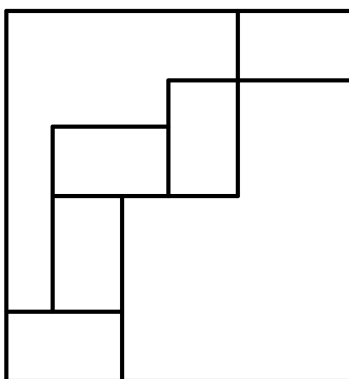


Riešenia 1. kola zimnej časti

1.1 Kóši Mučí Stvorenia ($\kappa \leq 0$)

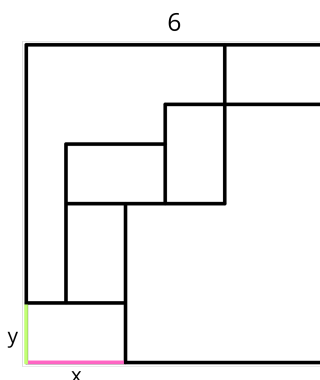
Zadanie. V krajine Al-Gebra, v meste Nerovno, stál doktor Kóši nad pracovným stolom pohrúžený do hlbokých myšlienok. Bol poverený nesmierne tajnou úlohou. Bolo vôbec správne spraviť to, čo po ňom žiadajú? Nakoniec sa rozhodol a dal si log zo svojej tajomnej flaštičky. Zo stola sledovali jeho premenu vystrašené oči. Pán Švarc sa zahnal kladivom...

Roh miestnosti okupovala zlovestná, štvorcová klietka so stranou dlhou 6 cm. V nej sa nachádzalo 5 rovnakých Obdĺžnikov, trasúcich sa pri pomyslení na údel ich kamaráta. Tisnú sa k sebe tak, ako na obrázku nižšie. Obrázok je však len ilustračný, teda niektoré dĺžky nemusia sedieť. Nájdite obsah jedného takeého Obdĺžnika.



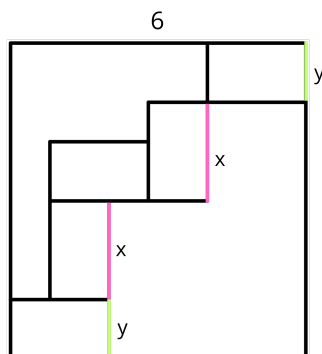
Riešenie. opravujú **Denys** (denys.andrukhovskiy@trojsten.sk) a **Maryna** (maryna.horodenchuk@trojsten.sk)

Pozrieme sa na túto úlohu bližšie. Označíme si dlhšiu stranu obdĺžnika ako x a kratšiu ako y .



Keďže obrázok je len ilustračný, tak nevieme hneď povedať, aký je pomer x, y . Vieme sa však pozrieť na to, že obdĺžniky sa dotýkajú. Takže, vieme pozrieť sa na to, ako sú obdĺžniky vnorené do štvorca, a ako sa strany obdĺžnika

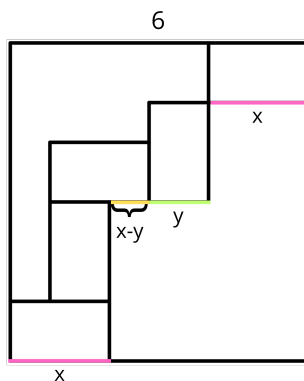
vyskladajú na stranu štvorca. Konkrétne, pozrime sa najskôr na zvislú stranu štvorca. Jednak vieme, že rovná sa 6 cm. Avšak, doplníme si do obrázka dĺžky niektorých zvislých strán.



Tieto strany sú zvislé, obdĺžniky s týmito stranami v zvislom smere sa nepretínajú, a keďže sa začínajú od spodku štvorca a sa končia hornou stranou, tak naozaj vieme povedať, že súčet týchto strán bude strana štvorca, teda

$$x + y + y + x = 6.$$

Z toho však ešte nevieme odvodiť dĺžku x a y . Čo sme ešte ale nespravili, je, že sme sa nepozreli na vodorovné strany štvorca. Analogicky si vieme doplniť zodpovedajúce strany obdĺžnikov do obrázka.



Máme označené dve strany x , jednu stranu y a ešte jednu časť strany x . Tvrdíme, že rovná sa $x - y$. Prečo? Lebo neoznačený zvyšok strany x je práve kratšia strana, teda označená časť je práve $x - y$. Potom, analogicky

$$x + (x - y) + y + x = 6.$$

To sa dá upraviť ako

$$x + (x - y) + y + x = 6,$$

$$3x = 6,$$

$$x = 2.$$

Takže, už vieme, že $x = 2$ cm. Teraz si spomeňme na rovnicu, ktorú sme odvodili skôr. Z nej dostaneme

$$2x + 2y = 6,$$

$$2 \cdot 2 + 2y = 6,$$

$$4 + 2y = 6,$$

$$2y = 2,$$

$$y = 1.$$

Takže, teraz vieme aj to, že $y = 1$ cm. Potom ale ľahko vieme zrátať obsah jedného obdĺžnika, keďže vieme, že rovná sa súčinu jeho strán. Preto obsah obdĺžnika je $S = 2\text{cm} \cdot 1\text{cm} = 2\text{cm}^2$.

1.2 Kandidáti Misiu Splnia ($\kappa \leq 0$)

Zadanie. V Pravom Uholníkovke medzitým zistili, že sa z mesta stratila hneď šesťica Obdĺžnikov. Tento prípad okamžite nahlásili hlavnej správkyni Pyte Gorovej. Tá neváhala a vyhlásila informačnú pohotovosť, aby našla dobrovoľníkov na výzvednú misiu. V okamihu sa jej zbehol hlúčik rôznych kandidátov od Jednouholníkov po Deväťuholníkov.

Kolkými spôsobmi vieme umiestniť čísla 1, 1, 3, 4, 5, 5, 6, 7, 8, 9 do políček tak, aby spĺňali uvedené nerovnosti?

$$\bigcirc < \bigcirc \leq \bigcirc < \bigcirc < \bigcirc > \bigcirc > \bigcirc > \bigcirc > \bigcirc > \bigcirc$$

Riešenie. opravujú **Adri** (adrianka.janackova@trojsten.sk) a **Baška** (barbora.novosadova@trojsten.sk)

Označme si políčka zľava doprava A až J, teda uvedená nerovnosť je $A < B \leq C < D < E > F > G > H > I > J$.

Žiadne z dopĺňaných čísel nie je menšie ako 1, preto obe čísla 1 musia byť na takých políčkach, od ktorých nie je žiadne menšie (nazývame ich minimálnymi). To sú jedine políčka A a J.

Podobne žiadne z dopĺňaných čísel nie je väčšie ako 9, preto 9 musí byť na takom políčku, od ktorého nie je žiadne väčšie (nazývame ho maximálnym). To je políčko E.

Ostáva nám umiestniť čísla 3, 4, 5, 5, 6, 7 a 8. Nerovnosť vyzerá takto: $1 < B \leq C < D < 9 > F > G > H > I > 1$.

Na políčkach F, G, H a I určite nemôžu byť dve čísla 5, keďže žiadne z týchto políčok sa nemôžu rovnať. Preto aspoň jedno z čísel 5 musí byť na niektorom z políčok B, C, D.

Ak je tam práve jedno číslo 5, môžu tam s ním byť ľubovoľné dve iné čísla z tých, ktoré nám ostali (3, 4, 6, 7 a 8). Poradie, v akom budú, je jednoznačné, keďže všetky sú rôzne, musia byť zoradené od najmenšieho po najväčšie. Na políčkach F, G, H, I potom bude druhé číslo 5 a tie čísla, ktoré ostali. Poradie bude opäť jednoznačné, tentokrát musia byť zoradené od najväčšieho po najmenšie. Počet rozdelení tohto typu je teda rovný počtu spôsobov, ako vybrať dve čísla z piatich. To je $\binom{5}{2} = \frac{5!}{2!3!} = 10$ spôsobov¹.

