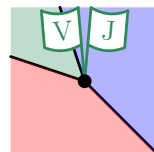


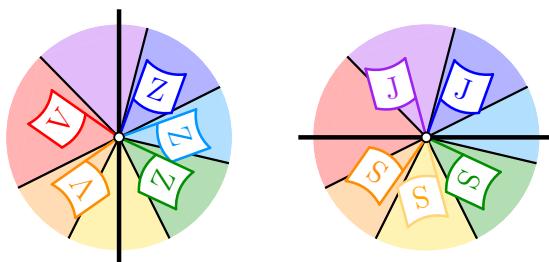
Úlohy domácího kola kategorie A

1. *Ostrov je rozdělený na několik království. Území každého království je konvexní mnohoúhelník, který má právě jeden nejsevernější, nejjižnější, nejvýchodnější a nejzápadnější bod. Každý král dostal 4 vlajky s písmeny S, J, V, Z, které umístil do těchto významných bodů svého království. (Například u trojmezí tří států na obrázku jsou takto zapíchnuté 2 vlajky.)*



Ve vnitrozemí je krtinec, kde se stýká 7 království. Určete všechny možné počty vlajek zapíchnutých do krtince. (Josef Tkadlec)

ŘEŠENÍ. Nejprve ukážeme, že do krtince je zapíchnuto 5 vlajek s písmeny V nebo Z. Nakreslíme přímku procházející krtincem ze severu na jih (svisle) a nazveme ji *poledník*. Žádná strana království neleží na poledníku, protože by neexistoval právě jeden jeho nejzápadnější nebo právě jeden jeho nejvýchodnější bod. Sledujme úhly jednotlivých



království s vrcholem v krtinci (tj. vnitřní úhly příslušných konvexních mnohoúhelníků v tomto vrcholu). Protože žádná hranice nevede svisle, některý úhel obsahuje polopřímku s počátkem v krtinci směřující na sever a některý úhel obsahuje polopřímku s počátkem v krtinci směřující na jih. Jde o úhly dvou různých království, jelikož království jsou konvexní. V těchto dvou královstvích nebude v krtinci vlajka V ani Z. Zbývající úhly leží buď celé na západ od poledníku a tehdy je krtinec nejvýchodnějším bodem království, nebo celé na východ od poledníku a tehdy je krtinec nejzápadnějším bodem. To znamená, že do krtince je zapíchnuto $7 - 2 = 5$ vlajek s písmeny V nebo Z. Podobně ukážeme, že je tam 5 vlajek s písmeny S nebo J. Celkem je tedy do krtince zapíchnuto 10 vlajek. Z obrázků výše je vidět, jak vlajky mohou být rozmístěny.

NÁVODNÉ A DOPLŇUJÍCÍ ÚLOHY:

Není-li uvedeno jinak, předpokládáme, že království má tvar konvexního mnohoúhelníku.

- N1. Načrtněte konvexní mnohoúhelník, který a) má, b) nemá právě jeden nejvýchodnější bod. [Konvexní mnohoúhelník má více nejvýchodnějších bodů právě tehdy, pokud některá jeho strana je rovnoběžná s osou y a celý mnohoúhelník se nachází západně od ní.]
- N2. Uvažujme v rovině body B a C tak, že bod C se nachází severozápadně od bodu B . Najděte všechny polohy bodu A , pro které má trojúhelník s vrcholy A, B, C právě jeden nejvýchodnější bod, a to bod B . [Vyhovují právě všechny body, které se nacházejí západně od poledníku procházejícího bodem B a zároveň neleží na přímce BC . Pod poledníkem myslíme přímku ze severu na jih.]

- N3. Načrtněte království, které má v jednom ze svých vrcholů 0, 1, 2, 3 nebo 4 vlajky, nebo rozhodněte, že takové neexistuje. [Daný vrchol nemůže být současně nejjižnějším a nejsevernějším bodem království. Podobně nemůže být současně nejvýchodnějším a nejzápadnějším bodem království. Možné počty jsou tak jen 0, 1, 2 a snadno se ověří, že všechny vyhovují.]
- N4. Uvnitř ostrova (jako ze zadání soutěžní úlohy) je bod X , ve kterém se stýkají tři království a jsou v něm zapíchnuty právě dvě vlajky. Jaké všechny kombinace písmen se na nich mohou objevit? [SV, SZ, JV, JZ. Uvažujme poledník procházející bodem X . Ani jedna strana ani jednoho království neleží na poledníku, protože by neexistoval právě jeden nejzápadnější nebo nejvýchodnější bod. Také se nemůže stát, že všechny tři hranice budou na jedné straně od poledníku, neboť by vzniklo nekonvexní království. Proto na jedné straně od poledníku musí být jedna hranice a na druhé dvě hranice – na této straně bude i vlajka V nebo Z. V bodě X tak musí být zapíchnuta právě jedna z vlajek V, Z a analogicky i právě jedna z vlajek S, J. To nám dává 4 možnosti, jak jsme uvedli na začátku.]
- D1. Ukažte, že pokud bychom v soutěžní úloze uvažovali nekonvexní království, mohlo by se stát, že v krtinci nebude zapíchnuta žádná vlajka. [Každé ze 7 království může být nekonvexní mnohoúhelník tvaru spirály, který má jeden vrchol v krtinci a pak se obtáčí kolem něj. Takto lze zajistit, že každý mnohoúhelník bude mít alespoň jeden svůj bod severně, jižně, východně i západně od krtince. To znamená, že v krtinci nebude ani jedna vlajka.]
- D2. Uvnitř konvexního desetiúhelníku $A_1A_2\ldots A_{10}$ je dán bod P , který neleží na žádné úhlopříčce. Dokažte, že některé dvě z polopřímek $A_1P, A_2P, \ldots, A_{10}P$ protínají stejnou stranu desetiúhelníku. [Uvažujme hlavní úhlopříčku A_1A_6 . Ta rozdělí desetiúhelník na dvě části a bod P leží uvnitř jedné z nich. Bez újmy na obecnosti ať leží uvnitř šestiúhelníku $A_1A_6A_7A_8A_9A_{10}$. Potom 6 polopřímek $A_1P, A_2P, \ldots, A_6P$ vstoupí do šestiúhelníku přes stranu A_1A_6 a opustí tento šestiúhelník přes zbývajících 5 stran, takže alespoň dvě polopřímky opustí šestiúhelník přes stejnou stranu. Tyto strany jsou zároveň strany původního desetiúhelníku, takže některé dvě polopřímky protnou stejnou stranu tohoto desetiúhelníku.]

2. Necht p, q jsou reálná čísla taková, že rovnici

$$|x^2 - 1| = px + q$$

s neznámou x vyhovují právě 4 navzájem různá reálná čísla.

a) Určete všechny možné hodnoty součtu těchto 4 čísel.

b) Dokažte, že součin těchto 4 čísel leží v intervalu $(-3, 1)$. (Patrik Bak)

ŘEŠENÍ. Rovnice ze zadání je pro $|x| \geq 1$ ekvivalentní rovnici

$$x^2 - 1 = px + q \quad (1)$$

a pro $|x| < 1$ zase rovnici

$$-x^2 + 1 = px + q. \quad (2)$$

Každá z těchto dílčích rovnic má nanejvýš 2 řešení. Protože podle zadání má původní rovnice 4 řešení, musí mít každá z těchto rovnic nutně právě 2 řešení.

