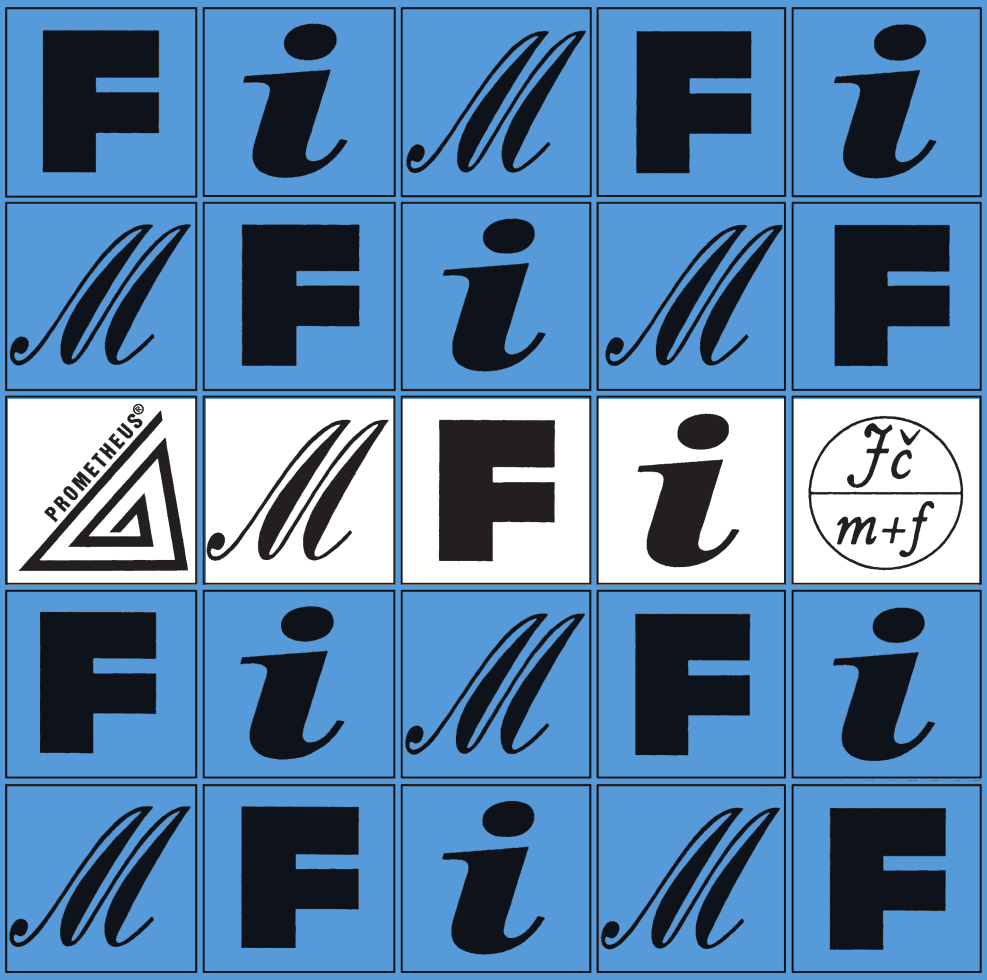
MATEMATIKA FYZIKA INFORMATIKA

1

ČASOPIS PRO VÝUKU NA ZÁKLADNÍCH A STŘEDNÍCH ŠKOLÁCH



ROČNÍK 27, ČÍSLO 1 LEDEN–ÚNOR 2018

MATEMATIKA – FYZIKA – INFORMATIKA

Časopis pro výuku na základních a středních školách
Ročník XXVII (2018), číslo 1
Vydává Prometheus, spol. s r. o. ve spolupráci s Jednotou českých matematiků a fyziků

Adresa redakce:
17. listopadu 12, 771 46 Olomouc. E-mail: MFI@upol.cz

Adresa vydavatele:
Prometheus, spol. s r. o., Čestmírova 10, 140 00 Praha 4

OBSAH

MATEMATIKA

Polibky kružnic: Philip Beecroft

PAVEL LEISCHNER

Pedagogická fakulta JU, České Budějovice

Anglický matematik *Phillip Beecroft* (1818–1862) žil v době vzniku a rozvoje projektivní geometrie. Ponceletův princip duality a metody s ním spojené jej pravděpodobně inspirovaly k níže uvedeným objevům. Seznámíme se s obsahem jeho článku o vzájemných dotycích kružnic [1], publikovaném roku 1842 v ročence *The Lady's and Gentleman's Diary* (dále jen *Diary*). Stejně jako on se nebudeme zabývat situacemi, v nichž mají aspoň tři kružnice tentýž bod dotyku.

