Řešení 5. série

Binární kódy

autor: *Vláďa*

Úloha 4.1. Na zahřátí si dáme snadnější příklad. Určitě znáš hru Myslím si číslo a to má vlastnost, je to velice podobné. Tedy mám binární lineární kód délky 5, který obsahuje 4 slova. Ještě ti o něm povím to, že vzdálenost každých dvou různých slov je alespoň 3. Schválně ukaž alespoň jeden příklad kódu, jaký si mohu myslet.

Řešení. Nechť C je hledaný binární lineární kód. Potom C jistě obsahuje nulové slovo. Aby byla vzdálenost mezi slovy ≥ 3, v každém nenulovém slově našeho kódu můžou být nuly nejvýše na dvou pozicích.

Slovo 11111 nepatří do C, protože slovo délky 5 nemůže mít zároveň vzdálenost ≥ 3 od 11111 a od $\mathbf{0}$. Každé $w \in C$, $w \neq \mathbf{0}$ tedy obsahuje jednu anebo dvě nuly.

C neobsahuje dvě slova s pouze jednou nulou, protože tato by se lišila nejvýše na dvou pozicích. Pokud by všechna tři nenulová slova v C obsahovala dvě nuly, nějaká dvě z těchto slov by měla nulu na stejné pozici (Dirichletův princip), pak je ale vzdálenost těchto slov ≤ 2.

Celkem jsme odvodili, že jednotlivá slova v C obsahují postupně $1, 2, 2$ a 5 nul, přičemž nenulová slova musí mít nuly na různých pozicích. Příkladem takového kódu je

$$C = \{00000, 11100, 00111, 11011\}.$$

Je snadné ověřit, že daný kód je skutečně lineární a splňuje podmínky zadání. Z výše uvedených pozorování navíc plyne, že jakékoliv další řešení vznikne permutací pozic v tomhle kódu.

Úloha 4.2. Dobře, tak tohle by ti šlo. Zkusíme, jak umíš pracovat s tímhle lineárním kódem. Tady máš binární lineární kód takový, že každá dvě slova v něm mají lichou vzdálenost, a mě by zajímalo, kolik nejvýše v něm může být slov.

Řešení. Každý binární lineární kód obsahuje slovo $\mathbf{0}$. Aby kód vyhovoval zadaní, všechny ostatní slova mají od prázdného lichou vzdálenost. Nutně musí mít lichý počet jedniček. Uvažme tedy vzdálenost dvou libovolných slov s lichým počtem jedniček. První slovo má $2k + 1$ jedniček, druhé $2l + 1$ jedniček. Nechť právě na n pozicích mají obě čísla jedničku, tedy se na těchto pozicích neliší. Jejich vzdálenost je tedy $2k+1+2l+1-2n = 2(k+l+1-n)$, což je sudé číslo. Dvě slova s lichým počtem jedniček mají vždy sudou vzdálenost, takže v hledaném kódu může být maximálně jedno z nich. Binární lineární kód, kde mají všechny slova lichou vzdálenost, může obsahovat maximálně dvě slova, konkrétně slovo $\mathbf{0}$ a libovolné slovo s lichým počtem jedniček.

Úloha 4.3. S tímhle lineárním kódem sis poradil. Teď tu pro tebe mám sadu binárních cyklických kódů délky 2015, z nichž každý obsahuje alespoň jedno slovo s lichým počtem jedniček. Ukaž, že najdeš slovo $\mathbf{1} = \overbrace{11\ldots1}^{2015}$ v každém z nich.

Řešení. Ze zadání víme, že náš kód obsahuje číslo s lichým počtem jedniček v zápise. Uvažme jeho cyklické posuny o všechna celá čísla od 0 do 2015, tedy i slovo samotné. Některé tyto posuny mohou být identické. Kód je lineární, proto společně s každými dvěma (ne nutně různými) slovy obsahuje také jejich součet. Zřejmě tedy obsahuje také součet libovolného počtu sčítanců. Konkrétně tedy obsahuje i součet všech 2015 cyklických posunů slova ze zadání.

