

Řešení 6. série

HRÁTKY S CIFRAMI

ÚLOHA 6.1. Kolik existuje devíticiferných čísel složených pouze z cifer 9 a 7 takových, že jsou dělitelná číslem 11?

ŘEŠENÍ. Číslo je dělitelné 11 právě tehdy, když rozdíl součtu cifer na sudých a lichých pozicích je dělitelný 11. (Celkový počet možností, které máme: 2^9)

Lichých pozic: 5

Možnosti rozdělení cifer (7 a 9) a jejich součtů na lichých pozicích:

min: $5 \cdot 7 = 35 \dots 1$ možnost

$4 \cdot 7 + 1 \cdot 9 = 37 \dots 5$ možností

$3 \cdot 7 + 2 \cdot 9 = 39 \dots \binom{5}{2} = 10$ možností

$2 \cdot 7 + 3 \cdot 2 = 41 \dots \binom{5}{2} = 10$ možností

$1 \cdot 7 + 4 \cdot 9 = 43 \dots 5$ možností

max: $5 \cdot 9 = 45 \dots 1$ možnost

dohromady $32 = 2^5$ možností

Sudých pozic: 4

Možnosti rozdělení cifer (7 a 9) a jejich součtů na sudých pozicích:

min: $4 \cdot 7 = 28 \dots 1$ možnost

$3 \cdot 7 + 1 \cdot 9 = 30 \dots 4$ možnosti

$2 \cdot 7 + 2 \cdot 9 = 32 \dots \binom{4}{2} = 6$ možností

$1 \cdot 7 + 3 \cdot 9 = 34 \dots 4$ možnosti

max: $4 \cdot 9 = 36 \dots 1$ možnost

dohromady $16 = 2^4$ možností

($3 \cdot 7 + 1 \cdot 9$ znamená, že na sudých pozicích jsou tři sedmičky a jedna devítka, počet možností zjistíme buď kombinatoricky, nebo výpisem)

Rozdíly: Součet na lichých pozicích je vždy lichý, součet na sudých sudý. Proto bude i rozdíl součtu čísel na lichých (L) a sudých (S) pozicích lichý.

Nejmenší rozdíl $L - S = 35 - 36 = -1$

Největší rozdíl $L - S = 45 - 28 = 17$

Jediný lichý násobek 11 mezi -1 a 17 je 11. Hledáme tedy možnosti kombinací čísel na lichých a sudých pozicích, které dávají rozdíl 11.

$11 = 39 - 28 \dots 10 \cdot 1 = 10$ možností

$11 = 41 - 30 \dots 10 \cdot 4 = 40$ možností

$$11 = 43 - 32 \dots 5 \cdot 6 = 30 \text{ možností}$$

$$11 = 45 - 34 \dots 1 \cdot 4 = 4 \text{ možností}$$

Dohromady máme 84 možností, tedy existuje 84 devíticiferných čísel, která se skládají pouze z cifer 9 a 7 a jsou dělitelná 11.

ÚLOHA 6.2. Hlídač napsal na tabuli n -ciferné číslo, kde se žádná cifra nevyskytuje dvakrát bezprostředně za sebou. Skupinka zná počet cifer n , ale je v jiné místnosti a číslo napsané na tabuli nezná. Má za úkol zjistit, kterou cifru má umazat, aby po umazání nově vzniklé $(n - 1)$ -ciferné číslo bylo co možná největší. V závislosti na n určete nejmenší počet pozic, na které se skupinka musí hlídače zeptat, aby mohla jednoznačně určit pozici, kterou mají smazat. V řešení také uveďte, na které pozice se skupinka bude konkrétně ptát.

ŘEŠENÍ. Hledaná pozice (označená k) musí mít takovou vlastnost, že cifra na pozici k (c_k) musí být menší než cifra na pozici $k + 1$ (c_{k+1} , číslujeme **zleva doprava**). Také musí platit, že se jedná o **zleva první** pozici s touto vlastností; pokud žádná taková neexistuje, znamená to, že je délka čísla $n \leq 10$, a pak je cifrou k vyškrtnutí cifra na pozici jednotek.

