2002/2003
52. ročník Matematickej olympiády *Riešenia úloh IMO*

---

1. *Nech A je podmnožina množiny $S = \{1, 2, \dots, 1\,000\,000\}$ obsahujúca práve 101 prvkov. Dokážte, že v S existujú čísla $t_1, t_2, \dots, t_{100}$ také, že množiny*

$$A_j = \{x + t_j : x \in A\} \quad \text{pre } j = 1, 2, \dots, 100$$

sú po dvoch disjunktné. (*Brazília*)

Riešenie. Vytvorme množinu všetkých rozdielov $\mathsf{D} = \{x - y : x, y \in \mathsf{A}\}$. Pretože A má 101 prvkov, obsahuje D okrem nuly najviac $2 \cdot \binom{101}{2} = 101 \cdot 100 = 10\,100$ ďalších (kladných aj záporných) čísel. Všimnime si, že dve z uvažovaných množín A_i, A_j sú disjunktné práve vtedy, keď $x + t_i \neq y + t_j$ pre ľubovoľné $x, y \in \mathsf{A}$, teda práve vtedy, keď $t_i - t_j \notin \mathsf{D}$. Našou úlohou je preto vybrať čísla $t_1, t_2, \dots, t_{100} \in \mathsf{S}$ tak, aby žiadny ich rozdiel nepadol do „zakázanej“ množiny D.

Spomenutý výber urobíme induktívne. Prvé číslo t_1 vyberieme z S ľubovoľne. Predpokladajme, že sme už pre niektoré $k \leqq 99$ vybrali čísla $t_1, t_2, \dots, t_k \in \mathsf{S}$ tak, že $t_i - t_j \notin \mathsf{D}$ pre ľubovoľné rôzne $i, j \in \{1, 2, \dots, k\}$ (pre $k = 1$ je to splnené triviálne). Číslo t_{k+1} musíme v S zvoliť tak, aby platilo $t_{k+1} - t_i \notin \mathsf{D}$ pre každé $i \in \{1, 2, \dots, k\}$. Pre pevné i tak má číslo t_{k+1} práve toľko „zakázaných“ hodnôt $t_i + d$, koľko je všetkých čísel $d \in \mathsf{D}$. Tých je, ako vieme, najviac $1 + 101 \cdot 100 = 10\,101$. Pre všetky $i \in \{1, 2, \dots, k\}$ tak celkom dostaneme najviac $k \cdot 10\,101$ zakázaných hodnôt, čo je najviac $99 \cdot 10\,101 = 999\,999$ čísel. V množine S je však 10^6 čísel, takže výber čísla t_{k+1} je možný.

Poznámka. Hodnota $|\mathsf{S}| = 10^6$ je zbytočne veľká (v predchádzajúcom riešení sme zanedbali skutočnosť, že v množine D leží s každým číslom aj číslo opačné). Dá sa ukázať, že pre ľubovoľnú k-prvkovú podmnožinu A množiny $\mathsf{S} = \{1, 2, \dots, n\}$ platí, že ak je m prirodzené číslo také, že

$$n > (m-1)\left(\binom{k}{2} + 1\right),$$

existujú v množine S čísla $t_1, t_2, \dots, t_m$ také, že množiny $\mathsf{A}_j = \{x + t_j : x \in \mathsf{A}\}$ ($j = 1, 2, \dots, m$) sú navzájom disjunktné. (Pre $k = 101$ stačí teda uvažovať množinu $\mathsf{S} = \{1, 2, \dots, 500\,051\}$.)

---

2. *Určte všetky dvojice prirodzených čísel (a, b) také, že*

$$\frac{a^2}{2ab^2 - b^3 + 1}$$

je prirodzené číslo. (*Bulharsko*)

Riešenie. (Podľa *Jana Moláčka.*) Ukážeme, že riešeniami sú práve všetky dvojice (a, b) tvaru $(8k^4 - k, 2k)$, $(k, 2k)$ a $(k, 1)$, kde $k \in \mathbb{N}$ je ľubovoľné. Hľadáme prirodzené čísla a, b, n, pre ktoré platí

$$\frac{a^2}{2ab^2 - b^3 + 1} = n. \tag{1}$$

Rovnosť (1) možno upraviť na tvar kvadratickej rovnice

$$a^2 - 2nb^2a + n(b^3 - 1) = 0.$$

s neznámou a. Jej koreňmi sú čísla

$$a_{1,2} = nb^2 \pm \sqrt{\left(nb^2\right)^2 - n\left(b^3 - 1\right)}. \tag{2}$$

