-1} \equiv 1 \pmod{p^2}$? Musí tvořit podgrupu v $\mathbb{Z}_{p^2}^*$ – najdi spor.
Hint 20. Rozmysli si, že A, B musí být disjunktní. Kam patří primitivní prvek?
Hint 21. Ber prvočíslo $p = 8k+1$.
Hint 22. Za zadaných předpokladů si rozmysli ekvivalence

$$\begin{aligned} x^p \equiv y^p \left(\bmod p^{k+1}\right) &\iff x \equiv y \left(\bmod p^k\right), \\ x^m \equiv y^m \left(\bmod p^k\right) &\iff x \equiv y \left(\bmod p^k\right) \end{aligned}$$

pro $p \nmid m$.
Hint 23. Nechť je p nejmenší prvočinitel n. Najdi spor diskrétním logaritmem (anebo řádem) mod p.
Hint 24. Vyřeš zvlášť $2 \mid n$. Potom stejně jako předchozí příklad.
Hint 25. Bacha, tady už $n = 1$ není jediné řešení. Může se hodit LTE.
Hint 26. Předpokládej zadanou dělitelnost. Rozmysli si, že $2 \nmid n$ a že -1 i 2 jsou kvadratické zbytky modulo každé prvočíslo $p \mid n$. Poté vyvoď spor pomocí prvočísla $p \mid n$, které minimalizuje $v_2(p-1)$.
Hint 27. 2 je primitivní prvek mod p.
Hint 28. Zjevně $a_n \in \{-1, 0, 1\}$. Vezmi primitivní prvek, dořeš nulu.
Hint 29. Vyrob geometrickou řadu s primitivním prvkem.

Hint 30. Rozliš případy podle toho, zda $p-1 \mid 120$. Vyrob geometrickou řadu s primitivním prvkem.
Hint 31. Uvažuj zvlášť mod 100 a mod 101. Využij toho, že 2 je primitivní prvek mod 101.
Hint 32. Pokud existuje primitivní prvek, je to hračka. Pro ostatní najdi spor.
Hint 33. Uvaž polynom $x^{\log a_1} + \cdots + x^{\log a_n}$. Zadání mu dává spoustu kořenů.
Hint 34. Nejdřív si najdi dostatek x takových, že levá strana má p-valuaci $q-1$. Poté dořeš tím, že nějaké z nich je mod p kořenem $x^{q-1} + \cdots + 1$, ale není kořenem $\sum_{j=1}^{q-1} jx^{j-1}$.
Hint 35. $\left(\frac{3}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = -1$, obě -4, -12 jsou primitivní prvky. Uprav s využitím $z = n - m$.
Hint 36. Ukaž, že $a-b$ má hodně prvočíselných dělitelů. Moduly p a $p-1$ jsou pro prvočíslo p nesoudělné!
Hint 37. Ukaž, že $a+b-c$ má hodně prvočíselných dělitelů. Navol si zbytky n v různých modulech dle libosti.

Indukce

Pavel Hudec

Abstrakt. Indukce je téma všudypřítomné v matematické olympiádě, zejména pak v kombinatorice. Na této přednášce si ukážeme několik pokročilejších metod, které se vážou k indukci, a příklady na ně.

Pohled z výšky

Indukce se v olympiádě využívá velmi často. Většinou se jedná pouze o standardní techniku, dokazování nějaké části úlohy nebo něco takového, co není přímo ta úloha. Jsou však i úlohy, v nichž je využití správného typu indukce nejdůležitější částí řešení. Bohužel v takovém případě neznám žádné věty, ale alespoň mohou pomoct následující myšlenky:

- *Kdy je úloha indukční* – Všimněme si, že standardně indukce funguje stylem, že převede úlohu na nějakou menší instanci stejné úlohy. Tedy nutnou podmínkou (ale obecně ne postačující) možnosti řešit úlohu indukcí je podobnost úlohy pro různé volby parametru, podle kterého indukujeme, a vzájemná převoditelnost.
- *Zesílení indukčního předpokladu* – Pokud nejde indukcí dokázat přímo původní tvrzení, musíme na to jít chytřeji. Občas vyjde to, že indukcí se dá dokázat silnější tvrzení. Pozor, v tomto případě musíme znovu v indukčním kroku dokázat to silnější tvrzení, původní tvrzení nestačí.
- *Volba parametru* – Občas funguje indukce na složitější funkci f z množiny stavů do přirozených čísel. To může být třeba stupeň polynomu, počet křížení, počet různobarevných dvojic vzdálených 3 od sebe a spousta dalších. Prvním krokem je dokázat tvrzení pro $f(X) = 1$, indukčním krokem pak dokázat ho pro $f(X) = n$ ze znalosti tvrzení pro všechny stavy s funkční hodnotou menší než n.
- I pokud ta úloha vypadá hodně indukčně, mějte na paměti, že tak vůbec nemusí jít vyřešit. Je potřeba nakonec zkoušet i jiné nápady.

Grafovky

Úloha 1. Dokažte, že souvislý graf, ve kterém mají všechny vrcholy sudý stupeň, lze nakreslit jedním tahem.

Úloha 2. Dokažte, že v úplném orientovaném grafu existuje cesta, která prochází každým vrcholem právě jednou a která vede po směru hran.

Úloha 3. V Americe se nachází n měst, která jsou spojena jednosměrnými leteckými linkami. V každém z těchto měst se nachází pamětihodnost. Cestovní kancelář chce zřídit v některých amerických městech pobočky, aby ke každé pamětihodnosti mohla uspořádat zájezd začínající v některé ze svých poboček za pomoci nejvýše dvou leteckých linek. Zároveň si chce počínat ekonomicky – nechce, aby měla pobočky ve dvou městech spojených leteckou linkou. Dokažte, že to vždy může zařídit.

(PraSe)

Bonus. Vyřešte předchozí úlohu bez použití indukce. Nebo to zkuste bez indukce alespoň pro úplný graf.

Úloha 4. Dokažte, že každý rovinný graf lze obarvit pěti barvami. Můžete využít, že rovinný graf na n vrcholech obsahuje nejvýše $3n-6$ hran.

Úloha 5. V KMS je niekoľko vedúcich a niektoré dvojice sa spolu kamarátia. Namiesto toho, aby si užívali pokojné vianočné sviatky, sa radšej hádajú, či je krajšia fialová alebo modrá farba. Na začiatku si každý vedúci myslí, že krajšia je fialová. Občas sa stane, že jeden vedúci zorganizuje stretnutie, ktorého sa zúčastní on a všetci jeho kamaráti. Po tomto stretnutí sa všetkým zúčastneným vedúcim zmení názor. Je možné bez ohladu na to, ako sa vedúci kamarátia, že po niekolkých stretnutiach si budú všetci vedúci myslieť, že je krajšia modrá? (KMS)

Úloha 6. Mějme n imonů, z nichž každá dvojice může či nemusí být spojená. Můžeme provádět dvě operace:

(i) Zničit imon, který je spojen s lichým počtem imonů.

(ii) Zdvojnásobit počet imonů vytvořením kopie ke každému existujícímu imonu. Dva okopírované imony budou spojeny právě tehdy, byly-li spojené jejich vzory. Dále se každý imon spojí se svou kopií. Žádná další spojení během této operace nevzniknou ani nezaniknou.

Dokažte, že lze docílit stavu, kdy nebudou žádné dva imony spojené.

(IMO shortlist 2013)

Úloha 7. Dokažte, že úplný r-partitní graf G na n vrcholech s rozdílem počtu vrcholů v libovolných dvou partitách nejvýše 1 splňuje následující tvrzení: Libovolný graf H na n vrcholech neobsahující K_{r+1} jako podgraf obsahuje nejvýše tolik hran jako G. (Turánova věta)

Zesílení indukčního předpokladu

Úloha 8. Ukažte, že

$$11 \cdot \binom{80}{40} \cdot 2^{-80} < 1.$$

Úloha 9. Dokažte, že pro každé $n \in \mathbb{N}$ platí

$$\left(1+\frac{1}{1^3}\right)\cdot\left(1+\frac{1}{2^3}\right)\cdots\left(1+\frac{1}{n^3}\right) < \frac{5}{2}.$$

Úloha 10. Nechť G je souvislý graf. Označme G^3 graf, v kterém jsou spojené ty vrcholy, mezi kterými v G existuje cesta délky nejvýše 3. Dokažte, že G má kružnici procházející všemi vrcholy.

Úloha 11. Je dána posloupnost $\{a_n\}_{n=1}^{\infty}$ přirozených čísel splňující $a_1 = 1$ taková, že pro každé přirozené k a n platí

$$a_n \mid a_k + a_{k+1} + \cdots + a_{k+n-1}.$$

V závislosti na n určete největší možnou hodnotu a_{2n}. (ELMO 2018–2)

Úloha 12. Je dána posloupnost celých čísel $a_0, a_1, \ldots$ a posloupnost přirozených čísel $b_0, b_1, \ldots$ taková, že $a_0 = 0$, $a_1 = 1$ a

$$a_{n+1} = \begin{cases} a_n b_n + a_{n-1}, & \text{pokud } b_{n-1} = 1, \\ a_n b_n - a_{n-1}, & \text{pokud } b_{n-1} > 1 \end{cases} \qquad \text{pro } n = 1, 2, \ldots$$

Dokažte, že alespoň jedno z čísel a_{2017} a a_{2018} je větší nebo rovno 2017.
(IMO shortlist 2017)

Tame the cuuube!

Úloha 13. Je dáno $n \in \mathbb{N}$. Dokažte, že z libovolné množiny $2^{n+1} - 1$ přirozených čísel lze vybrat 2^n-prvkovou podmnožinu se součtem dělitelným 2^n.

Úloha 14. Hedvika si myslela svých oblíbených n po dvou různých přirozených čísel. Z nudy pak začala psát na tabuli nejmenší společné násobky a největší společné dělitele všech dvojic jejích oblíbených čísel. Každé číslo napsala nejvýše jednou (protože co by se zvedala). Kolikrát nejméně se musela pro dané n zvednout? (KMS)

Úloha 15. Čaroděj Radek si točil se svými $2^n + 1$ oblíbenými po dvou různými konečnými množinami, které si obarvil na červeno nebo na modro tak, že obě barvy byly použity. Protože to dělal faaakt dlouho, popadávaly mu postupně na zem. Přesněji, každá dvojice červené a modré množiny mu v jeden okamžik spadla na zem, na které zůstal jejich otisk v podobě XORu těchto dvou množin. Protože si Radek potrpí na čistotu, nestrpí na zemi žádné skvrny. Aby mohl skvrny uklidit, může jednou za sekundu pronést složité zaklínadlo, kterým nechá zmizet libovolný počet stejných množin. Ukažte, že Radek se při uklízení faaakt nadře, tedy že mu bude trvat alespoň 2^n sekund. (TR*i*KS)

Úloha 16. Jednoho dne se nejvyšší kravská rada rozhodla svolat nejváženější kraví jazykovědce na kodifikaci kravího jazyka. Ta se dohadovala a dohadovala, až ji musela přerušit nejstarší členka kravské rady mocným zabučením. Jazyková rada se rozhodla vzít její přání na vědomí a zapsala zabučení jako slovo délky n složené z písmen B a U. Jednomyslně se rozhodla, že slovem bude jakýkoliv řetězec, který vznikne smazáním několika písmen ze zápisu zabučení. Nejvyšší radu by zajímalo, kolik nejvíce může nově kodifikovaný jazyk obsahovat slov. Poraďte jí.

Další úlohy

Úloha 17. Dokažte, že pro libovolné k existuje k-ciferné číslo, jehož desítkový zápis je složený z jedniček a dvojek a které je dělitelné 2^k.

Úloha 18. Ukažte, že pro žádný polynom P nemůže být $\{x \in \mathbb{Z} : P(x) \notin \mathbb{Z}\}$ neprázdná konečná.

Úloha 19. Nechť F_m značí m-té Fibonacciho číslo. Buď P polynom stupně 1008 takový, že $P(2n+1) = F_{2n+1}$ pro všechna $n = 0, 1, 2, \ldots, 1008$. Najděte vyjádření $P(2019)$ pomocí rozdílu dvou Fibonacciho čísel. (Putnam 2019)

Úloha 20. Dokažte, že pro každé přirozené číslo n, které není dělitelné třemi, platí, že šachovnici $n \times n$ lze rozřezat na jeden čtverec 1×1 a L-triomina.

Úloha 21. Dokažte pomocí indukce AG nerovnost pro obecnou n-tici nezáporných reálných čísel.

Úloha 22. Nechť k a n jsou přirozená čísla. Dokažte, že existují přirozená čísla $m_1, m_2, \ldots, m_k$ taková, že

$$1 + \frac{2^k - 1}{n} = \left(1 + \frac{1}{m_1}\right) \cdots \left(1 + \frac{1}{m_k}\right).$$

(IMO 2013–1)

Úloha 23. Mirkovi a Mateji se líbí velká čísla. Na výpravě za poznáním TREE(3) narazili na zlého černokněžníka. Černokněžník si na ně připravil tabulku $n \times m$, kterou vyplnil po dvou různými reálnými čísly. Mirek se dívá na řádky a líbí se mu z každého řádku r největších čísel. Podobně se Mateji líbí s největších čísel z každého sloupce. Mirek s Matejem přemůžou černokněžníka, pokud se jim společně líbí alespoň rs čísel z tabulky. Dokažte, že černokněžníka porazí a odhalí tajemství TREE(3).

Úloha 24. Je dáno celé číslo $N \geq 2$. V řadě stojí $N(N+1)$ navzájem různě vysokých fotbalistů. Trenér Vrba chce vyřadit některých $N(N-1)$ z nich tak, aby nová řada sestávající ze zbylých $2N$ fotbalistů splňovala následujících N podmínek:

(1) Nikdo nestojí mezi dvěma nejvyššími fotbalisty.
(2) Nikdo nestojí mezi třetím a čtvrtým nejvyšším fotbalistou.
$\vdots$
(N) Nikdo nestojí mezi dvěma nejnižšími fotbalisty.

Dokažte, že je to vždy možné. (IMO 2017–5)

Úloha 25. Je dána posloupnost $\{a_n\}_{n=1}^{\infty}$ přirozených čísel taková, že $a_1 = 1$ a pro všechna přirozená n větší než 1 je a_n nejmenší přirozené číslo, které je různé od všech předchozích prvků posloupnosti a které je nesoudělné s jejich součtem. Dokažte, že tato posloupnost obsahuje všechna přirozená čísla. (PraSe)

Úloha 26. Rado a kaktus hrají logickou hru s pravidelným $(2n+1)$-úhelníkem, kde $n > 1$ je přirozené číslo. Hrají střídavě, přičemž Rado začíná a každý z nich ve svém tahu začerní jeden dosud nezačerněný vrchol. Vyhraje ten, po jehož tahu na papíře nezbude žádný ostroúhlý trojúhelník s vrcholy v nezačerněných vrcholech původního $(2n+1)$-úhelníku. V závislosti na n určete, kdo má vyhrávající strategii. (PraSe)

Úloha 27. Banka města Bath vydává mince, na jejichž jedné straně je vyraženo písmeno H a na té druhé pak písmeno T. Pepa si n takových mincí postavil do řady zleva doprava a opakoval následující operaci: Ukazuje-li alespoň jedna mince H, pak Pepa obrátí k-tou minci zleva, kde k je počet mincí ukazujících H. Ukazují-li všechny mince písmeno T, posloupnost operací končí. Například pro $n = 3$ a počáteční konfiguraci THT by Pepa postupně získal $THT \to HHT \to HTT \to TTT$ a po těchto třech operacích by skončil.

(a) Ukažte, že pro libovolnou počáteční konfiguraci je Pepa nucen skončit po konečném počtu kroků.
(b) Pro každou počáteční konfiguraci C označíme $L(C)$ počet operací, které Pepa provede, než je nucen skončit. Například $L(THT) = 3$ a $L(TTT) = 0$. Pokud spočítáme hodnotu $L(C)$ pro každou z 2^n počátečních konfigurací, jaký bude aritmetický průměr všech spočítaných hodnot? (IMO 2019–5)

Literatura a zdroje

[1] Thomas Swayze; *Induction*, MOP 2018,
[2] Sasha Rudenko; *Tame the cube*, MOP 2018

Hinty

Hint 1. Dokazujte indukcí podle počtu hran. Najděte v grafu cyklus.

Hint 3. Vyberte si jedno město a najděte řešení pro zbytek. Co vám brání, aby se to řešení dalo rozšířit?

Hint 4. V každém rovinném grafu existuje vrchol stupně nejvýše 5.

Hint 5. Ano! Zvolte si vhodné podmnožiny množiny vedoucích, pro které z indukčního předpokladu tvrzení platí. Zatněte zuby a dodělejte to.

Hint 6. Nejsou barevné grafy mnohem hezčí? Zase to ale nesmíme přehánět, proto po obarvení počet barev budeme snižovat.

Hint 7. Indukujte podle r. V libovolném grafu neobsahujícím K_{r+1} najděte vrchol s největším stupněm. Použijte indukční předpoklad a sestrojte r-partitní graf o více hranách.

Hint 8. Označte $40 = n$ a vyjádřete 11 jako „hezkou" funkci n. Potom zindukujte podle n. Jako první krok vám dobře poslouží $n = 8$.

Hint 9. Posloupnost částečných součinů je rostoucí. Jak se dá taková posloupnost omezit, aby mohla indukce fungovat?

Hint 10. Stačí dokázat pro stromy. Dokažte, že dokonce může kružnice procházet každou hranou G.

Hint 11. Triviální odhad není dost dobrý. Ale nezahazujte ho, dá se snadno vylepšit. Upravujte vylepšený odhad a rozmyslete si, jak se tam dá potom použít indukce. Když to uděláte dobře, vypadne vám konstrukce jako případ rovnosti v tom odhadu. Případně se dá také na konstrukci přijít pomocí malých případů a zkoušet odhadovat, aby u ní nastala rovnost.

Hint 12. Drsňáci nepotřebují hinty. Drsňáci úlohu prostě vyřeší.

Hint 13. Indukujte podle n. Prvků je tam dost, aby to vyšlo.

Hint 14. Vyjde to n. Pro důkaz optimality rozdělte čísla na dvě menší množiny, které produkují navzájem různé společné násobky a dělitele.

Hint 15. Že jsou různé se dá udělat tak, že tam jeden prvek buď je, nebo není. Podívejte se na ten jeden prvek a uvažte množiny, které ho obsahují a které ho neobsahují.

Hint 16. Najděte optimální konstrukci a heuristický argument, proč je optimální.

Hint 18. Uvažte $Q(x) = P(x + 1) - P(x)$.

Hint 19. Jaké jsou hodnoty $Q(x) = P(x + 2) - P(x)$?

Hint 20. Jak se v této úloze dá indukovat? O něco silnější tvrzení už pak zindukujete.

Hint 21. Indukovat podle n přímo nejde. Jak se tedy dá dostat k velkým n? Pro zbývající n lze pak vždy snížit počet čísel o 1 šikovnou volbou posledního z nich.

Hint 22. Indukujte podle k a rozdělte úlohu na případy podle parity n.

Hint 23. Kdo tohle vyřeší, dostane koalu (pokud zbudou).

Hint 24. Ke které přednášce patří tahle úloha?

Hint 25. Pro prvočísla je to snadné. Postupně indukcí rozšiřujte dál, až obsáhnete všechna přirozená čísla.

Hint 26. Rado je opravdu marňák. Zkuste po dvojici tahů Rada a kaktusu najít menší instanci úlohy.

Hint 27. Uvažujte stavy $n+1$ mincí takové, že první mince ukazuje H. Ukažte, že cesty z nich do stavu $HH\dots H$ odpovídají po nějaké transformaci cestám ze stavů s n mincemi do stavu $TT\dots T$. Vyřešte rekurenci a vyjde $\frac{n(n+1)}{4}$.

Nullstellensatz

Jakub Löwit

Abstrakt. Na přednášce se budeme zabývat takzvanými *větami o nulách*, které dávají do souvislosti množiny polynomů a množiny jejich společných řešení. Nejzajímavější pro nás bude takzvaná *Combinatorial Nullstellensatz*, s jejíž pomocí hravě zvítězíme nad mnoha netriviálními kombinatorickými úlohami.

Věty o nulách

Definice. *Těleso* je množina K obsahující přinejmenším dva význačné prvky 0 a 1, společně s binárními operacemi „plus“ a „krát“, které splňují vcelku intuitivní axiomy (obě operace jsou asociativní a komutativní; přičítání nuly nic nemění; násobení jedničkou nic nemění; násobení je distributivní vůči sčítání; pro každý prvek a existuje prvek $-a$, který se s ním sečte na 0; pro každý nenulový prvek b existuje prvek b^{-1}, který se s ním vynásobí na 1).

Ačkoli různých těles existuje spousta, my bude pracovat jenom s několika dobře známými[*),†)]:

- $\mathbb{C}$ – komplexní čísla
- $\mathbb{R}$ – reálná čísla
- $\mathbb{Q}$ – racionální čísla
- $\mathbb{Z}_p$ – zbytky modulo **prvočíslo** p

Značení.

- Pro dané těleso K můžeme uvažovat *polynomy s koeficienty v K*. Množinu všech takových polynomů značíme $K[x_1, \ldots, x_n]$.
- Dostaneme-li n-tici čísel $(s_1, \ldots, s_n) \in K^n$ a polynom $f \in K[x_1, \ldots, x_n]$, můžeme do něj naše čísla dosadit, čímž dostaneme číslo $f(s_1, \ldots, s_n) \in K$.
- Pro libovolnou množinu polynomů $F \subseteq K[x_1, \ldots, x_n]$ tak dostáváme množinu jejich společných nul $V(F)$, tj. množinu všech n-tic $(s_1, \ldots s_n)$, které pro každý polynom $f \in F$ splňují $f(s_1, \ldots, s_n) = 0$.
- Naopak pro libovolnou množinu $S \subseteq K^n$ takových n-tic můžeme uvažovat množinu $I(S)$ všech polynomů, které se na ní nulují.