Rovnici (1) ekvivalentně upravíme na tvar

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

takže podle Viètových vztahů mají její dva kořeny součet p .

Podobně rovnici (2) upravíme na

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

takže podle Viètových vztahů mají její dva kořeny součet $-p$. Proto je součet všech čtyř kořenů 0. Ještě musíme ověřit,* že je vůbec možné součet 0 dosáhnout. To je skutečně možné, například pro volbu $p = 0$, $q = \frac{1}{2}$, kdy jsou kořeny $\frac{1}{2}\sqrt{6}$, $-\frac{1}{2}\sqrt{6}$, $\frac{1}{2}\sqrt{2}$, $-\frac{1}{2}\sqrt{2}$.

Abychom určili součin všech kořenů, opět použijeme Viètovy vztahy. Součin kořenů první rovnice je $-(q + 1)$ a v druhé rovnici je $q - 1$, proto je součin všech čtyř kořenů $-(q + 1)(q - 1) = 1 - q^2$, takže potřebujeme odhadnout q .

Rovnice (2) má 2 kořeny splňující $x^2 < 1$, každý z nich je z intervalu $(-1, 1)$. Součin těchto dvou kořenů je proto také z intervalu $(-1, 1)$. Podle Viètových vztahů je přitom roven $q - 1$, takže $q \in (0, 2)$. Proto pro součin všech čtyř kořenů původní rovnice platí $1 - q^2 \in (-3, 1)$, což bylo třeba dokázat v části b).

KOMENTÁŘ. Řešení rovnice $|x^2 - 1| = px + q$ si můžeme představit graficky jako průnik přímky $y = px + q$ a grafu funkce $y = |x^2 - 1|$. Tento graf vznikne z paraboly $y = x^2 - 1$ tak, že její část pod osou x (tedy pro $x \in (-1, 1)$) se překlápí osově souměrně podle osy x .

Úlohu je také možné řešit bez Viètových vztahů tak, že si všechna řešení vyjádříme parametricky pomocí p a q , a následně počítáme už jen s těmito vyjádřeními.

* Neověřením by se mohlo stát, že množina součtů všech 4 kořenů je prázdná

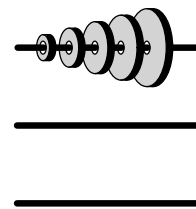
NÁVODNÉ A DOPLŇUJÍCÍ ÚLOHY:

- N1. Najděte všechna řešení rovnice $|x^2 - 1| = x + 1$. [2, 0 a -1. Rozebereme dva případy. Pokud $x^2 \geq 1$, pak $|x^2 - 1| = x^2 - 1$ a řešíme rovnici $x^2 - x - 2 = 0$, kterou lze upravit do tvaru $(x + 1)(x - 2) = 0$. Získáme tak dva kořeny -1 a 2, pro oba platí $x^2 \geq 1$. Pokud $x^2 < 1$, pak $|x^2 - 1| = -x^2 + 1$ a řešíme rovnici $x^2 + x = 0$. Získáme další kořen 0, přičemž pro tento kořen skutečně platí $x^2 < 1$, a kořen -1, který nevyhovuje, protože v tomto případě neplatí $x^2 < 1$. Takže původní rovnice má řešení 2, 0 a -1. Díky ekvivalentním úpravám zkouška není nutná.]
- N2. Určete počet řešení rovnice $|x - 2| = ax$ pro reálný parametr a . [Pokud $x \geq 2$, pak $|x - 2| = x - 2$, takže řešíme rovnici $x - 2 = ax$, které pro $a \neq 1$ vyhovuje $x = \frac{2}{1-a}$. Má platit $x \geq 2$, což je splněno právě pro $0 \leq a < 1$. Pokud $a = 1$, rovnice $x - 2 = ax$ nemá řešení. Nyní vyřešíme případ $x < 2$, kdy $|x - 2| = 2 - x$, takže řešíme rovnici $2 - x = ax$, které pro $a \neq -1$ vyhovuje $x = \frac{2}{a+1}$. Má platit $x < 2$, což je splněno právě pro $a < -1$ nebo $a > 0$. Pokud $a = -1$, pak rovnice $2 - x = ax$ nemá řešení. Rovnice ze zadání má 2 řešení pro $a \in (0, 1)$, 0 řešení pro $a \in [-1, 0)$ a 1 řešení pro zbývající hodnoty a .]
- N3. Připomeňte si Viètovy vztahy: Uvažujme kvadratickou rovnici $x^2 + px + q = 0$ s reálnými parametry p, q , která má dva různé reálné kořeny. Vyjádřete jejich součet a součin pomocí koeficientů. [Pokud má rovnice dva kořeny x_1 a x_2 , pak platí $x^2 + px + q = (x - x_1)(x - x_2) = x^2 - (x_1 + x_2)x + x_1x_2$. Takže součet kořenů splňuje $x_1 + x_2 = -p$ a součin kořenů splňuje $x_1x_2 = q$.]
- D1. Uvažujme dvě rovnice $x^2 + 2px + 2q^2 = 4$, $x^2 - 2qx + 2p^2 = 4$ s reálnými parametry p a q . Předpokládejme, že první má 2 různé reálné kořeny x_1, x_2 , druhá dva různé reálné kořeny x_3, x_4 . Určete všechny možné hodnoty $x_1^2 + x_2^2 + x_3^2 + x_4^2$. [Platí $x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1x_2$. Z Viètových vztahů $x_1 + x_2 = -2p$ a $x_1x_2 = 2q^2 - 4$. Potom $x_1^2 + x_2^2 = 4p^2 - 4q^2 + 8$. Podobně dostaneme $x_3^2 + x_4^2 = 4q^2 - 4p^2 + 8$. Takže jediná možná hodnota součtu je $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 16$. Její dosažitelnost snadno ověříme pro $p = q = 1$.]
- D2. Určete počet reálných kořenů rovnice $x^2 + 4 = a|x|$ v závislosti na reálném parametru a . [B-71-II-2]
- D3. Určete počet reálných kořenů rovnice $x \cdot |x + 6A| = 36$ v závislosti na reálném parametru A . [B-71-I-4]
- D4. Určete všechny hodnoty reálného parametru p tak, aby rovnice

$$2017 \cdot |1 - |1 - |1 - x|| = 2016x + p$$

měla právě tři řešení v oboru reálných čísel. [B-66-II-4]

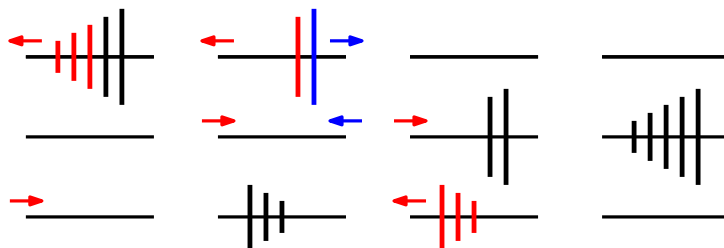
3. Jozef má hlavolam, který se skládá ze tří vodorovných tyčí a z $n \geq 2$ různě velkých kotoučů seřazených na první tyči podle velikosti, viz obrázek. V jednom tahu Jozef vysune z libovolné tyče krajní kotouč (zleva nebo zprava) a nasune jej na jinou tyč ze stejné strany. Hlavolam je vyřešený, pokud se všechny kotouče nachází na druhé tyči seřazené stejně jako na začátku. V závislosti na n určete nejmenší možný počet tahů, který je potřeba na vyřešení hlavolamu.