Když si tato slova napíšeme, jako bychom je chtěli sčítat pod sebou, bude v každém sloupečku stejný počet jedniček, jako v našem slově.

Na k-té pozici součtu slov je jednička právě tehdy, když je jednička na k-té pozici lichého počtu sčítanců. Protože počet jedniček na k-té pozici je v našem případě lichý, pro libovolné k je patrné, že na každé pozici součtu vyjde jednička. Kód tedy musí obsahovat slovo tvořené samými jedničkami.

Úloha 4.4. V dalším úkolu budeme pracovat s binárním cyklickým kódem délky $n \in \mathbb{N}$. Teď si budeš vypisovat na papír všechna jeho slova a počet slov s právě k jedničkami označíš jako P_k. Ukaž, že pro všechna $k \in \mathbb{N}$ je číslo $k \cdot P_k$ dělitelné n.

Řešení. Nechť p je tedy libovolné slovo daného cyklického kódu obsahující k jedniček. Pak označme p_m jeho cyklický posun o m (to je tedy také slovem onoho kódu). Nyní nechť M je nejmenší takové přirozené číslo, že $p = p_0 = p_M$, tedy že slovo p při posunu o M zůstane nezměněno. Zřejmě M je dělitelem M, neboť pokud $p = p_M = p_n$, pak také $p_{n-M} = p$ a opakovaným užitím téhož postupu získáme $p_l = p$, kde l je zbytek n po dělení M. Protože však M je nejmenší přirozené číslo s touto vlastností, jedinou možností je, že tento zbytek je nulový.

Pak tedy máme, že p se skládá z $\frac{n}{M}$ shodných úseků o délce M. Každý z těchto úseků nechť obsahuje K jedniček. Pak zřejmě $k = K \cdot \frac{n}{M}$ V kódu je tedy M slov $p_0, p_1, \ldots, p_{M-1}$, která jsou navzájem různá a protože jsou svými cyklickými posuny, obsahují stejný počet jedniček. Jejich „příspěvek“ ke $k \cdot P_k$ bude tedy $K \cdot \frac{n}{M} \cdot M = K \cdot n$ a je tedy dělitelný n.

Číslo $k \cdot P_k$ se zjevně skládá právě pouze z takovýchto „příspěvků“ a je tedy součtem čísel dělitelných n, samo tedy musí být n dělitelné.

Úloha 4.5. Hru vyruší Bubla: „Kluci, copak to hrajete?“ „BinKROS, zahraješ si s námi?“ reagoval Ňouma. „To ne, to já bych si raději zahrála na Pijáka.“ Bubla jim vysvětlila, že na Pijáka se hraje tak, že člověk začíná se 100 panáky (kofoly) a vždy může vypít buď 5, 15, 17 nebo 20 za sebou, přičemž v těchto případech mu kamarádi nalijí 17, 24, 2 nebo 14 nových panáků. (Vypije-li jich např. 15, dolijí mu 24, když vypije 20, dolijí mu 14 apod.) Cílem je vypít všechny panáky (v případě prázdného stolu už kamarádi nedolívají). „A je to vůbec možné?“ zeptal se hned Kouma. Rozhodněte, zda to lze a jak postupovat, aby hráč vypil všechny panáky.