Cvičení. Zamyslete se, jak se „hledání společných nul“ a „hledání nulujících se polynomů“ chová pro polynomy v jedné proměnné nad $\mathbb{C}$.

[*)] Takže pokud o tělesech nic nevíš, vůbec to nevadí a můžeš si místo obecného K po celou dobu představovat třeba reálná čísla $\mathbb{R}$. Pro jiná tělesa než $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ větu stejně používat nebudeme.

[†)] Naproti tomu $\mathbb{N}$, $\mathbb{Z}$ či $\mathbb{Z}_m$ pro složené číslo m tělesa nejsou – všem totiž chybí multiplikativní inverzy k některým nenulovým prvkům.

Obecně bychom rádi pochopili, jak spolu množiny polynomů a množiny jejich společných nul souvisí. Pro polynomy v jedné proměnné je situace vcelku přehledná – a přinejmenším jsme se už všichni s takovými příklady mnohokrát setkali. Naopak pro více proměnných se problém velmi rychle komplikuje. Přesto se v něm ale často dá najít jakýsi systém. A taková tvrzení se pak typicky nazývají *věty o nulách*.

No a proč nás zajímají? Důležitost souvislosti množin polynomů s jejich společnými nulami v rámci algebry je vcelku očividná. My si ale budeme chtít ilustrovat především důsledky pro řešení kombinatorických a teoriečíselných úloh. Pokud se nám takovou úlohu povede převést čistě do řeči polynomů a jejich hodnot, najednou se nám otevře silný a přehledný algebraický aparát, který můžeme použít. Ačkoli v této přednášce je náš arzenál představován „pouze“ jednou větou (avizovanou *Combinatorial Nullstellensatz*), tento přístup funguje obecněji. Čím větší znalost polynomů získáme, tím lépe budeme umět „převádět úlohy do algebry“.

Combinatorial Nullstellensatz

Zformulujme a dokažme tedy slíbenou větu, se kterou přišel v roce 1999 původem izraelský matematik Noga Alon. Sama o sobě tato věta není bůhvíjak „překvapivá“, ale je nehorázně užitečná právě při převádění kombinatorických problémů do algebry.

Pozorování.

- Buď K těleso, $f \in K[x]$ polynom s k různými kořeny $s_1, \dots, s_k \in K$. Potom $f = h \cdot (x - s_1) \cdots (x - s_k)$ pro nějaký polynom $h \in K[x]$.
- Buď K těleso, $f \in K[x]$ nenulový polynom stupně d. Pak f má nejvýš d kořenů.

Důkaz. Má-li f kořen v $r \in K$, zkusme jej vydělit (se zbytkem) polynomem $(x - r)$, čímž dostaneme vyjádření $f = h \cdot (x - r) + c$ pro nějaké $h \in K[x]$ nižšího stupně a konstantu $c \in K$. Jenže $f(r) = 0$ z předpokladu, takže $c = 0$, pročež $f = h \cdot (x - r)$. Induktivně (dokud má h nějaký kořen) proto můžeme pokračovat a získat

$$f = h \cdot (x - r_1) \cdots (x - r_j),$$

kde $h \in K[x]$ je polynom bez kořene. Tedy $r_1, \dots, r_j$ jsou všechny kořeny f (i s násobnostmi).

V první části jsou nyní všechna $s_1, \dots, s_k$ obsažena mezi $r_1, \dots, r_j$, což dává hledaný tvar, tj. f je skutečně (polynomiálním) násobkem $(x - s_1) \cdots (x - s_k)$. V druhé části dostáváme díky $f \neq 0$ nerovnost stupňů $k \leq j \leq d$, čímž jsme hotovi. ∎

Lemma (Rozklad na součet). Mějme těleso K a několik jeho konečných podmnožin $S_1, \dots, S_n$. Dále mějme polynom $f \in K[x_1, \dots, x_n]$, který se nuluje na celé množině $S_1 \times \cdots \times S_n$. Pro $i = 1, \dots, n$ označme $g_i = \prod_{j \in S_i} (x_i - s_j)$. Pak existují polynomy $h_1, \dots, h_n \in K[x_1, \dots, x_n]$ takové, že

$$f = h_1 g_1 + \cdots + h_n g_n.$$

Ty lze navíc zvolit tak, aby $\deg h_i + \deg g_i \leq \deg f$ pro všechna $i = 1, \dots, n$.

Poznámka. Rovnost z lemmatu lze vyjádřit slovy jako „f je lineární kombinace polynomů $g_1, \ldots, g_n$ s koeficienty v $K[x_1, \ldots, x_n]$“.

Poznámka. Všimněte si, že v případě $n = 1$ se lemma skutečně degeneruje na první část předchozího pozorování.

Důkaz. Nejprve zpozorujme, že postupným odečítáním polynomů tvaru $h_i' g_i$ jako ve znění lemmatu můžeme převést f na polynom f', ve kterém se každé x_i objevuje pouze v mocninách $0, 1, \ldots, |S_i| - 1$. Vskutku, g_i je polynom v proměnné x_i tvaru

$$x_i^{|S_i|} + \sum_{j=0}^{|S_i|-1} c_j x_i^j$$

pro nějaké konstanty c_j. Pokud se tedy v f vyskytuje člen obsahující $x_i^{|S_i|}$, odečtením vhodného polynomu tvaru $h_i' g_i$ ho umíme nahradit součtem $h_i' c_i x_i^j$ pro $j = 0, \ldots, |S_i| - 1$ (kde h_i' splňuje podmínku se stupni). Opakováním tohoto odečítání se tak skutečně zbavíme všech x_i s exponenty $\geq |S_i|$.

Takto upravený f' se stále nuluje na celém $S_1 \times \cdots \times S_n$. Tvrdíme, že $f' = 0$. To snadno ověříme indukcí na n, přičemž případ $n = 1$ plyne z předchozího pozorování. Pro $n \geq 2$ rozepišme f' jako součet členů podle exponentu u x_n, tj.

$$f' = \sum_{j=0}^{|S_n|-1} f_j' x_n^j,$$

kde $f_j' \in K[x_1, \ldots, x_{n-1}]$ jsou polynomy ve zbylých proměnných. Pokud se některý z f_j' nenuluje na některém $(s_1, \ldots, s_{n-1}) \in K^{n-1}$, částečným dosazením získáme nenulový polynom jedné proměnné $f'(s_1, \ldots, s_{n-1}, x_n)$ stupně nejvýše $|S_n| - 1$, který se nuluje na celém $|S_n|$, což je spor s předchozím pozorováním. Tedy všechny f_j se nulují na celém $S_1 \times \cdots \times S_{n-1}$, z indukčního předpokladu se tedy jedná o nulové polynomy, pročež také $f' = 0$.

Tím jsme hotovi: z konstrukce f' je jasné, že $f = f' + h_1 g_1 + \cdots + h_n g_n$ pro polynomy h_i, g_i jako ve znění lemmatu, ale zároveň jsme ukázali $f' = 0$. ∎

Nyní můžeme zajásat, protože naše napjatě očekávaná věta je pouze elegantním důsledkem předchozího explicitního lemmatu.

Věta (Combinatorial Nullstellensatz). Mějme těleso K, několik jeho konečných podmnožin $S_1, \ldots, S_n$, a polynom $f \in K[x_1, \ldots, x_n]$. Předpokládejme, že platí $\deg f = t_1 + \cdots + t_n$ pro $t_1, \ldots, t_n \in \mathbb{N}_0$ splňující

(i) $t_i < |S_i|$ pro všechna $i = 1, \ldots, n$,
(ii) koeficient u $x_1^{t_1} \cdots x_n^{t_n}$ v polynomu f je nenulový.

Potom existují $s_i \in S_i$ pro $i = 1, \ldots, n$ taková, že $f(s_1, \ldots, s_n) \neq 0$.

Poznámka. Všimněte si, že v případě $n = 1$ věta říká: Je-li $S \subseteq K$ konečná podmnožina a $f \in K[x]$ polynom stupně $\deg f = t < |S|$, pak existuje $s \in S$ splňující $f(s) \neq 0$.

Důkaz. Věta je důsledkem předchozího lemmatu – kdyby se f nuloval na celé množině $S_1 \times \cdots \times S_n$, mohli bychom jej přepsat jako

$$f = \sum_{i=1}^{n} h_i g_i,$$

kde $g_i = \prod_{j \in S_i} (x_i - s_j)$ a zároveň $\deg h_i + \deg g_i \leq \deg f$ pro všechna $i = 1, \ldots, n$. Součet členů maximálního stupně v f proto tvaru

$$\sum_{i=1}^{n} h_i' \cdot x_i^{|S_i|},$$

kde h_i' značí součet členů maximálního stupně v h_i. Má-li tedy nějaký člen polynomu f maximálního stupně nenulový koeficient, musí obsahovat některé x_i v mocnině $\geq |S_i|$. Jenže díky bodu (i) máme pro všechna i nerovnost $|S_i| > t_i$, takže člen (maximálního stupně) $x_1^{t_1} x_2^{t_2} \cdots x_n^{t_n}$ musí mít nulový koeficient, což je ve sporu s bodem (ii). Polynom f se tedy na celé množině $S_1 \times \cdots \times S_n$ nulovat nesmí. ■

Úlohy

Konečně nadchází čas si použití naší teorie pořádně procvičit. Při tom uvidíme důsledky *Combinatorial Nullstellensatz* zasahující do kombinatoriky a teorie grafů, kombinatorické geometrie, algebry, i teorie čísel.

Ačkoli následující úlohy nezřídka mají i pěkná elementární řešení, často je velmi neelementární na ně přijít. *Combinatorial Nullstellensatz* je skutečně silná, takže se není třeba divit, že ji často opravdu stačí přímočaře použít, a občas tak získat i obecnější výsledek. K její aplikaci nám stačí chytře zvolený polynom, jehož stupeň a vhodný „vedoucí koeficient“ máme pod kontrolou.

Úloha 1. V každém vrcholu pravidelného 100-úhelníku jsou napsaná dvě přirozené čísla. Ukažte, že lze z každého vrcholu smazat jedno číslo tak, aby v žádných dvou sousedních vrcholech nezbyla stejná čísla. (ARO 2007)

Úloha 2. Pro přirozené číslo n označme

$$S = \{(x, y, z) \mid x, y, z \in \{0, 1, \ldots, n\}, (x, y, z) \neq (0, 0, 0)\}.$$

Určete nejmenší přirozené číslo m, pro které může být S pokryta m rovinami, které neprochází počátkem. (IMO 2007, 6)

Úloha 3. Mějme prvočíslo p a dvě množiny A, B některých zbytků modulo p. Označme $A + B$ množinu těch zbytků, které lze získat jako $a + b$ pro $a \in A$, $b \in B$. Dokažte nerovnost $|A + B| \geq \min\{p, |A| + |B| - 1\}$. (Cauchy-Davenport)

Úloha$^\natural$ 4. Mějme prvočíslo p a polynomy $f_1, \dots, f_m \in \mathbb{Z}_p[x_1, \dots, x_n]$ splňující

$$\sum_{i=1}^{m} \deg f_i < n.$$

Ukažte, že pokud má soustava $f_1 = \dots = f_m = 0$ řešení nad $\mathbb{Z}_p$, pak má nějaké další řešení nad $\mathbb{Z}_p$. (Chevalley-Warning)

Úloha 5. Nadroviny $H_1, \dots, H_m$ v $\mathbb{R}^n$ pokrývají všechny vrcholy jednotkové hyperkrychle $\{0, 1\}^n$ kromě jednoho. Dokažte $m \geq n$.

Úloha$^\natural$ 6. Mějme prvočíslo p a graf$^{*)}$ G, jehož vrcholy mají stupeň nejvýše $2p-1$ a průměrný stupeň ostře větší než $2p-2$. Dokažte, že z G můžeme smazáním některých hran a vrcholů vyrobit neprázdný graf G', ve kterém má každý vrchol stupeň p.

Úloha 7. Buď p prvočíslo a A podmnožina $\mathbb{Z}_p$. Ukažte nerovnost

$$\big|\{x + y \mid x, y \in A, x \neq y\}\big| \geq \min\{p, 2|A| - 3\}.$$

Úloha 8. Buď p prvočíslo a d přirozené číslo. Dokažte, že pro libovolné celé číslo k existují celá čísla $x_1, \dots, x_d$ splňující $x_1^d + \dots + x_d^d \equiv k \pmod{p}$.

Úloha$^\natural$ 9. Buď p prvočíslo a A množina přirozených čísel splňující, že

(i) prvky množiny A mají dohromady $p-1$ prvočíselných dělitelů,
(ii) součin prvků jakékoli neprázdné podmnožiny $X \subseteq A$ není roven p-té mocnině přirozeného čísla.

Kolik nejvýše prvků může obsahovat množina A? (IMO Shortlist 2003)

Úloha 10. Mějme prvočíslo p a množiny $S_1, \dots, S_k$ zbytků modulo p, jež všechny obsahují 0. Předpokládejme $\sum_{i=1}^{k}(|S_i|-1) \geq p$. Ukažte, že pro libovolná $a_1, \dots, a_k \in \mathbb{Z}_p$ má rovnice $a_1x_1 + \dots + a_kx_k = 0$ nenulové řešení $(x_1, \dots, x_n) \in S_1 \times \dots \times S_k$.

Úloha 11. Mějme množiny $S_1, \dots, S_n$ zbytků modulo prvočíslo p, dále mějme polynomy $f_1, \dots, f_k \in \mathbb{Z}_p[x_1, \dots, x_n]$ splňující

$$(p-1)\sum_{i=1}^{k} \deg f_i < \sum_{j=1}^{n}(|S_i| - 1).$$

Ukažte, že pokud má rovnice $f_1 = \dots = f_k = 0$ řešení z $S_1 \times \dots \times S_n$, pak má další takové řešení.

Úloha$^\natural$ 12. Mějme prvočíslo p, přirozené číslo n a vektory $x_1, \dots, x_{(p-1)n+1}$ nad $\mathbb{Z}_p$. Dokažte existenci neprázdné podmnožiny $I \subseteq \{1, \dots, (p-1)n + 1\}$ splňující $\sum_{i \in I} x_i = 0$.

$^{*)}$ V grafu G dokonce můžeme povolit existenci násobných hran.

Úloha 13. Buď $G = (V, E)$ graf. Pro každý vrchol $v \in V$ máme množinu *zakázaných stupňů* $B(v)$. Dokažte:

(i) Pokud $B(v)$ obsahuje pouze kladná čísla a zároveň $\sum_{v \in V} |B(v)| < |E|$, pak lze smazáním některých hran získat podgraf H (s alespoň jednou hranou), jehož všechny vrcholy mají povolené stupně.

(ii) Pokud $B(v)$ může obsahovat i nulu a pro všechny $v \in V$ platí $|B(v)| \leq \frac{1}{2} \deg v$, tak lze smazáním některých hran získat podgraf H (klidně bez hran), jehož všechny vrcholy mají povolené stupně.

Úloha$^\natural$ 14. Buď n přirozené číslo. Ukažte, že z každých $2n - 1$ celých čísel lze vybrat n, jejichž součet je dělitelný n.

Úloha 15. Buď p prvočíslo, d přirozené číslo a $G = (V, E)$ graf s $|V| > d(p-1)$ vrcholy. Ukažte, že potom existuje neprázdná podmnožina vrcholů U taková, že počet klik na d vrcholech *protínajících* U je kongruentní 0 modulo p.

Úloha 16. Buď p prvočíslo a d přirozené číslo. Kolik nejméně prvků musí mít podmnožina $Y \subseteq \mathbb{Z}_p^d$, která protíná každou nadrovinu? (Brouwer-Schrijver)

Úloha 17. Buď $G = (V, E)$ **bipartitní** graf. Pro každý vrchol $v \in V$ máme dánu množinu *povolených barev* $L(v)$. Rádi bychom obarvili každý vrchol v některou barvou z $L(v)$ tak, aby sousedící vrcholy dostaly různé barvy. Předpokládejme, že hrany G lze orientovat tak, aby každý vrchol v měl vstupní stupeň $\deg_{\text{in}}(v) < |L(v)|$. Dokažte, že G lze korektně obarvit.

Úloha 18. Buď p prvočíslo, $k \leq p - 1$, a $a_1, \ldots, a_k \in \mathbb{Z}_p$ ne nutně různé zbytky. Dokažte, že pro jakékoli po dvou různé zbytky $b_1, \ldots, b_k \in \mathbb{Z}_p$ existuje permutace σ taková, že $a_1 + b_{\sigma(1)}, \ldots, a_k + b_{\sigma(k)}$ jsou také po dvou různé.

Úloha 19. Je dáno **sudé** přirozené číslo n. Mějme přirozené číslo k a vektory $v_1, \ldots, v_k \in \{\pm 1\}^n$ takové, že každý vektor $v \in \{\pm 1\}^n$ je kolmý na některý z nich. Ukažte, že nejmenší možná hodnota k je právě n.

Chevalley-Warning Theorem

Zdůrazněme nyní jednu z předchozích úloh, jejíž řešení dalo v minulém století pár matematikům celkem zabrat.

Věta (Chevalley-Warning). Mějme prvočíslo p spolu s polynomy $f_1, \ldots, f_m \in \mathbb{Z}_p[x_1, \ldots, x_n]$ splňujícími

$$\sum_{i=1}^{m} \deg f_i < n.$$

Pokud má soustava $f_1 = \cdots = f_m = 0$ nějaké řešení v $\mathbb{Z}_p^n$, pak má ještě další takové řešení. Přesněji, počet řešení této soustavy nad $\mathbb{Z}_p^n$ je násobkem p.

My většinu *Chevalley-Warningovy věty* dokázali jako důsledek *Nullstellensatz*. Mírně obecnější verze zmíněná výše ale z *Nullstellensatz* přímo nevyplývá. Přesto její důkaz není nijak přehnaně komplikovaný – jen celkem trikový.

Důkaz. Označíme-li $h = \prod_{i=1}^{m}(1 - f_i^{p-1})$, počet řešení soustavy $f_1 = \cdots = f_m = 0$ lze díky Malé Fermatově větě vyjádřit jako

$$\sum_{(a_1,\ldots,a_n)\in\mathbb{Z}_p^n} h(a_1,\ldots,a_n) = \sum_{(a_1,\ldots,a_n)\in\mathbb{Z}_p^n} \prod_{i=1}^{m} \left(1 - f_i(a_1,\ldots,a_n)^{p-1}\right).$$

Každý člen $x_1^{t_1}\cdots x_n^{t_n}$ polynomu h do výsledné sumy přispívá hodnotou

$$\sum_{(a_1,\ldots,a_n)\in\mathbb{Z}_p^n} x_1^{t_1}\cdots x_n^{t_n} = \prod_{i=1}^{n}\sum_{a\in\mathbb{Z}_p} a^{t_i}.$$

Ukážeme, že ve skutečnosti každý takový člen přispívá nulou. Z podmínky ze zadání je $\deg h < n(p-1)$, takže každý člen $x_1^{t_1}\cdots x_n^{t_n}$ polynomu h obsahuje některé x_j pouze v mocnině $0 \le t_j \le p-2$. Potom ale modulo p (například z existence primitivního prvku) platí

$$\sum_{a\in\mathbb{Z}_p} a^{t_i} = 0.$$

Dle předchozí rovnosti tedy každý člen h do sumy přispívá nulou, čímž jsme hotovi. ■

Chevalley-Warningova věta je sama o sobě velmi praktickým nástrojem – a oproti *Combinatorial Nullstellensatz* je na první pohled trochu přehlednější. Ve skutečnosti už jsme mnohé její aplikace viděli – například úlohy z předešlé sekce označené symbolem ♮ (a určitě i lecjaké další) se dají alternativně přímočaře nahlédnout z naší „slabší verze“ *Chevalley-Warningovy věty.* Ukažme si nyní úlohu, ve které tuto větu použijeme v plné síle.

Úloha 20. Buď p prvočíslo a $a_1,\ldots,a_{2p-1}$ zbytky modulo p. Buď b libovolný zbytek modulo p. Nahlédněte, že počet p-prvkových podmnožin $I \subset \{1,\ldots 2p-1\}$, součet jejichž prvků je kongruentní číslu b modulo p, je kongruentní 0 nebo 1 modulo p.

Hilbert's Nullstellensatz

Pro dodání jistého kontextu na závěr uveďme jinou (mnohem slavnější) nullstellensatz – tu Hilbertovu, která byla zformulována přibližně o sto let dřív. Ačkoli spolu obě věty souvisí, ani jedna není přímým důsledkem druhé. *Hilbertova Nullstellensatz* sice popisuje „množiny nulujících se polynomů“ pro libovolné $S \subseteq K^n$ (tj. ne nutně hyperkrychli), ale na druhou stranu funguje pouze nad extra pěknými tělesy K (těmi algebraicky uzavřenými).

Definice. Těleso K se nazývá algebraicky uzavřené, má-li každý nekonstantní polynom v jedná proměnné $f \in K[x]$ nějaký kořen.

Věta (Základní věta algebry*)). Komplexní čísla $\mathbb{C}$ jsou algebraicky uzavřená.

*) „…která není ani základní, ani algebry“, jak říká známá anekdota.

Cvičení. Rozmyslete si, že tělesa $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_p$ pro prvočíslo p **nejsou** algebraicky uzavřená .

Z našich známých příkladů je tedy algebraicky uzavřené pouze $\mathbb{C}$. Ačkoli je tento fakt obecně známý, důkaz vyžaduje netriviální práci.

Věta (Hilbert's Nullstellensatz). Buď K algebraicky uzavřené těleso, $G \subseteq K[x_1, \ldots, x_n]$ množina polynomů. Označme $V(G) \subseteq K^n$ množinu jejich společných nul. Pro libovolný polynom $f \in K[x_1, \ldots, x_n]$ je potom ekvivalentní:

(i) f se nuluje na celé množině $V(G)$,).
(ii) Existují $m, k \in \mathbb{N}$, pro které se dá f^m zapsat jako $f^m = f_1 g_1 + \cdots + f_k g_k$ pro vhodné $f_1, \ldots, f_k \in K[x_1, \ldots, x_n]$ a $g_1, \ldots, g_n \in G$.