Pretože jeden z koreňov $a_{1,2}$ je rovný hľadanému prirodzenému číslu a, odmocnenec vo vzťahu (2) musí byť štvorec, teda musí mať tvar

$$\left(nb^2\right)^2 - n\left(b^3 - 1\right) = d^2 \tag{3}$$

pre vhodné celé $d \geqq 0$. Také číslo d určite existuje, ak $b = 1$ (potom $b^3 - 1 = 0$, takže $d = nb^2$). Zaoberajme sa ale najprv náročnejším prípadom, keď $b > 1$. Ukážme, že pre také b z (3) vyplývajú odhady

$$nb^2 - \frac{b+1}{2} < d < nb^2 - \frac{b-1}{2}. \tag{4}$$

Pretože oba krajné výrazy sú kladné, môžeme obe nerovnosti umocniť; po dosadení d^2 a jednoduchých algebraických úpravách dostaneme dvojicu nerovností

$$(b+1)^2 < 4n(b^2+1) \quad \text{a} \quad (b-1)^2 + 4n(b^2-1) > 0,$$

ktoré zrejme platia, lebo $n \geqq 1$ a $b > 1$. Tým sú odhady (4) dokázané.

Všimnime si teraz, že rozdiel oboch krajných výrazov v (4) je rovný 1. Pre nepárne b by sa tieto výrazy dokonca rovnali dvom po sebe idúcim prirodzeným číslam, takže by žiadne celé d spĺňajúce podmienku (4) neexistovalo. Číslo b je preto párne, teda $b = 2k$ pre vhodné $k \in \mathbb{N}$; jediné celé d vyhovujúce nerovnostiam (4) je potom tvaru

$$d = nb^2 - \frac{b}{2} = 4nk^2 - k.$$

Pre také b a d prejde rovnosť (3) do tvaru

$$(4nk^2)^2 - n(8k^3 - 1) = (4nk^2 - k)^2,$$

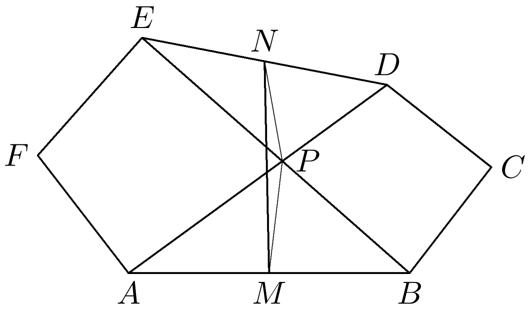
z ktorej ľahko vyplýva $n = k^2$; vzťahy (2) potom dávajú vyjadrenie

$$a_1 = 8k^4 - k \quad \text{a} \quad a_2 = k.$$

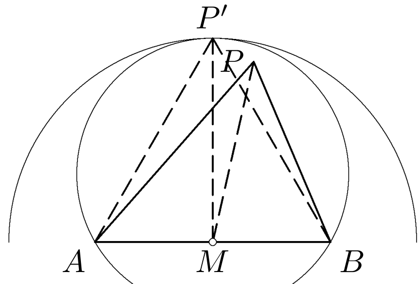
Pretože obe vypočítané hodnoty $a_{1,2}$ sú prirodzené čísla (pre každé $k \in \mathbb{N}$), dostávame dve (nekonečné) skupiny riešení $(a, b) = (8k^4 - k, 2k)$ a $(a, b) = (k, 2k)$, kde $k \in \mathbb{N}$. Zostáva rozobrať prípad, keď $b = 1$. Vtedy má zlomok zo zadania úlohy tvar

$$\frac{a^2}{2ab^2 - b^3 + 1} = \frac{a^2}{2a} = \frac{a}{2},$$

takže je rovný prirodzenému číslu práve vtedy, keď $a = 2k$ pre vhodné $k \in \mathbb{N}$. Treťou (a poslednou) skupinou riešení sú teda dvojice tvaru $(a, b) = (k, 1)$, kde $k \in \mathbb{N}$.