(Jozef Rajník)

ŘEŠENÍ. Nejprve ukážeme, že může existovat nejvýše jeden kotouč, který přesuneme při řešení zleva právě jednou. Pro spor předpokládejme, že jsou takové kotouče dva, označme je A a B , kde A je menší než B , tedy A je nalevo od B . Proto kotouč A musíme přesunout dříve než B , čili A se bude po přesunutí nacházet napravo od B . Kotouče A a B tak zůstanou v nesprávném pořadí, což je spor.

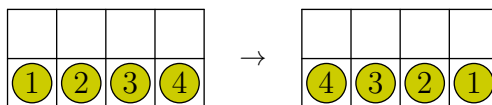
Analogicky může existovat nejvýše jeden kotouč, který přesuneme zprava právě jednou. Dostáváme tak, že nejvýše dva kotouče mohou být přesunuty jen jednou, zbývající musí být přesunuty alespoň dvakrát. Potřebujeme proto alespoň $(n - 2) \cdot 2 + 2 \cdot 1 = 2n - 2$ tahů.



Ukážeme, že $2n - 2$ tahů stačí. Nejdříve po řadě přesuneme $n - 2$ nejmenších kotoučů na třetí tyč z levé strany, takže na ní budou v opačném pořadí. Na první tyči zůstanou dva největší kotouče. Potom přesuneme druhý největší kotouč na druhou tyč z levé strany a největší kotouč z pravé strany. Oba největší kotouče tak budou na této tyči v původním pořadí. Nakonec po řadě přesuneme $n - 2$ nejmenších kotoučů ze třetí tyče na druhou tyč z levé strany. Jelikož na třetí tyči bylo těchto $n - 2$ kotoučů v opačném pořadí vzhledem k pořadí na začátku, po přesunech na druhou tyč budou tyto kotouče seřazené jako na začátku. Napravo od nich je druhý největší a potom největší kotouč. Kotouče jsou proto seřazené jako na začátku a celkově jsme potřebovali $(n - 1) + 1 + 1 + (n - 1) = 2n - 2$ tahů. Obrázek ilustruje tento postup pro $n = 5$.

NÁVODNÉ A DOPLŇUJÍCÍ ÚLOHY:

- N1. Uvažujme obdélníkový hrací plán 4×2 a na něm 4 žetony očíslované 1, 2, 3, 4 a rozmístěné jako na obrázku vlevo. V jednom tahu lze přesunout jeden žeton z jeho políčka na políčko sousedící stranou. Nejméně kolika tahy lze z původního rozestavení získat rozestavení na obrázku vpravo? Na jednom políčku se může nacházet i více než jeden žeton.



[Žeton 1 potřebujeme posunout o 3 políčka doprava, k čemuž jsou potřeba 3 tahy. Rovněž na žeton 4 potřebujeme alespoň 3 tahy. Žetony 2 a 3 potřebujeme posunout o políčko

vedle, tedy na každý z nich potřebujeme alespoň jeden tah. Dohromady tedy potřebujeme alespoň $3 + 1 + 1 + 3 = 8$ tahů. Tohoto počtu tahů lze zjevně dosáhnout.]

- N2. Vyřešte předchozí úlohu za předpokladu, že na jednom políčku se najednou nemůže nacházet více než jeden žeton. [Tahy rozdělíme na *vodorovné* (žeton přesouváme v rámci řádku) a *svislé* (v rámci sloupce). Vodorovných tahů potřebujeme alespoň 8 na základě úvah z předchozího úkolu. Pokud dva žetony neprovedou žádný svislý tah, tak jsou po celou dobu ve spodním řádku, a tedy je neumíme vyměnit. Proto nejvýše jeden žeton provede 0 svislých tahů. Každý ze zbývajících žetonů musí provést svislý tah, dokonce alespoň dva, jelikož se musí vrátit do spodního řádku. Tedy dohromady musí žetony provést alespoň $3 \cdot 2 = 6$ svislých tahů, což celkově dává alespoň $8 + 6 = 14$ tahů. Za 14 tahů umíme hlavolam vyřešit následovně: Nejprve žetony 2, 3, 4 přesuneme do horního řádku (3 tahy). Potom přesuneme žeton 1 zcela doprava (3 tahy). Přesuneme žeton 2 dolů a doprava (2 tahy). Žeton 3 přesuneme vlevo, dolů (2 tahy) a žeton 4 vlevo, vlevo, vlevo, dolů (4 tahy).]
- N3. Dokažte, že pro $n = 3$ nelze hlavolam ze soutěžního úlohy vyřešit na 3 tahy. [Každý kotouč musíme přesunout alespoň jednou, čili při třech tazích musí být každý kotouč přesunut právě jednou. Proto alespoň dva kotouče musí být vysunuty z první tyče ze stejné strany. Jelikož je už potom nepřesouváme, tak je musíme nasunout na druhou tyč. Potom ale nebudou na druhé tyči ve správném pořadí.]
- D1. Vyřešte úlohu N2 obecně pro herní plán $2n \times 2$ a $2n$ žetonů ve spodním řádku, kde n je kladné celé číslo. [A-72-I-3]
- D2. Uvažujme stejný hlavolam jako v soutěžní úloze s dodatečnými omezeními: kotouče lze vysouvat a nasouvat jen zleva a v každém okamžiku musí být kotouče na každé tyči uspořádány vzestupně podle velikosti zleva doprava. Jedná se vlastně o hlavolam známý pod názvem *Hanojské věže*. V závislosti na kladném celém čísle n určete nejmenší počet tahů nutných k vyřešení tohoto hlavolamu. [$2^n - 1$. Důkaz matematickou indukcí. Pro $n = 1$ je třeba $1 = 2^1 - 1$ přesun. Předpokládejme, že pro n kotoučů je nejmenší počet tahů $2^n - 1$. Abychom mohli přesunout největší kotouč na druhou tyč, musí být jako jediný na první tyči a zbývajících n kotoučů musí být na třetí tyči. K jejich přesunu potřebujeme podle indukčního předpokladu $2^n - 1$ tahů. Po přesunutí největšího kotouče na druhou tyč musíme na druhou tyč přesunout ještě zbývajících n kotoučů, na což opět potřebujeme alespoň $2^n - 1$ tahů. Celkově tak třeba alespoň $(2^n - 1) + 1 + (2^n - 1) = 2^{n+1} - 1$ tahů. Konkrétní posloupnost tahů přímo vyplývá ze způsobu získání tohoto odhadu.]
- D3. Uvažujme modifikaci Hanojských věží, kde je zakázáno přesouvat kotouče mezi první a třetí tyčí. Kolik nejméně tahů potřebujeme k přesunu všech kotoučů na *třetí* tyč? [$3^n - 1$. Naznačíme jen hlavní myšlenku důkazu indukcí. Pro přesun $n + 1$ kotoučů potřebujeme dvakrát přesunout největší kotouč. Největší kotouč musíme nejprve přesunout na druhou tyč. Proto musíme zbylých n kotoučů přesunout na třetí tyč ($3^n - 1$ tahů). Po přesunu největšího kotouče musíme zbytek přesunout zpět na první tyč (opět $3^n - 1$ tahů), abychom mohli největší kotouč přesunout na třetí tyč. Potom znovu přesuneme zbývajících kotoučů na třetí tyč ($3^n - 1$ tahů). Celkově dostáváme alespoň $3 \cdot (3^n - 1) + 2 = 3^{n+1} - 1$ tahů. Konstrukce opět vyplývá z popsaného postupu.]
- D4. V kruhu je 100 zelených mimozemšťanů, každý z nich má 100 tabletů. V rámci jednoho tahu libovolný mimozemšťan vezme několik svých tabletů a rozdělí je mezi ostatní mimozemšťany (ne nutně rovnoměrně a ne nutně mezi všechny). Po jakém nejmenším počtu tahů mohou mimozemšťané docílit, aby žádní dva z nich neměli stejný počet tabletů? [KMS 2018/19, 2. letní kolo, úloha 3]
- D5. Uvažujme šachovnici rozměrů 8×8 . Na každém z osmi políček v první řadě je bílá dáma a na každém z osmi políček v osmé řadě je černá dáma. V jednom tahu můžeme pohnout libovolnou dámou podle šachových pravidel (tedy vodorovně, svisle nebo diagonálně) na volné políčko. Tyto tahy opakujeme tak, aby se barvy pohybujících se dam střídaly. Určete nejmenší počet tahů, po kterém budou v první řadě všechny černé a v osmé řadě všechny bílé dámy. [KMS 2018/19, 2. letní kolo, úloha 7]