Cvičení. Všimněte si, že z předchozí věty třeba vyplývá:
Jsou-li $g_1, \ldots, g_k \in \mathbb{C}[x_1, \ldots, x_n]$ takové komplexní polynomy, že soustava rovnic $g_1 = \cdots = g_k = 0$ nemá řešení v $\mathbb{C}$, tak už nutně existují polynomy $h_1, \ldots, h_k \in \mathbb{C}[x_1, \ldots, x_n]$ splňující

$$h_1 g_1 + \cdots + h_n g_n = 1.$$

Literatura a zdroje

Úlohy z příspěvku jsou poměrně standardní a provařené (a upřímně je celkem těžké najít víc „olympiádních“ použití této metody). Většina příspěvku je převzatá z přehledné kapitolky v [1]. Pro další aplikace se dá podívat na původní článek [2]. Pro širší algebraický kontext lze použít článek [3].

[1] Titu Andreescu, Gabriel Dospinescu; *Problems from the Book*, XYZ Press
[2] Noga Alon; *Combinatorial Nullstellensatz*, 1999
[3] Terence Tao; *Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory*, 2014
[4] Evan Chen; *Combinatorial Nullstellensatz*, Berkley Math Circle, 2013
[5] Robert Šámal; *Kombinatorika a grafy III*, přednáška, 2018
[6] Štěpán Šimsa; *Combinatorial Nullstellensatz*, Sborník *i*KS, 2013

Hinty

Hint 1. Použijte Nullstellensatz na polynom $\prod_{i=1}^{100}(x_i - x_{i+1}) \in \mathbb{Q}[x_1, \dots, x_{100}]$, kde do každého S_i dosazujeme dvě různá čísla. Využijte sudost čísla 100.

Hint 2. Vyjde $m = 3n$. Kdyby $m < 3n$, vynásobte lineární rovnice všech příslušných rovin a nakonec odečtěte vhodný skalární násobek $\prod_{j=1}^{n}(x-j) \cdot \prod_{j=1}^{n}(y-j) \cdot \prod_{j=1}^{n}(z-j)$.

Hint 3. Kdyby platila opačná nerovnost, vezměte polynom $\prod_{c \in A+B}(x+y-c)$, který se nuluje na $A \times B$.

Hint 4. Při vybírání polynomu použijte Malý Fermatův fígl – pro všechna $x \in \mathbb{Z}_p$ platí: $x = 0$, právě když $\left(x^{p-1} - 1\right) \neq 0$. Použijte fígl, vynásobte všech m věcí dohromady, nakonec opravte triviální nenulu přičtením vhodného polynomu vyššího stupně $(p-1)n$.

Hint 5. Kdyby $m < n$, vynásobte rovnice rovin dohromady a přičtením polynomu stupně n opravte zbylou nenulu.

Hint 6. Každé hraně e přiřaďte jednu proměnnou x_e, do které budeme chtít dosazovat $\{0, 1\}$; pro každý vrchol pak s pomocí Malého Fermata napište jednu rovnici. Všimněte si nulového (ne)řešení.

Hint 7. Vynásobte $(x + y - c)$ přes všechna c jako na levé straně nerovnosti. Kde všude se nuluje polynom $(x - y)$? Buďte opatrní při ověřování předpokladů Nullstellensatz.

Hint 8. S pomocí řádů búno mějmte $d \mid p-1$. Polynom $\left(x_1^d + \cdots + x_d^d - k\right)^{p-1} - 1$ společně s Malým Fermatovým fíglem pak postačí.

Hint 9. Vyjde $(p-1)^2$, konstrukce je jasná. Čísla z A odpovídají vektorům délky $p - 1$. Kdyby $|A| \geq (p-1)^2 + 1$, uvažte $|A|$ proměnných s hodnotami v $\{0, 1\}$. Napište s Malým Fermatem pro každé z daných prvočísel rovnici stupně $p - 1$, jejichž součin se nuluje právě když platí druhá podmínka. Přičtením vhodného polynomu stupně $|A|$ opravte triviální nenulu.

Ve skutečnosti lze zapomenout na první podmínku a číslo $p-1$ nahradit obecným d. Stejný postup pak dává výsledek $d(p-1)$.

Hint 10. Vezměte $(a_1x_1 + \cdots + a_kx_k)^{p-1} - 1$ a odečtěte polynom stupně $\sum_{i=1}^{k}(|S_i| - 1)$ tak, aby se výsledek nuloval na celém $S_1 \times \cdots \times S_k$.

Hint 11. Kdyby to tak nebylo, vezměte polynom $\prod_{i=1}^{k}(1 - f_i^{p-1})$ a opravte jeho jediné neřešení odečtením vhodného polynomu stupně $\sum_{j=1}^{n}(|S_i| - 1)$.

Hint 12. Kdyby to tak nebylo, v každé z n složek s pomocí Malého Fermata napište jednu rovnici, vynásobte, pak přičtením opravte triviální nenulu.

Hint 13.

(i) Pro každou hranu e vezměte jednu proměnnou x_e, pro každý vrchol v napište $|B(v)|$ lineárních rovnic, které se nemají nulovat. Opravte triviální (ne)řešení.

(ii) Vezměte polynom stupně $\sum_{v \in V} |B(v)|$ ze začátku předchozí části. Hledejte vhodný nenulový „vedoucí“ koeficient. Může se hodit buď Hallova věta, nebo vhodná orientace grafu.

Hint 14. Pro n prvočíslo použijte *Chevalley-Warningovu větu* společně s Malým Fermatem. Pak ukažte, že dokazovaná vlastnost se dědí z činitelů na součin.

Hint 15. Pro každý vrchol $v \in V$ představte proměnnou x_v, která bude nabývat hodnot z $\{0, 1\}$ podle toho, zda $x \in U$ nebo $x \notin U$. Pro každou d-kliku v G napište polynom stupně d, který se po dosazení dává 1 či 0 v závislosti na tom, zda klika protíná U či nikoli. Pak sečtěte tyto polynomy přes všechny d-kliky a pomocí Malého Fermata vyrobte polynom stupně $d(p-1)$, který je nenulový právě pro hledaná U. Opravte triviální (ne)řešení.

Hint 16. Odpověď je $d(p-1)+1$, pro konstrukci stačí vzít „souřadnicové přímky". Pro spor ať $|Y| = d(p-1)$, BÚNO obsahuje Y počátek o. Pak $Y' = Y \setminus \{o\}$ protíná každou nadrovinu s rovnicí $a_1y_1 + \cdots + a_dy_d = 1$, kde $a_1, \ldots, a_d$ nejsou všechny nulové, tj. polynom $\prod_{(y_1,\ldots,y_n)\in Y'}(x_1y_1 + \cdots + x_dy_d) \in \mathbb{Z}_p[x_1, \ldots, x_d]$ se nuluje všude kromě počátku.

Hint 17. Pro každý vrchol $v \in V$ vezměte jednu proměnnou nabývající hodnot z $L(v)$, graf zorientujte a uvažte $\prod_{(u,v)\ \text{hrana}}(x_u - x_v)$. Pro použití *Nullstellensatz* teď stačí ukázat, že koeficient u $\prod_{v\in V} x_v^{\deg_{\text{in}}(v)}$ je nenulový. Každá orientace grafu G se stejnými vstupními a výstupními stupni do tohoto koeficientu přispěje ± 1, kde znaménko závisí na tom, kolik hran je třeba otočit. S pomocí Eulerovských tahů nahlédněte, že v případě bipartitního grafu je to vždy $+1$.

Hint 18. Vezměte $B = \{b_1, \ldots, b_k\}$ a proměnné $x_1, \ldots, x_k$. Kdyby tvrzení neplatilo, polynom

$$\prod_{1\le i<j\le k}(x_i - x_j) \cdot \prod_{1\le i<j\le k}(x_i - x_j + a_i - a_j)$$

by se nuloval na hyperkrychli $B^k \subseteq \mathbb{Z}_p^k$. Dokažte, že koeficient u $x_1^{k-1}\cdots x_k^{k-1}$ je $k!$.

Hint 19. Kdo to dořeší, dostane čokoládku.

Hint 20. Vezměte $2p-1$ proměnných, uvažte rovnice $\sum_{i=1}^{2p-1} x_i^{p-1} = 0$ a $\sum_{i=1}^{2p-1} x_i^{p-1}a_i$. Jak souvisí počet jejich společných řešení s hledaným počtem podmnožin I?

Algoritmy

Josef Minařík

Abstrakt. Překvapivě často se stává, že je možné jinak těžkou úlohu vyřešit docela jednoduchým algoritmem. Ukážeme si, jak takové algoritmy mohou vypadat a vyřešíme nějaké úlohy.

Pod pojmem *algoritmus* rozumíme nějaký přesný návod či postup, kterým lze provádět nějakou proceduru či řešit úlohu. Přestože by se mohlo zdát, že algoritmy se hodí spíš do olympiády z informatiky, můžeme s jejich pomocí vyřešit mnoho (nejen) kombinatorik. Může se vyplatit použití nějakého algoritmu, jestliže

- hledáme netriviální konstrukci,
- máme zadanou nějakou operaci,
- chceme redukovat nepřehlednou konfiguraci,
- hrajeme hru a hledáme výherní strategii.

Hladové algoritmy

Hladový algoritmus vždy provede to, co zrovna vypadá nejlépe. Algoritmus tedy vůbec „nepřemýšlí“ dopředu a vždy jde do lokálního optima. Někdy ale i tento „hloupý“ algoritmus může dojít k optimálnímu řešení.

Příklad. Potřebujeme zaplatit přesně N korun a máme neomezená množství bankovek a mincí standardních hodnot $(1, 2, 5, \ldots)$. Chceme použít co nejmenší množství mincí a bankovek, jak to máme udělat?

Úloha 1. V každém políčku tabulky $m \times n$ je napsáno reálné číslo. V jednom kroku můžeme změnit znaménka u všech čísel v jednom řádku nebo v jednom sloupci. Ukažte, že lze dosáhnout stavu, kdy bude součet v každém řádku i v každém sloupci nezáporný.

Úloha 2. Nechť d je nejvyšší stupeň daného grafu. Dokažte, že tento graf lze obarvit nejvýše $d + 1$ barvami tak, aby žádné dva vrcholy spojené hranou neměly stejnou barvu.

Úloha 3. Dokažte, že každé přirozené číslo lze zapsat jediným způsobem jako součet jednoho nebo více Fibonacciho čísel, z nichž žádné dvě nejsou po sobě jdoucí ve Fibonacciho posloupnosti.

Úloha 4. Kamínky vážící dohromady 9 tun je třeba přepravit pomocí náklaďáků. Víme, že žádný kamínek neváží víc než tunu a každý náklaďák uveze 3 tuny. Kolik nejméně náklaďáků je třeba, aby šlo všechny kamínky naráz přepravit?

(Německo 2000)

Úloha 5. Nechť n je přirozené číslo. Majda a Lucia hrají hru – Majda má k listů papíru, kde k je také přirozené číslo. Na každý z listů Majda napíše některá z čísel od 1 do n (může napsat klidně všechna nebo žádné) – zbývající čísla vždy dopíše na druhou stranu papíru (tj. na každém listu budou dohromady z obou stran všechna čísla od 1 do n). Nyní může Lucia otočit nějaké listy na druhou stranu. Pokud se Lucii povede, aby po tomto otočení byla vidět všechna čísla od 1 do n, zvítězí. Najděte nejmenší k, pro které Lucia vždy dovede zvítězit. (Nizozemsko 2014)

Úloha 6. Uvažujme tabulku se dvěma Řádky a n sloupci. Do každé buňky tabulky napíšeme kladné reálné číslo tak, aby součet čísel v každém sloupci byl roven 1. Ukažte, že umíme vybrat jedno číslo z každého sloupce tak, aby součet vybraných čísel v každém řádku byl nejvýše $\frac{n+1}{4}$. (Rusko 2005)

Úloha 7. Je možné vybrat 1983 různých přirozených čísel menších nebo rovných 100 000, z nichž žádné tři netvoří po sobě jdoucí členy aritmetické posloupnosti? (IMO 1983)

Úloha 8. Množinu tří nezáporných čísel $\{x, y, z\}$, kde platí $x < y < z$, nazveme *divnou*, pokud $\{z - y, y - x\} = \{a, b\}$ pro daná $0 < a < b$. Ukažte, že množina všech nezáporných celých čísel se dá zapsat jako sjednocení navzájem disjunktních divných množin. (IMO shortlist 2001, zobecněné)

Úloha 9. Buď n přirozené číslo. Najděte nejmenší celé číslo k s následující vlastností: Pro libovolná reálná čísla $a_1, \ldots, a_d$ taková, že $a_1 + a_2 + \cdots + a_d = n$ a $0 \le a_i \le 1$ pro všechna i od 1 do d je možné tato čísla rozdělit do k skupin (z nichž některé mohou být prázdné) tak, aby součet čísel v každé skupině nepřevyšoval 1. (IMO shortlist 2013)

Úloha 10. Lenka našla 100 krabic, v každé je nějaký počet jablek, banánů a ananasů. Ukažte, že si Lenka může vybrat 51 z těchto krabic tak, aby měla aspoň polovinu kusů každého ovoce. (PraSe)

Úloha 11. Strmilovská banka razí mince s hodnotou $\frac{1}{n}$ pro každé kladné celé číslo n. Mějme konečnou kolekci takových mincí (ne nutně různých hodnot), která má celkovou hodnotu nejvýše $99 + \frac{1}{2}$. Dokažte, že tuto kolekci je možné rozdělit na 100 nebo méně částí tak, aby každá část měla celkovou hodnotu nejvýše 1. (IMO 2014)

Úloha 12. Je dáno celé číslo $N \ge 2$. V řadě stojí $N(N+1)$ navzájem různě vysokých fotbalistů. Trenér Vrba chce vyřadit některých $N(N-1)$ z nich tak, aby nová řada sestávající ze zbylých $2N$ fotbalistů splňovala následujících N podmínek:

(1) Nikdo nestojí mezi dvěma nejvyššími fotbalisty.
(2) Nikdo nestojí mezi třetím a čtvrtým nejvyšším fotbalistou.
$\vdots$
(N) Nikdo nestojí mezi dvěma nejnižšími fotbalisty.

Dokažte, že je to vždy možné. (IMO 2017)

Úloha 13. Množina přímek v rovině v obecné pozici (tj. žádné tři neprocházejí stejným bodem, žádné dvě nejsou rovnoběžné) rozdělí rovinu na území, z nichž některá mají konečný obsah. Dokažte, že pro dostatečně velká n lze pro libovolnou množinu přímek v rovině v obecné pozici obarvit alespoň $\sqrt{n}$ přímek růžově tak, aby žádné konečné území nemělo zcela růžový okraj. (IMO 2014)

Invarianty a monovarianty

Najdeme něco, co se pro dané operace zachovává nebo mění jenom jedním směrem.

Příklad. V rovině je dáno n modrých a n červených bodů tak, že žádné tři neleží v přímce. Dokažte, že lze nakreslit n úseček tak, aby každý z $2n$ bodů byl spojený s právě jedním bodem jiné barvy a žádné dvě úsečky se nekřížily.

Úloha 14. Na zájezdu má každý turista nejvýše tři nepřátele (nepřátelství jsou vzájemná). Dokažte, že je možno turisty rozdělit do dvou autobusů tak, že nikdo nejede v autobuse s více než jedním svým nepřítelem.

Úloha 15. Nechť $a_1, \dots, a_n$ ($n > 3$) jsou reálná čísla taková, že

$$a_1 + a_2 + \cdots + a_n \geq n \qquad \text{a zároveň} \qquad (a_1)^2 + (a_2)^2 + \ldots + (a_n)^2 \geq n^2.$$

Dokažte, že $\max\{a_1, \dots, a_n\} \geq 2$. (USAMO 1999)

Úloha 16. V každém čtverečku tabulky m krát n je napsáno přirozené číslo. Povoleným tahem je přičtení celého čísla k ke dvěma sousedním čtverečkům tak, aby se v žádném z nich neobjevilo záporné číslo. Najděte nutnou a postačující podmínku pro to, aby bylo možné po konečně mnoha operacích docílit tabulky plné nul.

(IMO shortlist 1989)

Úloha 17. Ve vrcholech pravidelného šestiúhelníku je napsáno šest nezáporných celých čísel, jejichž součet je 2003^{2003}. Vladimír má povolenu následující operaci: vybrat si jeden vrchol a nahradit číslo v něm napsané za absolutní hodnotou rozdílu čísel napsaných v sousedních vrcholech. Dokažte, že Vladimír dovede provést takovou sekvenci tahů, po které bude ve všech šesti vrcholech napsáno číslo 0.

(USAMO 2003)

Úloha 18. Mějme n krabic $B_1, B_2, \dots, B_n$ poskládaných do řady. Je v nich dohromady n míčků.

(1) Je-li alespoň jeden míček v B_1, můžeme jej přesunout do B_2.
(2) Je-li alespoň jeden míček v B_n, můžeme jej přesunout do B_{n-1}.
(3) Jsou-li alespoň 2 míčky v B_k, kde $2 \leq k \leq n-1$, můžeme jeden z nich přesunout do B_{k-1} a druhý do B_{k+1}.

Dokažte, že pro libovolné počáteční rozložení míčků lze docílit toho, aby v každé krabici byl právě jeden míček. (China Girls 2011)

Úloha 19. Kubo má tři účty v bance, na každém z nich je celočíselné (kladné) množství peněz. Může dělat převody z účtu na účet pouze tehdy, zdvojnásobí-li tento převod množství peněz na cílovém účtu. Dokažte, že Kubo vždy umí převést všechny své peníze do dvou účtů (tj. ve třetím bude 0). Dovede je vždy všechny převést do jednoho? (IMO shortlist 1994)

Úloha 20. Červená Karkulka a Vlk hrají hru. Vlk nejprve na pásek papíru namaluje sto puntíků, z nichž každý je buď modrý, nebo červený. Na začátku každého tahu se odstřihne puntík nejvíce vlevo. Je-li červený, namaluje Vlk na pravý konec řady další modrý nebo červený puntík dle vlastního výběru. V opačném případě udělá totéž Karkulka. Cílem Karkulky je zajistit, aby po nějakém tahu byly všechny puntíky červené. Může se jí to podařit, ať hraje Vlk jakkoliv? (PraSe)

Úloha 21. Na tabuli je $n \geq 2$ přirozených čísel. V každém kroku vybereme dvě z nich a obě nahradíme jejich součtem. Určete všechna čísla n, pro která je takto vždy možno dospět (v konečném počtu kroků) k n shodným číslům. (MEMO 2008)

Úloha 22. Mějme n imonů, z nichž každá dvojice může či nemusí být spojená. Můžeme provádět dvě operace:

(i) Zničit imon, který je spojen s lichým počtem imonů.
(ii) Zdvojnásobit počet imonů vytvořením kopie ke každému existujícímu imonu. Dva okopírované imony budou spojeny právě tehdy, byly-li spojené jejich vzory. Dále se každý imon spojí se svou kopií. Žádná další spojení během této operace nevzniknou ani nezaniknou.

Dokažte, že lze docílit stavu, kdy nebudou žádné dva imony spojené. (IMO shortlist 2013)

Algoritmy redukce

Máme složitou úlohu, kterou za pomoci nějakého algoritmu převedeme na jednodušší, aniž bychom přitom porušili její strukturu nebo pointu.

Příklad. Mějme uspořádanou množinu šesti celých čísel $S = \{a, b, c, d, e, f\}$. Za tah považujeme operaci, kterou každé z těchto šesti čísel buď zvýšíme nebo snížíme o 1. Ukažte, že existuje konečná posloupnost tahů taková, která převede množinu S do takového tvaru, aby platilo $aef = bdf = cde$.

Úloha 23. Každé správné přátelství je na večírku nutné stvrdit pozváním na skleničku. Co však dělat, když mají účastníci hluboko do kapsy? Pomozte jim a dokažte, že se mohou zvát tak, aby každá dvojice přátel zašla na skleničku právě jednou a přitom aby pro každého člověka platilo, že počet lidí, které pozval, se bude lišit nejvýše o jedna od počtu lidí, kteří pozvali jeho. (PraSe)

Úloha 24. Mějme body $A_1, A_2, \ldots, A_n$ uspořádané na kružnici a bod O uprostřed. Na každém z bodů $A_1, A_2, \ldots, A_n$, O je umístěn konečný počet karet, $n \geq 3$. Máme povoleny následující operace:

(1) Pokud jsou na nějakém bodě A_i alespoň 3 karty, můžeme odebrat 3 karty a dát po jedné z nich do bodů A_{i-1}, A_{i+1}, O.

(2) Pokud je alespoň n karet v bodě O, můžeme je odtud odebrat a rozdat po jedné do bodů $A_1, A_2, \ldots, A_n$.

Dokažte, že pokud je celkový počet karet alespoň $n^2 + 3n + 1$ tak můžeme docílit situace, ve které bude v každém vrcholu alespoň $n + 1$ karet po konečně mnoha krocích. (China 2010)

Úloha 25. Mějme konečnou souvislou množinu S jednotkových čtverců vybraných z rovinné jednotkové mřížky. Tato množina je dokonale pokryta pravoúhlými rovnoramennými trojúhelníky s přeponou délky 2 – tyto trojúhelníky se nepřekrývají a nepřesahují mimo S. Navíc, každá přepona trojúhelníku je rovnoběžná buď s vodorovným nebo svislým směrem. Dokažte, že počet těchto trojúhelníků musí být dělitelný čtyřmi. (USAMTS 2015)

Úloha 26. Na matematické soutěži jsou někteří účastníci kamarádi. Kamarádství je vzájemné. Skupinu, ve které se každí dva spolu kamarádí, nazveme *parta*. Jako *velikost* party označme počet jejích členů. Za předpokladu, že největší velikost party je sudá dokažte, že lze účastníky rozdělit do dvou místností tak, aby největší velikost party v jedné místnosti byla stejná jako největší velikost party ve druhé. (IMO 2007)

Hry, konstrukce a náhodné úlohy

V této části najdete několik her a konstrukčních úloh s poměrně pěkným algoritmickým řešením, které se ale moc nehodí do žádné z předchozích kategorií.