Obr. 1



Obr. 2

---

3. *Je daný konvexný šesťuholník, ktorého ľubovoľné dve protiľahlé strany majú nasledujúcu vlastnosť: vzdialenosť ich stredov je $\sqrt{3}/2$ násobok súčtu ich dĺžok. Dokážte, že všetky uhly daného šesťuholníka sú rovnaké.*
(Konvexný šesťuholník $ABCDEF$ má tri dvojice protiľahlých strán: AB a DE, BC a EF, CD a FA.) (*Poľsko*)

Riešenie. Označme A, B, C, D, E, F vrcholy daného šesťuholníka a uvažujme tri uhlopriečky AD, BE a FC. Niektoré dve z nich nutne zvierajú uhol aspoň $60°$. Bez ujmy na všeobecnosti predpokladajme, že sú to uhlopriečky AD a BE. Označme P ich priesečník a M, N stredy protiľahlých strán AB a DE (obr. 1).

Pretože $|\measuredangle APB| = |\measuredangle EPD| \geqq 60°$, leží bod P vnútri kružnice opísanej rovnostrannému trojuholníku ABP' (obr. 2), takže platí $|MP| \leqq |MP'| = (\sqrt{3}/2)|AB|$ s rovnosťou práve vtedy, keď $P = P'$, čiže práve vtedy, keď je trojuholník ABP rovnostranný. Podobne odvodíme, že $|NP| \leqq (\sqrt{3}/2)|DE|$ s rovnosťou práve vtedy, keď je trojuholník DEP rovnostranný. Pre vzdialenosť stredov oboch protiľahlých strán AB, DE tak dostávame odhad

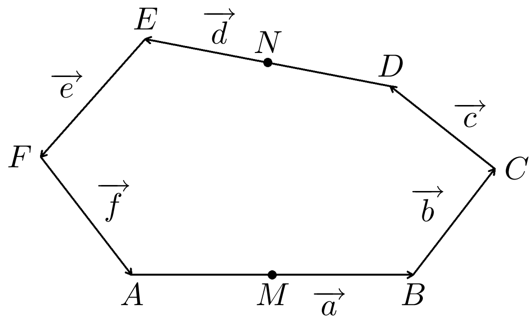
$$|MN| \leqq |MP| + |NP| \leqq \tfrac{1}{2}\sqrt{3}(|AB| + |DE|).$$

Z predpokladov úlohy teda vyplýva, že oba trojuholníky ABP a DEP sú rovnostranné a uhlopriečky AD, BE zvierajú uhol $60°$.

Zostávajúca uhlopriečka CF musí s jednou z uhlopriečok AD, BE zvierať uhol aspoň $60°$. Opäť môžeme bez ujmy na všeobecnosti predpokladať, že sa jedná napr. o uhlopriečku AD, priesečník uhlopriečok CE, AD označme Q. Úplne rovnako ako v predchádzajúcom prípade zistíme, že trojuholníky FAQ a CDQ sú rovnostranné. Keď nakoniec označíme R priesečník uhlopriečok BE a CF, ktoré podľa predchádzajúceho zvierajú nutne uhol $60°$, zistíme, že aj trojuholníky BCR a EFR sú rovnostranné. Odtiaľ vyplýva tvrdenie úlohy.

Iné riešenie. Označme A, B, C, D, E, F vrcholy daného šesťuholníka a $\overrightarrow{a} = \overrightarrow{AB}$, $\overrightarrow{b} = \overrightarrow{BC}, \dots, \overrightarrow{f} = \overrightarrow{FA}$ vektory určené jeho stranami, pritom $\overrightarrow{a} + \overrightarrow{b} + \dots +$

$+ \overrightarrow{f} = 0$. Ak označíme M, N stredy protiľahlých strán AB, DE, môžeme príslušný



Obr. 3

vektor $\overrightarrow{MN}$ vyjadriť dvoma spôsobmi (obr. 3).

$$\overrightarrow{MN} = \tfrac{1}{2}\overrightarrow{a} + \overrightarrow{b} + \overrightarrow{c} + \tfrac{1}{2}\overrightarrow{d} \quad \text{a} \quad \overrightarrow{MN} = -\tfrac{1}{2}\overrightarrow{a} - \overrightarrow{f} - \overrightarrow{e} - \tfrac{1}{2}\overrightarrow{d},$$

odkiaľ

$$\overrightarrow{MN} = \tfrac{1}{2}(\overrightarrow{b} + \overrightarrow{c} - \overrightarrow{e} - \overrightarrow{f}). \tag{1}$$