Ak sú na políčkach B, C a D dve čísla 5, musia byť na políčkach B a C, keďže len tieto dve políčka sa môžu rovnať. Potom D je od nich väčšie. Na políčku D preto môže byť číslo 6, 7 alebo 8, to sú teda ďalšie tri spôsoby (poradie

¹https://sk.wikipedia.org/wiki/Kombinačné_číslo

ostatných čísel, ktoré budú na políčkach F , G , H a I , je opäť jednoznačné). Dokopy teda vieme čísla do políčok umiestniť 13 spôsobmi.

1.3 Kulminuje Masívne Sprisahanie ($\kappa \leq 1$)

Zadanie. Výzvedná misia bola náročná. Apolonijs Brahmagupta Ceva sa v prestrojení prechádzal po uliciach Del Itela. Snažil sa nadviazať rozhovor s miestnymi, ale nejak nikto o Obdĺžnikoch nič nevedel. Už začínal byť zúfalý. Potom ho však oslovila postava, ktorá sa predstavila ako Mita Li: „Ak zháňaš Obdĺžnikov, od miestnych sa nič nedozvieš. Všetk vieš, ako Teória Čísel do všetkého pchá nos. Deje sa veľké sprisahanie a oni... Oni sú jeho súčasťou.“ Apolonia presvedčili pádne argumenty a jeho zmysel pre spravodlivosť začal vriieť. Zabudol na všetko a s vervou uhaňal späť do krajiny Geometrie, aby podal svojim krajanom svedectvo o krivdách, ktoré sa im v tajnosti dejú.

Pre číre rozhorčenie zabudol na potešenie z toho, aké šikovné prestrojenie sa mu podarilo. Svoj pravý uhol zamaskoval ako rovnosť inšpirovanú citátom hlavnej správkynne.

Kladné celé čísla a , b a prvočíslo p sú také, že

$$a^2 + p^2 = b^2.$$

Dokážte, že potom $2(b + p)$ je druhá mocnina celého čísla.

Riešenie. opravujú **Baška** (barbora.javorova@trojsten.sk) a **Brian** (brian.turza@trojsten.sk)

Na začiatok si vieme všimnúť, že rovnicu $a^2 + p^2 = b^2$ si vieme prepísať ako $p^2 = b^2 - a^2 = (b + a)(b - a)$. A keďže obe zátvorky nemôžu byť súčasne p , tak $b + a = p^2$ a $b - a = 1$. To môžeme vidieť z toho, že p je prvočíslo, takže buď delí obe zátvorky alebo p^2 delí jednu z nich a keďže zátvorka $b + a$ je väčšia ako $b - a$, tak môže deliť len ju.

Ak dáme tieto dve rovnice dohromady, dostaneme

$$b - a = 1,$$

$$b + a = p^2,$$

$$b + b - 1 = p^2,$$

$$2b - 1 = p^2,$$

$$b = \frac{p^2 - 1}{2}.$$

To môžeme dosadiť do výrazu zo zadania a dostaneme

$$2\left(\frac{p^2 - 1}{2} + p\right) = p^2 + 2p + 1 = (p + 1)^2.$$

Teda výraz $2(b + p)$ je skutočne druhou mocninou celého čísla.

Iné riešenie

Na to aby sme dokázali, že výraz $2(b + p)$ je druhou mocninou celého čísla, si môžeme výraz upraviť na $n = \sqrt{2}\sqrt{b + p}$, keďže súčet $b + p$ musí byť kladný, tak zápornú hodnotu upraveného výrazu môžeme odignorovať. Následne môžeme vidieť, že nám stačí dokázať, že $b + p$ je dvojnásobok druhej mocniny celého čísla.

Dôležitým pozorovaním je, že hodnoty a, p, b tvoria Pytagorejskú trojicu. Následne nám vie výrazne pomôcť využitie vzťahu $(2mn)^2 + (m^2 - n^2)^2 = (m^2 + n^2)^2$ tiež známeho ako Euklidov vzorec pre Pytagorejské trojice, pomocou ktorého vieme substituovať jednotlivé hodnoty v trojici kladných celých čísel a, p, b ako $a = 2mn$, $p = m^2 - n^2$, $b = m^2 + n^2$ pre Pytagorovu vetu $a^2 + p^2 = b^2$. Táto substitúcia je jednoznačne určená, keďže p je nepárne, teda nemôže byť substituované ako $p = 2mn$. Nepárnosť p môžeme vidieť napríklad z faktu, že neexistuje žiadna Pytagorejská trojica obsahujúca 2, teda jediné párne prvočíslo.

Keď sa teraz pozrieme na súčet $p + b$, tak dostaneme $p + b = m^2 - n^2 + m^2 + n^2 = 2m^2$, teda $p + b$ je dvojnásobok druhej mocniny celého čísla. Ak to vrátime späť do odmocnenej rovnice, získame

$$n = \sqrt{2}\sqrt{b + p} = \sqrt{2}\sqrt{2m^2} = 2m.$$

1.4 Krivdu Musia Splatiť ($\kappa \leq 2$)

Zadanie. Keď si Apoloniovu správu vypočuli v hlavnom meste krajiny Geometrie, nastalo pobúrenie. Ľud volal po pomste, a tak nastal čas povolať bojovníkov za spravodlivosť – Mocnostných Dosahovačov. „Mocnostní Dosahovači, morfujte!“ zvolala na nich hlavná správkyňa, keď sa dostavili na námestie. A tak začali morfovať.

Mocnostný Dosahovač je štvorec s dĺžkou strany 24 cm. Morfovanie prebieha nasledovne: Keď sa Mocnostný Dosahovač preloží na polovicu pozdĺž uhlopriečky, tak vznikne trojuholník ABC s pravým uhlom pri vrchole A. Potom sa zohne tak, aby bod C skončil niekde na strane AB a toto miesto si označí D. Platí, že vzniknutý ohyb pretne stranu BC v bode X. Mocnostný Dosahovač sa potom znova ohne tak, aby bod B skončil na bode X. Všimli sme si, že novovzniknutý ohyb prechádza bodom D. Aká je v centimetroch vzdialenosť medzi bodmi A a D?

Riešenie. opravujú Kopy (martin.kopcany@trojsten.sk) a Naťa (natalia.cigasova@trojsten.sk)

Keď prehýbame body na iné miesta, tak sa nám tam prenášajú aj uhly, aj dĺžky strán od prehybov. Taktiež by sme mohli povedať, že body, strany a uhly sú osovo súmerné, kde os súmernosti je priamka ohybu. Takže, keďže sme prehli bod C na bod D, vieme, že $|CX| = |XD|$ a keďže sme prehli bod B na bod X, tak vieme, že $|XD| = |DB|$. Preto platí, že $|CX| = |XD| = |DB|$. Keďže trojuholník ABC vznikol prehnutím štvorca cez uhlopriečku, tak uhol pri vrchole B bude mať veľkosť 45° . Vďaka zohnutiu bodu B do bodu X bude platiť, že $|\sphericalangle DBX| = |\sphericalangle DXB| = 45^\circ$. Z tohto následne vieme dopočítať tretí uhol v tomto trojuholníku ako $|\sphericalangle XDB| = 180^\circ - 45^\circ - 45^\circ = 90^\circ$.