Úloha 27. Na stole leží 2020 mincí. Provedeme 2020 tahů, kde v k-tém tahu otočíme nějakých k mincí. dokažte, že lze dosáhnout toho, aby všechny mince byly nahoru stejnou stranou. (Čína 1989)

Úloha 28. V řadě je N žárovek očíslovaných postupně 1 až N. Krokem rozumíme přepnutí tří žárovek, jejichž čísla a, b, c splňují $a + c = 2b$. Určete všechna N, pro něž lze konečnou posloupností kroků všechny žárovky zhasnout nezávisle na jejich počátečním stavu (*i*KS 1, C5)

Úloha 29. Nechť $n \geq 1$ je přirozené číslo a nechť $t_1 < t_2 < \cdots < t_n$ jsou kladná celá čísla. Ve skupině $t_n + 1$ lidí jsou hrány šachové partie. Dva lidé mohou sehrát partii nejvýše jednou. Dokažte, že je možné, aby platily zároveň tyto dvě podmínky:

- Počet her sehraných každou osobou je roven některému z čísel $t_1, t_2, \ldots, t_n$.
- Pro každé i, $1 \leq i \leq n$, existuje některá z osob, která sehraje právě t_i her.

(EGMO 2017)

Úloha 30. Máme kruh na jehož obvodu je umístěno $2n$ mincí. Můžeme provádět následující operaci: vybereme nějakou minci, na které je orel, a otočíme obě sousední mince. Najděte všechny počáteční pozice, pro které je možné se konečnou posloupností tahů dostat do stavu, kdy je pouze na jedné minci orel. (Japonsko 1998)

Úloha 31. Zdeněk si myslí číslo od 1 do n. Jonáše samozřejmě zajímá, jaké číslo si Zdeněk myslí, a tak ho chtěl uhádnout. Jonáš se může zeptat na libovolnou množinu čísel a Zdeněk mu vždy řekne, jestli daná množina obsahuje jeho číslo. Háček je ale v tom, že Zdeněk může lhát, naštěstí vždy maximálně k-krát po sobě. Jonášovi bude stačit, když najde množinu čísel velikosti nejvýše m a bude jistě vědět, že se tam Zdeňkovo číslo vyskytuje. Dokažte, že se mu to pro $m \geq 2^k$ podaří. (IMO 2012)

Úloha 32. Mějme krabice $B_1, B_2, \ldots, B_6$ poskládané za sebou. Každá z nich zpočátku obsahuje jednu minci. Máme povoleno následující:

(1) Vybrat neprázdnou krabici jinou než B_6, odebrat z ní 1 minci a přidat 2 mince do krabice za ní následující.
(2) Vybrat neprázdnou krabici jinou než B_5 a B_6, odebrat z ní 1 minci a prohodit obsahy mincí následujících dvou krabic.

Určete, jestli existuje konečná posloupnost operací povolených typů taková, aby bylo prvních 5 krabic prázdných a B_6 obsahovala přesně $2010^{2010^{2010}}$ mincí.

(IMO 2010)

Úloha 33. Nechť $k \geq 2$ a $n \geq k-1$ jsou daná přirozená čísla. Rado a Matěj hrají hru. Na začátku Rado na tabuli napíše za sebou n celých čísel. Matěj může v každém kroku zvolit libovolně dlouhý souvislý blok za sebou jdoucích čísel (klidně všechna, nebo naopak jenom jedno). Rado pak buď všechna čísla v tomto bloku zvýší o jedničku, nebo všechna o jedničku sníží. Matěj vyhraje, pokud se na tabuli objeví alespoň $n-k+2$ čísel dělitelných k. Ukažte, že Matěj umí vyhrát v konečném počtu kroků. (iKS 5, C5)

Úloha 34. Na sociální síti s 2019 uživateli jsou některé dvojice uživatelů přátelé, přičemž přátelství jsou vždy vzájemná. Vztahy v této síti se mohou měnit opakovaným provedením následující operace:

> Tři uživatelé A, B, C splňující, že A se přátelí s B i C a zároveň že B a C nejsou přáteli, změní svá přátelství tak, že B se spřátelí s C a zároveň A ukončí svá přátelství s B i s C. Všechna ostatní přátelství zůstanou beze změny.

Na začátku je v síti 1010 uživatelů, z nichž každý má 1009 přátel, a 1009 uživatelů, z nichž každý má 1010 přátel. Ukažte, že existuje vhodná posloupnost uvedených operací, po jejímž provedení nemá žádný uživatel sítě více než jednoho přítele.

(IMO 2019)

Literatura a zdroje

[1] Marian Poljak; *Algoritmy*, sborník iKS, 2017
[2] Cody Johnson; *Algorithms*, `https://people.bath.ac.uk/masgcs/algorithms.pdf`
[3] Pranav A. Sriram; *Olympiad Combinatorics*; `https://euclid.ucc.ie/mathenr/ IMOTraining/OlympiadCombinatoricsChapter1PSriram.pdf`

Hinty

Hint 1. Zbavujeme se záporných součtů.
Hint 2. To snad skoro ani není úloha.
Hint 3. Silná indukce.
Hint 4. Prostě většinu nějak naházíme na první tři náklaďáky.
Hint 5. Nešlo by tam něco binárně vyhledat?
Hint 6. Může se hodit to nějak seřadit a pak se to jenom rozdělí na správném místě.
Hint 7. Postupně vyber všechno co jde, najdi pattern.
Hint 8. Stačí projít čísla od 1, když nějaké číslo ještě nikde není, vytvoříme mu novou množinu.
Hint 9. Pomůže indukce, $\frac{n}{2n-1}$ je fajn číslo.
Hint 10. Vybereme krabici s největším počtem jablek a krabici s největším počtem banánů. Zbylé krabice setřídíme podle počtu jablek a postupně rozdělujeme do skupin, přičemž vyrovnáváme banány.
Hint 11. Zbav se mincí sudé velikostí, mince rozděl na malé a velké. Stejné velké dej do skupin, malé k nim pak přidej.
Hint 12. Rozděl fotbalisty do $N+1$ skupin podle výšky a potom projdi řadu zleva doprava.
Hint 13. Vždy když se obarví nějaká přímka, označ nejvýše dva vrcholy.
Hint 14. Snižujeme počet nepřátelství v rámci autobusů.
Hint 15. Zachovej součet $a_1 + a_2 + \cdots + a_n$, udělej hodně dvojek.
Hint 16. Nutná podmínka je jasná, pak to můžeš dělat třeba po řádcích.
Hint 17. Modulo 2 se hodí, zadaná operace nemůže zvýšit maximum.
Hint 18. Používej druhou a třetí operaci, dokud to jde. Musí tento proces někdy skončit?
Hint 19. Chceme snižovat minimum, binárka je docela fajn.
Hint 20. Každých 100 tahů se na puntíky podívej jako na číslo ve dvojkové soustavě.
Hint 21. Bude-li n sudé, můžeme čísla sloučit do dvojic. Může se hodit podělit všechna čísla největší mocninou 2, kterou jsou všechna dělitelná a dívat se na součet vzniklých čísel.
Hint 22. Nejsou barevné grafy mnohem hezčí? Zase to ale nesmíme přehánět, proto po obarvení počet barev budeme snižovat.
Hint 23. Zbav se cyklů, na stromech už je to jednoduché.
Hint 24. Nejdřív zkus provádět první operaci, dokud to jde – při jakém stavu to už nepůjde? Když teď hodněkrát provedeme druhou operaci, bude to skoro stačit, ale může se to pokazit. Nepůjde to ale nějak opravit?
Hint 25. Stačí to vyřešit jenom pro cykly, ty vyřešíme třeba tak, že je budeme zmenšovat, aniž bychom změnili počet trojúhelníků modulo 4.
Hint 26. Nejdřív dej do jedné místnosti největší partu a do druhé zbytek. Potom se to hodí nějak přibližně vyrovnat, aby velikosti největších part v obou místnostech byly už skoro stejné. Konec je třeba dorozebírat.
Hint 27. Operace provádíme pozpátku, potom postupně zleva zvyšujeme počet správně otočených mincí.
Hint 28. Jde to pro $N \geq 8$.
Hint 29. Rozmysli si to pro $n = 2$, pak to zobecni.

Hint 30. Najít nutnou podmínku je snadné, potom stačí ze všech orlů vytvořit souvislý blok a ten následně zmenšovat.
Hint 31. Postupně vylučuj možnosti, často se ptej na 2^k a použij binárku.
Hint 32. Jde to, $(x, 0, 0) \mapsto (x - y, 2^y, 0)$.
Hint 33. Díváme se na zbytky, označme nejpravější nenulové číslo x. Zajímavé je $(k-x)$-té nenulové číslo zleva.
Hint 34. Buď se můžeme dívat na komponenty, které nejsou úplný graf a mají aspoň jeden vrchol lichého stupně, nebo redukujeme na strom.

Method of Animation

Radek Olšák

Abstrakt. Když už v algebře pro polynom ověříme, že je nulový pro $d+1$ bodů, už je nulový všude. Pojďme něco podobného udělat s geometrií a ověřovat úlohy jen pro pár degenerovaných případů.

Definice (Základní projektivní prostor). Uvažme všechny přímky procházející počátkem v $\mathbb{R}^3$. Tuto množinu označíme $\mathfrak{P}$. Dále množinu všech rovin procházejících počátkem označíme $\mathfrak{L}$. Nyní zkus vnímat $\mathfrak{P}$ jako množinu „bodů“ a $\mathfrak{L}$ jako množinu „přímek“ našeho prostoru. Všimni si, že každé dva „body“ definují právě jednu „přímku“. A každé dvě „přímky“ se protnou v právě jednom „bodě“. Prostoru s touto vlastností se říká *projektivní*.

Definice (Homogenní souřadnice). Všimni si, že kdykoli máš bod v $\mathbb{R}^3$ a vynásobíš mu složky nějakou konstantou, leží stále na stejné přímce skrz počátek. Takže mu přiřadíme stále stejnou $p \in \mathfrak{P}$. Můžeme tedy využívat homogenní souřadnice z $\mathbb{R}^3$ k popisu „bodů“ našeho projektivního prostoru.

Definice (Namapováni na $\mathbb{R}^2$). Uvažme nyní rovinu $z = 1$. Každá přímka $p \in \mathfrak{P}$, která s ní není rovnoběžná, ji protne v právě jednom bodě. Máme tak skoro bijekci mezi $\mathbb{R}^2$ a homogenním $\mathbb{R}^3$. Aby byla bijekce úplná, dodáme $\mathbb{R}^2$ speciální body v nekonečnu – pro každý směr přímky jeden.

Důsledek. Máme tedy homogenní souřadnice $(a, b, c) = (\lambda a, \lambda b, \lambda c)$ určující body z rozšířeného $\mathbb{R}^2$. Souřadnice bodu v $\mathbb{R}^2$ získáme výpočtem

$$\left(\frac{a}{c}, \frac{b}{c}\right).$$

Pokud $c = 0$, jedná se o nevlastní bod ve směru vektoru (a, b).

Poznámka. Pokud už znáš barycentrické souřadnice, tak ty jsou také homogenní souřadnice, jen mají jinou bázi. Takže v nich je nevlastní přímka dána rovnicí $a + b + c = 0$. V našem prostoru je nevlastní přímka $c = 0$.

Definice (Pohyblivý bod). Abychom definovali *pohyblivý bod*, přidáme si proměnnou $t \in \mathbb{R} \cup \{\infty\}$. Pak pohyblivý bod můžeme definovat pomocí tří funkcí f, g, h určujících jeho souřadnice, tedy

$$P_t = \Big(f(t), g(t), h(t)\Big).$$

My budeme pracovat pouze s polynomy, takže chceme, aby f, g, h byly polynomy.

Definice (Pohyblivá přímka). Každá přímka se dá definovat jako množina všech X splňujících $A \cdot X = 0$ pro nějaký bod A, kde $\cdot$ značí standardní skalární součin v $\mathbb{R}^3$. Takže *pohyblivá přímka* pro nás bude asociována přesně tímto bodem.

Definice (Stupeň). Definujeme *stupeň bodu* $\Big(f(t), g(t), h(t)\Big)$ jako nejvyšší ze stupňů polynomů f, g, h. Potom má pevný bod stupeň 0.

Poznámka. Analogicky máme stupeň přímky jako stupeň bodu, který ji určuje.

Cvičení 1. Zkus si rozmyslet, jak vypadají pohyblivé body $(t, 1, 1)$ a $(1, 1, t)$.

Lemma (Přímka skrz pohyblivé body). Mějme pohyblivé body P, Q se stupni d_P, d_Q takové, že pro k různých t se rovnají. Pak přímka PQ má stupeň nejvýše $d_P + d_Q - k$.

Pozorování. Duálně se dá odhadnout stupeň průsečíku pohyblivých přímek.

Lemma (Dokazovací). Mějme tři pohyblivé body A, B, C se stupni d_A, d_B, d_C. Pak pokud leží v jedné přímce pro $d_A + d_B + d_C + 1$ různých t, pak leží v jedné přímce vždy.

Pozorování. Duálně se dá dokázat, že tři přímky prochází jedním bodem.

Lemma (Zdvojení na kuželosečkách). Mějme projektivní zobrazení φ mezi ω a Ω. Pak

- Pokud ω i Ω jsou obojí kuželosečky, nebo obojí přímky, pak φ zachovává stupeň pohyblivých bodů.
- Pokud ω je přímka a Ω kuželosečka, stupeň výsledného bodu je dvojnásobný.
- Pokud ω je kuželosečka a Ω přímka, stupeň výsledného bodu je poloviční.

Užitečná projektivní zobrazení

- Promítnutí skrz pevný bod z jedné přímky na druhou.
- Promítnutí z bodu na kuželosečce.
- Prostřelení skrz pevný bod P. Nalezení druhého průsečíku PX s danou kuželosečkou, po které se hýbe X.
- Nechť A leží na přímce a ω je kuželosečka, která se ji dotýká. Pak zobrazení z A do druhého bodu dotyku na ω je projektivní.
- Podobná zobrazení jsou projektivní.
- Inverze je projektivní.

Seriálové úlohy

Úloha 2 (Unlikely Concurrence). Mějme trojúhelník ABC. Označme body dotyku kružnice vepsané se stranami AB, BC postupně X, Y. Dokaž, že XY, střední příčka vzhledem k vrcholu C a osa úhlu u vrcholu A prochází jedním bodem. Následně označ tento bod R a dokaž, že $|\sphericalangle CRA| = 90°$.

Úloha 3 (Existence kamaráda). Říkáme, že body P, Q jsou *kamarádi* v ABC, pokud $|\sphericalangle PAB| = |\sphericalangle QAC|$, $|\sphericalangle PBA| = |\sphericalangle QBC|$ a $|\sphericalangle PCB| = |\sphericalangle QCA|$. Dokaž, že každý bod P, který neleží na stranách trojúhelníka ABC, má kamaráda.

Úloha 4 (Pascalova věta). Mějme tětivový šestiúhelník $ABCDEF$. Označme $X = AB \cap DE$, $Y = BC \cap EF$, $Z = CD \cap FA$. Dokaž, že X, Y, Z leží na jedné přímce.

Úloha 5 (Jacobi). Mějme trojúhelník ABC. Sestrojme body X, Y, Z tak, že $|\sphericalangle YAC| = |\sphericalangle ZAB|$, $|\sphericalangle ZBA| = |\sphericalangle XBC|$ a $|\sphericalangle YCA| = |\sphericalangle XCB|$. Dokaž, že AX, BY, CZ prochází jedním bodem.

Úloha 6 (Blanchet). V trojúhelníku ABC označme D patu výšky z vrcholu A. Na stranách AC a AB jsou postupně body E, F takové, že přímky BE a CF se protínají na AD v bodě G. Dokaž, že $|\sphericalangle EDA| = |\sphericalangle FDA|$.

Úloha 7 (Butterfly). Mějme kružnici ω a na ní tětivu AB se středem M. Na ω zvolme body K_1, L_1. Označme K_2 průsečík K_1M s ω různý od K_1. Obdobně definujme bod L_2. Nechť $X = K_1L_1 \cap AB$ a $Y = K_2L_2 \cap AB$. Pak $|XM| = |YM|$.

Úloha 8 (Kariya). Mějme trojúhelník ABC a I označme jeho vepsiště. Pak označme D_A, D_B, D_C paty I na strany a, b, respektive c. Body X, Y, Z leží postupně na polopřímkách ID_A, ID_B, ID_C tak, že $|IX| = |IY| = |IZ|$. Dokaž, že přímky AX, BY, CZ prochází jedním bodem.

Úloha 9. Mějme trojúhelník ABC. Označíme I jeho vepsiště a ω jeho kružnici opsanou. Přímka AI protne ω podruhé v bodě D. Mějme body E ležící na oblouku BDC a F ležící na BC takové, že

$$|\sphericalangle BAF| = |\sphericalangle CAE| < \frac{1}{2}|\sphericalangle BAC|.$$

Dále označme G střed IF. Dokaž, že průsečík přímek EI a DG leží na ω.

(IMO 2010/2)

Úloha 10. Mějme trojúhelník ABC s vepsištěm I. Kružnice vepsaná se dotýká strany BC v D. Body P, Q leží postupně na BI, CI tak, že $|\sphericalangle PAQ| = \frac{1}{2}|\sphericalangle BAC|$. Dokaž, že $|\sphericalangle QDP| = 90°$.

Úloha 11. Uvažme rovnostranný trojúhelník ABC a v něm bod P. Označme A_1 překlopené P podle BC. Analogicky B_1 překlopené P podle AC a C_1 překlopené P podle AB. Dokaž, že přímky AA_1, BB_1, CC_1 prochází jedním bodem.

Úloha 12. Nechť $ABCD$ je rovnoramenný lichoběžník s $AB \parallel CD$. Kružnice k procházející body A a B protíná AD v X a AC v Y. Tečna ke k z bodu B protíná CD v bodě Z. Ukaž, že X, Y a Z leží na jedné přímce. (PraSe 38 Myš-Maš/6)

Úloha 13. Mějme trojúhelník ABC. Označme M, N středy stran AB, AC. Na tečně ke kružnici opsané ABC v bodě A zvolme bod X. Označme ω_B kružnici procházející

MB dotýkající se přímky MX. Analogicky ω_C je kružnice skrz body NC dotýkající se NX. Dokaž, že ω_B a ω_C se protínají na BC.

Úloha 14. Mějme P, Q kamarády v ABC. Označme X patu Q na BC. Kružnice nad průměrem AP protíná opsanou ABC v K různém od A. Přímka AQ protíná opsanou ABC v T různém od A. Dokaž, že T, X, K leží na přímce.

Úloha 15. Hedvika našla v rovině kružnici k a bod P vně k. Z bodu P nakreslila dvě tečny ke k, body dotyku pojmenovala A a B. Bod Q umístila tak, aby A byl střed úsečky PQ. Následně přišel Tonda a na úsečce AB nakreslil bod L. Kružnice opsaná trojúhelníku PLB protnula k podruhé v bodě T. Ukaž, že ať už byl Tonda jakkoli zákeřný, vždy platí $|\sphericalangle PBT| = |\sphericalangle QLA|$. (PraSe 38 Tečny/7)

Úloha 16. Uvnitř ostroúhlého trojúhelníku ABC leží body P, Q takové, že platí $|\sphericalangle PBA| = |\sphericalangle QBC|$, $|\sphericalangle PCB| = |\sphericalangle QCA|$ a $|\sphericalangle PAC| = |\sphericalangle QAB|$. Nechť jsou O_1, O_2 středy kružnic opsaných po řadě trojúhelníků PBC a QBC. Dokaž, že platí $|\sphericalangle BAO_1| = |\sphericalangle CAO_2|$. ($i$KS 9. ročník G5)

Úloha 17. Mějme čtyřúhelník $ABCD$ takový, že $|\sphericalangle BAD| + 2|\sphericalangle BCD| = 180^\circ$. Označme E průsečík osy $\sphericalangle BAD$ s BD. Osa AE protíná BC a CD v X a Y. Dokaž, že A, C, X, Y leží na jedné kružnici.

Úloha 18. Mějme trojúhelník ABC. Na straně BC zvolme bod D. Na ose úhlu BAC zvolme bod I. Přímky BI, AI protínají kružnici opsanou ABD postupně v bodech P, Q. Analogicky přímky CI a AI protnou kružnici opsanou ACD v bodech R, S. Dokaž, že přímky RS, PQ, BC prochází jedním bodem.

Úloha 19. Mějme bod P na straně AB v trojúhelníku ABC. Na stranách AC a BC zvolíme S a T tak, aby $|AP| = |AS|$ a $|BP| = |BT|$. Kružnice opsaná PST protne AB a BC znovu v Q a R. Přímky PS a QR se protnou v L. Ukaž, že přímka CL půlí PQ.

Úloha 20. Mějme čtyřúhelník $ABCD$. Označme H ortocentrum ABC. Dále na AB a BC zvolme P, Q tak, aby $PH \parallel AD$ a $QH \parallel CD$. Dokaž, že kolmice na PQ skrz bod H prochází ortocentrem ACD.

Úloha 21. V trojúhelníku ABC označme A' a B' paty výšek z A a B. Na kružnici opsané ABC na oblouku ACB je bod D. Dále $P = AA' \cap BD$ a $Q = BB' \cap AD$. Dokaž, že střed PQ leží na $A'B'$.

Úloha 22. V trojúhelníku ABC se kružnice vepsaná se středem I dotýká stran AC a AB v bodech E, F. Obrazy bodů E, F ve středové symetrii přes I označme G, H. Buď Q průsečík GH a BC a M střed BC. Dokaž, že jsou přímky IQ a IM na sebe kolmé. (Taiwan TST 2014)

Úloha 23. Na straně BC v trojúhelníku ABC mějme body P, Q tak, že platí $|\sphericalangle BAP| = |\sphericalangle QAC|$. Osa úhlu ABC protíná AP a AQ postupně v bodech M a L. Osa úhlu ACB protíná AP a AQ postupně v K, N. Dokaž, že BC, MN a KL prochází jedním bodem.