Podľa predpokladu platí

$$|\overrightarrow{MN}| = \frac{\sqrt{3}}{2}|\overrightarrow{a} + \overrightarrow{d}| \geqq \frac{\sqrt{3}}{2}|\overrightarrow{a} - \overrightarrow{d}|. \tag{2}$$

Položme $\overrightarrow{x} = \overrightarrow{a} - \overrightarrow{d}$, $\overrightarrow{y} = \overrightarrow{c} - \overrightarrow{f}$, $\overrightarrow{z} = \overrightarrow{e} - \overrightarrow{b}$, z (1) a (2) tak dostaneme

$$|\overrightarrow{y} - \overrightarrow{z}| \geqq \sqrt{3}|\overrightarrow{x}|$$

a podobne

$$|\overrightarrow{z} - \overrightarrow{x}| \geqq \sqrt{3}|\overrightarrow{y}|,$$
$$|\overrightarrow{x} - \overrightarrow{y}| \geqq \sqrt{3}|\overrightarrow{z}|.$$

Práve uvedené nerovnosti môžeme pomocou skalárnych súčinov ekvivalentne prepísať ako

$$|\overrightarrow{y}|^2 - 2(\overrightarrow{y}, \overrightarrow{z}) + |\overrightarrow{z}|^2 \geqq 3|\overrightarrow{x}|^2,$$
$$|\overrightarrow{z}|^2 - 2(\overrightarrow{z}, \overrightarrow{x}) + |\overrightarrow{x}|^2 \geqq 3|\overrightarrow{y}|^2,$$
$$|\overrightarrow{x}|^2 - 2(\overrightarrow{x}, \overrightarrow{y}) + |\overrightarrow{y}|^2 \geqq 3|\overrightarrow{z}|^2.$$

Sčítaním všetkých troch nerovností vyjde

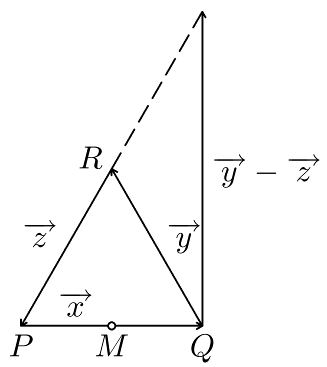
$$-|\overrightarrow{x}|^2 - |\overrightarrow{y}|^2 - |\overrightarrow{z}|^2 - 2(\overrightarrow{y}, \overrightarrow{z}) - 2(\overrightarrow{z}, \overrightarrow{x}) - 2(\overrightarrow{x}, \overrightarrow{y}) \geqq 0,$$

čiže $-|\overrightarrow{x}+\overrightarrow{y}+\overrightarrow{z}|^2 \geqq 0$. Odtiaľ však vyplýva, že $\overrightarrow{x}+\overrightarrow{y}+\overrightarrow{z}=0$ a že vo všetkých predchádzajúcich nerovnostiach platí rovnosť. Teda jednak

$$\begin{aligned}|\overrightarrow{y}-\overrightarrow{z}| &= \sqrt{3}|\overrightarrow{x}|,\\ |\overrightarrow{z}-\overrightarrow{x}| &= \sqrt{3}|\overrightarrow{y}|,\\ |\overrightarrow{x}-\overrightarrow{y}| &= \sqrt{3}|\overrightarrow{z}|,\end{aligned}$$

jednak vďaka rovnosti v (2) a v ďalších dvoch analogických nerovnostiach aj $\overrightarrow{a} \parallel \overrightarrow{d} \parallel \overrightarrow{x}$, $\overrightarrow{c} \parallel \overrightarrow{f} \parallel \overrightarrow{y}$, $\overrightarrow{e} \parallel \overrightarrow{b} \parallel \overrightarrow{z}$.

Keď zostrojíme trojuholník PQR tak, že $\overrightarrow{PQ}=\overrightarrow{x}$, $\overrightarrow{QR}=\overrightarrow{y}$, $\overrightarrow{RP}=\overrightarrow{z}$ (čo môžeme vďaka rovnosti $\overrightarrow{x}+\overrightarrow{y}+\overrightarrow{z}=0$), bude niektorý z jeho vnútorných uhlov mať veľkosť aspoň $60°$. Nech je to napr. uhol PRQ (obr. 4). Pre stred M strany PQ potom platí $|MR| = |\overrightarrow{y}-\overrightarrow{z}|/2 = \sqrt{3}|\overrightarrow{x}|/2 = \sqrt{3}|PQ|/2$, čo znamená, že trojuholník PQR je rovnostranný. Pre vnútorné uhly daného šesťuholníka to vzhľadom na dokázanú rovnobežnosť jeho protiľahlých strán s prislúchajúcimi vektormi $\overrightarrow{x}$, $\overrightarrow{y}$ a $\overrightarrow{z}$ znamená, že všetky jeho vnútorné uhly majú veľkosť $120°$.