4. Jsou dána nesoudělná přirozená čísla a a b taková, že i čísla $a^3 - 1$ a $b^3 - 1$ jsou nesoudělná. Dokažte, že čísla $a^2 - b$ a $b^2 - a$ jsou rovněž nesoudělná. (Patrik Bak)

ŘEŠENÍ. Sporem předpokládejme, že čísla $a^2 - b$ a $b^2 - a$ jsou soudělná, tedy existuje prvočíslo p , které je obě dělí. Potom toto prvočíslo dělí i jejich rozdíl, tedy

$$(a^2 - b) - (b^2 - a) = (a - b)(a + b) + a - b = (a - b)(a + b + 1).$$

Proto platí $p \mid a - b$ nebo $p \mid a + b + 1$.

- (i) Pokud $p \mid a - b$, máme $p \mid (a^2 - b) - (a - b) = a^2 - a = a(a - 1)$, takže $p \mid a$ nebo $p \mid a - 1$. Případ $p \mid a$ však spolu s $p \mid a - b$ dává $p \mid b$, což je spor s nesoudělností a , b . Musí proto platit $p \mid a - 1$, tedy $p \mid (a - 1)(a^2 + a + 1) = a^3 - 1$. Analogicky odvodíme i $p \mid b^3 - 1$, což je spor s nesoudělností čísel $a^3 - 1$ a $b^3 - 1$ ze zadání.
- (ii) Pokud $p \mid a + b + 1$, máme $p \mid (a^2 - b) + (a + b + 1) = a^2 + a + 1$, takže $p \mid (a - 1)(a^2 + a + 1) = a^3 - 1$. Analogicky odvodíme $p \mid b^3 - 1$, což je znovu spor s nesoudělností čísel $a^3 - 1$ a $b^3 - 1$.

V obou případech jsme obdrželi spor se zadáním, a proto platí, že čísla $a^2 - b$ a $b^2 - a$ jsou nesoudělná.

JINÉ ŘEŠENÍ. Sporem předpokládejme, že čísla $a^2 - b$ a $b^2 - a$ jsou soudělná. Potom existuje prvočíslo p , pro které platí $p \mid (a^2 - b)$ i $p \mid (b^2 - a)$. Z toho plyne $a^2 \equiv b \pmod{p}$ a $b^2 \equiv a \pmod{p}$. Dosazením do druhé kongruence dostáváme $a^4 \equiv (a^2)^2 \equiv b^2 \equiv a \pmod{p}$, tedy $p \mid a^4 - a = a(a^3 - 1)$.

Pokud by platilo $p \mid a$, tak z $b^2 \equiv a \equiv 0 \pmod{p}$ dostáváme $p \mid b^2$ a jelikož p je prvočíslo, tak i $p \mid b$, což je ve sporu s nesoudělností čísel a a b . Proto musí platit $p \mid a^3 - 1$.

Analogickým postupem dostaneme, že $p \mid b^3 - 1$. Tím by však prvočíslo p dělilo obě čísla $a^3 - 1$ a $b^3 - 1$, což je ve sporu se zadáním. Proto jsou čísla $a^2 - b$ a $b^2 - a$ nesoudělná.

NÁVODNÉ A DOPLŇUJÍCÍ ÚLOHY:

- N1. Jsou dána přirozená čísla a , b . Dokažte, že pokud existuje prvočíslo p takové, že $p \mid a + 6$ a $p \mid b - 3$, tak $p \mid a + 2b$. [Pokud $p \mid a + 6$ a $p \mid b - 3$, tak $p \mid (a + 6) + 2 \cdot (b - 3) = a + 2b$.]
- N2. Které z následujících dvojic čísel jsou nesoudělné pro všechny dvojice nesoudělných celých čísel a , b ? a) a , $a + b$, b) $a + b$, ab , c) $a^2 + b^2$, ab , d) $a + b$, $a - b$, e) a^3 , $(a + 1)^5$. [Nesoudělné jsou dvojice a), b), c), e). a) Ukážeme to sporem. Necht existuje společný dělitel $d > 1$ takový, že $d \mid a$ a $d \mid a + b$. Potom platí, že d dělí i rozdíl těchto čísel, tj. $d \mid b$, což je spor s nesoudělností a a b . b) Opět postupujeme sporem. Necht existuje prvočíslo p , které dělí $a + b$ i ab . Protože p je prvočíslo, musí platit $p \mid a$ nebo $p \mid b$. Bez újmy na obecnosti necht $p \mid a$. Potom z $p \mid a + b$ nutně plyne, že $p \mid b$, což je spor s nesoudělností čísel a a b . c) Postupujeme podobně jako v části b) s využitím toho, že pokud p je prvočíslo, tak z $p \mid b^2$ vyplývá, že $p \mid b$. d) Čísla $a + b$ a $a - b$ jsou soudělná například pro $a = 3$, $b = 1$, která jsou sama nesoudělná. e) Pro důkaz sporem necht existuje prvočíslo p , které dělí a^3 i $(a + 1)^5$. Jelikož p je prvočíslo a $p \mid a^3$, tak i $p \mid a$. Podobně z $p \mid (a + 1)^5$ plyne $p \mid a + 1$. Ale pak i $p \mid a + 1 - a = 1$, což je spor.]

* Relaci přirozené číslo A dělí přirozené číslo B zapisujeme $A \mid B$ a čteme „ A dělí B “ nebo „ B je dělitelné A “.

** Relaci dvě celá čísla A a B dávají stejný zbytek při dělení číslem C zapisujeme $A \equiv B \pmod{C}$ a čteme „ A je kongruentní B modulo C “.

D1. Dokažte, že pro každé celé číslo n je zlomek

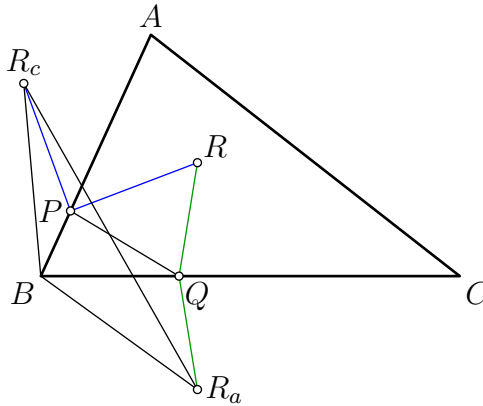
$$\frac{21n + 4}{14n + 3}$$

v základním tvaru. (IMO 1959, úloha 1)[Pro spor předpokládejme, že existuje prvočíslo p takové, že $p \mid 21n + 4$ a současně $p \mid 14n + 3$. Potom $p \mid 3 \cdot (14n + 3) - 2 \cdot (21n + 4) = 1$, což je ve sporu s tím, že p je prvočíslo.]