Úloha 24. Mějme pevný bod D a pevné přímky k, l, které procházejí společným bodem A. Na přímkách k, l jsou postupně body X a Y takové, že $|\angle XDA| = |\angle YDA|$. Dokaž, že přímka XY prochází pevným bodem.

Úloha 25. Na stranách BC a AC trojúhelníka ABC leží po řadě body A_1 a B_1. Body P a Q jsou zvoleny postupně uvnitř úseček AA_1 a BB_1 tak, že přímka PQ je rovnoběžná se stranou AB. Dále P_1 je bod na přímce PB_1, pro nějž platí, že B_1 leží uvnitř úsečky PP_1 a zároveň $|\sphericalangle PP_1C| = |\sphericalangle BAC|$. Podobně bod Q_1 leží na přímce QA_1 tak, že A_1 leží uvnitř úsečky QQ_1 a zároveň platí $|\sphericalangle CQ_1Q| = |\sphericalangle CBA|$. Dokaž, že body P, Q, P_1, Q_1 leží na jedné kružnici. (IMO 2019/2)

Úloha 26. Mějme trojúhelník ABC. Na straně BC leží bod P. Kružnice nad průměrem BP protne podruhé kružnici opsanou APC v Q. Přímka PQ a AC se protínají v M. Označme H ortocentrum trojúhelníka ABP. Dokaž, že když se P hýbe na BC, tak přímky HM prochází pevným bodem.

Další úlohy

Úloha 27 (Another Unlikely Concurrence). Dokaž, že v trojúhelníku ABC spojnice A-paty výšky a B-paty výšky protíná střední příčku vzhledem k vrcholu B na A-symediáně.

Úloha 28 (Newton). Dokaž, že v tečnovém čtyřúhelníku leží vepsiště na spojnici středů úhlopříček.

Úloha 29 (Simson). Dokaž, že Simsonova přímka bodu P pro ABC půlí PH, kde H je ortocentrum.

Úloha 30 (Miquel). Je dán čtyřúhelník $ABCD$. Označme průsečíky $AB \cap DC = P$ a $AD \cap BC = Q$. Dokaž, že kružnice opsané APD, PBC, QDC, QAB prochází jedním bodem.

Úloha 31. V ostroúhlém trojúhelníku ABC označme O střed kružnice opsané. Obraz bodu O v osové souměrnosti podle přímky AC označme P. Dokaž, že středy úseček AO a BP leží na téže kolmici k přímce BC.

(MO/A 2019/2020 krajské kolo)

Úloha 32. Mějme trojúhelník ABC s kružnicí opsanou ω a ortocentrem H. Přímka skrz H protíná AB a AC v E a F. Označme K opsiště AEF. Přímka AK protne ω podruhé v D. Dokaž, že kolmice na BC procházející D a přímka HK se protínají na ω.

Úloha 33. Mějme trojúhelník ABC. Označme $\check{S}_B$, $\check{S}_C$ Švrčkovy body pro B a C. Osy úhlů $\sphericalangle ABC$ a $\sphericalangle ACB$ protnou AC a AB postupně v bodech X, Y. Dokaž, že XY, $\check{S}_B\check{S}_C$ a tečna ke kružnici opsané v bodě A prochází jedním bodem.

Úloha 34. Mějme trojúhelník ABC s kružnicí opsanou ω. Tečny k ω v B a C se protínají v bodě P. Označme paty z P na AB a AC postupně X, Y. Dokaž, že přímka XY je kolmá na těžnici z bodu A.

Úloha 35. Mějme trojúhelník ABC. Označme M, N středy stran AB a AC a F střed MN. Dále D je pata výšky z vrcholu A. Dokaž, že kružnice opsané MBD a NCD se podruhé protínají na přímce DF.

Úloha 36. Mějme trojúhelník ABC. Kružnice jemu vepsaná se jeho stran AB a AC dotýká v bodech D, E. Označme D_1 překlopený bod D podle B. Analogicky nechť je E_1 překlopený bod E podle C. Přímky BE a CD se protínají v P. Konečně střed DE označme M. Dokaž, že MP je kolmá na D_1E_1.

Úloha 37. Mějme trojúhelník ABC a v něm bod P. Označme F, G body na BP a CP tak, že $FG \parallel BC$. Přímka FG protíná AB a AC v bodech K, L. Dokaž, že kružnice opsané FPL a GPK se podruhé protínají na AP.

Úloha 38. Mějme pravoúhlý trojúhelník s pravým úhlem u vrcholu A s kružnicí vepsanou ω. Kružnice ω se dotýká BC v D, AC v E a AB v F. Označme G bod dotyku strany AC a B-připsané kružnice. Dokaž, že $GF \perp DE$.

Úloha 39. Mějme rovnoběžník $ABCD$. Na úsečkách AB a BC zvolme body D, E tak, že $|AD| = |CE|$. Dokaž, že AE a CD se protínají na ose úhlu $\sphericalangle ADC$.

Úloha 40. Mějme trojúhelník ABC. Označme D patu A. Na AD zvolme bod H. Dále sestrojme čtverce $XADB$ a $DHYC$. Přímky CH a BH protínají AB, resp. AC v bodě K, resp. L. Dokaž, že X, Y, K, L leží na jedné přímce.

Úloha 41. Mějme konvexní čtyřúhelník $ABCD$. Označme D, E paty C na postupně AB a AD. Dále označme jako F, resp. H paty A na DC, resp. CB. Označme G_1 a G_2 ortocentra trojúhelníků ADC a ABC. Dokaž, že přímky G_1G_2, EH, DF, BD prochází jedním bodem.

Úloha 42. Mějme dva rovnostranné trojúhelníky ABC a DEF sdílící střed (oba značíme ve směru hodinových ručiček). Dokaž, že přímky AD, BF, CE prochází jedním bodem.

Úloha 43. Nechť ABC je trojúhelník. Kružnice procházející B a C protíná stranu AB v C_0 a stranu AC v B_0. Dokaž, že BB_0, CC_0 a HH_0 procházejí jedním bodem, kde H, H_0 jsou postupně ortocentra trojúhelníků ABC, AB_0C_0.

Úloha 44. Mějme tětivový čtyřúhelník $ABCD$. Kružnice procházející body AB protne AC, resp. BD v bodě E, resp. F. Dále $Q = BE \cap AD$ a $P = AF \cap BC$. Dokaž, že $PQ \parallel BC$.

Úloha 45. Mějme kružnici k a na ní dvě tětivy A_1A_2 a B_1B_2 protínající se v D. Obraz D v inverzi podle k je D'. Přímka A_1B_1 protne osu DD' v X. Dokaž, že $XD \parallel A_2B_2$.

Úloha 46. Mějme trojúhelník ABC s kružnicí opsanou ω. Tečna k ω v A protíná BC v P, zatímco E je libovolný bod na PO. Bod D leží na BE tak, že $AD \perp AB$. Dokaž, že $|\sphericalangle EAB| = |\sphericalangle ACD|$.

Úloha 47. Mějme trojúhelník ABC s opsanou Ω a vepsanou ω se středem I. Nechť je X libovolný bod na BC. Přímka skrz I kolmá na IX protne tečnu k ω rovnoběžnou s BC v Y. Přímka AY protne Ω podruhé v Z. Budiž T bod dotyku A-*Mixtilinear incircle*$^{*)}$ s Ω. Dokaž, že X, Z, T leží na přímce.

Úloha 48. Nechť je AB průměr kružnice ω a budiž ℓ tečna k ω v B. Zvolme body C, D na ℓ tak, že B leží mezi nimi. Nechť jsou E a F jsou průsečíky AC a AD s ω různé od A. Dále nechť jsou G, H druhé průsečíky CF, DE s ω. Dokaž, že $|AH| = |AG|$.

Úloha 49. Mějme kružnici Ω se středem O a přímku ℓ. Kolmice k ℓ skrz O protíná Ω v A a B. Na Ω zvolme body P, Q. Dále $PA \cap \ell = X_1$, $PB \cap \ell = X_2$, $QA \cap \ell = Y_1$ a $QB \cap \ell = Y_2$. Dokaž, že průsečík kružnic opsaných AX_1Y_1 a AX_2Y_2 různý od A leží na Ω.

Úloha 50. Mějme trojúhelník ABC s tupým úhlem u B. Označme O jeho opsiště a ω jeho kružnici opsanou. Nechť je N střed oblouku AC obsahujícího B. Kružnice opsaná NBO protíná AC v X, Y. Přímky BX, BY protínají ω podruhé v K, L. Dokaž, že K, L a překlopený N podle AC leží na přímce.

Úloha 51. Mějme trojúhelník ABC a v něm kamarády P, Q. Přímky AP, BP, CP protínají strany v D, E, F. Označme O opsiště. Přímka kolmá na EF protíná DO v X. Dokaž, že $XQ \perp BC$.

Úloha 52. Mějme rovnoramenný lichoběžník $ABCD$ takový, že $AB \parallel CD$. Označme E střed AC. Dále označme ω a Ω kružnice opsané ABE a CDE. Nechť P je průsečík tečny k ω v A a tečny k Ω v D. Dokaž, že PE je tečna k Ω.

Úloha 53. Mějme trojúhelník ABC s ortocentrem H. Budiž ω kružnice opsaná BHC. Vezměme bod P na ω. Přímky BP, CP protnou přímky AC, AB po řadě v X, Y. Dokaž, že když se P hýbe po ω, tak kružnice opsané $AXPY$ prochází pevným bodem různým od A.

Úloha 54. Mějme trojúhelník ABC s ortocentrem H. Nechť D leží uvnitř ABC a $|DB| = |DC|$. Dále nechť BD, BC protínají CA, AB v E, F a budiž $EF \cap BC = K$. Označme X ortocentrum DBC. Dokaž, že $HX \perp AK$

Úloha 55. Mějme kružnice ω_1 a ω_2 protínající se v A, B. Vezměme $P \in \omega_1$ a $Q \in \omega_2$ tak, že $|\sphericalangle PAB| = |\sphericalangle QAB|$. Dokaž, že nezávisle na P, Q kružnice opsané APQ prochází pevným bodem různým od A.

Úloha 56. Mějme trojúhelník ABC a bod D na AB. Označme I bod uvnitř ABC na ose $\sphericalangle ACB$. Druhé průsečíky AI a CI s kružnicí opsanou ACD označme P, Q. Obdobně druhé průsečíky BI a CI s opsanou BCD označme R, S. Ukaž, že přímky AB, PQ, RS prochází jedním bodem.

Úloha 57. Mějme trojúhelník ABC a označme D bod na BC. Kružnice ABD protíná AC podruhé v E. Kružnice opsaná ACD protíná AB podruhé v F. Nechť je A_0 překlopené A podle BC. Dále budiž $P = A_0C \cap DE$ a $Q = A_0B \cap DF$. Dokaž, že přímky AD, BP, CQ prochází jedním bodem. (RMM 2016/1)

$^{*)}$ Kružnice dotýkající se kružnice opsané a přímek AB a AC.

Úloha 58. Mějme trojúhelník ABC. Označme ℓ_A druhou vnější tečnu kružnic B-připsané a C-připsané. Analogicky označme ℓ_B a ℓ_C. Na ℓ_A leží bod D. Druhá tečna z D ke kružnici B-připsané protíná ℓ_C v E. Analogicky druhá tečna z D ke kružnici C-připsané protíná ℓ_B v F. Dokaž, že EF je tečna ke kružnici A-připsané.

Těžké, často bez hintů, pro borce

Úloha 59. Mějme ABC ostroúhlý trojúhelník s kružnicí opsanou ω a nechť M je střed BC. Pohyblivý bod P leží na AM. Kružnice opsané BPM a CPM protnou ω podruhé v D, E. Přímky DP a EP protnou podruhé kružnice opsané CPM a BPM v X a Y. Dokaž, že nezávisle na poloze P kružnice opsané AXY prochází pevným bodem různým od A.

Úloha 60. Mějme kružnice Ω a ω takové, že jsou opsaná, resp. vepsaná nějakého trojúhelníka. Na Ω leží bod P. Dokaž, že Simsonovy přímky P vůči všech trojúhelníkům s vepsanou ω a opsanou Ω prochází pevným bodem.

Úloha 61. Mějme konvexní čtyřúhelník $ABCD$ splňující $|\sphericalangle ABC| = |\sphericalangle ADC| < 90°$. Osy úhlů $\sphericalangle ABC$, $\sphericalangle ADC$ protnou AC v E, F a navzájem se protnou v P. Označme M střed AC a ω kružnici opsanou BPD. Přímky BM, DM protnou podruhé ω v X, Y. Označme $Q = XE \cap YF$. Dokaž, že $PQ \perp AC$ (ISL 2016 G6)

Úloha 62. Označme M libovolný bod na kružnici opsané ABC. Tečny z M ke kružnici vepsané ABC protnou přímku BC v X_1 a X_2. Dokaž, že kružnice opsaná MX_1X_2 prochází bodem dotyku A-mixtilinear incircle*). (Taiwan TST 2014/3)

Úloha 63. Mějme trojúhelník ABC s kružnicemi opsanou Ω a vepsanou ω. Označme A' bod dotyku A-mixtilinear-excircle*). Dále sestrojme trojúhelník $A'B'C'$ takový, že má Ω jako opsanou a ω jako vepsanou. Ten existuje z Ponceletova porismatu. Pak se $B'C'$ dotýká vepsané v X. Dokaž, že kružnice opsaná BXC se dotýká ω.
(110 Geometry Problems / 77)

Literatura a zdroje

[1] Zack Chroman, Gopal K. Goel, Anant Mudgal; *The Method of Animation*, 2019, `https://artofproblemsolving.com/community/c6h1952595p14062313`

[2] Vladyslav Zveryk; *The Method of Moving Points*, 2019, `https://artofproblemsolving.com/community/q1h1884540p12835147`

[3] yayups; *Moving points tutorial*, 2019, `https://artofproblemsolving.com/community/c473124h1763266_moving_points_tutorial`

[4] Lenka Kopfová, Radek Olšák; *Projektivní geometrie*, PraSečí seriál, 2019/2020

*) Kružnice dotýkající se přímek AB, AC a z venku opsané.

Hinty

Hint 2. Hýbej s C po AC. Střední příčka je rovnoběžná se stranou.
Hint 3. Hýbej s P po AP.
Hint 4. Hýbej třeba s A po kružnici opsané. Existují právě tři z ostatních bodů takové, že když se jim A rovná, věta je triviální.
Hint 5. Hýbej s X po BX.
Hint 6. Hýbej s G po výšce.
Hint 7. Hýbej s K_1 po kružnici.
Hint 8. Přímky AX, BY, CZ budou mít všechny stupeň 1, takže stačí čtyři případy.
Hint 9. Rozhýbej E po ω. vezmi $E = B$, $E = C$, $E = D$.
Hint 10. Hýbej s P po BI. Pro třetí případ vyber P vepsiště menšího trojúhelníka.
Hint 11. Najdi vhodnou přímku, po které P hýbat, aby se zachovala přímka AA_1.
Hint 12. Hýbej s D po CD.
Hint 13. Označ D průsečík ω_C a BC. Všimni si, že $|\sphericalangle XND| = |\sphericalangle ACB|$. Takže zobrazení z X do D se dá vnímat jako rotace o pevný úhel.
Hint 14. Označte X' průsečík KT a BC. Zafixujte ABC a bod T. Hýbejte s Q po AT. Ukažte, že $Q \mapsto X$ a $Q \mapsto X'$ jsou projektivní.
Hint 15. Převeď podmínku o úhlech na $LQ \parallel AT$.
Hint 16. Hýbej s P po PB. Jako třetí bod zvol P na ose ACB a tuhle konfiguraci vyřeš znovu hýbáním.
Hint 17. Označ I vepsiště BAD. Hýbej s C po kružnici opsané BID.
Hint 18. Hýbej s I po AI. Najdi dva triviální případy a za třetí zvol nevlastní bod. Pak rozhýbej D.
Hint 19. Uvědom si, že I je opsiště PST. Pata na AB je pak středem PQ. Hýbej s P po AB. Dokaž, že se přímky CD, PS a QR protínají v jednom bodě.
Hint 20. Zafixuj A, B, C, P a hýbej s Q po BC. Uvaž $Q = B$, $Q = BC_\infty$ a $PQ \parallel AC$.
Hint 21. Hýbej s P po AA'. Definuj Q' jako průsečík BB' a vystejnolehlené $A'B'$ z P koeficientem 2.
Hint 22. Hýbej s A po AB.
Hint 23. Najdi zobrazení zobrazující $B \mapsto C$, $M \mapsto N$ a $L \mapsto K$.
Hint 24. Najdi projektivní zobrazení zobrazující X na Y.
Hint 25. Dokresli průsečíky X, Y přímky PQ s CB a CA. Pak Q_1CQX je tětivový. Převeď tětivovost PQP_1Q_1 pomocí nových kružnic a mocnosti na průsečík přímek. Hýbej s B_1 po CA.
Hint 26. Zobrazení z P do M je projektivní. Dokresli kružnici opsanou a dobře tohle zobrazení definuj.
Hint 27. Hýbej s vrcholem C po AC. Symediána je překlopená těžnice. Stačí tři případy.
Hint 28. Hýbej s A po AB. Zafixuj vepsanou kružnici.
Hint 29. Hýbej s A po opsané. H má stupeň 2.
Hint 30. Rozhýbej P po AB a zafixuj A, B, C, Q. Zapomeň kružnici opsanou PAD.
Hint 31. Rozhýbej B po opsané.
Hint 32. Pro standardní řešení si všimni, že $|\sphericalangle KAF| + |\sphericalangle FEA| = 90°$. Pro víc odhadovací řešení rozhýbej D po ω a shazuj stupně pomocí lemma.

Hint 33. Úloha platí i když přímka $\check{S}_BXB$ není osa úhlu.
Hint 34. Rozhýbej A po opsané. Budeš muset najít 5 případů z toho 4 jsou triviální.
Hint 35. Hýbej s B po BC.
Hint 36. Hýbej s C po AC a zafixuj vepsanou. Budeš muset ověřit 5 případů.
Hint 37. Hýbej s F po BP. Všimni si, že kružnice opsaná GPK prochází pevným bodem. Kde bude průsečík, když F je nevlastní?
Hint 38. Hýbej s C po AC s pevnou ω. Stačí tři případy. Všechny jsou triviální.
Hint 39. Hýbej s D po AB. Všechno je projektivní.
Hint 40. Hýbej s H. Zvol hezké pozice čtverce $DHYC$.
Hint 41. Všimni si, že $EFDH$ leží na jedné kružnici.
Hint 42. Rozhýbej D po přímce.
Hint 43. Hýbej s C_0 po AB. Budeš potřebovat čtyři případy. Steinerova kuželosečka ti říká tři, čtvrtý najdeš.
Hint 44. Tahle úloha by už ti měla opravdu přijít lehká. Hýbej s E po AC.
Hint 45. Hýbej s A_1 po opsané. Zbavíš se tak jedné tětivy a převedeš tedy problém na úlohu jen s jednou tětivou. A to už snad ubashíš ne? :-)
Hint 46. Hýbej s E.
Hint 47. I, T a $\check{N}_A$ leží v přímce, kde $\check{N}_A$ je střed oblouku BC na Ω obsahující A.
Hint 48. Rozhýbej třeba C.
Hint 49. Inverzí dokaž, že zobrazení na Ω bude projektivní.
Hint 50. Zobrazení z X do K opravdu je projektivní.
Hint 51. Hýbání kamarádů po přímce skrz vrchol je hezky projektivní.
Hint 52. *Lemma.* Mějme trojúhelník ABC. AD je jeho těžnice. $X \in AD$ a ω_B a ω_C jsou kružnice opsané AXB a AXC. Dokresli tečny ℓ_B, ℓ_C k ω_B, ω_C v B, C. Označ $Y = \ell_B \cap \ell_C$. Pak Y leží na A-symediáně ABC.
Hint 53. Dokaž, že všechny středy takových kružnic leží na přímce.
Hint 54. Ověř čtyři případy. Dva jsou triviální.
Hint 55. Zinvertuj podle A.
Hint 56. Rozhýbej I.
Hint 57. Rozhýbej D. Zobrazení do P i Q jsou projektivní. Dva případy ti dá Steinerova kuželosečka. Další dva jsou když P, resp. Q je A_0. Taky triviálně funguje nevlastní D, ale je to jen jeden případ.
Hint 58. Kuželosečka je pevně dána pěti tečnami. EF generuje tečny k Steinerově kuželosečce. Tři tečny jsou triviální.
Hint 59. X se hýbe po kružnici. XP má stupeň 1.
Hint 60. Rozhýbej vrchol trojúhelníka. Definuj Simsonovu přímku symetricky v BC, aby jsi mohl spočítat stupeň. Použij body pata P na BC a střed PH. Vyjde ti, že Simsonova přímka má stupeň nejvýš 8.

Postupnosti

Tomáš Sásik

Abstrakt. V matematických súťažiach sa často vyskytujú úlohy s postupnosťami, ktoré sa snažia byť čo najviac rôznorodé. Keď však vyriešime veľa úloh zameraných na postupnosti, získame potrebný cvik a intuíciu na správne myšlienky. Taktiež zistíme, že niektoré princípy sa pri riešení týchto úloh predsa len opakujú a keď sa stretneme druhýkrát s takouto úlohou, máme ju skoro zadarmo. Preto si v tomto príspevku ukážeme najčastejšie používané triky na postupnosti a taktiež veľa zaujímavých úloh.