Obr. 4

Poznámka. Z uvedeného riešenia je zrejmé, že ľubovoľný šesťuholník spĺňajúci predpoklady úlohy dostaneme tak, že z niektorého rovnostranného trojuholníka „odrežeme“ pri každom jeho vrchole zhodný rovnostranný trojuholník.

---

4. *Nech $ABCD$ je tetivový štvoruholník. Označme postupne P, Q a R päty kolmíc z bodu D na priamky BC, CA a AB. Dokážte, že $|PQ| = |QR|$ práve vtedy, keď sa osi uhlov ABC a ADC pretínajú na priamke AC.* (*Fínsko*)

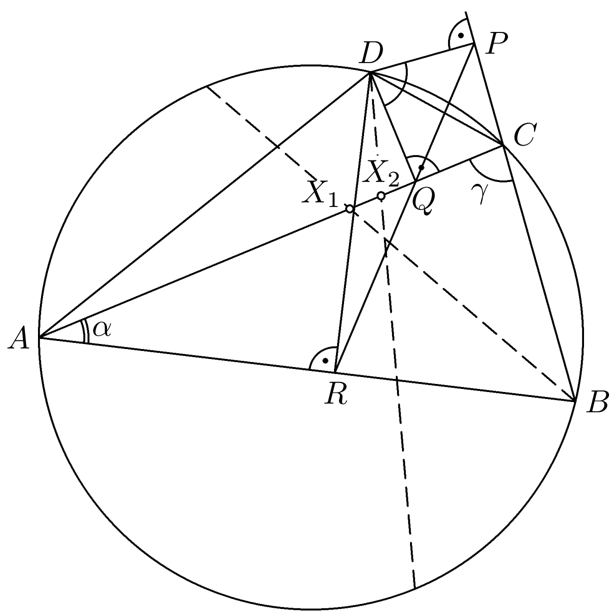
Riešenie. Označme po rade X_1, X_2 priesečníky osi uhla ABC a osi uhla ADC s uhlopriečkou AC daného tetivového štvoruholníka $ABCD$ (obr. 5). Zo známej vlastnosti osi uhla vyplýva jednak $|AX_1|/|CX_1| = |AB|/|CB|$ (v trojuholníku ABC), jednak $|AX_2|/|CX_2| = |AD|/|CD|$ (v trojuholníku ACD). Osi uhlov ABC a ADC sa teda pretnú na uhlopriečke AC práve vtedy, keď $X_1 = X_2$, čiže práve vtedy, keď $|AD|\cdot|CB| = |AB|\cdot|CD|$. Podľa Tálesovej vety ležia päty P a Q na kružnici s priemerom CD, takže pre veľkosť tetivy PQ tejto kružnice platí

$$|PQ| = |CD|\sin|\measuredangle PCQ| = |CD|\sin\gamma,$$

kde $\gamma = \measuredangle ACB$ (bez ohľadu na to, či päta P padne dovnútra strany BC alebo nie). Podobne ležia päty R a Q na kružnici s priemerom AD, takže pre veľkosť tetivy QR tejto kružnice platí