Označme si dĺžku strán $|BD| = |DX| = |XC| = a$. Trojuholník BDX je rovnoramenný pravouhlý s odvesnami dĺžky a . Jeho prepona bude mať teda z Pytagorovej vety veľkosť $\sqrt{2}a$. Podobne z Pytagorovej vety si vieme vypočítať dĺžku uhlopriečky pôvodného štvorca. Vyjde nám, že má dĺžku $24\sqrt{2}$. Túto dĺžku teda vieme vyjadriť dvoma rôznymi spôsobmi ako

$$24\sqrt{2} = |BC| = |CX| + |XB| = a + \sqrt{2}a,$$

z čoho dostaneme, že

$$a = \frac{24\sqrt{2}}{1 + \sqrt{2}}.$$

Z tohto vieme následne zistiť dĺžku úsečky AD ako

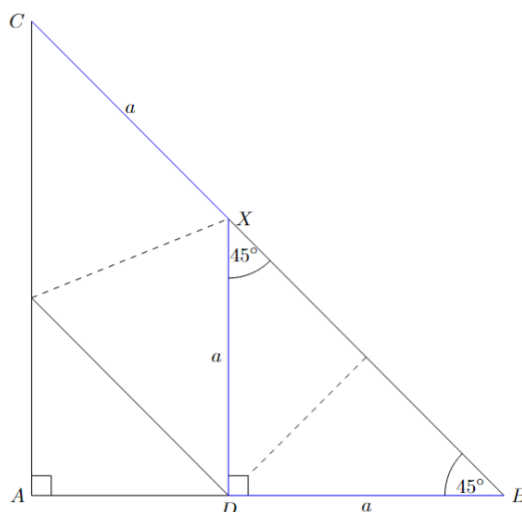
$$|AD| = |AB| - |DB| = 24 - \frac{24\sqrt{2}}{1 + \sqrt{2}},$$

$$|AD| = 24 - \frac{24\sqrt{2}(1 - \sqrt{2})}{1 - 2},$$

$$|AD| = 24 + 24\sqrt{2} - 24 \cdot 2,$$

$$|AD| = 24 \cdot (\sqrt{2} - 1),$$

Pričom úpravu z prvého riadku na druhý riadok sme spravili vďaka rozšíreniu zlomku výrazom $1 - \sqrt{2}$.



Iné riešenie

Keďže máme zadané presné dĺžky strán a v obrázku sa nikde nenachádza „bod voľnosti“, niekedy sa môže oplatiť využiť k riešeniu goniometriu. Najprv si všimneme, že uhly pri vrcholoch B a C v trojuholníku ABC majú veľkosť 45° .

Prehyb, ktorý prehne bod B do X , zároveň prenesie tento uhol, a teda $|\angle BXD| = |\angle XBD| = 45^\circ$. Z toho vieme dopočítať tretí uhol v tomto trojuholníku ako $|\angle XDB| = 180^\circ - 45^\circ - 45^\circ = 90^\circ$.

Označme si druhý bod prehybu bodu C do D ako Y . Z toho, že trojuholník YDX je len prehnutý YCX , tak bude platiť, že $|\angle XDY| = |\angle XCY| = 45^\circ$ a $|CY| = |YD|$.

Z toho vieme vypočítať veľkosť uhla ADY ako $|\angle ADY| = |\angle ADB| - |\angle XDB| - |\angle YDX| = 180^\circ - 90^\circ - 45^\circ = 45^\circ$. Z trojuholníka ADY vieme odvodiť, že $|\angle AYD| = 180^\circ - 90^\circ - 45^\circ$. K nemu susedný uhol CYD bude mať teda veľkosť $180^\circ - 45^\circ = 135^\circ$.

Vieme z prehnutia, že trojuholník CYD je rovnoramenný, a teda v ňom uhly pri vrcholoch C a D budú oba mať veľkosť $\frac{180^\circ - 135^\circ}{2} = 22^\circ 30'$. Z vlastností funkcie tangens v pravouhlom trojuholníku CAD vieme teda zistiť veľkosť

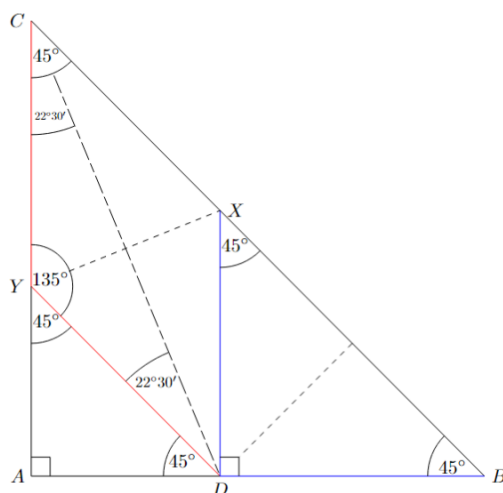
strany AD nasledovne:

$$\tan 22^\circ 30' = \frac{|AD|}{|CA|},$$

$$|AD| = |CA| \cdot \tan 22^\circ 30',$$

$$|AD| = 24 \cdot (\sqrt{2} - 1).$$

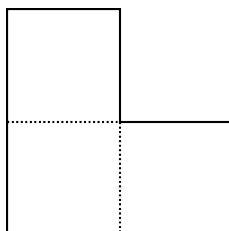
Táto vyčíslená hodnota tangensu k správnomu riešeniu nie je nutná. Postačujúce je, ak odovzdáte riešenie vo forme predposledného riadka. Dá sa vypočítať napríklad použitím vety o tangense polovičného uhla. Uviedol som ju tu len pre overenie, že sa naozaj zhoduje s výsledkom z prvého riešenia.



1.5 Kombistanom Maširujú Supervojaci ($\kappa \leq 6$)

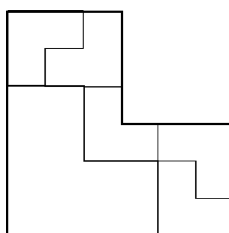
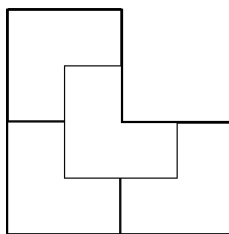
Zadanie. Mocnostní Dosahovači pri svojom pochode na Teóriu Čísel nelegálne prekročili hranice Kombistanu. Kombistanci odmietli nechať svoju krajinu zadupať do zeme, tak sa rozhodli niečo s tým urobiť. Zobrali svoje L-ká a začali ich deliť na menšie. Nikto netuší, ako im to pomôže, ale Kombistanci to aj tak nevzdávajú.

Ukážte, že pre všetky $n \geq 9$ vieme L-ko (štvorec bez jednej štvrtiny, ako na obrázku) rozdeliť na n podobných (nie nutne rovnako veľkých) L-iek.



Riešenie. opravujú **Mati** (matus.zelko@trojsten.sk) a **Ema** (ema.humenska@trojsten.sk)

Ako prvú vec si všimneme, že L -ko je možné rozdeliť na 4 a 6 častí takto:

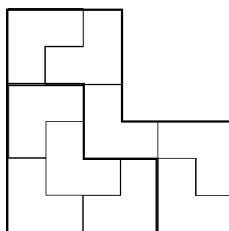


Ďalej, každým rozdelením L -ka na 4 časti nám pribudnú 3 L -ká do počtu a každým rozdelením na 6 pribudne 5 L -iek.

Potrebujeme zahrnúť každé $n \geq 9$. To vieme dostať pridávaním násobku 3 k trom prípadom:

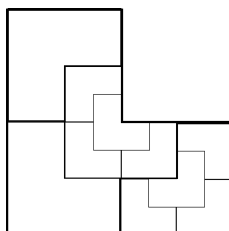
- Zvyšok po delení trom je 0.