Proč? Kdyby bylo $n = 1$, pak by úloha měla triviální řešení, předpokládejme tedy, že je n alespoň 2. Nechť k označuje první pozici takovou, že $c_k < c_{k+1}$. To znamená, že pro všechny pozice $1, 2, \dots, k - 1$ platilo, že cifra na pozici i byla větší než cifra na pozici $i + 1$; tedy $c_i > c_{i+1}$. Kdybychom nyní vyškrtli c_i , na její pozici by se posunula cifra **menší** než ta, která tam byla předtím (např. v 987 škrtneme 8, získáme 97), kdybychom ale místo toho škrtnli c_{i+1} , ona větší cifra by zůstala na stejném místě, a tedy výsledek by byl větší (987, škrtneme 7, získáme 98). Proto vidíme, že když vezmeme libovolnou dvojici takovou, že $c_i > c_{i+1}$, vždy je lepší škrtnout tu druhou cifru v pořadí. Tuto úvahu můžeme ale postupně aplikovat na všechny po sobě jdoucí dvojice pozic z čísel $1, 2, \dots, k - 1$ - z pozic i a $i + 1$ je lepší škrtnout $i + 1$, ale z $i + 1$ a $i + 2$ je lepší škrtnout $i + 2$, z $i + 2$, $i + 3$ preferujeme $i + 3$ atd.

Toto se ale změní pro dvojici $k, k + 1$, zde už neplatí, že získáme větší číslo škrtnutím cifry na pozici $k + 1$, poprvé je výhodnější škrtnout cifru více vlevo. Pokud tedy škrtneme c_k , získáme větší číslo než škrtnutím kterékoliv z cifer předchozích; nyní ukažme, že tím dostaneme i větší číslo, než kdybychom škrtnli kteroukoli z cifer následujících.

Číslo, které je na tabuli, vypadá takto: $\overline{c_1 c_2 \dots c_{k-1} c_k c_{k+1} \dots c_{l-1} c_l c_{l+1} \dots c_{n-1} c_n}$. V tomto vyjádření jsme si označili l nejdřívejší pozici větší než k takovou, že $c_l < c_{l+1}$. Pro všechny pozice mezi k a l platí to samé, co pro $1, 2, \dots, k - 1$, tedy je jasné, že vhodným kandidátem je nejdříve c_l . Porovnejme nyní vyškrtnutí c_k a c_l ; když vyškrtneme c_k , pak výsledné číslo K bude $n - 1$ ciferné a na k -té pozici bude c_{k+1} , zatímco když vyškrtneme c_l , bude na k -té pozici $c_k < c_{k+1}$, a protože se čísla v prvních $k - 1$ pozicích rovnají, bude $K > L$. Jelikož toto platí pro všechna $l < k$ taková, že $c_l < c_{l+1}$, je pro nás nejvýhodnější vybrat ke smazání pozici k .

Už jsme tedy ukázali, že musíme vybrat první číslo k takové, že $c_k < c_{k+1}$; které pozice ale musíme otestovat, abychom ho spolehlivě našli? Může se stát, že na tabuli bude třeba číslo 851, zde platí, že žádné takové k neexistuje, a v tomto případě vidíme, že je nejlepší vyškrtnout 1. Takovýchto čísel je ale omezený počet, platí totiž, že jakmile $n > 10$, nějaké vyhovující k už nutně najdeme. Kdyby tomu tak nebylo, pak by muselo platit, že $c_1 > c_2 > c_3 \dots > c_9 > c_{10} > c_{11}$, což není možné - máme k dispozici 10 cifer a nejlépe, jak je můžeme zvolit za sebou, je 9876543210, pokud bychom přidali jakékoliv z předchozích čísel, už bychom získali vyhovující k na 10. pozici, a pokud by kterékoliv dřívější mělo jinou

hodnotu, byla by k jedna z prvních deseti pozic. Vidíme tedy, že je postačující se podívat na prvních deset cifer, a z nich již dovedeme posoudit, kterou z cifer škrtnout.

Shrnutí: Pro $n > 10$ se stačí podívat na prvních deset cifer; pro $n \leq 10$ se stačí podívat na n cifer.

ÚLOHA 6.3. Kolik musí mít číslo n v desítkové soustavě cifer, aby v něm byla obsažena všechna dvojciferná čísla (jeho cifry musí být v n těsně za sebou)?

ŘEŠENÍ. Aby v n bylo obsaženo všech 90 dvojciferných čísel, musí takové číslo každou z číslic 1 až 9 obsahovat alespoň 10krát. Každá z těchto číslic totiž musí minimálně jednou stát na místě desítek před jednou z cifer 0 až 9. Číslice 0 musí být v čísle n alespoň 9krát. Alespoň jedna 0 totiž musí stát na místě jednotek za každou z číslic 1 až 9. Aby tedy číslo n splňovalo zadanou podmínku musí mít alespoň $9 \cdot 10 + 9 = 99$ cifer.