$$|QR| = |AD| \sin |\measuredangle RAQ| = |AD| \sin \alpha,$$

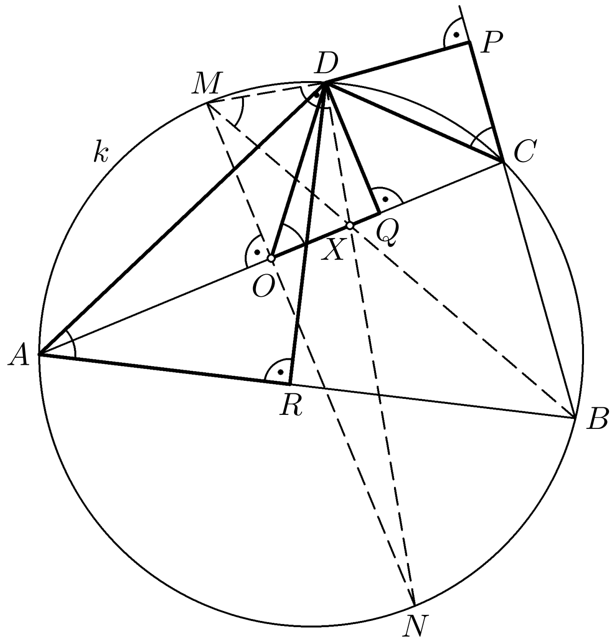
kde $\alpha = \measuredangle BAC$. Vidíme teda, že rovnosť $|PQ| = |QR|$ je ekvivalentná s rovnosťou $|CD| \sin \gamma = |AD| \sin \alpha$, čo je podľa sínusovej vety pre trojuholník ABC ekvivalentné s rovnosťou $|AD| \cdot |CB| = |AB| \cdot |CD|$. Tým je tvrdenie úlohy dokázané.



Obr. 5

Iné riešenie. (Podľa *Mareka Krčála.*) Označme M a N body, v ktorých os uhla ABC, resp. os uhla ADC pretne kružnicu k opísanú danému tetivovému štvoruholníku $ABCD$ (obr. 6). Vzhľadom na to, že každý z bodov M, N rozpoľuje príslušný oblúk AC kružnice k, je MN osou uhlopriečky AC a zároveň priemerom kružnice k. Označme O stred úsečky AC. Bez ujmy na všeobecnosti predpokladajme, že uhol BAD nie je tupý (inak by sme vymenili označenie vrcholov A a C), takže päta P kolmice z bodu D na BC padne mimo úsečku BC. Z vlastností tetivového štvoruholníka vyplýva $|\measuredangle DCP| = |\measuredangle BAD|$ a z rovnosti obvodových uhlov nad tetivou BD rovnosť $|\measuredangle BMD| =$

$= |\measuredangle BAD|$. Trojuholníky ARD a CPD sú teda podobné.



Obr. 6

Predpokladajme, že priesečník X oboch spomenutých osí uhlov leží na priamke AC. Pretože MN je priemer kružnice k, podľa Tálesovej vety $|\measuredangle XDM| = |\measuredangle NDM| = 90°$, takže štvoruholník $OXDM$ je tetivový. Teda tiež $|\measuredangle XOD| = |\measuredangle XMD| = |\measuredangle BMD|$ a vidíme, že trojuholník OQD je podobný s trojuholníkmi ARD a CPD. Uvažujme zobrazenie, ktoré vznikne zložením otočenia okolo stredu D o uhol $90° - |\measuredangle BAD|$ a rovnoľahlosti so stredom D a koeficientom $|DR|/|DA|$. Toto zobrazenie zobrazí bod A do bodu R, bod C do bodu P a bod O do bodu Q. Pretože O je stred úsečky AC, je jeho obraz v tomto zobrazení, teda bod Q, stredom úsečky PR, ktorá je obrazom úsečky AC.

Obrátene, ak je Q stred úsečky PR, je obrazom bodu O v uvedenom zobrazení, takže trojuholník OQD je podobný s trojuholníkmi ARD a CPD (tie sú podobné vždy). Ak teraz označíme X priesečník priamky BM s uhlopriečkou AC, bude $XDMO$ tetivový, a teda veľkosť uhla XDM bude $90°$. Odtiaľ vyplýva, že bod X leží na osi ND uhla ADC.

---

5. *Nech n je prirodzené číslo a $x_1, x_2, \dots, x_n$ reálne čísla také, že $x_1 \leqq x_2 \leqq \dots \leqq x_n$.*

(a) Dokážte, že

$$\left(\sum_{i=1}^{n}\sum_{j=1}^{n}|x_i - x_j|\right)^2 \leqq \frac{2(n^2-1)}{3}\sum_{i=1}^{n}\sum_{j=1}^{n}(x_i - x_j)^2.$$

(b) Ukážte, že rovnosť platí práve vtedy, keď $x_1, x_2, \dots, x_n$ je aritmetická postupnosť.