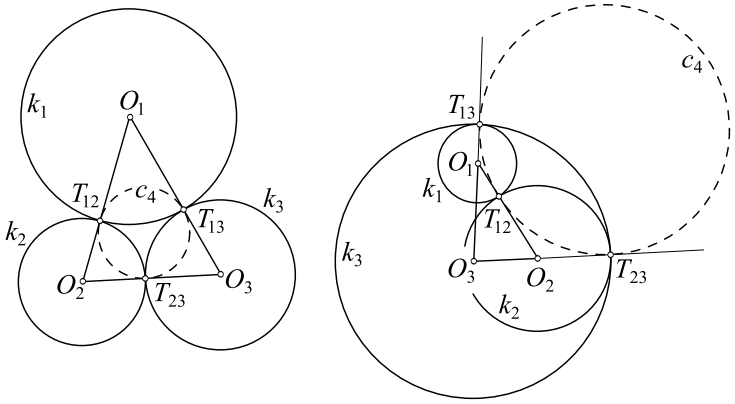
Beecrofrt nejprve uvedl, že jsou jen dvě možné konfigurace pro kružnice $k_1(O_1; r_1)$, $k_2(O_2; r_2)$ a $k_3(O_3; r_3)$, které se navzájem dotýkají v bodech T_{23}, T_{13} a T_{12}. Body dotyku přitom jednoznačně určují *duální* (*doplňkovou*) *kružnici* $c_4(C_4; \rho_4)$ opsanou trojúhelníku $T_{23}T_{13}T_{12}$.

V *první konfiguraci* (obr. 1 vlevo) je dotyk všech tří kružnic vnější a kružnice c_4 je trojúhelníku $O_1O_2O_3$ vepsána. *Druhá konfigurace* se vyznačuje jedním vnějším a dvěma vnitřními dotyky a kružnice c_4 je trojúhelníku $O_1O_2O_3$ připsána.

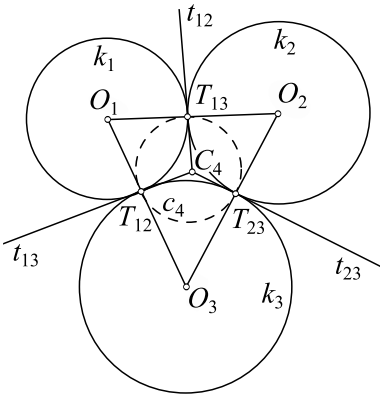
Polohu kružnice c_4 Beecroft zdůvodnil vlastnostmi tečen z bodu ke kružnici. Plyne též z faktu, že společné tečny t_{23}, t_{13} a t_{12} kružnic v jejich bodech dotyku T_{23}, T_{13}, a T_{12} jsou chordály příslušných dvojic kružnic (obr. 2, resp. obr. 3). Mají proto společný průsečík C_4, potenční střed kružnic k_1, k_2 a k_3 stejně vzdálený od bodů T_{23}, T_{13}, T_{12}, a tedy i od přímek O_2O_3, O_1O_3, O_1O_2.

Beecroft dále určil poloměr ρ_4 pomocí poloměrů r_1, r_2 a r_3. Pro každou z konfigurací vyšel jiný vztah, což mu komplikovalo další úvahy. Na rozdíl od něj přijmeme následující znaménkovou dohodu, jež zaručí pro obě konfigurace stejný výsledek. Ten pak vyjádříme větou 1.

Znaménková dohoda Tvoří-li tři navzájem se dotýkající kružnice druhou konfiguraci, pak poloměru (a tedy i křivosti) té kružnice, jež má s druhými dvěma vnitřní dotyk, přiřadíme záporné znaménko.



Obr. 1 Dvě konfigurace vzájemného dotyku tří kružnic



Obr. 2 Střed C_4 kružnice c_4 je potenčním středem kružnic k_1, k_2 a k_3

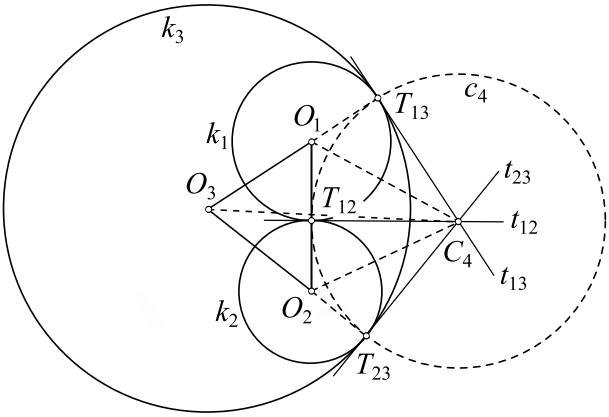
Věta 1

Pro obě konfigurace kružnic $k_1(O_1; r_1)$, $k_2(O_2; r_2)$, $k_3(O_3; r_3)$ a $c_4(C_4; \rho_4)$ platí

$$\frac{1}{\rho_4^2} = \frac{1}{r_1 r_2} + \frac{1}{r_2 r_3} + \frac{1}{r_3 r_1}. \tag{1}$$

Důkaz. Pro situaci z obr. 3 platí

$$S_{O_1O_3C_4} + S_{O_3O_2C_4} - S_{O_1O_2C_4} = S_{O_1O_2O_3}.$$



Obr. 3 K důkazu vztahu (1)