Počiatočné L rozdelíme na 6 častí (počet L -jek zvýšime o 5) a následne nejaké z nich rozdelíme na 4 (pridáme 3), máme teda $1 + 5 + 3 = 9$ častí.



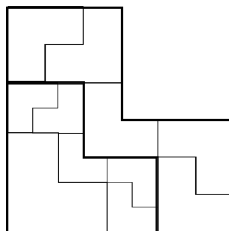
- Zvyšok po delení trom je 1.

Počiatočné L rozdelíme na 4 a potom dve z nich rozdelíme opäť na 4, máme teda $1 + 3 + 3 + 3 = 10$ častí.



- Zvyšok po delení tromi je 2.

Počiatkové L rozdelíme na 6 častí, nejakú z nich opäť na 6, do tretice dostávame $1 + 5 + 5 = 11$ častí.



Keďže v každom prípade vieme niektorý z útvarov tvaru L rozdeliť na 4, čím sa nám počet L -iek zvýši o 3, tak sme schopní dosiahnuť každé číslo, ktoré je aspoň 9.

1.6 Kombá Mužstva Spravíme

Zadanie. Keď sa o pochode Mocnostných Dosahovačov dozvedeli v Teórii Čísel, ihneď sa začali chystať na boj, ktorý ich čaká. Povolali svoje elitné jednotky, dvojky, trojky, štvorky, päťky, šestky, ... Keď sa všetci zaradili, nastal čas deliť ich do formácií.

Nech m, n sú kladné celé čísla. Dokážte, že nasledujúce tvrdenia sú ekvivalentné:

- Žiadne prvočíslo $p \leq n$ nedelí číslo m .
- Pre každé kladné celé číslo $k \leq n$ je kombinačné číslo² $\binom{m+k-1}{k}$ deliteľné m .

Riešenie. opravujú **Mišo M.** (michal.molnar@trojsten.sk) a **Sebik** (sebik.hajdu@trojsten.sk)

Na to, aby boli dve tvrdenia ekvivalentné, musí z jedného vyplývať druhé a z druhého prvé. Ukážeme teda postupne tieto dve implikácie.

Najprv predpokladajme, že máme nejaké kladné celé čísla m, n , pričom žiadne prvočíslo $p \leq n$ nie je deliteľom čísla m . Chceme ukázať nejakú vlastnosť kombinačného čísla. Zvoľme teda $k \leq n$ ľubovoľne a pozrime sa na to, ako bude dané kombinačné číslo vyzerať.

$$\binom{m+k-1}{k} = \frac{(m+k-1)!}{(m-1)! \cdot k!} = \frac{(m+k-1) \cdot (m+k-2) \cdot \dots \cdot (m+1) \cdot m}{k \cdot (k-1) \cdot \dots \cdot 1}$$

Vieme, že kombinačné číslo je celé, takže menovateľ sa vykráti s čitateľom. Nás zaujíma, či po tomto vykrátení bude výsledok deliteľný číslom m . Pozrime sa teda na prvočísla, ktoré sa vyskytujú v menovateli. Pre každé takéto prvočíslo q platí, že $q \leq k$, keďže q je deliteľom čísla menšieho alebo rovného k . Potom nutne $q \leq n$, a teda podľa predpokladu platí, že q nie je deliteľom čísla m . Keďže je to prvočíslo, z čísla m v čitateli sa nič nevykráti a výsledná hodnota bude skutočne násobkom m . Takže máme prvú implikáciu dokázanú.

Pozrime sa teraz na druhú implikáciu. Tu predpokladáme, že čísla m a n spĺňajú, že pre každé $k \leq n$ je číslo $\binom{m+k-1}{k}$ násobkom m . Na základe tohto predpokladu by sme chceli dokázať niečo pre prvočísla, ktoré sú menšie alebo rovné n .

²Kombinačné číslo $\binom{a}{b}$ označuje počet spôsobov, ktorými je možné z a vecí vybrať nejakých b , pričom nám nezáleží na poradí.

Vezmime si teda ľubovoľné prvočíslo $p \leq n$. Zjavne preň platí, že $\binom{m+p-1}{p}$ je násobok čísla m . Rozpíšme si toto kombinačné číslo rovnako ako vyššie.

$$\binom{m+p-1}{p} = \frac{(m+p-1) \cdot (m+p-2) \cdot \dots \cdot (m+1) \cdot m}{p \cdot (p-1) \cdot \dots \cdot 1}$$

Keďže je to násobok m , po vydelení týmto číslom musíme opäť dostať celé číslo. To bude mať tvar

$$\frac{(m+p-1) \cdot (m+p-2) \cdot \dots \cdot (m+1)}{p \cdot (p-1) \cdot \dots \cdot 1}.$$

Keďže sa všetko musí vykrátiť a keďže p je prvočíslo, tak musí byť deliteľom jedného z čísel v čitateli. Môžeme označiť, že p je deliteľom $m+a$, kde $1 \leq a \leq p-1$. Potom však platí, že číslo m má zvyšok $p-a$ po delení p . Keďže $a \neq 0$ ani $a \neq p$, tak číslo m nie je násobkom p . Toto platí bez ohľadu na voľbu p , takže sme dokázali aj druhú implikáciu.

1.7 Krviprelievanie, Mordovanie, Smútok

Zadanie. Došlo k najhoršiemu. Na bojisku sa strhla haravara a krviprelievaniu nebolo konca-kraja. Veľmi rýchlo sa ukázala taktická prevaha Geometrov, ktorí sa poľahky zorientovali v spleť situácii a do máp si zakreslili všetky styčné body trojuholníkového bojiska.

Majme trojuholník CGN. Vnútri neho leží na osi uhla GCN bod L. Nech X, Y postupne označujú body ležiace na stranách CG a CN, ktoré spĺňajú $|\sphericalangle CNL| = |\sphericalangle XLG|$ a $|\sphericalangle CGL| = |\sphericalangle YLN|$. Dokážte, že bod L je stred kružnice vpísanej trojuholníku CGN práve vtedy, keď body L, X, Y ležia na priamke.

Riešenie. opravujú **Bebe** (alzbeta.klimentova@trojsten.sk) a **Lukáš** (lukas.gaborik@trojsten.sk)

Výrok, že body Y, X a L ležia na jednej priamke práve vtedy, keď bod L je stredom kružnice vpísanej do trojuholníka CGN, je ekvivalencia. Preto, aby sme dokázali, že tento výrok platí vždy, musíme dokázať dve tvrdenia:

1. Ak je bod L stredom kružnice vpísanej do trojuholníka CGN, potom body Y, X a L ležia na jednej priamke.
2. Ak body Y, X a L ležia na jednej priamke, potom bod L je stredom kružnice vpísanej do trojuholníka CGN.

Prvá implikácia

Zo zadania vieme, že platí $|\sphericalangle LNY| = |\sphericalangle GLX| = \alpha$ a $|\sphericalangle XGL| = |\sphericalangle YLN| = \beta$. Predpokladajme, že bod L je stredom kružnice vpísanej do trojuholníka CGN. Z toho vyplýva, že priamky GL a NL sú postupne osami uhlov $\sphericalangle XGN$ a $\sphericalangle GNY$. Z toho ďalej vyplýva, že $|\sphericalangle XGL| = |\sphericalangle LGN| = \beta$ a $|\sphericalangle GNL| = |\sphericalangle LNY| = \alpha$. Z trojuholníka NGL vieme, že $|\sphericalangle NLG| = 180^\circ - \alpha - \beta$.

Aby body Y, X a L ležali na jednej priamke, musí platiť, že uhol $|\sphericalangle YLX| = 180^\circ$.