Řešení. V následujícím ukážeme, že hráč nemůže vypít všechny panáky. Tím, že se poslední kolo již nedolévá, hráč vyhraje právě, když se mu podaří dostat se do stavu, kdy má na stole 5, 15, 17 nebo 20 panáků. Potom už snadno vyhraje vypitím příslušného počtu. K tomu, aby se do některého z těchto stavů dostal, může kombinovat „tahy“ pouze čtyř typů:

- Vypít 5 panáků, s tím že mu pak dolijí 17 panáků. Tedy přibude 12 panáků
- Vypít 15 panáků, s tím že mu pak dolijí 24 panáků. Tedy přibude 9 panáků
- Vypít 17 panáků, s tím že mu pak dolijí 2 panáky. Tedy ubude 15 panáků
- Vypít 20 panáků, s tím že mu pak dolijí 14 panáků. Tedy ubude 6 panáků

Žádným z těchto „tahů“ však hráč nezmění zbytek počtu panáků na stole po dělení třemi. Protože 100 dává zbytek 1 po dělení třemi a žádný z kýžených počtů 5,15,17,20 zbytek 1 po dělení třemi nedává, nemůže hráč nikdy vyhrát.

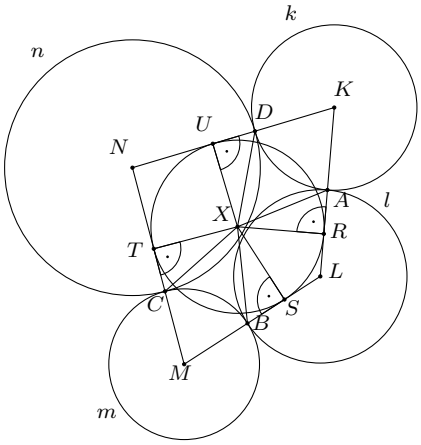
Úloha 4.6. Těch pět (přidal se Matěj a Liběnkou) hrálo na Pijáka (stále s kofolou) dlouho do noci, a tak nebylo divu, že měla Liběnka ráno kruhy pod očima. „Jé, podívej,“ usmál se na její kruhy u snídaně Henry „když tyhlety kružnice označíme k, l, m a n, platí, že k se dotýká l v bodě A, l se dotýká m v bodě B, m se dotýká n v bodě C a n se dotýká k v bodě D. Navíc jsou všechny dotyky **vnější**.“ „Nojo,“ zívl Matěj, „to ale pak body $ABCD$ leží buď na jedné kružnici nebo na přímce, ne?“ Zvládnete tuto skutečnost dokázat?

Řešení. Řešení této úlohy je skutečně mnoho. Začneme těmi zajímavějšími:

Kruhová inverze: Uvažme kruhovou inverzi se středem v bodě A (a libovolným poloměrem). Kružnice k a l přejdou v rovnoběžné přímky (neboť se v A dotýkají) k' a l'. Kružnice m' a n' se vzájemně dotýkají v bodě C'. Navíc k' je tečnou n' a l' je tečnou m'. Platí tedy, že bod C' je středem stejnolehlosti, ve které m' přejde v n' a k' přejde v l'. Pak tedy zřejmě body B', C', D' musí ležet na přímce a tedy A, B, C, D na jedné kružnici.

Tečnový čtyřúhelník: Touhle cestou se vydalo poměrně mnoho řešitelů, kupodivu však nikdo nedotáhl řešení do korektního konce.

Středy kružnic k, l, m, n označme po řadě K, L, M, N a jejich poloměry r_k, r_l, r_m, r_n. Pak zcela jistě platí, že body A, B, C, D leží na stranách čtyřúhelníku $KLMN$ a navíc pro tyto strany platí $|KL| + |MN| = r_k + r_l + r_m + r_n = |LM| + |NK|$, což je nutná a postačující podmínka pro to, aby byl čtyřúhelník $KLMN$ tětivový. Tím ale důkaz **není hotov**, protože body A, B, C, D v obecném případě **nejsou** body dotyku kružnice vepsané $KLMN$. My ale víme, že kružnice mu vepsat lze a tak si body dotyku označme např. $R \in KL$, $S \in LM$, $T \in MN$, $U \in NK$. Dále si střed této vepsané kružnice označme jako X. Pak z následujícího obrázku je zřejmé, že trojúhelníky ARX, BSX, CTX a DUX jsou shodné, neboť jsou to pravoúhlé trojúhelníky, jejichž jedna odvěsna je vždy poloměr téže kružnice, zatímco rovnost druhé odvěsny získáme ze vztahu $|KR| = |KU|$ a $|KA| = |KD|$ a dalších analogických rovností pro ostatní body. Pak tedy $|AX| = |BX| = |CX| = |DX|$, a body A, B, C, D tak musí ležet na jedné kružnici.