D2. Necht a, b, c, n jsou kladná celá čísla taková, že jsou splněny následující podmínky: a) čísla $a, b, c, a + b + c$ jsou po dvou nesoudělná; b) číslo $(a + b + c)(a + b)(b + c)(c + a)(ab + bc + ca)$ je n -tou mocninou celého čísla. Dokažte, že součin abc lze zapsat jako rozdíl dvou n -tých mocnin celých čísel. [A-68-III-3]

5. Uvnitř ostroúhlého trojúhelníku ABC je dán bod R . Na stranách AB a BC leží po řadě body P a Q tak, že obvod trojúhelníku PQR je nejmenší možný. Podobně na stranách BC a AC leží po řadě body S a T tak, že obvod trojúhelníku RST je nejmenší možný. Přímky PQ a ST se protínají v bodě K . Dokažte, že pokud platí $|\sphericalangle BAK| = |\sphericalangle CAR|$, pak trojúhelníky PQR a RST mají stejný obvod. (Michal Pecho)

ŘEŠENÍ. Označme R_a a R_c body souměrně sdružené s R po řadě podle přímek BC a AB . Nejprve se zaměříme na trojúhelník PQR . Necht P leží na AB a Q na BC libovolně. Ze souměrnosti platí $|R_cP| = |PR|$ a $|R_aQ| = |QR|$. Proto je obvod trojúhelníku PQR roven délce lomené čáry R_cPQR_a a bude nejmenší možný právě tehdy, když bude délka této lomené čáry nejmenší možná. Z trojúhelníkové nerovnosti je délka lomené čáry R_cPQR_a alespoň $|R_cR_a|$, proto bude nejkratší, právě když body P a Q budou průsečíky úsečky R_aR_c po řadě se stranami AB a BC . Ještě musíme ověřit, že úsečka R_aR_c skutečně protíná strany AB a AC .



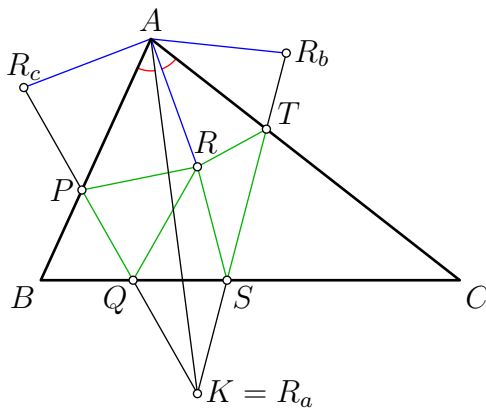
Nejprve ukážeme, že úsečka R_aR_c protne polopřímky BA , BC . Platí $|\sphericalangle R_aBR_c| = |\sphericalangle R_aBR| + |\sphericalangle RBR_c| = 2 \cdot |\sphericalangle CBR| + 2 \cdot |\sphericalangle RBA| = 2 \cdot |\sphericalangle CBA| < 180^\circ$, takže úhel R_aBR_c je konvexní a úsečka R_aR_c protíná obě polopřímky BA , BC .

Nyní zdůvodníme, že úsečka R_aR_c protne i polopřímky AB a CB . Z ostroúhlosti trojúhelníku ABC máme $|\sphericalangle BAC| < 90^\circ$ a $2 \cdot |\sphericalangle BAC| < 180^\circ$. To znamená, že obraz úhlu BAC v osově souměrnosti podle přímky AB bude ležet v polorovině ACB . Jelikož R leží uvnitř úhlu BAC , jeho obraz R_c v osově souměrnosti podle přímky AB leží v polorovině ACB . Analogicky ukážeme, že R_c leží v polorovině ACB , a proto i úsečka R_aR_c leží v polorovině ACB a protíná polopřímky AB a BC . To spolu s faktem, že úsečka R_aR_c protíná i polopřímky BA a CB dává, že úsečka R_aR_c skutečně protíná strany AB a BC , jak jsme chtěli dokázat.

Dále necht R_b je bod souměrně sdružený s R podle přímky AC . Stejně jako výše ukážeme, že S a T jsou průsečíky R_aR_b postupně se stranami BC a AC . Bod R_a leží na přímkách PQ a ST , proto je totožný s bodem K ze zadání. Obvod trojúhelníku PQR je tak roven $|R_cK|$ a obvod trojúhelníku RST je roven $|R_bK|$.

Ukážeme, že platí $|R_cK| = |R_bK|$. Trojúhelníky AR_cK a AR_bK mají společnou stranu AK a ze souměrností plyne $|AR_c| = |AR| = |AR_b|$. Také platí

$$\begin{aligned} |\sphericalangle KAR_b| &= |\sphericalangle KAC| + |\sphericalangle CAR_b| = |\sphericalangle KAC| + |\sphericalangle CAR| = \\ &= |\sphericalangle KAC| + |\sphericalangle BAK| = |\sphericalangle BAC| \end{aligned}$$



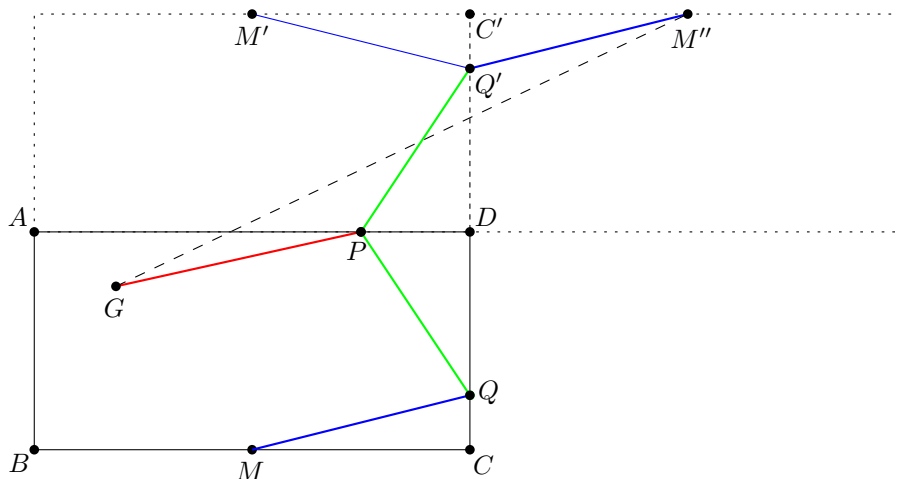
a zároveň

$$|\sphericalangle R_cAK| = |\sphericalangle R_cAB| + |\sphericalangle BAK| = |\sphericalangle BAR| + |\sphericalangle CAR| = |\sphericalangle BAC|,$$

takže $|\sphericalangle R_cAK| = |\sphericalangle BAC| = |\sphericalangle KAR_b|$. Trojúhelníky AR_cK a AR_bK jsou tak shodné podle věty *sus*. Proto jsou i délky úseček R_cK a R_bK stejné. Jelikož jsou tyto délky postupně rovny obvodům trojúhelníků PQR a RST , rovnají se i tyto obvody.