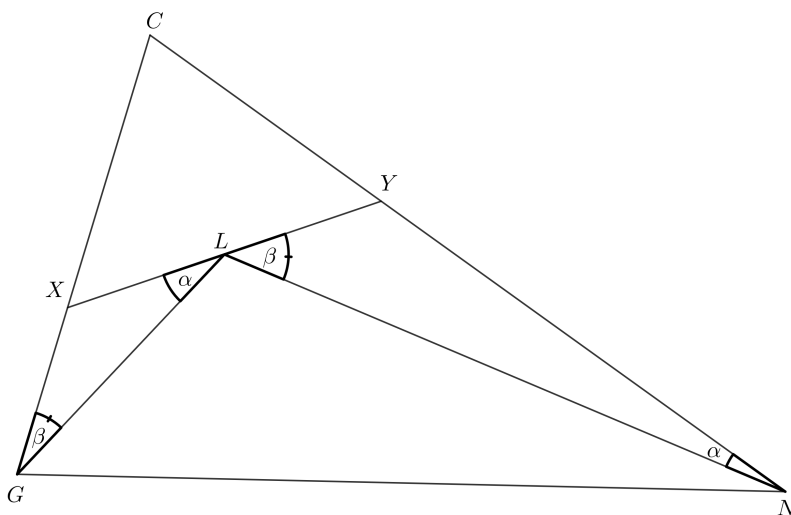
Teraz sa vráťme k tomu, čo chceme dokázať, teda

$$|\sphericalangle YLX| = |\sphericalangle YLN| + |\sphericalangle NLG| + |\sphericalangle GLX| = \beta + (180^\circ - \alpha - \beta) + \alpha = 180^\circ.$$

Tým sme dokázali, že ak je L stredom kružnice vpísanej do trojuholníka CGN , tak body Y , X a L ležia na jednej priamke.

Druhá implikácia

K tejto implikácii, keďže je náročnejšia, si načrtne aj obrázok. Často sa však stáva, že ak si nakreslíme obrázok, ktorý je pomerne presný, tak omylom použijeme veci, ktoré na ňom nejak vyzerajú a ešte sme ich nedokázali (napr. že niečo je os uhla). Preto nie je na škodu si kresliť obrázky, ktoré až tak reprezentatívne nie sú. Z tohto obrázka určite neusúdime, že NL je osou uhla CNG bez toho, aby sme to dokázali.



Chceme dokázať, že ak body Y , X a L ležia na jednej priamke, potom bod L je stredom kružnice vpísanej do trojuholníka CGN .

Ponecháme si označenia z prvej časti, teda $|\angle LNY| = |\angle GLX| = \alpha$ a $|\angle XGL| = |\angle YLN| = \beta$. Z trojuholníkov NLY a LGX vieme povedať, že sú podobné podľa vety o podobnosti uu a platí

$$|\angle LXG| = |\angle LYN| = 180^\circ - \alpha - \beta.$$

Ak predpokladáme, že body Y , X a L ležia na jednej priamke, potom tiež platí, že $|\angle NLG| = 180^\circ - \alpha - \beta$.

Aby sme dokázali, že bod L je stredom kružnice vpísanej do trojuholníka CGN , musíme preukázať, že priamky GL a NL sú osami uhlov $\angle XGN$ a $\angle GNY$. Na to by nám stačilo ukázať, že $|\angle XGL| = |\angle LGN| = \beta$ a $|\angle GNL| = |\angle LNY| = \alpha$. V tomto prípade by platilo, že trojuholníky NGL , LGX a NLY sú podobné podľa vety uu , stačí nám teda ukázať podobnosť týchto trojuholníkov.

Na to sa môžeme skúsiť pozrieť cez vetu sus . Spoločný uhol už máme, lebo $|\angle NLG| = |\angle LXG| = |\angle LYN| = 180^\circ - \alpha - \beta$, preto nám už zostáva len dokázať, že pomer strán je rovnaký, čiže

$$\frac{|NL|}{|LG|} = \frac{|LX|}{|GX|} = \frac{|NY|}{|LY|}.$$

Vieme, že $|\sphericalangle LYC| = |\sphericalangle LXC| = 180^\circ - (180^\circ - \alpha - \beta) = \alpha + \beta$. Z toho vyplýva, že trojuholník CXY je rovnoramenný, takže $|XL| = |LY|$, lebo priamka CL je osou uhla $\sphericalangle XCY$ v rovnoramennom trojuholníku.

Ako sme ukázali na začiatku tejto implikácie, GXL a LNY sú podobné, a preto platí

$$\frac{|XL|}{|LG|} = \frac{|NY|}{|NL|},$$

čo znamená, že $\frac{|NL|}{|LG|} = \frac{|NY|}{|XL|}$, teda $\frac{|NL|}{|LG|} = \frac{|NY|}{|LY|}$.

Tým sme dokázali, že trojuholníky GLN a LNY sú podobné, a preto platí, že $|\sphericalangle LGN| = |\sphericalangle YLN| = \beta$ a $|\sphericalangle LNG| = |\sphericalangle LNY| = \alpha$. Z toho vyplýva, že GL a NL sú osami uhlov, a teda bod L je skutočne stredom kružnice vpísanej do trojuholníka CGN .

1.8 Karteziánova Mocná Sieť

Zadanie. Bitka vyzerala pre Teóriu Čísel beznádejne. Vtom prišli na pomoc bojovníci Al-Gebry na svojich formulách. Medzi nimi aj Kartezián ozbrojený svojou nekonečnou sieťou, ktorá pokryla celé bojisko a znehybnila Mocnostných Dosahovačov. Tým ich premenil na sériu praobyčajných rovníc. Aby sa podarilo bitku o osud celej matematiky zvrátiť, stačí tieto rovnice vyriešiť.

Nájdite všetky reálne čísla x, y, z , ktoré sú riešeniami sústavy rovníc

$$x^2 + x - 1 = y,$$

$$y^2 + y - 1 = z,$$

$$z^2 + z - 1 = x.$$

Riešenie. opravujú Štepi (martin.stepanek@trojsten.sk) a Ema (ema.cudaiova@trojsten.sk)

Z každej rovnice si môžeme dať jednotku na druhú stranu a potom upraviť ľavú stranu, čím dosiahneme o niečo krajší tvar

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

$$y(y+1) = z+1,$$

$$z(z+1) = x+1.$$

Teraz máme na oboch stranách podobné výrazy, tak by sme sa ich chceli nejak zbaviť. Problém je, že rovnaké premenné sú v rôznych rovniciach. To vieme vyriešiť dvoma spôsobmi. Jednak tie rovnice vieme sčítať. Po vynásobení a vykrátení dostaneme $x^2 + y^2 + z^2 = 3$. Okrem toho ich vieme aj vynásobiť, čím dostaneme

$$xyz(x+1)(y+1)(z+1) = (x+1)(y+1)(z+1).$$

Chceli by sme vykrátiť tie zátvorky, ale na to potrebujeme, aby boli nenulové. Predpokladajme teda, že nejaká zo zátvoriek je 0, bez ujmy na všeobecnosti nech je to $x+1$. Dosadením $x = -1$ do pôvodnej sústavy dopyčujeme, že vtedy aj $y = z = -1$. V opačnom prípade (keď sú všetky zátvorky nenulové) dostávame $xyz = 1$.

Máme tu teraz nejaký súčet a súčin, čo by nám mohlo pripomenúť AG-nerovnosť. Tá ale platí len pre nezáporné čísla, a x , y a z môžu byť aj záporné. Našťastie v súčte máme ich štvorce, ktoré nezáporné sú, tak ich pridajme aj do súčinu: ak $xyz = 1$, potom aj $x^2y^2z^2 = 1$.