Pravou stranu této rovnosti vyjádříme pomocí Heronova vzorce a obsahy trojúhelníků na levé straně pomocí výšky ρ_4 z jejich společného vrcholu C_4. Navíc využijeme vztahy $|O_1O_2| = r_1 + r_2$, $|O_2O_3| = -r_3 - r_2$, $|O_1O_3| = -r_3 - r_1$ a (polovina obvodu trojúhelníku $O_1O_2O_3$) $s = -r_3$. Obdržíme

$$\frac{\rho_4}{2}\big((-r_3 - r_1) + (-r_3 - r_2) - (r_1 + r_2)\big) = \sqrt{(-r_3 - r_1 - r_2)r_1r_2(-r_3)}$$

a odtud

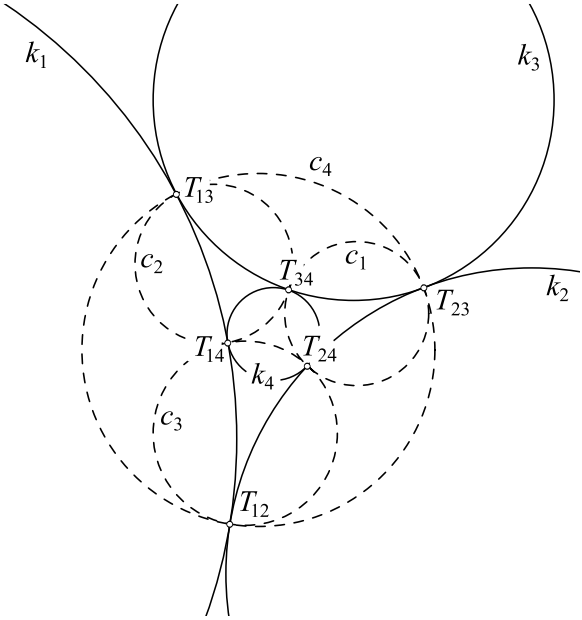
$$\rho_4^2 = \frac{r_1r_2(-r_3)}{-r_1 - r_2 - r_3} = \frac{r_1r_2r_3}{r_1 + r_2 + r_3}, \quad \text{tj.} \quad \frac{1}{\rho_4^2} = \frac{1}{r_1r_2} + \frac{1}{r_2r_3} + \frac{1}{r_3r_1}.$$

Tím je pro druhou konfiguraci dokázán vztah (1). Analogický důkaz pro první konfiguraci přenecháváme čtenáři.

Dále se budeme stejně jako Beecroft zabývat čtveřicemi navzájem se dotýkajících kružnic. Základní kružnice značíme $k_i(O_i; r_i)$, kde $i \in \{1, 2, 3, 4\}$, a jejich křivosti $\kappa_i = \frac{1}{r_i}$. Označení duálních kružnic volíme $c_i(C_i; \rho_i)$ ve shodě s obr. 4 a jejich křivosti značíme $\varepsilon_i = \frac{1}{\rho_i}$. Věta 2 je přímým důsledkem počátečních úvah.

Věta 2 (Beecroftova)

Čtveřice kružnic, které se navzájem dotýkají v šesti různých bodech, určují duální čtveřici kružnic, jež se navzájem dotýkají ve stejných šesti bodech tak, že každá kružnice z jedné čtveřice protíná kolmo tři kružnice druhé čtveřice v bodech vzájemného dotyku těch tří (obr. 4).



Obr. 4 Navzájem duální čtveřice kružnic

Obě čtveřice kružnic mají stejné vlastnosti a jsou jednoznačně určeny šesti společnými body dotyku. (Beecroft použil termín *concordant circles*). Pokud nalezneme nějaký vztah mezi poloměry nebo křivostmi těchto kružnic, získáme z něj analogické vztahy záměnami $r_i \leftrightarrow \rho_i$ a $\kappa_i \leftrightarrow \varepsilon_i$. Platit budou i vztahy vzniklé cyklickými záměnami indexů.

Kvůli dalším úvahám zapíšeme rovnost (1) pomocí křivostí kružnic a nahradíme ji pro všechny patřičné skupiny kružnic z obr. 4 rovnostmi

$$\kappa_4^2 = \varepsilon_1\varepsilon_2 + \varepsilon_2\varepsilon_3 + \varepsilon_3\varepsilon_1, \quad \varepsilon_4^2 = \kappa_1\kappa_2 + \kappa_2\kappa_3 + \kappa_3\kappa_1 \quad \text{a cykl.} \qquad (2)$$

K nalezení dalších vztahů Beecroft použil jen standardní algebraické úpravy.

Věta 3

Součet křivostí čtveřice navzájem se dotýkajících kružnic je vždy kladný a je roven součtu křivostí doplňkové čtveřice kružnic.