(*Írsko*)

Riešenie. Obe strany dokazovanej nerovnosti nezmenia hodnotu, keď od všetkých členov x_i odpočítame rovnaké číslo c. Keď vyberieme za c aritmetický priemer danej

n-tice členov x_i, bude „posunutá" postupnosť členov $x_i := x_i - c$ spĺňať podmienku

$$\sum_{i=1}^{n} x_i = 0. \tag{1}$$

Dodajme, že spomenuté „posunutie" zachová tiež usporiadanie čísel x_i podľa veľkosti a nezmení ani nič na tom, či dotyčná n-tica tvorila aritmetickú postupnosť alebo nie. Za predpokladu (1) upravíme oba súčty z dokazovanej nerovnosti na

$$\begin{aligned}
\sum_{i=1}^{n}\sum_{j=1}^{n} |x_i - x_j| &= 2 \sum_{1 \leqq i < j \leqq n} (x_j - x_i) = \\
&= 2\sum_{i=1}^{n}\bigl(\underbrace{(1+\dots+1)}_{(i-1)\text{ krát}} - \underbrace{(1+\dots+1)}_{(n-i)\text{ krát}}\bigr)x_i = \\
&= 2\sum_{i=1}^{n}(2i-n-1)x_i,\\
\sum_{i=1}^{n}\sum_{j=1}^{n}(x_i - x_j)^2 &= n\sum_{i=1}^{n} x_i^2 - 2\sum_{i=1}^{n} x_i \sum_{j=1}^{n} x_j + n\sum_{j=1}^{n} x_j^2 = \\
&= 2n\sum_{i=1}^{n} x_i^2.
\end{aligned}$$

Po dosadení a krátení štyrmi zistíme, že máme dokázať nerovnosť

$$\left(\sum_{i=1}^{n}(2i-n-1)x_i\right)^2 \leqq \frac{(n^2-1)n}{3}\sum_{i=1}^{n} x_i^2. \tag{2}$$

Ukážme, že (2) je Cauchyho nerovnosť

$$\left(\sum_{i=1}^{n} x_i y_i\right)^2 \leqq \sum_{i=1}^{n} x_i^2 \sum_{i=1}^{n} y_i^2 \tag{3}$$

pre n-ticu členov $y_i = 2i - n - 1$, $i = 1, 2, \dots, n$. Naozaj, pre takú n-ticu platí

$$\begin{aligned}
\sum_{i=1}^{n} y_i^2 = \sum_{i=1}^{n}(2i-n-1)^2 &= 4\sum_{i=1}^{n} i^2 - 4(n+1)\sum_{i=1}^{n} i + n(n+1)^2 = \\
&= 4\cdot\frac{n(n+1)(2n+1)}{6} - 4(n+1)\cdot\frac{n(n+1)}{2} + n(n+1)^2 = \\
&= \frac{(n^2-1)n}{3}.
\end{aligned}$$

Tým je dôkaz nerovnosti (2) hotový.

Ako je dobre známe, rovnosť v Cauchyho nerovnosti (2) nastane práve vtedy, keď existuje reálne číslo p, pre ktoré platí n-tica rovností

$$x_i = py_i = p(2i - n - 1) \quad (i = 1, 2, \dots, n). \tag{4}$$

Overme, že túto podmienku za predpokladu (1) spĺňajú práve tie konečné postupnosti $x_1, x_2, \ldots, x_n$, ktoré sú aritmetické. Naozaj, Ak platia rovnosti (4), je konečná postupnosť $x_1, x_2, \ldots, x_n$ aritmetická s diferenciou $2p$. Naopak, ak je postupnosť $x_1, x_2, \ldots, x_n$ aritmetická a d je jej diferencia, tak pre každé $i = 1, 2, \ldots, n$ platí rovnosť $x_i = x_1 + (i-1)d$ a súčet všetkých členov x_i je daný vzťahom

$$\sum_{i=1}^{n} x_i = \frac{n(x_1 + x_n)}{2}.$$

Podmienka (1) preto znamená, že $x_1 + x_n = 0$, čiže $x_1 + x_1 + (n-1)d = 0$. Odtiaľ dostávame $x_1 = d(1-n)/2$, preto členy x_i majú pre každé i vyjadrenie

$$x_i = \frac{d(1-n)}{2} + (i-1)d = \frac{(1-n+2i-2)d}{2} = \frac{(2i-n-1)d}{2},$$

čo je (4) pre $p = d/2$.