AG-nerovnosť nám hovorí, že

$$\frac{x^2 + y^2 + z^2}{3} \geq \sqrt[3]{x^2y^2z^2},$$

ale my chceme, aby obe strany boli rovné 1. Veta o AG-nerovnosti nám navyše hovorí, že rovnosť nastáva práve vtedy, keď sú všetky tie čísla rovnaké, teda $x^2 = y^2 = z^2 = 1$. Prípad, keď je x , y alebo z rovné -1 sme už vyriešili, takže ostáva len riešenie $x = y = z = 1$.

Riešenie rozoberaním prípadov

Nevýhoda predošlého riešenia je, že treba poznať AG-nerovnosť a dosť trikovo ju použiť. Ak nám také niečo nenapadne, vieme úlohu vyriešiť aj priamočiarejšie, aj keď také riešenie bude o niečo dlhšie a bude treba viac počítať.

Nech $f(x) = x^2 + x - 1$, potom sústava je $f(x) = y, f(y) = z, f(z) = x$. Nech M je nejaká množina čísel, potom $f(M)$ budeme označovať jej *obraz*, teda množinu $f(x)$ pre všetky $x \in M$. Platí, že $\min f(x) = -5/4$ a funkcia ho dosahuje pre $x = -1/2$ (ide o vrchol paraboly, ktorý sa nachádza uprostred riešenia $f(x) = 0$), takže všetky neznáme musia byť aspoň $-5/4$. Teraz rozoberieme, čo môže byť x .

Môžeme si všimnúť, že ak $x = 1$, máme riešenie $x = y = z = 1$, a ak $x = -1$, máme riešenie $x = y = z = -1$. Ďalej dokážeme, že iné riešenie neexistuje.

Ak $x > 1$, potom $f(x) > x$, teda postupným dosadením do sústavy dostaneme $x < y < z < x$, čo je spor.

Ďalej sa pozrime na prípad $-5/4 \leq x \leq 0$. Všimnime si, že $f([-5/4, -1])$ je podmnožinou $[-1, 0]$ a $f([-1, 0]) = [-5/4, -1]$ (tie zátvorky znamenajú uzavreté intervaly). Ak teda x zvolíme v jednom z týchto intervalov, dosadením do sústavy zistíme, že musí byť zároveň v tom druhom. Navyše, tieto dva intervaly majú jediný spoločný bod, a to -1 . Jediná možnosť je teda $x = -1$, čo nám dá riešenie $x = y = z = -1$.

Ďalej môžeme predpokladať, že ani $y, z \notin [-5/4, 0]$, inak by sme totiž dostali to isté čo v prípade x , ibaže hodnoty neznámych by boli cyklicky posunuté.

Ostáva ešte prípad $0 < x < 1$, kedy platí $f(x) < x$. Keďže predpokladáme, že $y \notin [-5/4, 0]$, tak aj $y \in (0, 1)$. Takto ďalej dostaneme, že $x > y > z > x$, čo je spor. Žiadne ďalšie riešenia teda neexistujú.

Riešenie derivovaním

Nakoniec tu máme riešenie, ktoré je síce najkratšie, ale vyžaduje najviac počítania, takže ho asi nechcete robiť ručne, ale použiť nejaký program ako napríklad WolframAlpha. Podotýkame však, že v KMS za riešenia s využitím výpočtovej techniky obvykle nedávame veľa bodov.

Dosaďme prvú rovnicu do druhej a to do tretej. Po úprave dostaneme

$$((x^2 + x - 1)^2 + x^2 + x - 1 - 1)^2 + (x^2 + x - 1)^2 + x^2 + x - 1 - 1 - 1 - x = 0,$$

$$(x - 1)(x + 1)(x^6 + 4x^5 + 5x^4 + 2x^3 + 1) = 0.$$

Máme teda korene ± 1 (ktoré vedú k riešeniam $x = y = z = \pm 1$), a ďalej chceme dokázať, že ten polynóm 6-teho stupňa v zátvorke (označme ho P) nemá žiadne reálne korene. P má kladný vedúci koeficient, teda v $\pm\infty$ má hodnotu $+\infty$, takže aby mal koreň, musí mať minimum ≤ 0 . Polynómy ale majú vo všetkých lokálnych minimách nulovú deriváciu. Derivácia P je $2x^2(x+1)(3x^2+7x+3)$, čoho korene už vieme jednoducho nájsť a overiť, že všetky lokálne minimá P sú kladné, teda P nemá korene a žiadne ďalšie riešenia neexistujú.

1.9 Konferencia Mierová Súdi

Zadanie. „Ticho, ticho v súdnej sieni. Vážení zástupcovia Al-Gebry, Kombistanu, Matematickej ľudovo-demokratickej Analýzy a moji krajanovia z kráľovstva Teórie Čísel. Krajina Geometrie na čele s hlavnou správkynou Pyťou Gorovou sa dopustila zločinu proti matematike. Podľa paragrafu π zákona o spolunažívaní matematických štruktúr a pozmeňujúcich návrhov schválených počas Zermelových reforiem, ďalej podľa zákona ...“

V kruhu okolo stola sedí $n \geq 2$ veľvyslancov. Tí na začiatku nespia, ale každý sa pozerá na nejakého jedného iného veľvyslancu. Občas sa nejaký (naraz najviac 1) veľvyslanec, ktorý nespí, postaví, vyhlási „Mňa už to nebaví!“ a odíde. Všetci veľvyslanci, ktorí sa na neho pozerali, následne zavrú oči a zaspia. Tento proces sa opakuje, kým všetci veľvyslanci buď neodišli, alebo nezaspali. Veľvyslanec, ktorý na konci spí, sa nazýva unudený.

1. V závislosti od n určte najväčšie k také, že bez ohľadu na to, na koho sa pozerajú jednotliví veľvyslanci, existuje postupnosť odchádzania veľvyslancov taká, že na konci bude unudených aspoň k z nich.
2. V závislosti od n určte najmenšie l také, že bez ohľadu na to, na koho sa pozerajú jednotliví veľvyslanci, existuje postupnosť odchádzania veľvyslancov taká, že na konci bude unudených najviac l z nich.
3. Dokážte, že pre každé konkrétne rozostavenie veľvyslancov (kde zohľadňujeme, na koho sa pozerajú) je najväčší a najmenší možný počet unudených veľvyslancov dokopy najviac n .

Riešenie.

opravuje Šošo (jakub.sosovicka@trojsten.sk)

Uvažujme orientovaný graf, kde veľvyslanci budú vrcholy a hrana u, v existuje práve vtedy, keď sa príslušný veľvyslanec u pozerá na veľvyslancu v . Vyberme ľubovoľný vrchol v_0 . Ten je v nejakom komponente súvislosti grafu. Posúvajte sa dopredu z v_0 v smere hrán. Postupne budeme navštevovať vrcholy, a keďže ich je konečne veľa, tak narazíme na vrchol, ktorý sme už navštívili. Preto máme v komponente cyklus. Zároveň si môžeme všimnúť, že viac cyklov v komponente mať nemôžeme, keďže z cyklu nevedie hrana von, teda by neexistovala cesta medzi týmito cyklami. Rovnako nemôžeme mať 2 cykly zdieľajúce vrchol, keďže z každého vrchola vedie iba jedna hrana. Preto máme v komponente práve jeden cyklus, teda keď odoberieme z neho hranu, dostaneme strom. Inak povedané, každý komponent grafu obsahuje cyklus a každý vrchol cyklu je koreňom stromu, ktorý sa „napája na cyklus“ (môže byť aj veľkosti 1).