Důkaz. První tvrzení je zřejmé. Má-li totiž některá kružnice zápornou křivost, pak je ve čtveřici jen jedna a absolutní hodnota její křivosti je nejmenší.

K důkazu druhého tvrzení sečteme každou z rovností (2) se všemi, které z ní vzniknou cyklickými záměnami. Dostáváme

$$\sum_i \kappa_i^2 = 2\sum_{i<j} \varepsilon_i\varepsilon_j \quad \text{a} \quad 2\sum_{i<j} \kappa_i\kappa_j = \sum_i \varepsilon_i^2.$$

Ze vztahu

$$\Big(\sum_i \kappa_i\Big)^2 = \Big(\sum_i \varepsilon_i\Big)^2$$

vzniklého sečtením obou předchozích rovností plyne

$$\sum_i \kappa_i = \sum_i \varepsilon_i. \tag{3}$$

Věta 4

Pro uvažované čtveřice kružnic platí

$$2\varepsilon_4 = \kappa_1 + \kappa_2 + \kappa_3 - \kappa_4, \quad 2\kappa_4 = \varepsilon_1 + \varepsilon_2 + \varepsilon_3 - \varepsilon_4 \quad \text{a cykl.}, \tag{4}$$

$$\sum_i \kappa_i^2 = 2\sum_{i<j} \kappa_i\kappa_j \quad \text{a} \quad \sum_i \varepsilon_i^2 = 2\sum_{i<j} \varepsilon_i\varepsilon_j, \tag{5}$$

$$\kappa_1 + \varepsilon_1 = \kappa_2 + \varepsilon_2 = \kappa_3 + \varepsilon_3 = \kappa_4 + \varepsilon_4 = \frac{1}{2}\sum_i \kappa_i = \frac{1}{2}\sum_i \varepsilon_i. \tag{6}$$

Důkaz. Ze vztahů (2) a (3) plyne

$$\begin{aligned}\kappa_1^2 + \kappa_2^2 + \kappa_3^2 - \kappa_4^2 = \\ = 2\varepsilon_4(\varepsilon_1 + \varepsilon_2 + \varepsilon_3) = 2\varepsilon_4(\kappa_1 + \kappa_2 + \kappa_3 + \kappa_4) - 2\varepsilon_4^2 = \\ = 2\varepsilon_4(\kappa_1 + \kappa_2 + \kappa_3 + \kappa_4) - 2(\kappa_1\kappa_2 + \kappa_2\kappa_3 + \kappa_3\kappa_1).\end{aligned}$$

Odtud s úpravou pomocí vzorce pro rozdíl čtverců obdržíme (4):

$$2\varepsilon_4 = \frac{(\kappa_1+\kappa_2+\kappa_3)^2-\kappa_4^2}{\kappa_1+\kappa_2+\kappa_3+\kappa_4} = \kappa_1+\kappa_2+\kappa_3-\kappa_4.$$

Abychom dokázali vztah (5), umocníme první z rovností (4), zaměníme její strany a za ε_4^2 dosadíme ze vztahu (2). Dostaneme

$$(\kappa_1+\kappa_2+\kappa_3-\kappa_4)^2 = 4(\kappa_1\kappa_2+\kappa_2\kappa_3+\kappa_3\kappa_1) \tag{7}$$

a odtud (5).

Vztahy (6) jsou důsledkem rovností (4) a (3), neboť například

$$2(\kappa_1-\kappa_4) = (\varepsilon_2+\varepsilon_3+\varepsilon_4-\varepsilon_1)-(\varepsilon_1+\varepsilon_2+\varepsilon_3-\varepsilon_4) \Rightarrow$$
$$\Rightarrow \kappa_1+\varepsilon_1 = \kappa_4+\varepsilon_4.$$

V závěru své práce určoval Beecroft poloměr r kružnice, jež se dotýká tří daných a navzájem se dotýkajících kružnic s poloměry r_1, r_2 a r_3. Uvedl, že po odmocnění vztahu (7) (při vyjádření pomocí poloměrů kružnic) snadno nalezneme obě řešení

$$\frac{1}{r} = \frac{1}{r_1}+\frac{1}{r_2}+\frac{1}{r_3} \pm 2\sqrt{\frac{1}{r_1r_2}+\frac{1}{r_2r_3}+\frac{1}{r_3r_1}}. \tag{8}$$

Poznamenejme, že ve skutečnosti diskutoval obě konfigurace, protože neužíval znaménkovou dohodu. Závěry jej přivedly k poznatku, že při použití vztahu (8) odpovídá záporný kořen kružnici, jež má vnitřní dotyky se zadanými třemi kružnicemi.

Pokračování článku vyšlo o tři roky později a zabývá se analýzou obecného Pappova řetězce kružnic, který můžeme vidět na obr. 5). Zde se jím nebudeme zabývat.

V předchozím dílu seriálu jsme ukázali, že vztah (5) je ekvivalentní se Soddyho rovností

$$2\sum_i \kappa_i^2 = \Big(\sum_i \kappa_i\Big)^2, \tag{9}$$

kterou v tomto tvaru Beecroft neuvedl.