Věta o obvodovém, středovém a úsekovém úhlu Další možné řešení je napsat si všechny možné úhly, které v úloze vystupují, napsat si co pro ně platí užitím věty o obvodovém, středovém a úsekovém úhlu a poté z toho vyvodit, že $ABCD$ musí být tětivový čtyřúhelník, ale tohle řešení je natolik přímočaré a nezajímavé, že se jím zde zabývat nebudeme.

Úloha 4.7. „A co jsi dělal celou noc ty, Henry?“ zeptal se Kouma. „Původně jsem měl v plánu se k vám připojit, ale pak jsem se zamyslel nad přirozenými čísly m a n, pro která platí $m^2 - n^3 = 17$ a napadlo mě, že pak číslo $n^2 + 2m + 2$ musí být složené. Ale už se mi to nepodařilo dokázat.“ Budete úspěšnější než Henry a dokážete to?

Řešení. Podle Petra Vinceny: Zadanou rovnost si upravíme:

$$\begin{aligned} m^2 - n^3 &= 17 \\ m^2 - 16 &= n^3 + 1 \\ (m+4)(m-4) &= (n+1)(n^2 - n + 1) \end{aligned}$$

Nyní si povšimneme, že $(m+4)+(m-4)+(n+1)+(n^2-n+1) = n^2+2m+2$. Zavedeme-li substituci $a = m+4, b = m-4, c = n+1, d = n^2-n+1$, stačí nám dokázat, že pokud $ab = cd$, pak už nutně $a+b+c+d$ je složené číslo.

Zřejmě jde o přirozená čísla (jediným kandidátem na nekladnost je $m-4$ a protože je jediný, musí být také kladný). Označme $x = (a, c), r = (b, d)$, kde $(\cdot, \cdot)$ značí největšího společného dělitele. Pak nechť $a = xy, c = xz$ a $b = rs, d = rt$, kde y, z, s, t jsou přirozená čísla a navíc $(y, z) = (s, t) = 1$. Rovnost $ab = cd$ lze pak přepsat na

$$\begin{aligned} xyrs &= xzrt \\ ys &= zt \\ \frac{y}{z} &= \frac{s}{t} \end{aligned}$$

Protože $(y, z) = (s, t) = 1$, jsou oba zlomky v základním tvaru a platí tedy $y = s$ a $z = t$, neboli $b = ry, d = rz$. Získáváme tedy konečně

$$a + b + c + d = xy + xz + ry + rz = x(y+z) + r(y+z) = (x+r)(y+z),$$

což je určitě číslo složené a důkaz je hotov.

Podle Jana Jurky: Zadanou rovnost si upravíme:

$$\frac{m^2 - n^3 - 17}{n+1} = 0$$

Dále tedy

$$n^2 + 2m + 2 = n^2 + 2m + 2 + \frac{m^2 - n^3 - 17}{n+1} = \frac{2mn + 2n + n^2 + 2m + 2 + m^2 - 17}{n+1} =$$
$$= \frac{(m+n)^2 + 2(m+n) - 15}{n+1} = \frac{(m+n-3)(m+n-5)}{n+1}$$

Zbývá tedy ukázat, že oba činitelé v čitateli jsou větší než jmenovatel a i po jeho zkrácení tedy půjde o složené číslo. To ale platí, protože pokud by $m \leq 4$ pak (neboť $n \geq 1$)

$$17 = m^2 - n^3 \leq 4^2 - 1^3 = 15,$$

což je spor. Důkaz je tedy hotov.