Začnime podúlohou 2. V každom komponente môžeme zo „stromových častí“ začať odoberať vrcholy od listov (veľvyslanci, na ktorých sa nikto nepozerá začnú odchádzať). Takto odoberieme všetky stromy bez toho, aby nejaký vrchol zaspal. Ostal nám cyklus $v_1 v_2 \dots v_k$, kde hrany sú $\{v_i, v_{i+1}\}$, $\{v_k, v_1\}$. Z neho môžeme odoberať vrcholy postupne $v_1, v_2, \dots, v_{k-1}$, pričom zaspí iba vrchol v_k . Teda pre každý komponent vieme dosiahnuť, aby zaspal práve jeden vrchol. Menej unudených vrcholov mať nemôžeme, keďže v komponente je cyklus a ak odoberieme vrchol z cyklu (čo musíme, lebo vrcholy z cyklu sa pozerajú do cyklu), tak jeden vrchol zaspí. Teda minimum unudených vrcholov je počet komponentov, čo je najviac $\lfloor \frac{n}{2} \rfloor$. Tento počet spĺňa konštrukcia, kde máme samé dvojcykly prípadne jeden trojcyklus, ak je n nepárne.

Pokračujme 3. podúlohou. V každom komponente veľkosti k môžeme mať vždy najmenej 1 unudený vrchol a najviac $k - 1$ unudených vrcholov, keďže aspoň jeden vrchol musíme odstrániť. Teda za každý komponent je tento súčet najviac k . Sčítaním cez všetky komponenty dostávame požadované tvrdenie.

Na 1. podúlohu je odpoveď $\left\lceil \frac{n}{3} \right\rceil$. Pre konštrukciu zvolíme samé trojcykly, prípadne jeden 4-cyklus alebo 5-cyklus podľa zvyšku n po delení tromi. Z každého trojcyklu môže byť najviac 1 vrchol unudený a z 4-cyklu, resp. 5-cyklu najviac 2, keďže unudených vrcholov musí byť najviac toľko ako odídených, pokiaľ sa na každý vrchol pozerá 1 vrchol. Tým dostaneme $\left\lceil \frac{n}{3} \right\rceil$ unudených vrcholov. Stačí ukázať, že $\left\lceil \frac{n}{3} \right\rceil$ unudených vrcholov vždy vieme mať.

Predpokladajme sporom, že by to tak nebolo pre nejaký graf s našimi vlastnosťami (teda pre taký graf, kde z každého vrcholu vedie práve jedna hrana). Vyberme najmenší taký graf (počtom vrcholov), pre ktorý to neplatí. Predpokladajme, že v nejakom komponente existuje list l (nevedie do neho hrana), ktorého nasledovník nie je v cykle. Potom odstránime nasledovníka. Všetky vrcholy, z ktorých viedla hrana do nasledovníka vrátane l zaspia. Dostávame znovu graf s našimi vlastnosťami, pričom sme odobrali k vrcholov a z toho $k - 1$ vrcholov zaspalo. To je viac ako tretina a z minimality grafu vieme odstraňovať vrcholy, aby aspoň tretina zvyšných zaspala. Dokopy teda máme viac ako tretinu unudených, čo je spor. Preto taký list neexistuje, teda všetky vrcholy majú vzdialenosť od cyklu najviac 1.

Nech má komponent k vrcholov. Označme $f(v)$ počet hrán vedúcich do vrcholu v . Vrcholy mimo cyklu majú $f(v) = 0$ a súčet všetkých $f(v)$ je k (počet hrán, teda aj počet vrcholov). Pokiaľ je počet vrcholov v cykle párný, vyberme vrcholy na párných miestach alebo na nepárnych miestach, ktoré majú väčší súčet $f(v)$. Ich súčet $f(v)$ je zároveň počet unudených vrcholov, ktorý je preto aspoň polovica. To je aspoň tretina, čo sme chceli dokázať. Pokiaľ je cyklus nepárny, tak vyberme vrchol u z cyklu s najmenším $f(u)$. Zostane nám párný počet vrcholov na cykle a z nich opäť vyberme vrcholy na párných alebo nepárnych miestach s väčším súčtom $f(v)$. Pokiaľ má cyklus c vrcholov, počet unudených vrcholov bude aspoň $\frac{c-1}{2c}k \geq \frac{k}{3}$, keďže priemerná hodnota $f(v)$ na cykle je $\frac{k}{c}$, vyberieme $\frac{c-1}{2}$ vrcholov a $c \geq 3$. Dokopy ich preto bude tiež aspoň $\frac{n}{3}$, čo bolo treba dokázať.

Iné riešenie (trochu trikové)

Preveďme si úlohu na graf ako v prvom riešení. Už vieme, že ak odoberieme v komponente hranu z cyklu, dostaneme strom. Ignorujme na chvíľu takúto hranu h . Nech má daný komponent k vrcholov. Vrchol v , z ktorého vychádzala h je teraz koreňom stromu. Ofarbíme strom bipartitne dvomi farbami - párne vrstvy namodro (tie, obsahujúce v) a nepárne vrstvy načerveno. Pokiaľ odoberieme celú modrú množinu vrcholov, pričom najprv odoberieme vrchol v (aby náhodou nezaspal pri odoberaní iného vrchola), zaspia všetky červené vrcholy. Pokiaľ odstránime celú červenú množinu, zaspia všetky modré vrcholy okrem v a možno aj vrchol v (ak h išla do červeného vrcholu). Dokopy zaspí aspoň $k - 1$ vrcholov a najviac k . Pri jednej možnosti odobrania máme preto aspoň $\frac{k-1}{2}$ unudených vrcholov a pri druhej najviac $\frac{k}{2}$ unudených vrcholov.

Teraz ľahko vyriešime 1. aj 2. podúlohu. Pokiaľ $k = 2$, tak z daného komponentu vieme vynútiť 1 unudený vrchol. Pre $k \geq 3$ platí $\frac{k-1}{2} \geq \frac{k}{3}$, teda vieme vynútiť aspoň tretinu unudených vrcholov z každého komponentu. Preto vieme vynútiť aspoň tretinu unudených vrcholov aj v celom grafe. Preto je odpoveď na 1. podúlohu $\left\lceil \frac{n}{3} \right\rceil$ (konštrukcia je rovnaká ako v prvom riešení).

Z každého komponentu vieme vynútiť aspoň polovicu neunudených vrcholov, teda aj v celom grafe. Odpoveď na 2. podúlohu je teda $\left\lfloor \frac{n}{2} \right\rfloor$ (konštrukcia je opäť rovnaká).

Pre tretiu úlohu uvažujme najväčšiu možnú množinu unudených vrcholov. Nech je ich u . Tieto vrcholy sa na seba zrejme nepozerajú. Preto ich môžeme postupne odobrať. Zvýšia nám ostatné vrcholy, z ktorých odoberáme ľubo-

voľne. Počet unudených vrcholov je potom najviac $n - u$, keďže aspoň u bolo odobratých. Najmenší možný počet unudených vrcholov preto nemôže byť viac ako $n - u$. Preto súčet najmenšieho a najväčšieho počtu unudených vrcholov je najviac n , čo bolo treba dokázať.

1.10 Komandá Mriežku Strážia

Zadanie. *Súd súdil spravodlivo a usúdil, že odsúdiť Geometrov na osud vazalov je súdne. Hrdinní Al-Gebraici budú spravovať ich zem po mnoho rokov. A tak vláda Al-Gebry vyslala svojich vojakov, aby strážili mier na tomto území.*

Územie krajiny Geometrie si vieme predstaviť ako tabuľku $p \times p$, kde $p \geq 5$ je prvočíslo. Dokážte, že počet spôsobov, ako možno rozmiestniť p nerozlišiteľných vojakov do tejto tabuľky tak, aby bol na každom políčku najviac jeden vojak a zároveň neboli všetci vojaci v jednom riadku (v jednom stĺpci však byť môžu), je deliteľný p^5 .