Ukážeme-li, že číslo n jde z 99 cifer složit, máme vyhráno. Jedním z možných způsobů (který hezky popsal Vašek Janáček) je:

Postupně pro každé i od 1 do 9 napíšeme číslici i následovanou všemi čísly $10i + j$ pro $j > i$. Za to dopíšeme číslo $10i$. Na toto číslo skutečně použijeme $9 \cdot 3 + 2 \cdot (8 + 7 + \dots + 1 + 0) = 27 + 2 \cdot 36 = 27 + 72 = 99$ cifer (pro každou číslici píšeme 3 znaky – jednu tuto číslici na začátku a tuto číslici s nulou na konci) a k tomu ještě dvakrát tolik číslic, kolik je větších číslic).

Celkem takto vzniklé n vypadá takto:

112131415161718191022324252627282920334353637383930445464748494055657585950667
686960778797088980990

ÚLOHA 6.4. Najděte všechna prvočísla p taková, že platí následující tvrzení:

Pro každé přirozené k existuje přirozené číslo n splňující následující podmínky:

1. p dělí n ;
2. uvážíme-li všechna čísla, která vzniknou z čísla n tak, že cyklicky zaměníme všechny cifry, dostaneme alespoň k různých hodnot (například pro $n = 2530$ bychom cyklickými záměnami dostali čísla 2530, 5302, 3025 a 253);
3. pro každé prvočíslu platí, že pokud dělí alespoň jednu z cyklických záměn čísla n , tak už dělí všechny.

Nezapomeňte dokázat správnost své odpovědi!

ŘEŠENÍ. Ukážeme, že tvrzení z úlohy platí pro libovolné p různé od pěti.

Začněme tou jednodušší částí – ukažme, že pro $p = 5$ tvrzení neplatí. Ukážeme, že již pro $k = 2$ neexistuje žádné přirozené číslo, které by naše podmínky splňovalo. Nechť pro spor n je takové, že tyto podmínky splňuje. Jelikož číslo je dělitelné pěti právě tehdy, když jeho poslední cifra je 0 nebo 5, tak víme, že poslední cifra čísla n je 0 nebo 5. Ze třetí podmínky víme, že 5 má dělit všechny cyklické záměny čísla n . Jelikož cyklickými záměnami jsme schopni dostat na poslední pozici libovolnou cifru n , tak n nemůže obsahovat jiné cifry než 0 a 5. Pokud by obsahovalo samé pětky, tak není splněno to, že cyklickými záměnami dostaneme alespoň dvě různé hodnoty. Víme tedy, že n obsahuje alespoň jednu 0. Tím pádem ale existuje cyklická záměna n s touto nulou na konci. Takováto cyklická záměna je tedy sudá. Podle poslední podmínky musí být tedy sudé všechny cyklické záměny čísla

n , což znamená, že musí být sudé všechny cifry čísla n . Dohromady s tím, že každá cifra n je buď 0 nebo 5 tak dostáváme, že všechny cifry jsou 0, tedy $n = 0$. Což je spor s tím, že cyklickými záměnami čísla n dostaneme alespoň dvě různé hodnoty (případně s tím, že n je přirozené, jelikož v Brkosu 0 není přirozené číslo).

Zbývá ukázat, že pro všechna ostatní prvočísla tvrzení platí. Nechť $p \neq 5$ je tedy libovolné prvočíslo a k je libovolné přirozené. n budeme hledat ve tvaru

$$\begin{aligned} n &= \underbrace{\overline{a_1 a_2 \dots a_k a_1 a_2 \dots a_k \dots a_1 a_2 \dots a_k}}_{l\text{-krát}} \\ &= \overline{a_1 a_2 \dots a_k} \cdot \underbrace{100 \dots 0100 \dots 01 \dots 00 \dots 01}_{l \text{ jedniček, mezi každými dvěma } k-1 \text{ nul}} \\ &= \overline{a_1 a_2 \dots a_k} \sum_{i=0}^{l-1} 10^{ik} = \overline{a_1 a_2 \dots a_k} \frac{10^{lk} - 1}{10^k - 1} \end{aligned}$$

pro vhodné l , přičemž číslo $\overline{a_1 a_2 \dots a_k} =: a$ zvolíme tak, že všechny jeho cyklické záměny budou různé. Pak určitě splníme druhou podmínku (dostaneme dokonce právě k různých cyklických záměn). Navíc platí, že všechny cyklické záměny n jsou dělitelné číslem $\frac{10^{lk}-1}{10^k-1} =: m$. Naše strategie bude následující: ukážeme, že l je možné zvolit tak, že