Užitočné prístupy

- Vypísať si prvých pár členov a odpozorovať pattern.
- Indukcia.
- Vyjadriť n-tý člen explicitne.
- Upraviť si rekurentný vzorec do krajšieho tvaru.
- Zadefinovať si novú postupnosť, napr. $b_n = \frac{1}{a_n}$ ak rekurentný vzorec má zložitý menovateľ alebo keď obsahuje $\sqrt{\text{Výraz}(a_n)}$, tak $b_n = \sqrt{\text{Výraz}(a_n)}$.
- Pozrieť sa na diferencie alebo prefixové súčty

$$d_n = a_n - a_{n-1}, \qquad S_n = a_0 + a_1 + \cdots + a_n.$$

- Pozrieť sa na najväčší/najmenší člen (prípadne ukázať, že sa rovnajú).
- Dokázať rastúcosť/klesajúcosť, periodickosť, skúmať podpostupnosti…

Príklad. Môžeme si všimnúť, že keď vyberieme každé druhé Fibonacciho číslo $1, 2, 5, 13, 34, \ldots$, tak spĺňajú lineárnu rekurenciu $F_{n+1} = 3F_n - F_{n-1}$ a zároveň kvadratickú rekurenciu $F_n^2 + 1 = F_{n-1}F_{n+1}$. Predstavme si, že by sme mali túto postupnosť zadanú len pomocou kvadratickej rekurencie $F_{n+1} = \frac{F_n^2+1}{F_{n-1}}$. Ako by sa z nej dala odvodiť tá pekná lineárna? Takto:

$$1 = F_{n-1}F_{n+1} - F_n^2 = F_{n-2}F_n - F_{n-1}^2,$$
$$\frac{F_{n+1} + F_{n-1}}{F_n} = \frac{F_n + F_{n-2}}{F_{n-1}} = \frac{F_1 + F_3}{F_2} = 3.$$

Pozorovanie (Teleskopická suma). Občas sa hodí použiť nasledujúcu identitu:

$$a_n = a_0 + \sum_{k=1}^{n} (a_k - a_{k-1}).$$

Príklad.
$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = \sum_{k=1}^{n} \frac{1}{k} - \frac{1}{k+1} = 1 - \frac{1}{n+1},$$
$$\sum_{k=1}^{n} kk! = \sum_{k=1}^{n} (k+1)! - k! = (n+1)! - 1.$$

Lema (Abelova sumácia). Majme postupnosti $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$ reálnych čísel. Označme $S_k = \sum_{i=1}^{k} a_i$. Potom platí
$$\sum_{k=1}^{n} a_k b_k = S_n b_n + \sum_{k=1}^{n-1} S_k (b_k - b_{k+1}).$$

Manipulácie s rekurentne danými postupnosťami

Úloha 1. Nájdite všetky reálne čísla a_0 také, že postupnosť daná $a_{n+1} = 2^n - 3a_n$ pre $n \geq 0$ je rastúca. (Britská MO 1980)

Úloha 2. Uvažujme postupnosť $\{a_n\}_{n=1}^{\infty}$, $a_1 = \frac{1}{2}$,
$$a_{n+1} = \frac{a_n^2}{a_n^2 - a_n + 1}, \quad \text{pre } n \geq 1.$$
Dokážte, že pre všetky n platí
$$\sum_{k=1}^{n} a_k < 1.$$
(Rumunsko TST 2003)

Úloha 3. Nech postupnosť $a_1, a_2, \ldots$ kladných reálnych čísel spĺňa
$$a_{k+1} \geq \frac{k a_k}{a_k^2 + (k-1)}$$
pre všetky $k \geq 1$. Dokážte, že $a_1 + a_2 + \cdots + a_n \geq n$ pre všetky $n \geq 2$.
(ISL 2015 A1)

Úloha 4. Postupnosť reálnych čísel $a_0, a_1, a_2, \ldots$ je daná rekurentne
$$a_0 = -1, \qquad \sum_{k=0}^{n} \frac{a_{n-k}}{k+1} = 0 \quad \text{pre } n \geq 1.$$
Dokážte, že $a_n \geq 0$ pre všetky $n \geq 1$. (ISL 2006 A2)

Úloha 5. Postupnosti $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$ sú dané predpisom $a_1 = 1$, $b_1 = 2$ a pre všetky $n \geq 1$ platí
$$a_{n+1} = \frac{1 + a_n + a_n b_n}{b_n}, \qquad b_{n+1} = \frac{1 + b_n + a_n b_n}{a_n}.$$
Dokážte, že $a_{2008} < 5$. (Rusko MO 2008)

Úloha 6. Majme postupnosť reálnych čísel $a_0, a_1, \ldots, a_n$ definovanú vzťahom $a_0 = \frac{1}{2}$, $a_k = a_{k-1} + \frac{a_{k-1}^2}{n}$ pre $1 \leq k \leq n$. Dokážte, že $1 - \frac{1}{n} < a_n < 1$. (Fínsko 1980)

Dokazovanie celočíselnosti

Úloha 7. Postupnosť je daná nasledovne:

$$a_{n+3} = \frac{a_{n+1}a_{n+2} + 5}{a_n}, \ n \in \mathbb{N} \qquad \text{a} \qquad a_1 = a_2 = 1, \ a_3 = 2.$$

Dokážte, že všetky členy tejto postupnosti sú celé čísla.

Úloha 8. Máme rekurentne danú postupnosť

$$a_{n+2} = \frac{2a_{n+1} - 3a_{n+1}a_n + 17a_n - 16}{3a_{n+1} - 4a_{n+1}a_n + 18a_n - 17}, \quad n \in \mathbb{N}_0$$

s počiatočnými hodnotami $a_0 = a_1 = 2$. Dokážte, že a_n tvaru $1 + \frac{1}{m^2}$ pre $n \in \mathbb{N}_0$, kde $m \in \mathbb{N}$.

Úloha 9. Nech $Q_0(x) = 1$, $Q_1(x) = x$ a

$$Q_n(x) = \frac{(Q_{n-1}(x))^2 - 1}{Q_{n-2}(x)}$$

pre všetky $n \geq 2$. Ukážte, že ak n je prirodzené číslo, tak $Q_n(x)$ je polynóm s celočíselnými koeficientami. (Putnam 2017 A2)

Úloha 10. Majme postupnosť $\{a_n\}_{n=1}^{\infty}$ danú rekurentne:

$$a_1 = c, \qquad a_{n+1} = ca_n + \sqrt{(c^2-1)(a_n^2-1)}.$$

Dokážte, že ak c je prirodzené číslo, tak všetky členy postupnosti budú prirodzené. (KMS 16/17-Z3-10)

Úloha 11. Zistite, či existujú kladné celé čísla a, b také, že všetky členy postupnosti $\{x_n\}_{n=1}^{\infty}$, $x_1 = 2010$, $x_2 = 2011$,

$$x_{n+2} = x_n + x_{n+1} + a\sqrt{x_n x_{n+1} + b}$$

sú celé čísla. (IberoAmerican MO 2010)

Úloha 12. Rozhodnite, či existuje nekonečná postupnosť $a_1, a_2, \ldots$ prirodzených čísel, ktorá spĺňa

$$a_{n+2} = a_{n+1} + \sqrt{a_{n+1} + a_n}$$

pre všetky prirodzené n. (EGMO 2015)

Abelova sumácia a nerovnosti

Úloha 13. Pre dve dané reálne postupnosti $\{a_k\}_{k=1}^n$ a $\{b_k\}_{k=1}^n$ dokážte, že

$$\sum_{i=1}^n a_i x_i \leq \sum_{i=1}^n b_i x_i \quad \text{pre ľubovoľné } x_1 \leq x_2 \leq \cdots \leq x_n$$

je ekvivalentné s

$$\sum_{i=1}^n a_i = \sum_{i=1}^n b_i \quad \text{a zároveň} \quad \sum_{i=1}^k a_i \geq \sum_{i=1}^k b_i \quad \text{pre všetky } 1 \leq k \leq n-1.$$

Úloha 14. Nech $\{a_k\}_{k=1}^n$ a $\{b_k\}_{k=1}^n$ sú dve reálne postupnosti, pričom $\{a_k\}$ je nezáporná a klesajúca. Predpokladajme, že $\sum_{i=1}^k a_i \leq \sum_{i=1}^k b_i$ pre všetky k. Dokážte, že $\sum_{i=1}^n a_i^2 \leq \sum_{i=1}^n b_i^2$.

Ďalšie nerovnosti a rekurencie

Úloha 15. Máme postupnosť $a_1, a_2, a_3, \ldots$ nezáporných čísel. Pre všetky prirodzené m, n platí $a_{n+m} \leq a_n + a_m$. Potom dokážte

$$a_n \leq m a_1 + \left(\frac{n}{m} - 1\right) a_n.$$

(Čína 1997)

Úloha 16. Postupnosť $a_1, a_2, a_3, \ldots$ spĺňa nerovnosť $|a_{k+m} - a_k - a_m| \leq 1$ pre všetky k, m. Dokážte, že pre všetky prirodzené k, m platí nasledujúca nerovnosť:

$$\left|\frac{a_k}{k} - \frac{a_m}{m}\right| \leq \frac{1}{k} + \frac{1}{m}.$$

(Rakúsko-Poľsko 1980)

Úloha 17. Nech $a_1, a_2, a_3, \ldots$ je postupnosť nezáporných reálnych čísel, pre ktorú platí $a_k - 2a_{k+1} + a_{k+2} \geq 0$ pre $k \geq 1$ a $\sum_{j=1}^n a_j \leq 1$. Dokážte, že $0 \leq a_k - a_{k+1} \leq \frac{2}{k^2}$ pre $k \geq 1$. (ISL 1988)

Úloha 18. Pre postupnosť danú vzťahom $a_1 = \frac{1}{2}$, $a_{n+1} = a_n - n a_n^2$ dokážte, že $a_1 + a_2 + \cdots + a_n < \frac{3}{2}$ pre všetky $n \geq 1$.

Úloha 19. Majme ohraničenú postupnosť $\{a_n\}_{n=1}^\infty$ spĺňajúcu

$$a_n < \sum_{k=n}^{2n+2006} \frac{a_k}{k+1} + \frac{1}{2n+2007} \quad \text{pre } n \geq 1.$$

Dokážte, že $a_n < \frac{1}{n}$ pre $n \geq 1$. (Čína MO 2007)

Úloha 20. Nech $\{a_k\}_{k=1}^n$ je postupnosť kladných reálnych čísel. Dokážte:

$$\sum_{k=1}^n \frac{k}{a_1 + a_2 + \cdots + a_k} < 2 \sum_{i=1}^n \frac{1}{a_i}.$$

Ľahšie zábavky

Úloha 21. Uvažujme postupnosť $\{a_n\}_{n=1}^{\infty}$ danú predpisom $a_n = \lfloor n\sqrt{2003} \rfloor$ pre všetky $n \geq 1$. Dokážte, že pre ľubovoľné prirodzené čísla m, p existuje m členov postupnosti $\{a_n\}_{n=1}^{\infty}$ vytvárajúcich geometrickú postupnosť s kvocientom p.

(Rumunsko TST 2003)

Úloha 22. Postupnosť kladných celých čísel $\{a_n\}_{n=1}^{\infty}$ je daná tak, že a_1 je ľubovoľné prirodzené číslo a pre $n \geq 1$ máme $a_{n+1} = \frac{a_n}{5}$ ak a_n je deliteľné 5, $a_{n+1} = \lfloor a_n\sqrt{5} \rfloor$ ak a_n nie je deliteľné 5. Dokážte, že od nejakého člena je postupnosť rastúca.

(Rusko MO 2003)

Úloha 23. Nech $0 < a_1 \leq a_2 \leq a_3 \leq \ldots$ je neohraničená postupnosť celých čísel. Zaveďme postupnosť $\{b_n\}$, pričom $b_n = m$, ak a_m je prvý člen postupnosti väčší alebo rovný n. Je dané $a_{19} = 85$. Aká je najväčšia možná hodnota súčtu $a_1 + a_2 + \cdots + a_{19} + b_1 + b_2 + \cdots + b_{85}$? (USAMO 1985)

Úloha 24. Nech $a_1, a_2, \ldots$ je postupnosť celých čísel s nekonečne veľa kladnými členmi a nekonečne veľa zápornými členmi. Predpokladajme, že pre všetky prirodzené čísla n čísla $a_1, a_2, \ldots, a_n$ majú n rôznych zvyškov po delení n. Dokážte, že každé celé číslo sa v postupnosti nachádza práve raz. (ISL 2005 N2)

Úloha 25. Postupnosť $\{x_n\}_{n=0}^{\infty}$ je daná nasledovne: $x_0 = a$, $x_1 = 2$,

$$x_n = 2x_{n-1}x_{n-2} - x_{n-1} - x_{n-2} + 1 \quad \text{pre } n \geq 2.$$

Nájdite všetky celé čísla a také, že $2x_{3n} - 1$ je štvorec pre všetky $n \geq 1$.

(Baltic Way 2005)

Strednejšie príklady

Úloha 26. Postupnosť reálnych čísel $a_0, a_1, \ldots$ je daná nasledovne. Člen a_0 je ľubovoľné reálne číslo a pre $n \geq 0$ platí $a_{n+1} = \lfloor a_n \rfloor \cdot \{a_n\}$, kde $\lfloor x \rfloor$ značí najväčšie celé číslo menšie rovné od x a $\{x\} = x - \lfloor x \rfloor$. Dokážte, že $a_n = a_{n+2}$ pre všetky dostatočne veľké n. (ISL 2006 A1)

Úloha 27. Ukážte, že existuje nekonečná ohraničená postupnosť $\{a_n\}_{n=1}^{\infty}$ taká, že pre každé dve rôzne prirodzené čísla m, n platí $|a_m - a_n| \geq \frac{1}{m-n}$.

(Rusko MO 1978)

Úloha 28. Uvažujme postupnosť $x_0, x_1, \ldots, x_{n_0-1}$ celých čísel a postupnosť d_1, $d_2, \ldots, d_k$ prirodzených čísel za predpokladov

$$n_0 = d_1 > d_2 > \cdots > d_k \qquad \text{a} \qquad \mathrm{NSD}(d_1, d_2, \ldots, d_k) = 1.$$

Pre všetky $n \geq n_0$ definujme

$$x_n = \left\lfloor \frac{x_{n-d_1} + x_{n-d_2} + \cdots + x_{n-d_k}}{k} \right\rfloor.$$

Dokážte, že postupnosť $\{x_n\}_{n=1}^{\infty}$ je od niektorého člena konštantná.

(USA TST 2011)

Úloha 29. Máme danú postupnosť reálnych čísel $a_1, a_2, \ldots, a_n$. Pre všetky $1 \leq i \leq n$ definujme

$$d_i = \max\{a_j \mid 1 \leq j \leq i\} - \min\{a_j \mid i \leq j \leq n\}$$

a nech $d = \max\{d_i \mid 1 \leq i \leq n\}$.

(a) Dokážte, že pre ľubovoľné reálne čísla $x_1 \leq x_2 \leq \cdots \leq x_n$ platí

$$\max\left\{|x_i - a_i| \;\middle|\; 1 \leq i \leq n\right\} \geq \frac{d}{2}. \qquad (*)$$

(b) Ukážte, že existujú také reálne čísla $x_1 \leq x_2 \leq \cdots \leq x_n$, že v $(*)$ nastáva rovnosť.

(IMO 2007 P1)

Úloha 30. Nech $a_0 < a_1 < a_2 < \ldots$ je nekonečná postupnosť kladných celých čísel. Ukážte, že existuje práve jedno prirodzené číslo n, pre ktoré platí

$$a_n < \frac{a_0 + a_1 + \cdots + a_n}{n} \leq a_{n+1}.$$

(IMO 2014 P1)

Úloha 31. Postupnosť prirodzených čísel $\{a_n\}_{n=1}^{\infty}$ obsahuje všetky prirodzené čísla aspoň raz. Pre každé dve rôzne prirodzené čísla m, n postupnosť spĺňa

$$\frac{1}{1998} < \left|\frac{a_n - a_m}{n - m}\right| < 1998.$$

Dokážte, že $|a_n - n| < 2000000$ pre všetky prirodzené n. (Rusko MO 1999)

Ťažšie a zaujímavé úlohy

Úloha 32. Postupnosť $x_1, x_2, \ldots$ je definovaná ako $x_1 = 1$ a $x_{2k} = -x_k$, $x_{2k+1} = (-1)^{k+1} x_k$ pre $k \geq 1$. Dokážte, že

$$x_1 + x_2 + \cdots + x_n \geq 0$$

pre všetky $n \geq 1$. (ISL 2010 A4)

Úloha 33. Predpokladajme, že postupnosti $a_0, a_1, \ldots, a_{2n}$ a $b_0, b_1, \ldots, b_{2n}$ reálnych čísel spĺňajú nasledujúce podmienky:

(i) $a_i + a_{i+1} \geq 0$ pre $0 \leq i \leq 2n - 1$,

(ii) $a_{2j+1} \leq 0$ pre $0 \leq j \leq n - 1$,

(iii) $\sum_{k=2p}^{2q} b_k \geq 0$ pre všetky $0 \leq p \leq q \leq n$.

Dokážte, že $\sum_{i=0}^{2n}(-1)^i a_i b_i \geq 0$ a zistite, kedy nastáva rovnosť. (Čína TST 2010)

Úloha 34. Pre prirodzené n máme danú postupnosť $\varepsilon_1, \ldots, \varepsilon_{n-1}$, kde $\varepsilon_i = 0$ alebo $\varepsilon_i = 1$. Ďalej sú dané postupnosti $a_0, \ldots, a_n$, $b_0, \ldots, b_n$ spĺňajúce $a_0 = b_0 = 1$, $a_1 = b_1 = 7$,

$$a_{i+1} = \begin{cases} 2a_{i-1} + 3a_i, & \text{ak } \varepsilon_i = 0, \\ 3a_{i-1} + a_i, & \text{ak } \varepsilon_i = 1, \end{cases} \qquad \text{pre všetky } i = 1, \ldots, n-1,$$

$$b_{i+1} = \begin{cases} 2b_{i-1} + 3b_i, & \text{ak } \varepsilon_{n-i} = 0, \\ 3b_{i-1} + b_i, & \text{ak } \varepsilon_{n-i} = 1, \end{cases} \qquad \text{pre všetky } i = 1, \ldots, n-1.$$

Dokážte $a_n = b_n$. (ISL 2009 C3)

Úloha 35. Nech $a_1, a_2, \ldots$ je postupnosť reálnych čísel a s je prirodzené číslo, pričom platí

$$a_n = \max\{a_k + a_{n-k} \mid 1 \leq k \leq n-1\} \quad \text{pre všetky } n > s.$$

Ukážte, že existujú prirodzené čísla $l \leq s$ a N také, že $a_n = a_l + a_{n-l}$ pre všetky $n \geq N$. (IMO 2010 P6)

Úloha 36. Predpokladajme, že $s_1, s_2, s_3, \ldots$ je rastúca postupnosť prirodzených čísel, ktorej podpostupnosti

$$s_{s_1}, s_{s_2}, s_{s_3}, \ldots \qquad \text{aj} \qquad s_{s_1+1}, s_{s_2+1}, s_{s_3+1}, \ldots$$

sú obe aritmetické postupnosti. Dokážte, že postupnosť $s_1, s_2, s_3, \ldots$ je sama o sebe aritmetická postupnosť. (IMO 2009 P3)

Literatura a zdroje

[1] Alexander Remorov; *Sequences*, Winter Camp 2012, `http://alexanderrem.weebly.com/uploads/7/2/5/6/72566533/sequences.pdf`

[2] Kin Y. Li; *Mathematical Excalibur Vol.18 No.3 – Sequences*, `https://www.math.ust.hk/excalibur/v18_n3.pdf`

[3] Kin Y. Li; *Mathematical Excalibur Vol.20 No.4 – Inequalities of Sequences*, `https://www.math.ust.hk/excalibur/v20_n4.pdf`

[4] Po-Shen Loh; *VII. Sequences*, Winter Camp 2012, `https://www.math.cmu.edu/~ploh/docs/math/7-sequences-solns.pdf`

[5] Arkady M. Alt; *Math Olympiads Training Problems*

[6] Anca Mustata; *Algebra - Sequences*, IMO Training Camp 2017, `https://euclid.ucc.ie/ mathenr/IMOTraining/2017JuneCamp/2017JuneAlgebraSequencesAnca.pdf`

[7] Anca Mustata; *Algebra: Sequences and Functions Tips and Tricks*, `https://euclid.ucc.ie/mathenr/IMOTraining/Anca%20Notes/Algebra/AlgebraSequences.pdf`

Hinty

Hint 1. Vyjadrite n-tý člen explicitne.
Hint 2. Uvažujte postupnosť prevrátených hodnôt. (Dokonca je to „známa“ Sylvestrova postupnosť.)
Hint 3. Z nerovnosti v zadaní odhadnite člen a_k nejakým výrazom tak, aby sa dala použiť teleskopická suma.
Hint 4. Zoberme si dve po sebe idúce rekurencie zo zadania a chceli by sme sa nejako zbaviť jediného záporného člena a_0.
Hint 5. Skombinovať postupnosti / zadefinovať si jednoduchšie post. Je výhodné mať rovnaké menovatele.
Hint 6. $\frac{1}{a_{k-1}} - \frac{1}{a_k} = ?$
Hint 7. Vyjadriť konštantu 5 dvomi spôsobmi, porovnať a upraviť do vhodného tvaru pre získanie jednoduchšej rekurencie.
Hint 8. Zoberme postupnosť m-iek, tipnime rekurenciu a dokážme indukciou.
Hint 9. Rovnako ako úloha 7.
Hint 10. Výraz pod odmocninou vyjadríme pomocou predchádzajúceho člena.
Hint 11. Výraz pod odmocninou vyjadríme pomocou predchádzajúcich členov. Iný postup: rovnicu prenásobíme vhodným členom.
Hint 12. Zbaviť sa odmocniny, deliteľnosť.
Hint 13. Abelova sumácia.
Hint 14. Abelova sumácia + Cauchy-Schwarzova nerovnosť.
Hint 15. Označme $n = km + r$, využite $a_{pq} \leq pa_q$.
Hint 16. Prenásobme km, potom indukcia trebárs na súčet $k + m$.
Hint 17. Uvažujte postupnosť diferencií. Môže sa hodiť $\frac{k^2}{2} \leq \frac{k(k+1)}{2} = 1 + 2 + \cdots + k$.
Hint 21. $a_{np} \approx pa_n$.
Hint 22. Ako vyzerá a_{n+2}, keď je post. rastúca?
Hint 23. Čo sa stane, keď zväčšíme niektorý člen o 1?
Hint 24. Čo sa stane, keď sa niektoré dva členy zo začiatku postupnosti líšia o veľa?
Hint 25. Pomôže dvojnásobné použitie rekurencie. Pre jednoduchšiu prácu je vhodné zadefinovať mierne inú postupnosť.
Hint 26. Uvažujte postupnosť $\lfloor a_n \rfloor$, následne post. $\{a_n\}$.
Hint 27. Stačí nájsť tak, aby platilo $|a_m - a_n| \geq \frac{c}{m-n}$ pre ľubovoľnú konštantu c: Aritmetická s diferenciou $\sqrt{2}$.
Hint 28. Dokážte, že je periodická.
Hint 29. Čo zač je vlastne d?
Hint 30. Pozrite sa na $\sum_{k=0}^{n} a_k - na_n$.
Hint 31. Dokážte, že ak $m > n$ a $a_m \leq a_n$, tak $m - n < 2000000$.
Hint 32. Zosumujte prvých $4k$ členov, potom použite indukčný predpoklad.
Hint 33. Predefinujte si a-čka na kladné. Použiť Abelovu sumáciu na prvých k členov + silná indukcia. Iný prístup: modifikovať postupnosť a-čiek pomocou najmenšieho + silná indukcia.
Hint 34. Chceli by sme vzťah medzi a-čkami a b-čkami bez ε. Máme dve rovnice, takže jednej premennej sa vieme zbaviť. Potom teleskopicky sčítať a ono to vyjde.