V Diary byly též čtenářům předkládány různé problémy k řešení. Problém č. 1736, jehož autor se podepsal zkratkou β, doplnil Beecroftovy poznatky. Přepsali jsme jej do věty 5.

Věta 5

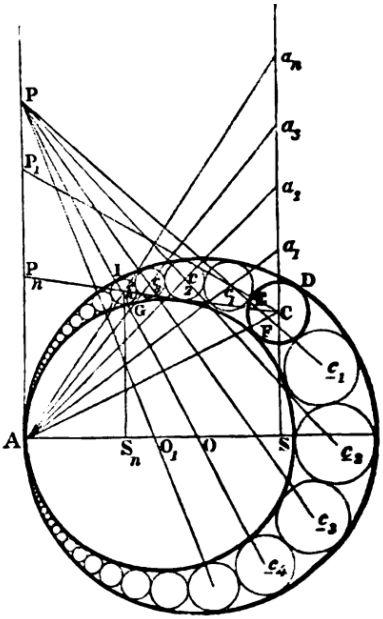
Pro uvažované čtveřice kružnic platí

$$\sum_i \kappa_i \varepsilon_i = 0. \tag{10}$$

Důkaz. (Podle Diary 1846, str. 51.) Po přepsání první z rovností (5) do tvaru

$$\begin{aligned} 0 \;=\; & \kappa_1(-\kappa_1+\kappa_2+\kappa_3+\kappa_4)+\kappa_2(\kappa_1-\kappa_2+\kappa_3+\kappa_4)+ \\ & +\kappa_3(\kappa_1+\kappa_2-\kappa_3+\kappa_4)+\kappa_4(\kappa_1+\kappa_2+\kappa_3-\kappa_4) \end{aligned}$$

a dosazení za výrazy v závorkách ze vztahů (4) obdržíme (10).



Obr. 5 Ilustrace z ročenky Diary 1845, str. 92

Jiný důkaz. (Coxeter [2].) S využitím vztahů (6) a (9) obdržíme

$$\sum_i \kappa_i \varepsilon_i = \sum_i \kappa_i \left(\frac{1}{2}\Big(\sum_i \kappa_i\Big) - \kappa_i \right) = \frac{1}{2}\Big(\sum_i \kappa_i\Big)^2 - \sum_i \kappa_i^2 = 0.$$

V první polovině 20. století byl časopis Diary včetně Beecroftovy práce téměř zapomenut, stejně jako Steinerovy výsledky popsané v předchozích dílech seriálu. Vztah (9) byl od roku 1936 považován za objev Fredericka Soddyho, který jej bez důkazu popsal formou básně *The Kiss Precise* v časopise Nature. Díky básni se vztah stal populární. O rozšíření poznatků, které s ním souvisí se zasloužili zejména dva významní geometři britského původu, H. S. M. Coxeter (1907–2003) a D. Pedoe (1910–1998).

Coxeter věnoval této problematice několik stránek své knihy *Introduction to Geometry*. V prvním vydání z roku 1961 uvedl zajímavé trigonometrické odvození rovnosti (9). Krátce nato jej L. Bankoff (1908–1997) seznámil s Beecroftovými pracemi. Ty Coxetera zaujaly do té míry, že v druhém vydání z roku 1969 nahradil své původní odvození Beecroftovým, které publikoval i jinde. V příspěvku [3] zdůraznil význam věty 1, která platí i v neeukleidovských geometriích.

Tímto článkem končí náš sedmidílný seriál zaměřený na historii objevu jednoho vztahu. Vznikl ze snahy doplnit Kotlasovu diplomovou práci [4], ve které se čtenář může seznámit s dalšími poznatky. Například s důkazem vztahu (9) užitím kruhové inverze a zmíněným Coxeterovým trigonometrickým odvozením. Úvodem do podrobnějšího studia mohou být články [3]) a [5]) s odkazy na další literaturu.

Literatura

[1] *Beecroft, P.:* Properties of circles in mutual contact, The Lady's and Gentleman's Diary, 1842, s. 91–96. Dostupné na: https://catalog.hathitrust.org/Record/000071981

[2] *Coxeter, H. S. M.:* The Problem of Apollonius, The American Mathematical Monhly, roč. 75 (1968), č. 1, s. 5–15.

[3] *Coxeter, H. S. M.:* An Absolute Property of Four Mutually Tangent Circles, In: Non-Euclidean Geometries: János Bolyai Memorial Volume, Volume 581, Springer, New York, 2006.

[4] *Kotlas, M.:* Polibky kružnic. Jihočeská univerzita v Českých Budějovicích, Pedagogická fakulta, Katedra matematiky, České Budějovice, 2011 (diplomová práce).

[5] *Pedoe, D.:* On a Theorem in Geometry, The American Mathematical Monhly, roč. 74 (1967), č. 6, s. 627–640.