- všechna prvočísla různá od 2 a 5, která dělí některou cyklickou záměnu čísla a , dělí dokonce číslo m ;
- pokud $p \neq 2$, tak $p|m$.

Toto nám zaručí, že n bude splňovat podmínky 1 a 3 pro všechna prvočísla jiná než 2 a 5. Když a navíc zvládneme zvolit tak, že bude mít všechny cifry sudé a nenulové, tak bude platit, že číslo n ani žádná z jeho cyklických záměn nebudou dělitelné pěti a navíc bude platit, že všechna tato čísla jsou sudá, takže n bude splňovat všechny podmínky, které na něj klademe. Konec probírání strategie a vzhůru k samotné konstrukci!

Začneme tím, jak zvolit číslo a . Vhodným kandidátem je například číslo $\underbrace{22 \dots 24}_{k-1\text{krát}}$. Toto

číslo zřejmě splňuje, že má všechny cifry sudé a nenulové a navíc všechny jeho cyklické záměny jsou různé (liší se tím, na které pozici mají čtyřku).

Než se pustíme do závěrečné části (volby l), tak budeme muset zmínit jednu známou větu z teorie čísel. Budeme jí říkat Eulerova věta, ale vezte, že se jedná o slabší tvrzení. Pro ty, kdo neznají Eulerovu větu, bude důkaz uveden na konci celého řešení.

„**Eulerova věta**“: Nechť m je přirozené číslo, které není dělitelné dvojkou ani pětkou, pak existuje přirozené číslo – označme nějaké takové $\varphi(m)$ – takové, že platí

$$10^{\varphi(m)} \equiv 1 \pmod{m}.$$

Pokud neznáte kongruence (zápis pomocí trojrovníčka), tak Eulerova věta neříká nic jiného než, že $10^{\varphi(m)}$ dává zbytek 1 po vydělení číslem m , respektive $m|10^{\varphi(m)} - 1$. Vyzbrojení touto znalostí se můžeme konečně pustit do hledání vhodného l :

Označme P (konečnou!) množinu, která vznikne tak, že vezmeme všechna lichá prvočísla, která dělí nějakou cyklickou záměnu čísla a , a pokud $p \neq 2$, tak ho přidáme taky. Vyberme nyní libovolné $q \in P$. Označme v_q nejvyšší mocninu prvočísla q , která dělí číslo $10^k - 1$.

Zvolíme-li nyní číslo l tak, že bude platit $l = \varphi(q^{v_q+1})x$ (pro nějaké $x \in \mathbb{N}$), tak dostaneme následující:

$$10^{lk} - 1 \equiv (10^{\varphi(q^{v_q+1})})^{xk} - 1 \equiv 1^{xk} - 1 \equiv 0 \pmod{q^{v_q+1}}.$$

Odtud dostáváme, že $q^{v_q+1} | 10^{lk} - 1$, tedy $q | \frac{10^{lk}-1}{10^k-1}$. Stačí tedy zvolit l jako součin

$$l = \prod_{q \in P} \varphi(q^{v_q+1}),$$

pak zřejmě bude splňovat vše, co jsme po něm požadovali, čímž je úloha vyřešena, jelikož vhodným n je například číslo

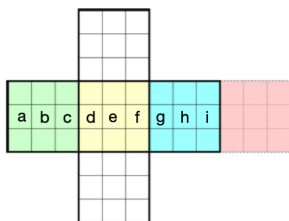
$$\underbrace{22 \dots 24}_{k-1 \text{ krát}} \cdot \frac{10^{lk} - 1}{10^k - 1}.$$

Slíbený důkaz „Eulerovy věty“: Uvažme čísla $10^1, 10^2, \dots, 10^{m+1}$ a zkoumejme, jaké zbytky dávají po vydělení číslem m . Jelikož možných zbytků je pouze m , tak alespoň dvě z uvedených mocnin musejí dávat stejný zbytek. Nechť jsou to 10^r a 10^s ($r > s$). To znamená, že $m | 10^r - 10^s = 10^s(10^{r-s} - 1)$. Jelikož m a 10 jsou nesoudělná, tak to znamená, že $m | 10^{r-s} - 1$. Stačí tedy zvolit $\varphi(m) = r - s$. Tím je tvrzení dokázáno.