NÁVODNÉ A DOPLŇUJÍCÍ ÚLOHY:

- N1. V rovině je dána přímka ℓ a dva body A, B ležící ve stejné polorovině určené přímkou ℓ . Najděte bod X ležící na přímce ℓ , pro který je hodnota $|AX| + |XB|$ co nejmenší. [Hledaný bod je průsečíkem přímek AB' a ℓ , kde B' je bod osově souměrný s bodem B podle přímky ℓ . Necht B' je bod osově souměrný s bodem B podle přímky ℓ . Potom pro libovolný bod X přímky ℓ platí ze symetrie $|XB| = |XB'|$. Z trojúhelníkové nerovnosti $|AX| + |XB| = |AX| + |XB'| \geq |AB'|$, přičemž rovnost nastává právě tehdy, když X leží na AB' . Takže hledaný bod X je průsečíkem přímek AB' a ℓ .]
- N2. Uvažujme obdélník $ABCD$. Označme M střed strany BC . Uvnitř trojúhelníku ABD je dán bod G . a) Určete bod P strany AD , pro který je délka lomené čáry GPM minimální. b) Určete body P strany AD a Q strany CD , pro které je délka lomené čáry $GPQM$ minimální. [a) Bod P je průsečíkem GM' s AD , kde M' je bod osově souměrný s M podle přímky AD . Úloha se řeší podobně jako úloha N1. b) Necht $P \in AD$ a $Q \in CD$ jsou libovolné. Označme M', C' a Q' body souměrně sdružené po řadě s M, C a Q podle přímky AD . Ze symetrie platí $|PQ'| = |PQ|$ a $|Q'M'| = |QM|$. Dále necht M'' je bod souměrně sdružený s M' podle CD . Ze symetrie platí $|Q'M'| = |Q'M''|$, protože Q' leží



na CD . Délka lomené čáry $GPQM$ je tak rovna délce lomené čáry $GPQ'M''$, která bude minimální právě tehdy, když P a Q' budou průsečíky přímky GM'' po řadě se stranami AD a CD . Tím jsme sestrojili hledaný bod P a bod Q' . Hledaný bod Q je obrazem bodu Q' v osově souměrnosti podle přímky AD . Z polohy bodu G je patrné, že Q' bude ležet na úsečce $C'D$ a proto bod Q bude ležet na úsečce CD .]

- N3. Uvnitř ostrého úhlu XOY je dán bod A . Najděte body M a N ležící po řadě na polopřímkách OY a OX , pro které je obvod trojúhelníku AMN minimální. [Řešení bude zveřejněno až po termínu odevzdání.]
- D1. Je dán úhel XOY , jehož velikost je menší než 45° , a bod A na polopřímce OX . Najděte body M a N polopřímek po řadě OY , OX pro které je součet $|AM| + |MN|$ nejmenší. [Ať N leží na polopřímce OX libovolně. Dále ať OX' je polopřímka souměrně sdružená s polopřímkou OX podle přímky OY a označme N' bod osově souměrný s N podle přímky OY . Označme d vzdálenost bodu A od přímky OX' . Pak platí $|AM| + |MN| = |AM| + |MN'| \geq d$, přičemž rovnost nastane právě tehdy, když N' bude kolmým průmětem bodu A do polopřímky OX' a bod M bude ležet na úsečce AN' . Jelikož $|\sphericalangle XOY| < 45^\circ$, platí $|\sphericalangle XOY'| = 2 \cdot |\sphericalangle XOY| < 90^\circ$, takže kolmý průmět bodu A do přímky OX' leží na polopřímce OX' . Hledaný bod M je proto průsečíkem úsečky AN' s polopřímkou OY , kde N' je kolmý průmět bodu A do polopřímky OX' a hledaný bod N je bod osově souměrný s bodem N' podle přímky OY .]
- D2. Je dán konvexní úhel XOY a jeho vnitřní bod M . Najděte body A, B po řadě polopřímek OX, OY , přičemž $|OA| = |OB|$, pro které je součet $|MA| + |MB|$ nejmenší. [Ať α je velikost úhlu XOY . Necht' M' je obrazem bodu M v otočení se středem v bodě O o úhel α v kladném směru. Necht' A a B jsou body na polopřímkách OX a OY takové, že platí $|OA| = |OB|$. Platí $|\sphericalangle AOM| = \alpha - |\sphericalangle MOB| = |\sphericalangle BOM'|$. Zároveň platí $|OM| = |OM'|$. Trojúhelníky AOM a BOM' jsou tak shodné podle věty *sus*, takže $|AM| = |BM'|$. Tedy $|MA| + |MB| = |M'B| + |BM| \geq |M'M|$, přičemž rovnost nastává právě tehdy, když bod B leží na MM' . Jelikož úhel MOM' je konvexní, úsečka MM' protíná polopřímku OY , přičemž tento průsečík je hledaným bodem B . Hledaný bod A už snadno najdeme jako bod na polopřímce OX takový, že $|OA| = |OB|$.]
- D3. Je dán ostroúhlý trojúhelník ABC . Pro každý jeho vnitřní bod X označme X_a, X_b, X_c jeho obrazy v osových souměrnostech postupně podle přímk BC, CA, AB . Dokažte, že všechny trojúhelníky $X_aX_bX_c$ mají společný bod. [A-70-III-6]

6. Na tabuli jsou napsána 4 přirozená čísla. Žirafa vykonává následující kroky: pokaždé si vybere jedno z čísel na tabuli, smaže ho a místo něj napíše jeho druhou mocninu. Může vždy žirafa po konečně mnoha krocích dosáhnout toho, aby rozdíl některých dvou čísel na tabuli byl násobkem 97? (Josef Tkadlec)

ŘEŠENÍ. Budeme se dívat na zbytky po dělení 97 a všechny kongruence budeme chápat modulo 97. (Definici kongruence naleznete mezi návodnými úlohami.)

Uvažujme libovolný zbytek $a \in \{0, 1, \dots, 96\}$. Postupným umocňováním čísla a dostáváme posloupnost

$$a, a^2, a^4, a^8, a^{16}, a^{32}, a^{64}, a^{128}, \dots$$

Jelikož 97 je prvočíslo, z malé Fermatovy věty máme $a^{97} \equiv a$. Platí $(a^{32})^2 \equiv a^{64}$ a také $(a^{64})^2 \equiv a^{128} \equiv a^{97} \cdot a^{31} \equiv a \cdot a^{31} \equiv a^{32}$. Jelikož zbytek každého členu této posloupnosti závisí jen na zbytku toho předchozího, od pátého umocnění dále se musí opakovat už jen zbytky a^{32} , a^{64} . Uvažovaná posloupnost zbytků je tedy od pátého členu periodická s (ne nutně nejkratší) periodou 2, ve které se periodicky střídají (ne nutně různé) zbytky a^{32} a a^{64} .

Určíme všechny zbytky r , které se mohou objevit v této periodické části. Jelikož máme periodu 2, tak musí platit $(r^2)^2 \equiv r^4 \equiv r$, tedy $97 \mid r^4 - r = r(r^3 - 1) = r(r - 1)(r^2 + r + 1)$. Jelikož 97 je prvočíslo, musí být dělitelem jednoho z členů posledního součinu. Pokud $97 \mid r$, pak $r \equiv 0 \equiv r^2$, takže v posloupnosti se od nějakého členu bude vyskytovat pouze zbytek 0. Podobně pokud $97 \mid r - 1$, pak $r \equiv 1 \equiv r^2$, takže i v tomto případě se bude vyskytovat od nějakého členu pouze jeden zbytek, a to 1. Zároveň jsou to jediné dva případy s periodou 1, protože z $r^2 \equiv r$ vyplývá $97 \mid r^2 - r = r(r - 1)$, a tedy r dává zbytek 0 nebo 1.