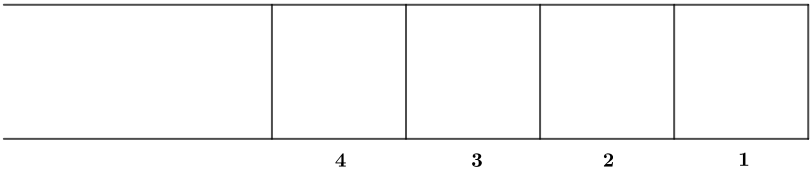
Matematika hrou

IVAN CHAJDA

Přírodovědecká fakulta UP, Olomouc

V učitelství matematiky se stále objevují snahy, jak žákům zpřístupnit poněkud abstraktní matematické znalosti, a jak motivovat zájem žáků o tento předmět. S jedním takovým hravým přístupem přišel před nedávnem *James Tauton*, který spolu s *Briannou Donaldson* napsal přehledný článek [1] a na internetu umístil i názornou prezentaci [2]. Rád bych v tomto článku i českým čtenářům přiblížil tento přístup, který J. Tauton nazývá *stroj na exploze* (*exploding machine* v angl. originále).

Celé zařízení se sestává z proužku papíru, na kterém jsou oddělená políčka, očíslovaná zprava doleva, viz obr. 1.



Obr. 1

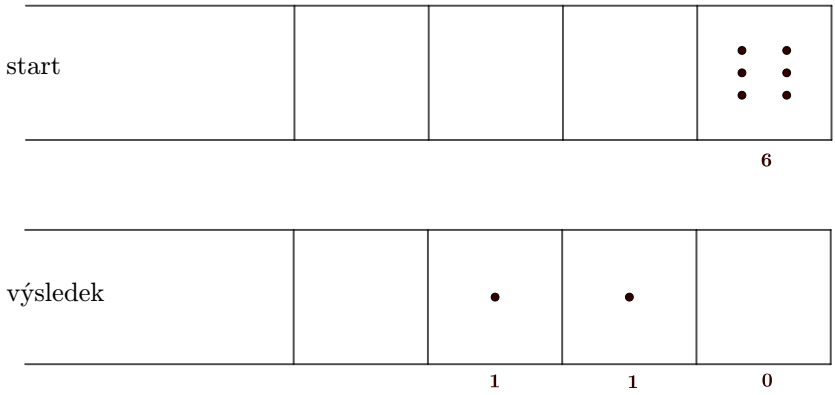
Dle dané úlohy je pak stroj „naprogramován“, tj. je zadáno, jak budou „exploze“ bodů probíhat. Žákům lze nejlépe tento stroj vysvětlit na příkladu. Do políčka č. 1 „nasypeme“ n bodů. Stroj pracuje takto:

Každé dva body v políčku 1 explodují, tj. zmizí z políčka č. 1, a tím vznikne bod v políčku č. 2. Takto exploze pokračují, dokud v políčku č. 1 nezůstane buď jeden bod nebo prázdné políčko. Celý proces se pak opakuje s políčkem č. 2, kde opět každé dva body „explodují“ a tím vymizí z políčka č. 2, a současně vznikne bod v políčku č. 3. A tak dále, dokud v každém políčku nezůstane nejvýše jeden bod.

Například do políčka č. 1 „nasypeme“ 6 bodů. Po ukončení všech explozí v políčku č. 1 zůstane toto políčko prázdné a v políčku č. 2 budou 3 body. Po následující „explozi“ bude v políčku č. 2 jeden bod a v políčku č. 3 také jeden bod, viz obr. 2.

Čili náš „stroj na exploze“ převede číslo 6 na 110, což není nic jiného, než převod čísla 6 v desítkové soustavě do soustavy dvojkové. A to zcela me-

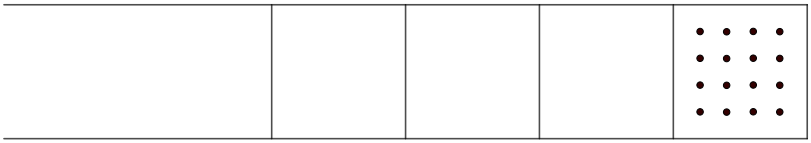
chanicky, dokonce zábavnou formou. Žáci tak dostanou hravou pomůcku na převod dekadických čísel na čísla dyadická.



Obr. 2

A nyní následuje vcelku jednoduchá analogie, daná malou modifikací našeho „stroje na exploze“. Totiž budou explodovat nikoli 2 body, ale body tři, a touto explozí v i-tém políčku přibyde jeden bod v políčku $i+1$.