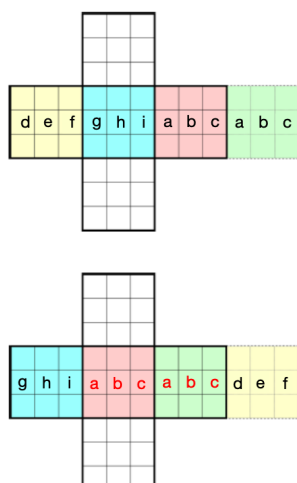
ÚLOHA 6.A. Na Rubikově kostce $3 \times 3 \times 3$ se hraje sudoku tak, že na její políčka na povrchu píšeme čísla. Sudoku vyřešíme, pokud pro každou stěnu kostky platí následující: z kostky odstraníme protilehlou stěnu, rozbalíme ji do pláště tvaru kříže a dále zkontrolujeme, že se žádná dvě čísla neohrožují tak, jako v klasickém sudoku (tedy v každém řádku, sloupci, i čtverci 3×3 , který odpovídá jedné stěně kostky, se může nacházet každé číslo nejvýše jednou). Dokažte, že tímto způsobem nelze vyřešit sudoku na Rubikově kostce.

ŘEŠENÍ. Obrázky v tomto vzorovém řešení jsem si s mírnými úpravami vypůjčil z řešení Katky Matulové, které tímto děkuji. Úloha se dala vyřešit několika způsoby, zde si ukážeme jeden z nich.

Krychli si postavíme na libovolnou plochu a její čtyři boční stěny si obarvíme čtyřmi různými barvami. Horní a spodní stěnu necháme bílé, protože je v důkazu ani nebudeme potřebovat. Nejprve si krychli rozložíme tak, aby uprostřed kříže byla žlutá stěna a BÚNO do prostředního řádku zelené, žluté a modré stěny, které se nachází v kříži, doplníme číslice 1–9 zde pro zdůraznění obecnosti nahrazené písmeny a–i.



Nyní si krychli rozložíme tak, aby uprostřed kříže byla modrá stěna a díky tomu se nám do kříže nově dostane stěna červená. Aby byla zachována pravidla sudoku, musíme do prostředního řádku červené stěny doplnit cifry a–c, které chybí v prostředním řádku žluté a modré stěny.



Pokud nyní krychli s takto doplněnými dvanácti ciframi rozložíme tak, aby uprostřed kříže byla například červená stěna, vidíme, že v prostředním řádku červené a zelené stěny jsou ty stejné číslice, což odporuje pravidlům sudoku.

Tímto jsme se dostali do sporu a dokázáno jest, že podle pravidel v zadání opravdu nelze všechna pole na krychli vyplnit číslicemi.

ÚLOHA 6.B. Madam Cornélie se rozhodla utkat se v lukostřelbě s plukovníkem Motýlem. Každý má deset šípů, které střílí na terč a odstraňují je z něj. V libovolném pořadí oba střílí a odstraňují svoje vlastní šípy, např.

1. Madam Cornélie: vystřelila,
2. Madam Cornélie: vystřelila,
3. Plukovník Motýl: vystřelil,
4. Madam Cornélie: odstranila,
5. Plukovník Motýl: vystřelil, ...

Jediná podmínka je, aby ani jeden neodstranil více šípů, než doposud vystřelil. Kolik různých průběhů hry existuje?

ŘEŠENÍ. Při výpočtu úlohy využijeme Catalanova čísla. Pokud se podíváme pouze na tahy Madam Cornélie, vidíme, že pravidla pro vystřelení a posbírání přesně odpovídají pravidlům pro dobré uzávorkování; '(' odpovídá vystřelení a ')' odpovídá posbírání. Protože má Madam Cornélie 10 šípů, je počet kombinací vystřelení a sesbírání (bez uvážení tahů Plukovníka Motýla) C_{10} , tedy desáté Catalanovo číslo. Pro Plukovníka Motýla platí totéž, jeho tahů je také C_{10} .