Hint 35. Uvažujme postupnosť $b_n = a_n - n\frac{a_l}{l}$, ktorá spĺňa pôvodnú rekurenciu. Jej podpostupnosti $\{b_{kl+r}\}$ sú záporné, neklesajúce, a preto nadobúdajú len konečne veľa hodnôt.
Hint 36. Dokážte, že postupnosť diferencií je konštantná, lebo je ohraničená a maximum sa rovná minimu.

Kruté vety v teórii čísel

Michal Staník

Abstrakt. V príspevku preberieme niekoľko ťažkých tvrdení z teórie čísel a ukážeme si niekoľko úloh, v ktorých sa dajú použiť. Budeme sa zaoberať Betrandovým postulátom, Dirichletovou, Zsigmondyho a Mihailescovou vetou.

Príspevok je kópiou príspevku od Rada Švarca z roku 2016. Týmto mu ďakujem za umožnenie jeho použitia.

Bertrandov postulát

Veta (Bertrandov postulát). Pre každé prirodzené $n > 1$ existuje prvočíslo p také, že $n < p < 2n$.

Úloha 1. Ukážte, že ak p_i označuje i-té prvočíslo, potom

$$\frac{p_n + p_{n+2}}{p_{n+1}} > \frac{3}{2}.$$

Úloha 2. Ako *pekné* číslo nazveme také prirodzené n, že vždy, keď pre prirodzené m platí $1 < m < n$ a $(m, n) = 1$, potom m je prvočíslo. Nájdite všetky pekné čísla.

(Estónsko TST 1997)

Úloha 3. Nájdite všetky n, pre ktoré je $n!$ druhou mocninou celého čísla.

Úloha 4. Existuje n také, že pre všetky $t \geq n$ platí, že medzi t a t^2 leží aspoň 2020 prvočísel?

Úloha 5. Dokážte, že každé prirodzené číslo sa dá zapísať ako súčet navzájom rôznych nezložených čísel.

Úloha 6. Dokážte, že čísla v množine $\{1, 2, \ldots, 2n\}$ vieme popárovať tak, že súčet každého páru je prvočíslo.

Úloha 7. Nech

$$a_n = \sum_{i=n}^{2n} \frac{(2i+1)^n}{i}.$$

Ukážte, že a_n nikdy nie je celé číslo.

Úloha 8. Nájdite všetky prirodzené n, pre ktoré je počet kladných deliteľov čísla $[1, 2, \ldots, n]$ mocninou dvojky. (Estónsko TST 2004)

Úloha 9. Určite všetky prirodzené k, pre ktoré existuje nekonečne mnoho prirodzených n takých, že

$$n + k \nmid \binom{2n}{n}.$$

(Čína 2015)

Úloha 10. Určite všetky prirodzené x, y, pre ktoré platí

$$x! + y! = x^y.$$

(MEMO 2007)

Úloha 11. Nech F_i je i-té Fibonacciho číslo (začínajúce $F_1 = F_2 = 1$). Nech

$$a_n = \left\lfloor \sum_{i=1}^{n} \sqrt{F_i} \right\rfloor \qquad \text{a} \qquad b_n = \left\lfloor \sum_{i=1}^{n} \sqrt{p_i} \right\rfloor.$$

Ukážte, že $a_n = b_n$ len pre konečne mnoho hodnôt n.

Dirichletova veta

Veta (Dirichletova veta). Ak a je prirodzené číslo, b celé číslo a $(a, b) = 1$, potom je v aritmetickej postupnosti $an + b$ nekonečne mnoho prvočísel.

Úloha 12. Existujú prirodzené čísla a a b také, že kedykoľvek sú p a q rôzne prvočísla väčšie než 1000, potom aj $ap + bq$ je prvočíslo? (Peterburg 1996)

Úloha 13. Nech S je množina všetkých prevrátených hodnôt prirodzených čísel. Potom pre každé $k > 2$ ukážte, že v S existuje k-členná nekonštantná aritmetická postupnosť taká, že k nej nevieme pridať žiadny ďalší prvok z S tak, aby postupnosť zostala aritmetická. (Veľká Británia 1997)

Úloha 14. Dokážte, že ak s, a a b sú prirodzené čísla a $(a, b) = 1$, potom existuje nekonečne mnoho n takých, že $an + b$ je súčinom s rôznych prvočísel.

Úloha 15. Nech m je kladné nepárne číslo. Ukážte, že existuje nekonečne veľa kladných n takých, že $mn + 1 \mid 2^n - 1$. (Mongolsko TST 2008)

Úloha 16. Pre každé prirodzené n ukážte, že existuje prirodzené k také, že

$$p_{k-1} < p_k - n < p_k + n < p_{k+1}.$$

(AMM E4772)

Úloha 17. Nájdite všetky polynómy $P(x)$ s racionálnymi koeficientami také, že ak p je prvočíslo, potom aj $P(p)$ je prvočíslo. (AMM E1632)

Úloha 18. Nájdite všetky polynómy $P(x)$ s celočíselnými koeficientami také, že ak p a q sú rôzne prvočísla, potom $P(p)$ a $P(q)$ sú nesúdeliteľné čísla. (Mathematical Reflection O318)

Úloha 19. Dokážte, že pre každú dvojicu prirodzených čísel m, n existuje prirodzené k také, že všetky čísla $\varphi(k), \varphi(k+1), \ldots, \varphi(k+m)$ sú deliteľné n. (AMM E4524)

Úloha 20. Dokážte, že existuje nekonečná množina S po dvoch nesúdeliteľných prirodzených čísel taká, že pre ľubovoľné $n \in S$ neexistuje žiadna trojica nenulových celých čísel x, y, z taká, že $(n, xyz) = 1$ a $x^n + y^n + z^n = 0$. (AMM 1978)

Úloha 21. Ukážte, že existuje nekonečne veľa prirodzených čísel n takých, že číslo $n^4 + 1$ má prvočíselného deliteľa väčšieho než $2n$. (MKS 30–2–8)

Úloha 22. Ukážte, že existuje nekonečne veľa prirodzených čísel n takých, že číslo $n^2 + 1$ má prvočíselného deliteľa väčšieho než $2n + \sqrt{2n}$. (IMO 2008)

Zsigmondyho veta

Veta (Zsigmondyho veta). Nech $a > b$ sú nesúdeliteľné prirodzené čísla. Ak $n > 1$, potom:

- Existuje prvočíslo p také, že $p \mid a^n - b^n$ a pre $1 \leq i < n$ platí $p \nmid a^i - b^i$. Výnimkou sú prípady $(a, b, n) = (2, 1, 6)$ a $(a, b, n) = (a, 2^k - a, 2)$ pre nejaké prirodzené k.
- Existuje prvočíslo q také, že $q \mid a^n + b^n$ a pre $1 \leq i < n$ platí $q \nmid a^i + b^i$. Výnimkou je prípad $(a, b, n) = (2, 1, 3)$.

Urobme dohodu – ak sa v hinte objaví niečo, čo s úlohou absolútne nesúvisí, znamená to, že príklad sa dá vyriešiť len triviálnou aplikáciou veta a hint by teda znel jedine „proste priamočiaro použi vetu".

Úloha 23. Ukážte, že postupnosť $a_n = 3^n - 2^n$ neobsahuje tri členy tvoriace geometrickú postupnosť. (Rumunsko TST 1994)

Úloha 24. Nájdite všetky trojice prirodzených čísel (a, b, p), kde p je prvočíslo a $2^a + p^b = 19^a$. (Taliansko TST 2003)

Úloha 25. Nájdite všetky dvojice prirodzených čísel (a, n) také, že vždy, keď prvočíslo p delí $a^n - 1$, existuje prirodzené $m < n$ také, že $p \mid a^m - 1$. (USA TST 2012)

Úloha 26. Nájdite všetky nezáporné celé riešenia rovnice $3^m - 5^n = a^2$.

Úloha 27. Nájdite všetky nezáporné celé riešenia rovnice $5^m - 3^n = a^2$. (Balkán 2009)

Úloha 28. Nech $p < q$ sú nepárne prvočísla. Dokážte, že $2^{pq} - 1$ má aspoň tri rôzne prvočíselné delitele. (Poľsko 2010)

Úloha 29. Nájdite všetky dvojice prirodzených čísel (x, y) také, že pre nejaké prvočíslo $p^x - y^p = 1$. (MO 1996)

Úloha 30. Nájdite všetky pätice prirodzených čísel (a, n, p, q, r), pre ktoré platí $a^n - 1 = (a^p - 1)(a^q - 1)(a^r - 1)$. (Japonsko 2011)

Úloha 31. Nájdite všetky trojice prirodzených čísel (a, m, n), pre ktoré platí $a^m + 1 \mid (a+1)^n$. (ISL 2000)

Úloha 32. Nájdite všetky štvorice prirodzených čísel (x, r, p, n), také, že p je prvočíslo, $n, r > 1$ a $x^r - 1 = p^n$. (MOSP 2001)

Úloha 33. Nájdite všetky prirodzené riešenia rovnice

$$(a+1)(a^2+a+1)\dots(a^n+a^{n-1}+\dots+1) = a^m + a^{m-1} + \dots + 1.$$

Úloha 34. Nech $b, m, n \in \mathbb{N}$, $b > 1$ a $m \neq n$. Predpokladajme, že $b^m - 1$ a $b^n - 1$ majú rovnaké množiny prvočíselných deliteľov. Ukážte, že $b+1$ je mocninou dvojky. (ISL 1997, Čína TST 2005)

Úloha 35. Nech A je konečná množina prvočísel a $a > 1$ prirodzené číslo. Ukážte, že existuje iba konečne veľa prirodzených n takých, že všetky prvočíselné delitele čísla $a^n - 1$ ležia v A. (Problems from the Book)

Úloha 36. Nájdite všetky šestice prirodzených čísel (a, b, c, p, q, r), také, že p, q, r sú prvočísla a $p^{2a} = q^b r^c + 1$. (Srbsko TST 1977)

Úloha 37. Nájdite všetky prirodzené n, pre ktoré majú n a $2^n + 1$ rovnakú množinu prvočíselných deliteľov. (iKS 3–3)

Úloha 38. Patrik miluje prvočísla. Niektoré miluje veľmi, iné viac, ale má niekoľko prvočísel, ktoré miluje najviac. Všetky tieto prvočísla si schoval do konečnej neprázdnej množiny P. K narodeninám by si od vás prial také prirodzené číslo n, ktoré sa dá zapísať ako $a^p + b^p$ pre nejaké $a, b \in \mathbb{N}$ (kde p je prvočíslo) práve vtedy, keď $p \in P$. Rozhodnite, či môžete jeho prianie splniť pre každú množinu P. (iKS 5–3)

Mihailescova veta

Veta (Mihailescova veta). Ak pre prirodzené čísla a, b, m, n platí $a^m - b^n = 1$, potom $m = 1$ alebo $n = 1$, alebo $(a, b, m, n) = (3, 2, 2, 3)$.

Úloha 39. Ukážte, že $n^7 + 1$ nikdy nie je štvorec. (India TST)

Úloha 40. Prirodzené čísla $x > 2$, $y > 1$ a z spĺňajú rovnicu $x^y + 1 = z^2$. Nech p, resp. q je počet rôznych prvočíselných deliteľov x, resp. y. Ukážte, že potom $p \geq q+2$. (Rusko 2005)

Úloha 41. Nájdite všetky dvojice prirodzených čísel (x, y) také, že pre nejaké prvočíslo $p^x - y^p = 1$. (MO 1996)

Úloha 42. Nájdite všetky štvorice prirodzených čísel (x, r, p, n), také, že p je prvočíslo, $n, r > 1$ a $x^r - 1 = p^n$. (MOSP 2001)

Úloha 43. Koľko najmenej rôznych prvočíselných deliteľov môže mať výraz $19^{4n}+4$ pre $n \geq 1$? (Turecko juniori 2014)

Úloha 44. Nájdite všetky prvočísla p také, že $p(2^{p-1}-1) = a^k$ pre nejaké prirodzené a a $k > 1$. (iKS 2–1)

Literatúra a zdroje

[1] Rado van Švarc; *Kruté věty v N*, *i*KS 2016
[2] *Art of Problem Solving*, `https://artofproblemsolving.com/community`

Hinty

Hint 1. Vynásobte dvomi a použite Bertranda.
Hint 2. Ukážte, že pre $i \geq 4$ je $p_1 p_2 \cdots p_i > p_{i+1}^2$.
Hint 3. Uvážte p medzi $\frac{n}{2}$ a n.
Hint 4. $n = 2^{2020}$.
Hint 5. Indukcia.
Hint 6. Indukcia.
Hint 7. Preveďte na spoločného menovateľa.
Hint 8. Vadí nám, keď je tam nejaké prvočíslo dvakrát.
Hint 9. Pre $k > 1$ nájdeme prvočíslo p, také, že $k < p < 2k$ a volíme $n = p^i + p - k$.
Hint 10. Keď $x > y$, zvoľ prvočíslo medzi $\frac{x}{2}$ a x.
Hint 11. $p_{i+2} < p_{i+1} + p_i$.
Hint 12. Hľadajte prvočísla s rozdielom, ktorý je násobkom $a + b$.
Hint 13. Nech $a_1 = \frac{1}{(kn)!}$ a $d = \frac{n}{(kn)!}$.
Hint 14. Indukcia.
Hint 15. Zvoľte dostatočne vysoké prvočíslo $p = \varphi(m)k + 1$ a potom $n = \frac{2^p - 2}{m}$.
Hint 16. Zvoľte prvočíslo $p \equiv (q-1)! - 1 \pmod{q!}$, kde q je dosť veľké prvočíslo.
Hint 17. Nech $Q(x)$ je $P(x)$ prenásobený tak, že má celočíselné koeficienty. Potom nech $m_i = Q(p)n_i + p$, kde p je prvočíslo také, že $p \nmid Q(p)$.
Hint 18. Zvoľte p veľké, uvážte prvočíslo r také, že $r \mid P(p)$ a vezmite $q = rk + p$.
Hint 19. Uvedomte si, že ak prvočíslo p delí a, potom $p - 1 \mid \varphi(a)$.
Hint 20. Ak už vyberieme čísla $n_1, \ldots, n_k$, vezmeme prvočíslo $p \equiv -1 \pmod{4n_1 n_2 \cdots n_k}$ a pridáme $n_{k+1} = \frac{p(p-1)}{2}$.
Hint 21. Zvoľte $p = 8k + 1$, g ako primitívny prvok modulo p a $n = g^k$.
Hint 22. Zvoľte $p = 20k + 1$, vezmite najmenšie n, ktoré spĺňa $n^2 \equiv -1 \pmod{p}$ a uvážte jeho vzdialenosť od $\frac{p-1}{2}$.
Hint 23. Nech pre $x < y < z$ je $(3^y - 2^y)^2 = (3^x - 2^x)(3^z - 2^z)$ a pozrite sa na prvočísla $3^z - 2^z$.
Hint 24. Americkí vedci zistili, že 21,3857 % štatistík je presnejších, než si môžu dovoliť.
Hint 25. Waterboarding v Guantanamo Bay znie fakt cool, keď ani o jednom z toho neviete, čo to je.
Hint 26. Modulo 4 zistíme, že m je párne. Rozložte rozdiel štvorcov.
Hint 27. Modulo 3 zistíme, že m je párne. Rozložte rozdiel štvorcov.
Hint 28. $2^p - 1 \mid 2^{pq} - 1, \quad 2^q - 1 \mid 2^{pq} - 1$.
Hint 29. Keby som dostal korunu vždy, keď ma dievča považuje za neatraktívneho, mal by som toľko peňazí, že by ma dievčatá považovali za atraktívneho.
Hint 30. V Škótsku žije aspoň jedna ovca, ktorá je biela aspoň z jednej strany.
Hint 31. Štúdia zistila, že ženy, ktoré trpia ľahkou nadváhou, žijú dlhšie než muži, ktorí sa o tom zmienia.
Hint 32. Zmysel pre čierny humor je ako nohy. Niektorí ľudia ich majú, iní nie.
Hint 33. Využite vzorec na výpočet súčtu geometrickej postupnosti.
Hint 34. Aj tie najdlhšie cesty sa začínajú jedným malým krokom. Rovnako sa začína aj pád do priekopy.

Hint 35. Kanadský psychológ predáva za 20 dolárov knihu, ktorá vás naučí, ako otestovať IQ vášho psa. Ak si ju kúpite, váš pes je chytrejší než vy.
Hint 36. $p^a + 1$ a $p^a - 1$ sú (skoro) nesúdeliteľné.
Hint 37. Uvážte prvočíslo p, ktoré delí $2^n + 1$ a využite malú Fermatovu vetu.
Hint 38. Ak S je súčin všetkých prvočísel z P, zvoľte 2^{S+1}.
Hint 39. Pýtal som sa severokórejských matematikov, ako sa im žije v ich domovine. Vraj si nemôžu sťažovať.
Hint 40. Ži každý deň, ako by to bol tvoj posledný. Raz budeš mať pravdu.
Hint 41. Môj dedko má levie srdce a doživotný zákaz vstupu do zoo.
Hint 42. Čo majú spoločné alkoholik a pedofilný nekrofil? Obaja majú radi studenú dvanástku.
Hint 43. $a^4 + 4 = (a^2 - 2a + 2)(a^2 + 2a + 2)$.
Hint 44. Rozlož zátvorku.

Špirálka a Big Picture

Ákos Záhorský

Abstrakt. Príspevok sa zaoberá užitočnou technikou na riešenie geometrických úloh, špirálnou podobnosťou, a tiež nejakými menej známymi, ale silnými geometrickými situáciami ohľadom geometrie trojuholníka. Obsahuje 28 úloh na špirálku všetkých obtiažností a 8 ďalších cvičení o Big Picture.

Úvod do špirálky

Špirálna podobnosť je geometrické zobrazenie, ktoré je zložením otočenia a rovnoľahlosti. Je určená stredom O, orientovaným uhlom ϕ a koeficientom rovnoľahlosti $k > 0$. Zvykne sa označovať $S(O, k, \phi)$.

Pozorovanie.

- Ak $\phi = 0°$, dostávame rovnoľahlosť s koeficientom k.
- Ak $\phi = 180°$, dostávame rovnoľahlosť s koeficientom $-k$.
- Ak $k = 1$, dostávame otočenie dané uhlom ϕ.

Tvrdenie 1. Nech A, B, C, D sú body v rovine také, že $AC \nparallel BD$ a $AB \not\equiv CD$. Nech sa priamky AC a BD pretínajú v X. Nech sa kružnice ABX a CDX pretínajú znova v O. Potom O je stred jednoznačnej špirálnej podobnosti, ktorá zobrazuje AB na CD.

Pozorovanie.

- Ak $A \in CD$ a $A \not\equiv D$, tak stred špirálnej podobnosti zobrazujúcej AB na CA je bod S ležiaci na kružnici opísanej trojuholníku BAD taký, že kružnica opísaná trojuholníku CSD sa dotýka priamky BD.
- Ak $A \equiv D$, tak stred špirálnej podobnosti zobrazujúcej AB na CA je bod O_A taký, že kružnica opísaná trojuholníku COA sa dotýka priamky BA a kružnica opísaná trojuholníku BOA sa dotýka priamky AC.

Tvrdenie 2. Nech špirálna podobnosť so stredom O prevádza AB na CD. Potom O je tiež stred špirálnej podobnosti, ktorá prevádza AC na BD.

Tvrdenie 3. Je daná špirálna podobnosť $S(O, k, \phi)$ taká, že $180° > \phi > 0°$. Potom všetky trojuholníky OXX^O sú si navzájom podobné pre všetky body X, kde X^O značí obraz bodu X podľa $S(O, k, \phi)$

Tvrdenie 4. Je daný štvoruholník $ABCD$ s nerovnobežnými stranami. Nech sa dvojice priamok AB, CD resp. AD, BC pretínajú v bodoch P, Q. Potom kružnice opísané trojuholníkom PAD, PBC, QDC, QAB prechádzajú jedným bodom. Tento bod sa nazýva *vonkajší Miquelov bod* štvoruholníka $ABCD$.

(Anti-) Švrček a Big Picture

Značenie. V trojúhelníku ABC označme I střed kružnice vepsané (vepsiště) a I_A, I_B, I_C středy kružnic připsaných (připsiště) příslušející vrcholům A, B, C.

Tvrdenie 5. V trojúhelníku ABC mají osa strany BC, vnitřní osa úhlu CAB a kružnice opsaná společný bod. Tento bod neoficiálně nazýváme *Švrčkův bod* příslušející vrcholu A a značíme jej $\check{S}_A$.