Příklad: „nasypeme“ do políčka č. 1 právě 16 bodů, viz obr. 3:



Obr. 3

Po první sérii výbuchů zůstane v políčku č. 1 jeden bod a vznikne 5 bodů v políčku č. 2 (obr. 4):

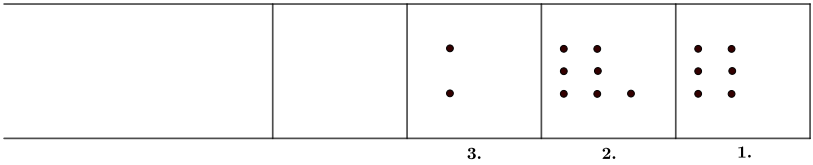
Obr. 4

Po explozi v políčku č. 2 tam zůstanou dva body a vznikne jeden bod v políčku č. 3, čímž se proces ukončí. Získané číslo 120 je převod dekadického čísla 16 na jeho vyjádření v trojkové soustavě.

Chytřejším žákům je nyní již zřejmé, jak upravit náš stroj na exploze tak, aby převáděl čísla z desítkové soustavy do číselné soustavy o základu k, a to pro libovolné přirozené číslo $k > 1$. Úloha je velmi zajímavá zejména pro $k > 10$, což si žáci mohou hravě sami ověřit.

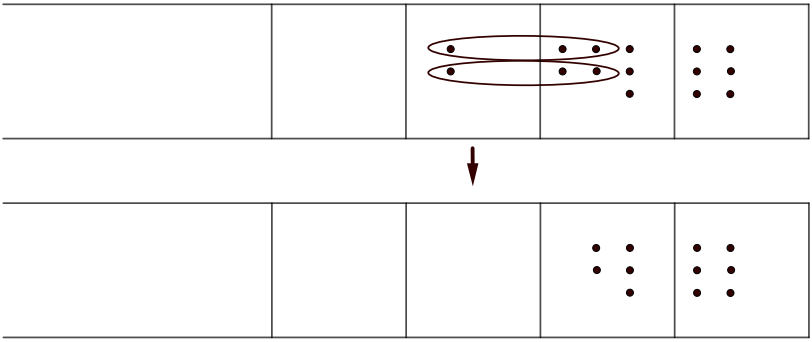
Převádění čísel do jiné číselné soustavy ovšem není jediná úloha, kterou stroj na exploze dovede. Další takovou úlohou je například dělení čísel, což žákům občas činí potíže, a není pro ně příliš zábavná.

Tentokrát modifikujeme náš stroj takto. Budeme např. dělit číslo 276 číslem 12. Do našeho stroje tedy umístíme 6 bodů do políčka č. 1, 7 bodů do políčka č. 2, a dva body do políčka č. 3, viz schéma na obr. 5.



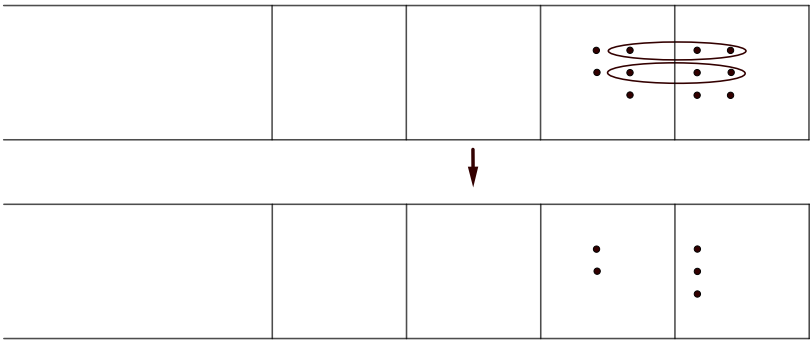
Obr. 5

Protože dělíme číslem 12, které je dvojciferné, budeme postupovat odpředu, tj. od políčka č. 3, a každá exploze bude spotřebovávat 1 bod z políčka č. 3 a 2 body z políčka č. 2, čímž vznikne jeden bod v políčku č. 2. Tedy po první sérii výbuchů bude náš stroj obsazen takto (obr. 6):



Obr. 6

Analogicky postupujeme dále, tj. od políčka č. 2 k políčku č. 1, takže po další sérii výbuchů již dostaneme konečný výsledek (obr. 7):



Obr. 7

Tím je proces ukončen, a tedy $276 : 12 = 23$.

Pokud se předchozí úloha jeví jako příliš primitivní, je třeba ukázat, že prakticky stejný stroj pracuje i při dělení mnohočlenů, což je už pro žáky úloha obtížnější. Využijeme toho, jak byl stroj nastavený, a budeme dělit mnohočlen $2x^2+7x+6$ mnohočlenem $x+2$. Tedy opět „nasypeme“ 2 body do políčka č. 3, 7 bodů do políčka č. 2 a 6 bodů do políčka č. 1. Jelikož dělíme mnohočlenem $x+2$, budeme vždy ubírat 1 bod z políčka $i+1$ a 2 body z políčka i, čímž vzniknde 1 bod v políčku č. i, tedy postup i obrázky jsou shodné s výše uvedenými, jiná je pouze interpretace. Výsledek je tedy

$$(2x^2 + 7x + 6) : (x + 2) = 2x + 3.$$

To není zdaleka vše, co tento stroj na exploze dokáže. Čtenáři, kterého tento výklad zaujal, doporučujeme shlédnout některou z prezentací, které najdete na webu v odkazu [2].