Nyní si představíme, jak do sebe zapadají tahy Madam a Plukovníka. Dohromady mají 40 tahů chronologicky za sebou, některé z nich budou Madam a některé Plukovníka. Které jsou které? Pokud vybereme z těchto 40 těch 20 Plukovníkových, je už jasně dáno, které patří Madam. Protože vybíráme dvacetiprvkovou podmnožinu z čtyřicetiprvkové množiny, těchto způsobů výběru toho, kdy kdo táhl, je $\binom{40}{20}$.

Celkem tedy existuje C_{10} možností, jak bude střílet Motýl, C_{10} možností tahů Madam a $\binom{40}{20}$ možností distribuce těchto tahů, celkem je tedy $C_{10}^2 \cdot \binom{40}{20}$ možných průběhů hry.

ÚLOHA 6.C. Uvažme libovolné slovo, které sestává pouze z prvních sedmi písmen anglické abecedy (za slovo považujeme libovolnou konečnou posloupnost písmen – takže *aaabag* je také slovo). Proházením písmen podle nějakého klíče v naší sedmiprvkové abecedě zašifrujeme libovolné slovo. Výsledný znak závisí jen na tom, jaký byl původní znak, nikoliv na jeho pozici nebo kontextu. Nezaměňujeme dva znaky za stejný, aby se zpráva dala dešifrovat.

Například, klíč $L = (a \mapsto b, b \mapsto c, c \mapsto a, d \mapsto d, e \mapsto e, f \mapsto f, g \mapsto g)$ aplikovaný na naše slovo *aaabag* vytvoří slovo *bbcbg*. Druhou aplikací téhož klíče dostaneme slovo *cccag*, a konečně třetí aplikací získáme *aaabag*, tedy původní slovo.

Definujme *magické číslo klíče K na slovo w* jako počet aplikací klíče K na slovo w tak, abychom získali původní slovo. Například, magické číslo klíče L na slovo *aaabag* je 3. Najděte nějaký klíč K a slovo w tak, aby magické číslo klíče K na slovo w bylo co největší.

ŘEŠENÍ. Magické číslo představuje počet aplikací klíče na původní slovo.

Uvědomme si, že změny jednotlivých písmen slova jsou nezávislé. Nemůžeme mít více než 7 různých písmen. Slova delší než 7 tedy nemusíme vůbec uvažovat.

V klíči definujeme přechod pro každé písmeno - každé písmeno se mění na nějaké jiné (popř. zůstane tím stejným), ale žádná dvě se nemění na to samé.

Protože se po několika aplikacích klíče dostaneme opět na stejné písmeno, můžeme si přechody představit jako cykly.

Například přechod $(a \rightarrow b, b \rightarrow c, c \rightarrow a)$ tvoří cyklus délky 3: $(a \rightarrow b \rightarrow c)$ a při aplikaci klíče se každé písmeno změní na následující za nejbližší šipkou.

Maximální délka cyklu pro sedmipísmennou abecedu je 7. Dále, pokud se v klíči objeví více cyklů stejné délky, stačí uvažovat pouze jeden z nich. Stejně tak, pokud se vyskytnou dva cykly a délka jednoho je násobkem délky druhého, stačí uvažovat delší z nich. Pokud totiž aplikujeme klíč tolikrát, kolik je délka cyklu, všechny cykly, jejichž délka toto číslo dělí, dostanou svá písmena do původní podoby. Magickým číslem je proto nejmenší společný násobek délek cyklů klíče. Cykly délky 1 nemusíme uvažovat, nijak neovlivní výsledek.

Máme 7 písmen. Pokud klíč tvoří právě jeden cyklus, bude maximálně délky 7, stejně tak jeho magické číslo. Jednocykly toto číslo neovlivní.

Pokud klíč tvoří dva cykly, mohou nastat následující možnosti:

1 cyklus délky 5, 1 délky 2 \rightarrow magické číslo 10

2 cyklus délky 4, 1 délky 3 \rightarrow magické číslo 12

2 cyklus délky 4, 1 délky 2 (+ 1 cyklus délky 1) \rightarrow magické číslo 4

2 cyklus délky 3, 1 délky 3 (+ 1 cyklus délky 1) \rightarrow magické číslo 3

Dále bychom se opakovali.