Riešenie.

opravuje Michal Staník (michal.stanik@trojsten.sk)

Začnime tým, že si spočítame počet spôsobov, ako možno rozmiestniť p vojakov do zadanej tabuľky. Ak už riešite úlohu 10, malo by to byť jednoduché cvičenie z kombinatoriky. Máme p^2 políčok, z nich chceme vybrať p , vojaci sú nerozlišiteľní, takže na poradi nezáleží. Počet možností teda vieme vyjadriť kombinačným číslom $\binom{p^2}{p}$. Od toho ale ešte musíme odpočítať možnosti, ktoré zadanie vylučuje – keď sú všetci vojaci v jednom riadku. Takých možností je p , pretože máme p riadkov a ak sú v nejakom riadku všetci vojaci, môže to byť iba jedným spôsobom – zaberajú všetky políčka. Chceme teda dokázať, že

$$p^5 \mid \binom{p^2}{p} - p.$$

Postupne budeme tento výraz upravovať, zjednodušovať a vynímať z neho p , až dokým nebudeme mať päť p -čok (v súčine), ktoré sme z neho vyňali alebo ktoré ho delia. Poďme na to! Začnime rozpísaním kombinačného čísla podľa definície ako

$$\binom{p^2}{p} - p = \frac{p^2(p^2 - 1) \cdots (p^2 - p + 1)}{p!} - p = p \left(\frac{(p^2 - 1) \cdots (p^2 - p + 1)}{(p - 1)(p - 2) \cdots 1} - 1 \right).$$

Prvé p sme vyňali, chceme teda ešte nájsť štyri p -čka v prvočíselnom rozklade veľkej zátvorky. Tú môžeme vynásobiť $(p - 1)!$, pretože toto číslo je nesúdeliteľné s prvočíslom p , a teda chceme, aby p^4 delilo výraz

$$(p^2 - 1)(p^2 - 2) \cdots (p^2 - (p - 1)) - (p - 1)!.$$

Predstavme si, že začneme roznásobovať tie zátvorky v člene naľavo od mínus. Z každej vyberieme p^2 alebo malé číslo (menšie ako p) s mínusom. Ak vyberieme aspoň dvakrát člen p^2 , dostaneme niečo deliteľné p^4 , čo nás pri určovaní deliteľnosti p^4 nezaujíma. Zaujímajú nás teda členy, kedy vyberieme práve jedno p^2 (a zo všetkých zátvoriek vyberieme malé číslo) alebo žiadne p^2 . Žiadne p^2 sa dá iba jedným spôsobom, kedy dostaneme $(p - 1)!$ (mínusov je párny počet), čo sa nasčíta na nulu s $-(p - 1)!$, ktorý už vo výraze máme.

Aké členy dostaneme s vybraním práve jedného p^2 ? Zo všetkých ostatných zátvoriek vyberieme malé číslo, máme tak súčin všetkých čísel od -1 do $-(p - 1)$, kde jedno číslo chýba (to zo zátvorky, z ktorej sme vyberali p^2). To

vieme zapísať ako $\frac{(p-1)!}{-i}$, ak i je to chýbajúce číslo. Dostali sme

$$p^2 \left(\frac{(p-1)!}{-1} + \frac{(p-1)!}{-2} + \dots + \frac{(p-1)!}{-(p-1)} \right).$$

Z Eulerovej vety vieme, že ak $\varphi(n)$ je počet čísel menších alebo rovných n nesúdeliteľných s n , tak pre všetky a nesúdeliteľné s n platí

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

$$a \cdot a^{\varphi(n)-1} \equiv 1 \pmod{n}.$$

Ďalej platí $\varphi(p^2) = p^2 - p$, takže inverzné prvky (ktoré sa vynásobia s číslom na jednotku) dostaneme umocnením na $p^2 - p - 1$.

Späť k nášmu výrazu: vyňali sme ďalšie dve p -čka, takže už iba chceme, aby p^2 delilo výraz

$$\frac{(p-1)!}{1} + \frac{(p-1)!}{2} + \dots + \frac{(p-1)!}{p-1} \equiv (p-1)!(1^{p^2-p-1} + \dots + (p-1)^{p^2-p-1}) \pmod{p^2}.$$

Je jedno, že sme to prenásobili mínus jednotkou, deliteľnosť to nezmení.

Činiteľ $(p-1)!$ je nesúdeliteľný s p^2 a je v súčine so zvyškom výrazu, môžeme ho teda dať preč, nemá vplyv na deliteľnosť p^2 . Členy v zátvorke popárujeme (člen a^{p^2-p-1} s členom $(p-a)^{p^2-p-1}$) a pomocou binomickej vety (umocňovanie súčtu) máme

$$\begin{aligned} \sum_{a=1}^{\frac{p-1}{2}} (a^{p^2-p-1} + (p-a)^{p^2-p-1}) &= \sum_{a=1}^{\frac{p-1}{2}} (a^{p^2-p-1} + p^2(\dots) + p(p^2-p-1)a^{p^2-p-2} - a^{p^2-p-1}) \equiv \\ &\equiv \sum_{a=1}^{\frac{p-1}{2}} p(p^2-p-1)a^{p^2-p-2} \pmod{p^2}. \end{aligned}$$

Člen $p^2(\dots)$ reprezentuje nejaké členy súčtu, kde je p v aspoň druhej mocnine, a teda sú všetky deliteľné p^2 , čiže nás nezaujímajú.

Výborne, máme ďalšie vyňaté p . Ostáva ukázať, že

$$\begin{aligned} p \left| (p^2-p-1) \sum_{a=1}^{\frac{p-1}{2}} a^{p^2-p-2}, \right. \\ \left. p \left| \sum_{a=1}^{\frac{p-1}{2}} a^{-2}, \right. \right. \end{aligned}$$

pretože p a $p^2 - p - 1$ sú nesúdeliteľné a $a^{p^2-p} \equiv (a^{p-1})^p \equiv 1^p \equiv 1 \pmod{p}$.

Členy v súčte sú všetky rôzne modulo p , pretože ak by sa dva rovnali, tak

$$a^{-2} \equiv b^{-2} \pmod{p},$$

$$b^2 \equiv a^2 \pmod{p},$$

$$0 \equiv a^2 - b^2 = (a - b)(a + b) \pmod{p}.$$

z čoho na intervale od 1 do $\frac{p-1}{2}$ nutne platí $a = b$.

Uvedomme si, že v súčte je každý kvadratický zvyšok³ práve raz. Navyše vieme, že $a^2 \equiv (-a)^2$, takže súčet všetkých kvadratických zvyškov, každého práve raz, dostaneme aj sčítaním a^2 od 1 do $\frac{p-1}{2}$. Náš súčet mínus druhých mocnín je teda v skutočnosti súčet druhých mocnín od 1 do $n = \frac{p-1}{2}$. O ňom vieme, že je to $\frac{1}{6}n(n+1)(2n+1)$. Keďže $p \geq 5$, šestina nás nezaujíma (je nesúdeliteľná s p) a $(2n+1) = p$ je deliteľné p , čím je dôkaz hotový.

Na záver: krokov je síce veľa, ale úpravy sú ekvivalentné v zmysle, že všetky výrazy cestou musia byť deliteľné tým, čím chceme, ak má dokazované tvrdenie platiť. Preto ak sa znižuje mocnina p a zjednodušujú sa nám výrazy, nevieme sa dostať úplne do slepej uličky (možno sa dostaneme k niečomu, čo je ťažšie dokázať, ale aspoň máme stále platné tvrdenie, tak by sme ho mohli byť schopní dokázať).

³číslo vyjadriteľné ako $a^2 \pmod{p}$ pre nejaké a