Ukážka. Nechť ABC je ostroúhlý trojúhelník, ve kterém $AB \neq AC$. Kružnice nad průměrem BC protíná strany AB a AC postupně v bodech M a N. Označme jako O střed strany BC. Vnitřní osy úhlů BAC a MON se protínají v R. Dokažte, že se kružnice opsané trojúhelníkům BMR a CNR podruhé protínají na straně BC

Cvičenie 6. Nechť AL a BK jsou vnitřní osy úhlů v různostranném trojúhelníku ABC, kde L leží na straně BC a K na straně AC. Osa úsečky BK protíná přímku AL v M. Bod N je zvolen na přímce BK tak, že $LN \parallel MK$. Ukažte, že $LN = NA$. (Junior Balkan 2010)

Tvrdenie 7. V trojúhelníku ABC je $BICI_A$ tětivový čtyřúhelník a příslušná kružnice má střed v $\check{S}_A$.

Ukážka. Buď ABC trojúhelník s vepsištěm I. Bod P uvnitř tohoto trojúhelníku splňuje vztah $\angle PBA + \angle PCA = \angle PBC + \angle PCB$. Ukažte, že $AP \geq AI$, přičemž rovnost nastává právě tehdy, když $P = I$.

Cvičenie 8. Buď BC průměr kružnice ω se středem v O. Nechť A je bod na ω takový, že $\angle AOB < 120°$. Buď D střed toho oblouku AB, který neobsahuje C. Dále přímka vedená skrze O rovnoběžná s DA protíná AC v I a osa úsečky OA protíná ω v bodech E a F. Dokažte, že I je vepsiště trojuholníka CEF.

Cvičenie 9. Buď $ABCD$ tětivový čtyřúhelník. Ukažte, že vepsiště trojúhelníků ABC, BCD, CDA, DAB tvoří obdélník. (Japanese theorem)

Tvrdenie 10. V trojúhelníku ABC mají osa strany BC, vnější osa úhlu BAC a kružnice opsaná společný bod, který budeme značit jako $\check{N}_A$. Tento bod neoficiálně (ještě neoficiálněji než Švrčkův bod) nazýváme *antišvrk* příslušející bodu A.

Tvrdenie 11. Pro zadaný trojúhelník ABC je I_CBCI_B tětivový čtyřúhelník se středem v $\check{N}_A$.

Cvičenie 12 (těžké). Buď $ABCD$ tětivový čtyřúhelník. Ukažte, že připsiště trojúhelníků ABC, BCD, CDA, DAB (všech 12 bodů) leží na obvodu jednoho obdélníka.

Tvrdenie 13 (The Big Picture). V trojúhelníku ABC s naším značením platí, že I je kolmiště trojúhelníku $I_AI_BI_C$ a kružnice opsaná ABC je Feuerbachovou kružnicí trojúhelníku $I_AI_BI_C$.

Ukážka. V trojúhelníku ABC platí $AB < BC$. Označme jako M střed AC. Dokažte, že $\angle IMA = \angle I\check{N}_BB$.

Cvičenie 14 (těžší). V trojúhelníku ABC s vepsištěm I označme D, E po řadě průsečíky os vnitřních úhlů u vrcholů A, B se stranami BC, AC. Dále označme P, Q body, ve kterých přímka DE protne kružnici opsanou trojúhelníku ABC. Dokažte, že poloměr kružnice opsané trojúhelníku PIQ je dvakrát větší než poloměr kružnice opsané trojúhelníku ABC.

Tvrdenie 15. Mají-li kružnice k a l mají vnitřní dotyk v bodě T a tětiva AB kružnice k se dotýká kružnice l v bodě U, potom UT je osa úhlu ATB.

Ukážka. Dvě kružnice ω_1 a ω_2 se zvenku dotýkají v bodě T a obě se zevnitř dotýkají kružnice ω postupně v bodech R a S. Nechť Q je druhý průsečík RT s ω. Ukažte, že $\angle QST = 90°$.

Tvrdenie 16 (Shooting lemma). Buď M střed oblouku PQ na kružnici ω a nechť přímka p procházející M protíná přímku PQ v X a ω v Y. Potom platí

(1) $MX \cdot MY = MP^2$,
(2) pokud je I vepsiště trojuhelníka PYQ, potom $MX \cdot MY = MI^2$,
(3) pokud další přímka p_0 procházející M protíná PQ v X_0 a ω v Y_0, potom X, Y, X_0, Y_0 leží na jedné kružnici.

Ukážka. Kružnice ω_1 a ω_2 se obě zevnitř dotýkají kružnice ω postupně v bodech A a B. Společná tečna ω_1 a ω_2 se jich dotýká postupně v bodech C a D. Ukažte, že $ABDC$ je tětivový čtyřúhelník.

Cvičenie 17. Přímka l protíná kružnici Γ v bodech A, B. Kružnice ω_1 a ω_2 jsou vepsané do stejné úseče určené přímkou l a mají vnější dotyk. Dokažte, že jejich vnitřní společná tečna prochází pevným bodem, pohybují-li se ω_1 a ω_2 ve vymezené úseči.

Cvičenie 18. Nechť kružnice Ω a ω mají vnitřní dotyk v bodě P, přičemž ω leží uvnitř Ω. Buď AB tětiva Ω, která se dotýká ω v bodě C. Průsečík PC s Ω různý od P si označme jako Q. Nechť tečny z bodu Q ke kružnici ω protínají kružnici Ω v bodech R a S. Vepsiště trojúhelníků APB, ARB a ASB si postupně označíme jako I, X a Y. Ukažte, že $\angle PXI + \angle PYI = 90°$.

Cvičenie 19. Buď ABC trojúhelník s kružnicí opsanou Γ, vepsištěm I a bodem D ležícím na straně BC. Buď ω kružnice dotýkající se úsečky AD v bodě F, strany BC bodě E a kružnice Γ v bodě K. Dokažte, že I leží na přímce EF.

Cvičenie 20. Buď ABC trojúhelník s kružnicí opsanou Γ, vepsištěm I a bodem D ležícím na straně BC. Nechť ω_1 a ω_2 jsou kružnice se středy O_1 a O_2, které se obě dotýkají úsečky AD, přímky BC a kružnice Γ. Ukažte, že O_1, O_2 a I leží na jedné přímce.

Úlohy

Úloha 1. Buď AB tětiva kružnice k a S její střed. Vedeme bodem S libovolné další dvě tětivy KL, MN této kružnice, aby KM nebylo rovnoběžné s AB. Průsečíky přímky AB s přímkami KM, LN označme postupně X, Y. Dokažte, že S je středem XY. (Butterfly Theorem)

Úloha 2. Kružnice k, l sa pretínajú v bodoch A, B. Bodom A sa otáča priamka, ktorá pretína kružnicu k znova v bode K a kružnicu l znova v bode L. Akú množinu vykresľuje stred úsečky KL? A čo množina bodov N ležiacich na KL takých, že $KN = 2 \cdot NL$?

Úloha 3. Po troch rôznobežných priamkach sa rovnomerne pohybujú body A, B, C. Dokážte, že ak sú v dvoch rôznych časoch trojuholníky ABC podobné, tak potom sú podobné v každom okamihu.

Úloha 4. Je daný konvexný štvoruholník $ABCD$. Označme M_1, resp. M_2 stredy špirálnych podobností, ktoré zobrazujú AB na CD, resp. AC na DB (zvané aj ako *vnútorné Miquelove body*). Pre každý z týchto stredov nájdite štyri kružnice prechádzajúce vrcholmi A, B, C, D a jedným z priesečníkov priamok AB, CD, AC, BD alebo AD, BD.

Úloha 5. V rovine sú dané štvorce $ABCD$ a $A_0B_0C_0D_0$ značené proti smeru hodinových ručičiek. Označme A_1 stred úsečky AA_0 a B_1, C_1, D_1 analogicky. Dokážte, že $A_1B_1C_1D_1$ je štvorec.

Úloha 6. Štvorce $ABCD$ a $A_1B_1C_1D_1$ reprezentujú mapy rovnakej oblasti, nakreslené v rôznych mierkach, ležiace jedna na druhej. Dokážte, že existuje práve jeden bod O na menšej mape, ktorý leží presne nad bodom O_1 na väčšej mape tak, že body O a O_1 reprezentujú rovnaký bod krajiny. Taktiež popíšte konštrukciu tohto bodu pomocou pravítka a kružidla.

Úloha 7. Nech $ABCD$ je tetivový štvoruholník. Dokážte, že päty kolmíc z D postupne na priamky AB, AC, BC ležia na priamke. Táto priamka sa nazýva *Simsonova* vzhľadom k trojuholníku ABC k bodu D.

Úloha 8. V trojuholníku ABC platí $\angle BAC = 60^\circ$. Bod O leží vnútri ABC tak, že $\angle AOB = \angle BOC = \angle COA$. Body D, E sú stredy strán AB, AC. Dokážte, že body A, D, O, E ležia na kružnici.

Úloha 9. Nech ABC je ostrouhlý trojuholník s výškou AD. Body X, Y ležia po rade na kružniciach opísaných trojuholníkom ABD, ACD tak, že X, D, Y ležia na priamke a $X \not\equiv D$, $Y \not\equiv B$. Označme ďalej M stred strany BC a M_0 stred úsečky XY. Dokážte, že priamky MM_0 a AM_0 sú na seba kolmé.

Úloha 10. Je daný trojuholník ABC. Označme D druhý priesečník kružnice, ktorá sa dotýka strany AB v bode A a prechádza bodom C, a kružnice, ktorá sa dotýka strany AC v bode A a prechádza bodom B. Označme E ten bod polpriamky AB, pre ktorý $AE = 2 \cdot AB$, a F ten bod polpriamky CA, pre ktorý $CF = 2 \cdot CA$. Dokážte, že A, D, E, F ležia na jednej kružnici.

Úloha 11. Je daný trojuholník ABC. Mimo neho zostrojíme obdĺžniky $ABKL$ a $ACMN$ tak, že $BK = AC$ a $CM = AB$. Dokážte, že priamky BN, CL a KM prechádzajú jedným bodom.

Úloha 12. Trojuholník ABC je rovnostranný. M je bod na strane AB a P je bod na strane CB tak, že $MP \parallel AC$. D je ťažisko MBP a E je stred PA. Nájdite uhly trojuholníka DEC.

Úloha 13. Nech $ABCD$ je konvexný štvoruholník a E, F nech sú body na stranách AD, BC také, že $\frac{AE}{ED} = \frac{BF}{FC}$. Polpriamka FE pretína polpriamky BA a CD v S a T. Dokážte, že kružnice opísané trojuholníkom SAE, SBF, TCF a TDE prechádzajú spoločným bodom.

Úloha 14. Nech $ABCDE$ je konvexný päťuholník taký, že $\angle BAC = \angle CAD = \angle DAE$ a $\angle CBA = \angle DCA = \angle EDA$. Uhlopriečky BD a CE sa pretínajú v P. Dokážte, že priamka AP rozpoľuje stranu CD.

Úloha 15. Konvexný štvoruholník $ABCD$ je vpísaný do kružnice so stredom O. Uhlopriečky AC a BD sa pretínajú v P. Kružnice opísané trojuholníkom ABP a CDP sa pretínajú v bodoch P a Q. Predpokladajme, že O, P a Q sú rôzne body. Dokážte, že $\angle OQP = 90°$.

Úloha 16. Nech $ABCD$ je daný konvexný štvoruholník s rovnako dlhými nerovnobežnými stranami BC a AD. Nech E, F sú vnútorné body strán BC a AD také, že $BE = DF$. Priamky AC a BD sa pretínajú v P, priamky BD a EF v Q a priamky EF a AC v R. Uvážme všetky trojuholníky PQR pri meniacej sa polohe bodov E, F. Dokážte, že kružnice opísané týmto trojuhlníkom majú spoločný bod rôzny od P.

Úloha 17. Nech ABA_0B_0 je konvexný štvoruholník, v ktorom sa AA_0 pretína s BB_0 v S. Nech T je druhý priesečník kružníc ABS a A_0B_0S. Nech C, C_0 sú body na úsečkách AB, A_0B_0. Nech K a L sú body na úsečkách SB a SA_0 také, že K, B, C, T sú na kružnici a A_0, C_0, T, L tiež. Dokážte, že body C, C_0, K, L sú kolineárne práve vtedy, keď $\frac{CA}{BC} = \frac{C_0A_0}{C_0B_0}$.

Úloha 18. Kružnice S_1 a S_2 sa pretínajú v bodoch P a Q. Rôzne body A_1, B_1 (rôzne aj od P a Q) sú zvolené na S_1. Priamky A_1P, B_1P pretínajú S_2 znova v A_2, B_2 a priamky A_1B_1, A_2B_2 sa pretínajú v C. Dokážte, že s meniacimi sa bodmi A_1, B_1 stredy kružníc opísaných trojuholníkom A_1A_2C ležia na fixnej kružnici.

Úloha 19. Daný je konvexný štvoruholník $ABCD$, pričom $\angle ABC = \angle ADC = 135°$. Na polpriamkach AB, AD sú postupne zvolené body M, N také, že $\angle MCD = \angle NCB = 90°$. Kružnice opísané trojuholníkom AMN a ABD sa druhýkrát pretnú v bode $K \not\equiv A$. Dokážte, že priamky AK a KC sú navzájom kolmé.

Úloha 20. Body P, Q ležia na uhlopriečkach AC a BD štvoruholníka $ABCD$ tak, že $\frac{AP}{AC} + \frac{BQ}{BD} = 1$. Priamka PQ pretína strany AD a BC v bodoch M a N. Dokážte, že kružnice opísané trojuholníkom AMP, BNQ, DMQ, a CNP majú spoločný bod.

Úloha 21. Nech $ABCD$ je konvexný štvoruholník. Uhlopriečky AC a BD sa pretínajú v P. Nech O_1 a O_2 sú stredy kružníc opísaných trojuholníkom APD a BPC. Nech M, N a O sú stredy AC, BD a O_1O_2. Dokážte, že O je stred kružnice opísanej trojuholníku MPN.

Úloha 22. K stranám konvexného štvoruholníka $ABCD$ pripíšeme zvonku podobné trojuholníky ABW, BCX, CDY, DAZ. Dokážte, že $WXYZ$ je rovnobežník.

Úloha 23. V konvexnom štvoruholníku $ABCD$ sú uhlopriečky rovnako dlhé. Dokážte, že ak zvonku každej strany pripíšeme rovnostranný trojuholník, tak spojnice dopísaných vrcholov týchto trojuholníkov sú na seba kolmé.

Úloha 24. V ostrouhlom trojuholníku ABC sú úsečky AD, BE, CF výšky a H je ortocentrum. Kružnica ω so stredom v O prechádza bodmi A, H a pretína strany AB, AC znova v Q, P. Nech sa kružnica opísaná trojuholníku OPQ dotýka BC v R. Dokážte, že $\frac{CR}{BR} = \frac{ED}{FD}$.

Úloha 25. Nech $ABCD$ je konvexný štvoruholník taký, že $AB \nparallel CD$ a nech X je bod vnútri $ABCD$ taký, že $\angle ADX = \angle BCX < 90°$ a $\angle DAX = \angle CBX < 90°$. Ak sa osi úsečiek AB a CD pretínajú v bode Y, tak dokážte, že $\angle AYB = 2 \cdot \angle ADX$.

Úloha 26. Body A_1, B_1 a C_1 sú zvolené na stranách BC, CA a AB trojuholníka ABC. Kružnice opísané trojuholníkom AB_1C_1, BC_1A_1 a CA_1B_1 pretínajú kružnicu opísanú trojuholníku ABC znova v bodoch A_2, B_2 a C_2. Body A_3, B_3 a C_3 sú obrazy A_1, B_1 a C_1 v stredových súmernostiach podľa stredov strán BC, CA a AB. Dokážte, že trojuholníky $A_2B_2C_2$ a $A_3B_3C_3$ sú podobné.

Úloha 27. Nech $A_1B_1C_1$ a $A_2B_2C_2$ sú trojuholníky také, že A_1A_2, B_1B_2, C_1C_2 sa pretínajú v bode S. Nech C_3 je stred špirálnej podobnosti, ktorá zobrazuje A_1B_1 na A_2B_2. Analogicky definujeme A_3 a B_3. Dokážte, že body A_3, B_3, C_3, S ležia na kružnici.

Úloha 28. Nech ABC je trojuholník s kružnicou opísanou k a nech je P ľubovoľný bod. Priamky PA, PB, PC pretínajú k znova v bodoch D, E, F. Trojuholník XYZ je obraz trojuholníka DEF v špirálnej podobnosti so stredom v bode P. Priamky prechádzajúce X, Y, Z a kolmé na PA, PB, PC pretínajú BC, CA, AB v bodoch K, L, M. Dokážte, že body K, L, M ležia na jednej priamke.

Literatura a zdroje

[1] Patrik Bak; *Špirálna podobnosť*, Sborník *i*KS 2016
[2] David Hruška, Rado van Schwarz; *Geometrie trojuhelníka*, PraSečí seriál, 2016/2017

Hinty

Hint 1. (projektivní) BÚNO AB je průměr (je třeba si zachovat poměry na této přímce).
Hint 2. Všimnime si, že všetky trojuholníky BKL sú podobné. Použite tvrdenie 3. Iná možnosť je nakresliť si tam ešte inú úsečku K_0, L_0 a pozrieť sa, akú konfiguráciu máme.
Hint 3. Označme trojuholníky v tých okamihoch ako ABC, $A_0B_0C_0$. Uvážte stred O špirálnej podobnosti, ktorá zobrazuje ABC na $A_0B_0C_0$.
Hint 4. Skombinujte tvrdenia 1 a 2 rovnako ako pri dôkaze tvrdenia 4.
Hint 5. Uvážme stred O špirálnej podobnosti, ktorá tieto štvorce na seba prevádza.
Hint 6. Nie je hľadaný bod stredom špirálnej podobnosti prevádzajúcej tieto štvorce na seba? Nezabudnite si rozmysliet', kde leží.
Hint 7. Uvážte na AC bod S taký, že $DAP \sim DSQ \sim DCR$.
Hint 8. Podobá sa to na známu konfiguráciu. Cez úsekový uhol nahliadnite, že je to naozaj ona.
Hint 9. Známa konfigurácia. A je stredom špirálnej podobnosti, ktorá na seba všeličo zobrazuje. Ako to spojiť so stredmi BC a XY?
Hint 10. Máme známu konfiguráciu, D je stred špirálnej podobnosti zobrazujúcej AB na CA. Čo ešte kam zobrazuje?
Hint 11. Všimnime si, že bod A je stredom špirálnej podobnosti, ktorá na seba prevádza uvažované podobné obdĺžniky. Spomeňte si, ako sa konštruuje.
Hint 12. Očividne si musíme dodefinovať nejaké tie body. Uvážme stredy BP a MP, ozn. ich napr. Q, R. Zrejme sú koolineárne s E. Skúste z nich niečo vykúzliť.
Hint 13. Nie je ten spoločný bod náhodou stred nejakej špirálnej podobnosti? Skúste uvážiť tú vhodnú, ktorá využije najviac informácií zo zadania.
Hint 14. Všimnite si, že A je stredom nejakej (nie jednej) špirálnej podobnosti. Ako by ste spätne zostrojili stred vhodnej z nich?
Hint 15. Q je zjavne stred istých špirálnych podobností. To by sme chceli využiť. Uvážte na AD, BC také body, aby to pripomínalo už videné konfigurácie a samozrejme aby tieto body mali niečo spoločné s O.
Hint 16. Nie je ten spoločný bod náhodou stred nejakej špirálnej podobnosti? Zamyslite sa nad touto možnosťou s prihladnutím na fakt, že A, F, D ležia na priamke v rovnakom pomere ako C, E, B.
Hint 17. T je stred určitej špirálnej podobnosti. Tá generuje podobné trojuholníky.
Hint 18. Pozrite sa dobre na obrázok. Nie je Q náhodou nejaký Miquelov bod? Čo z toho plynie? Skúste zjednodušiť úlohu o nejaké body.
Hint 19. Úloha sa podobá na chcenú konfiguráciu, ale nie je to ono. Skúste niečo definovať na priamkach AD a AB.
Hint 20. Takto napísaná podmienka nič nehovorí. Skúste sa s ňou pohrať, až kým nedostanete tvar, ktorý vám niečo napovie.
Hint 21. Kde sa pretínajú kružnice opísané trojuholníkom APD a BPC, o ktorých stredoch sa v tejto úlohe bavíme? Nie je to náhodou stred nejakej špirálnej podobnosti? Skúste z toho vyťažiť vhodné podobné trojuholníky.
Hint 22. Dokázať, že štvoruholník je rovnobežník, možno napríklad tak, že ukážeme, že uhlopriečky sa navzájom rozpoľujú. Uvážme preto ich stredy. Čo ďalšie sa teraz hodí uvážiť?

Hint 23. Uvážte stred vhodnej špirálnej podobnosti, ktorá nám umožní „spojiť" trojuholníky z opačných strán. Najlepšie tak, aby sme vedeli využiť $AC = BD$.
Hint 24. Nakreslite si dobrý obrázok. Aj keď sa to nezdá, táto konfigurácia je veľmi bohatá. Významnú úlohu, zdá sa, hrá istá špirálna podobnosť so stredom v bode H. Zamyslite sa nad obrazom bodov R, Q, O, P.
Hint 25. Trojuholníky XAD, XCB sú podobné, ale nie tak, aby šla použiť priamo špirálna podobnosť. Nič nie je stratené. Zobrazte bod X osovo podľa BC. Zrazu máme trojuholníky XAD, X_0BC podobné a správne orientované. Označte T špirálnu podobnosť, ktorá prevádza jeden na druhý. Čo možno povedať o stredoch odpovedajúcich úsečiek? Nezabudnite, že rovnaký argument funguje aj na opačnej strane.
Hint 26. Nakreslite si bod A hore. Bod A_2 je zjavne stred akejsi špirálnej podobnosti. Tá generuje podobné trojuholníky. Skúste napísať také podobnosti, aby ste z nich niečo odvodili o C_3, B_3.

Obsah