Nakonec rozebereme případ, kdy $97 \mid r^2 + r + 1$. Ukážeme, že této podmínce vyhovují právě dva různé zbytky. Zbytky $r \equiv 0$ a $r \equiv 1$ nevyhovují. Postupným umocňováním čísla 2 zjistíme, že vyhovují zbytky $2^{32} \equiv 35$ a $2^{64} \equiv 35^2 \equiv 61$. Pro spor předpokládejme, že podmínka $97 \mid r^2 + r + 1$ je splněna pro tři různé zbytky $r \in \{2, 3, \dots, 96\}$, označme je x , y , z . Potom $97 \mid x^2 + x + 1$ a $97 \mid y^2 + y + 1$, takže $97 \mid x^2 + x + 1 - y^2 - y - 1 = (x - y)(x + y + 1)$. Protože zbytky x , y jsou různé, musí platit $97 \mid x + y + 1$. Analogicky pro x a z dostaneme $97 \mid x + z + 1$. Takže $97 \mid (x + y + 1) - (x + z + 1) = y - z$, tedy $y \equiv z$, což je hledaný spor.

Když budeme umocňovat na druhou jedno z čísel, tak počínaje pátým umocněním se nám budou dále opakovat zbytky, a to jednou z těchto možností:

- (i) dalším umocňováním dostaneme vždy zbytek 0.
- (ii) dalším umocňováním dostaneme vždy zbytek 1.
- (iii) dalším umocňováním se budou střídát v nějakém pořadí zbytky 35 a 61, což jsou právě ty zbytky, které splňují $97 \mid r^2 + r + 1$.

A jelikož jsou na tabuli 4 čísla, pro dvě z nich musí nastat stejná možnost. Pokud se zopakuje jedna z prvních dvou možností, tak odečtením dostaneme zbytek 0. Pokud se zopakuje třetí možnost, pak umocníme příslušná čísla tak, aby obě dávala zbytek 35 a po odečtení dostaneme zbytek 0. Takže vždy můžeme dosáhnout, že rozdíl některých dvou čísel bude násobkem 97.

KOMENTÁŘ 1. Konkrétní hodnoty zbytků 35 a 61 ve skutečnosti najít nepotřebujeme – stačí ukázat, že existují *nejvýše* dva zbytky r splňující $97 \mid r^2 + r + 1$. Jelikož periodu 1 máme jen pro zbytky 0 a 1, které výše uvedené podmínce nevyhovují, v bodu (iii) jsou posloupnosti, kde se střídají dvě různá čísla. Tato čísla, pokud vůbec existují, vyhovují podmínce $97 \mid r^2 + r + 1$, proto musí být stejná nezávisle na počátečním čísle na tabuli.

KOMENTÁŘ 2. To, že existují nejvýše dva zbytky r splňující $97 \mid r^2 + r + 1$, lze ukázat i jinak. Například je možné to (pracně) ověřit pro všechny zbytky od 2 po 96, resp. ověřit kongruenci $r^4 \equiv r$. Jinou možností je odvolat se na fakt, že $r^2 + r + 1$ je kvadratický polynom, který má modulo prvočíslo 97 nejvýše dva kořeny. (Tyto kořeny lze také vyčíslit explicitně pomocí diskriminantu $1^2 - 4 \cdot 1 \cdot 1 \equiv -3 \equiv 26^2$ jako $(-1 \pm 26) \cdot 2^{-1} \equiv (-1 \pm 26) \cdot 49$, což dává 35 a 61.)

JINÉ ŘEŠENÍ. Všimněme si, že 97 je prvočíslo. Pokud jsou alespoň dvě čísla na tabuli násobkem 97, tak jejich rozdíl bude také dělitelný 97. Předpokládejme proto, že jsou na tabuli napsána alespoň 3 čísla a, b, c , která nejsou dělitelná 97.

Jelikož 97 je liché prvočíslo, existuje primitivní prvek* r modulo 97, tedy číslo r takové, že mezi čísly $r^1, r^2, \dots, r^{96}$ se vyskytují všechny nenulové zbytky modulo 97. To znamená, že existuje přirozené číslo α takové, že $r^\alpha \equiv a$. Po pěti umocněních dostaneme $a^{32} \equiv r^{32\alpha}$. Z malé Fermatovy věty máme $r^{96} \equiv r^{32 \cdot 3} \equiv 1$. Číslo α můžeme vyjádřit pomocí nezáporných celých čísel m, n , kde $n < 3$, jako $\alpha = 3m + n$. To znamená, že zbytek $a^{32} \equiv r^{32\alpha} \equiv r^{32 \cdot 3m + 32n} \equiv (r^{32 \cdot 3})^m \cdot r^{32n} \equiv 1 \cdot r^{32n}$ je roven jednomu ze zbytků $r^{32 \cdot 0}, r^{32 \cdot 1}, r^{32 \cdot 2}$. Podobně pro b a c najdeme exponenty β a γ takové, že platí $r^\beta \equiv b$ a $r^\gamma \equiv c$. Analogicky dostaneme, že zbytky $b^{32} \equiv r^{32\beta}$ a $c^{32} \equiv r^{32\gamma}$ jsou rovny jednomu ze zbytků $r^{32 \cdot 0}, r^{32 \cdot 1}, r^{32 \cdot 2}$.

Pokud dávají dvě z čísel a^{32}, b^{32}, c^{32} stejný zbytek, pak 97 dělí jejich rozdíl. Pokud dávají všechna tři čísla různé zbytky, bez újmy na obecnosti ať platí $b^{32} \equiv r^{32}$ a $c^{32} \equiv r^{32 \cdot 2}$. Pak stačí b umocnit na druhou a rozdíl $b^{64} - c^{32}$ bude násobkem 97.

KOMENTÁŘ. Vzhledem k tomu, že modulo 97 existuje jen konečně mnoho zbytků, můžeme úlohu řešit i tak, že sledujeme, na jaký zbytek se každý zbytek zobrazí po umocnění na druhou. Tento proces si můžeme představit jako orientovaný graf, kde má každý vrchol právě jednu výstupní hranu. Pomocí toho lze ukázat, že z každého ze čtyř čísel na tabuli se po jistém konečném počtu kroků stane jedno ze tří čísel: 0, 1 nebo 61. (Zbytek 61 se zobrazí na zbytek 35 a zbytek 35 se zobrazí na zbytek 61.)

NÁVODNÉ A DOPLŇUJÍCÍ ÚLOHY:

Před řešením této úlohy vám doporučujeme seznámit se s kongruencemi. Zápis $a \equiv b \pmod{d}$ vyjadřuje, že celá čísla a, b dávají stejný zbytek po dělení kladným celým číslem d . Čteme jej *a je kongruentní s b modulo d*. Pro hlubší seznámení s kongruencemi výborně poslouží brožurka [Aloise Apfelbecka Kongruence](#) z edice *Škola mladých matematiků*.