---

6. *Nech p je prvočíslo. Dokážte, že existuje prvočíslo q také, že pre žiadne celé číslo n nie je číslo $n^p - p$ deliteľné q.* (*Francúzsko*)

Riešenie. Pripomeňme si najskôr vlastnosti mocnín $n^1, n^2, \ldots, n^k, \ldots$ pri delení prvočíslom q. Ak je n celé číslo nesúdeliteľné s q, tak $n^{q-1} \equiv 1 \pmod{q}$ (tzv. malá Fermatova veta), naviac množina tých prirodzených k, pre ktoré $n^k \equiv 1 \pmod{q}$, je tvorená všetkými násobkami najmenšieho z nich (čo je buď číslo $q-1$, alebo niektorý jeho deliteľ). Uvažujme preto rozklad

$$p^p - 1 = (p-1)S, \quad \text{kde } S = p^{p-1} + p^{p-2} + \cdots + p + 1, \tag{1}$$

a za „kandidáta“ na vhodné prvočíslo q vyberme niektoré z prvočísiel deliacich súčet S (neskôr upresníme, akú doplňujúcu vlastnosť prvočiniteľa q čísla S budeme ešte potrebovať a prečo také q vôbec existuje). Pretože $q \mid S$ a $S \mid (p^p - 1)$, platí $q \mid (p^p - 1)$, t. j. $p^p \equiv 1 \pmod{q}$.

Pripusťme, že pre vybrané q tvrdenie úlohy neplatí, teda existuje celé n s vlastnosťou $n^p \equiv p \pmod{q}$. Umocnením tejto kongruencie na p dostaneme $n^{p^2} \equiv p^p \pmod{q}$, čo spolu s kongruenciou zo záveru predchádzajúceho odstavca znamená, že $n^{p^2} \equiv 1 \pmod{q}$. Číslo n je teda nesúdeliteľné s číslom q a podľa poznatkov pripomenutých v úvode riešenia vieme, že najmenšie prirodzené k s vlastnosťou $n^k \equiv 1 \pmod{q}$ musí byť deliteľom čísla p^2, teda jedno z čísel 1, p, p^2. Toto číslo musí byť súčasne deliteľom čísla $q-1$ (malá Fermatova veta), takže to nebude číslo p^2, pokiaľ nebude číslo p^2 deliť číslo $q-1$, teda pokiaľ $q \not\equiv 1 \pmod{p^2}$. To je práve tá doplňujúca vlastnosť prvočísla q, ktorú sme skôr spomenuli. Odložme na chvíľu dôkaz existencie takého prvočísla q a dokončime úvahy o mocninách čísla n.

Pokiaľ teda $q \not\equiv 1 \pmod{p^2}$, platí kongruencia $n^k \equiv 1 \pmod{q}$ pre $k = 1$ alebo pre $k = p$, v oboch prípadoch máme $n^p \equiv 1 \pmod{q}$. Porovnaním s kongruenciou $n^p \equiv p \pmod{q}$ potom dostaneme $p \equiv 1 \pmod{q}$, takže každá z p mocnín p^j zo súčtu S je kongruentná s číslom 1 (modulo q), takže $S \equiv p \pmod{q}$. Pretože však $q \mid S$, platí $S \equiv 0 \pmod{q}$. Porovnaním vychádza $p \equiv 0 \pmod{q}$, čo je spor s tým, že $p \equiv 1 \pmod{q}$. Preto žiadne celé n s vlastnosťou $n^p \equiv p \pmod{q}$ neexistuje, pokiaľ spĺňa prvočíslo q

podmienku $q \not\equiv 1 \pmod{p^2}$. Existenciu takého prvočiniteľa q (z rozkladu čísla S) teraz dokážeme.

Určme zvyšok súčtu S pri delení číslom p^2. Pretože $p^2 \mid p^j$ $(j \geqq 2)$, platí

$$S = p^{p-1} + p^{p-2} + \cdots + p + 1 \equiv 0 + 0 + \cdots + 0 + p + 1 \pmod{p^2},$$

teda $S \equiv p+1 \not\equiv 1 \pmod{p^2}$. Odtiaľ už vyplýva, že aspoň jeden z prvočiniteľov q_j čísla $S = q_1 q_2 \dots q_r$ nie je kongruentný s 1 (modulo p^2). (Vynásobením r kongruencií $q_j \equiv 1 \pmod{p^2}$ by sme totiž dostali $S \equiv 1 \pmod{p^2}$.)

Dôkaz je hotový a úloha vyriešená.