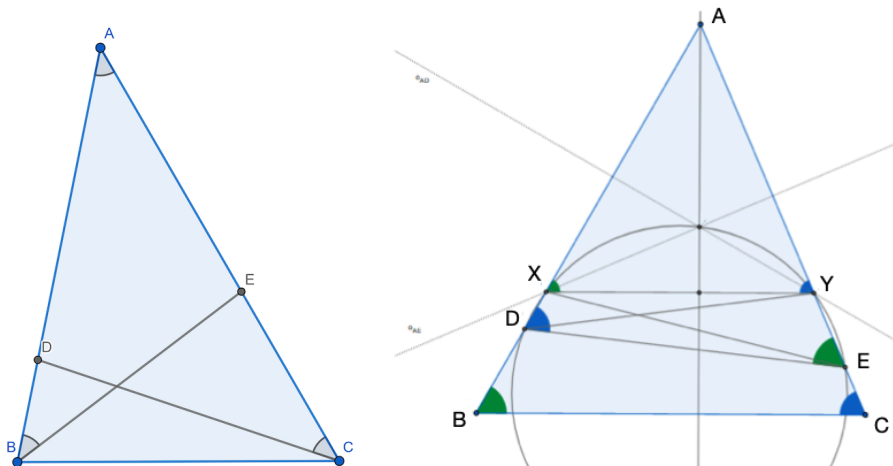
Více než dva cykly nemusíme uvažovat. Nejmenší tři různé délky cyklů jsou 2, 3, 4, už pro ten bychom ale potřebovali 9 různých písmen.

Největší magické číslo je tedy 12 a získáme ho, pokud se klíč skládá z jednoho cyklu délky 3 a jednoho délky 4.

Příklad klíče: $K = (a \rightarrow b, b \rightarrow c, c \rightarrow a, d \rightarrow e, e \rightarrow f, f \rightarrow g, g \rightarrow d)$

Příklad slova: $w = ae$

ÚLOHA 6.D. Je dán ostroúhlý trojúhelník ABC . Uvnitř jeho stran AB a AC leží po řadě body D a E tak, že $|CD| = |DA|$ a $|BE| = |EA|$. Bod F je střed kružnice opsané trojúhelníku ADE . Dokažte, že AF je kolmá na BC .



ŘEŠENÍ. Děkuji Huu Quy Nguyen, z jehož řešení jsem si půjčil levý obrázek.

Nejdříve ukážeme, že platí $\triangle ABC \sim \triangle AED$. Jelikož trojúhelníky $\triangle AEB$ a $\triangle ADC$ jsou rovnoramenné, tak $|\angle DBE| = |\angle BAC| = |\angle DCE|$. Úhly $\angle DBE$ a $\angle DCE$ jsou obvodové úhly stejnému oblouku. Tedy čtyřúhelník $BCED$ je tětívový. Jelikož $|\angle ABC| = \pi - |\angle CED| = |\angle AED|$ a $|\angle ACB| = \pi - |\angle CDE| = |\angle ADE|$, jsou trojúhelníky $\triangle ABC$ a $\triangle AED$ podobné podle věty uu .

Označme X a Y průsečíky os úseček AE a AD s přímkami AB a AC . Rovnoramenné trojúhelníky $\triangle ADY$ a $\triangle AEX$ mají úhly při základně $|\angle ABC|$. Jsou tedy podle věty uu podobné trojúhelníkům $\triangle ABE$ a $\triangle ACD$. Protože trojúhelníky $\triangle ADY$ a $\triangle AEX$ mají menší základnu a jsou podobné $\triangle ABE$ a $\triangle ACD$, pak $|AY| < |AE|$ a $|AX| < |AD|$. Neboli X (respektive Y) leží uvnitř úsečky $|AD|$ (respektive $|AE|$).

Analogicky ukážeme (pomocí tětívového čtyřúhelníku $DEYX$ a věty uu), že trojúhelník $\triangle EDA \sim \triangle XYA$. Dostaneme tedy $|\angle ABC| = |\angle AXE|$, protože již víme, že platí $\triangle ABC \sim \triangle AED$. Tedy $BC \parallel XY$.

Jelikož je trojúhelník $\triangle AXE$ rovnoramenný se základnou AE a XF je osa úsečky AE , tak XF je výška na AE , neboli AY . Stejně tak je YF výška na AX . Bod F je tedy ortocentrum (průsečík výšek) trojúhelníku $\triangle AXY$, tedy $AF \perp XY$. Protože $BC \parallel XY$ tak dokonce $AF \perp BC$, což jsme chtěli dokázat.