- N1. Vyzkoušejte si soutěžní úlohu pro menší čísla než 97, například pro 5 a 7. [Lze ukázat, že pro číslo 7 tvrzení úlohy platí. Pro číslo 5 tvrzení také platí, a dokonce by platilo i kdyby na tabuli byla napsána pouze 3 přirozená čísla.]
- N2. Necht p je prvočíslo a a celé číslo, které není dělitelné číslem p . Ukažte, že vezmeme-li všechny nenulové zbytky $1, 2, \dots, p-1$ po dělení číslem p , vynásobíme je číslem a a následně opět vezmeme zbytky po dělení číslem p , dostaneme stejnou množinu zbytků

* Pokud jste se s primitivními prvky ještě nesetkali, více informací naleznete například na [Wikipedii](#).

- jako na začátku. [Ukážeme, že zobrazení, které přiřadí zbytku $x \in \{1, 2, \dots, p-1\}$ zbytek $a \cdot x$ po dělení p , je prosté. Pokud platí $a \cdot x \equiv a \cdot y \pmod{p}$, pak $a(x-y) \equiv 0 \pmod{p}$. Protože a není dělitelné číslem p , musí platit $x-y \equiv 0 \pmod{p}$, tedy $x \equiv y \pmod{p}$. To znamená, že zobrazení, které přiřadí $x \in \{1, 2, \dots, p-1\}$ zbytek $a \cdot x$ po dělení p , je prosté. A protože x i zbytek $a \cdot x$ po dělení p jsou prvky množiny $\{1, 2, \dots, p-1\}$, násobení číslem a modulo p jen přeuspořádá tuto množinu.]
- N3. Nechť p je prvočíslo a a celé číslo, které není dělitelné číslem p . Ukažte, že existuje právě jeden zbytek b , pro který platí $a \cdot b \equiv 1 \pmod{p}$. (Takový prvek b se nazývá *inverzní prvek k a modulo p* a označujeme jej a^{-1}). [Využijeme úlohu N2 pro a . Jelikož násobením všech nenulových zbytků číslem a dostaneme stejnou množinu zbytků, musí existovat b takové, že $a \cdot b \equiv 1 \pmod{p}$. Jak jsme ukázali v úloze N2, toto zobrazení je prosté, proto je b jednoznačně určeno.]
- N4. Dokažte *malou Fermatovu větu*: Nechť p je prvočíslo a a celé číslo, které není dělitelné číslem p . Potom p dělí číslo $a^{p-1} - 1$. [Chceme ukázat, že platí $1 \equiv a^{p-1} \pmod{p}$. S využitím úlohy N2 dostáváme, že platí $1 \cdot 2 \cdot \dots \cdot (p-1) \equiv a \cdot 2a \cdot \dots \cdot (p-1)a \pmod{p}$, takže $(p-1)! \equiv a^{p-1}(p-1)!$. Jelikož $(p-1)!$ není dělitelné p , tak $1 \equiv a^{p-1} \pmod{p}$.]
- N5. Nechť p je prvočíslo a a, b, c jsou celá čísla, přičemž p nedělí a . Dokažte, že podmínka $p \mid ax^2 + bx + c$ je splněna nejvýše pro dvě různé hodnoty $x \in \{0, 1, 2, \dots, p-1\}$. [Pro spor předpokládejme, že podmínka $p \mid ax^2 + bx + c$ je splněna pro tři různé hodnoty $x \in \{0, 1, 2, 3, \dots, p-1\}$, označme je y, z, w . Potom $p \mid ay^2 + by + c$ a $p \mid az^2 + bz + c$, takže $p \mid ay^2 + by + c - (az^2 + bz + c) = a(y-z)(y+z) + b(y-z) = (y-z)(ay + az + b)$. Protože p nedělí $y-z$, musí platit $p \mid ay + az + b$. Analogicky pro y a w dostáváme, že $p \mid ay + aw + b$. Takže $p \mid ay + az + b - (ay + aw + b) = a(z-w)$. Ale p nedělí ani a ani $z-w$, což je hledaný spor.]
- N6. Dokažte, že číslo $2^{2025} - 8$ je dělitelné 56. [Mocniny dvojky dávají při dělení 56 po řadě zbytky 2, 4, 8, 16, 32, 8, 16, 32, 8, 16, 32, ... Jelikož zbytek následující mocniny je jednoznačně určen zbytkem předešlé mocniny, tak po zbytku 8 se bude opakovat už jen trojice zbytků 8, 16, 32. Jelikož 2025 je dělitelné třemi a každá mocnina s exponentem dělitelným třemi dává zbytek 8, tak $2^{2025} - 8 \equiv 8 - 8 \equiv 0 \pmod{56}$.]
- D1. Nechť p je liché prvočíslo. Číslo $a \in \{1, 2, \dots, p-1\}$ nazýváme *kvadratický zbytek modulo p*, pokud existuje celé číslo x , pro které platí $x^2 \equiv a \pmod{p}$. Dokažte, že v množině $\{1, 2, \dots, p-1\}$ je stejně mnoho kvadratických zbytků modulo p jako čísel, která nejsou kvadratickým zbytkem modulo p . [Všimněme si, že $x^2 \equiv y^2$ platí právě tehdy, když $(x-y)(x+y) \equiv x^2 - y^2 \equiv 0$, tedy právě tehdy, když platí $x \equiv y$ nebo $x \equiv -y$. Z toho vyplývá, že mezi $1^2, 2^2, \dots, (p-1)^2$ se nám vyskytne každý kvadratický zbytek právě dvakrát, jednou jako x^2 a jednou jako $(p-x)^2$, pro vhodné x , kde $x < p-x$. Proto se stačí dívat jen na první polovinu, tedy na $1^2, 2^2, \dots, (\frac{p-1}{2})^2$, tyto zbytky jsou modulo p navzájem různé, takže kvadratických zbytků je $\frac{p-1}{2}$, což je právě polovina ze všech nenulových zbytků.]
- D2. Dokažte jednu část *Wilsonovy věty*: pokud p je prvočíslo, pak $(p-1)! \equiv -1 \pmod{p}$. [Podle úlohy N2 existuje ke každému zbytku a inverzní prvek a^{-1} , tedy zbytek takový, že $a \cdot a^{-1} \equiv 1$. Určíme, kdy platí $a \equiv a^{-1}$. Vynásobením a dostáváme $a^2 \equiv 1$, z toho $(a-1)(a+1) \equiv 0$, takže $a \equiv 1$ nebo $a \equiv -1 \equiv p-1$, protože p je prvočíslo. To znamená, že v množině zbytků $\{1, 2, \dots, p-1\}$ umíme všechna čísla až na 1 a $p-1$ uspořádat do dvojic, jejichž součin dává zbytek 1. Proto platí $(p-1)! \equiv 1 \cdot 2 \cdot \dots \cdot (p-1) \equiv 1 \cdot (p-1) \equiv -1$.]
- D3. Dokažte, že každá nekonečná posloupnost $(a_0, a_1, a_2, \dots)$ celých čísel taková, že platí $a_0 \geq 1$ a $a_{n+1} \in \{2022a_n - 1, 2022a_n + 1\}$ pro všechny indexy n , obsahuje nekonečně mnoho složených čísel. [A-71-II-4]
- D4. Uvažujme posloupnost $a_1, a_2, \dots$ definovanou vztahem $a_n = 2^n + 3^n + 6^n - 1$ pro $n = 1, 2, \dots$. Určete všechna kladná celá čísla, která jsou nesoudělná s každým členem této posloupnosti. [IMO-2005-P4]