Literatura

[1] *Tauton, J., Donaldson, B.*: The Global Math Project: Uplifting Mathematics for All, Notices Amer. Math. Asoc., roč. 64 (2017), č. 7, s. 712–716.

[2] *Tauton, J.*, Exploding Dots, Experience 9. Dostupné na: gdaymath.com/courses/esploding-dots/

Hvězdicové mnohoúhelníky

MARTINA ŠTĚPÁNOVÁ

Matematicko-fyzikální fakulta UK, Praha

Každý žák základní školy by měl znát pojem *pravidelný n-úhelník*. Běžně se jím rozumí konvexní útvar. Existují však také nekonvexní mnohoúhelníky, které sice přívlastek *pravidelné* v názvu nemají, ale mohli bychom jim ho – vzhledem k jejich symetrii – směle přisoudit. Máme na mysli tzv. *hvězdicové n-úhelníky*, útvary ve výuce na jakémkoli stupni škol opomíjené.

V dalším textu se budeme držet zažitých zvyklostí, tj. termínem *pravidelný n-úhelník* budeme označovat výhradně konvexní pravidelný n-úhelník.

Hvězdicové n-úhelníky můžeme zavést více způsoby. Uvedeme dnes nejběžněji používaný přístup:

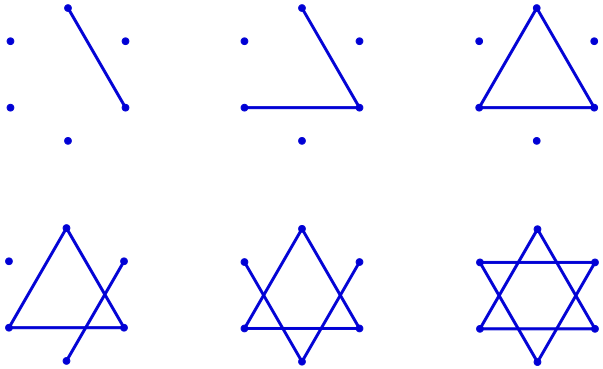
Definice 1

Nechť n a k jsou přirozená čísla, kde $n \geq 5$, $2 \leq k < \frac{n}{2}$, a nechť je na (pomyslné) kružnici pravidelně rozmístěno n bodů (vrcholy pravidelného n-úhelníku). Vybereme jeden z těchto bodů a spojíme ho úsečkou s k-tým bodem, tento bod s dalším k-tým bodem atd. dokud se nenavrátíme do výchozího bodu (uvažujeme přitom body v pořadí, v jakém jsou umístěny na kružnici, a to např. ve směru hodinových ručiček). Jestliže poté zůstanou některé body nepropojené, vybereme jeden z nich a celý proces zopakujeme až do okamžiku, kdy budou všechny body využity[1)] (viz obr. 1 a 2). Vznikne geometrický útvar, jehož obvod tvoří uzavřená lomená čára s $2n$ stranami. Všechny body roviny ohraničené zmíněnou lomenou čarou včetně této hranice nazveme *hvězdicový n-úhelník* (obecněji *hvězdicový mnohoúhelník*). Dané body nazveme *vrcholy* hvězdicového n-úhelníku.

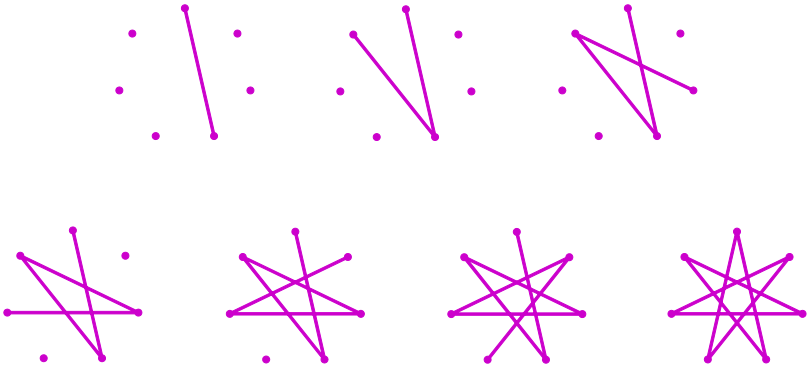
V právě uvedené definici se někdy nepožaduje pravidelné rozmístění bodů po kružnici, termín *hvězdicový n-úhelník* je tedy používán i v obec-

[1)] Každý z bodů tedy spojíme s jeho k-tým „sousedem“, počítáme-li body ve směru hodinových ručiček.

nějším případě. Teorie takových nepravidelných útvarů je však komplikovaná a nebudeme se jí dále zabývat.



Obr. 1 Vznik hvězdicového šestiúhelníku $\{6, 2\}$



Obr. 2 Vznik hvězdicového sedmiúhelníku $\{7, 3\}$

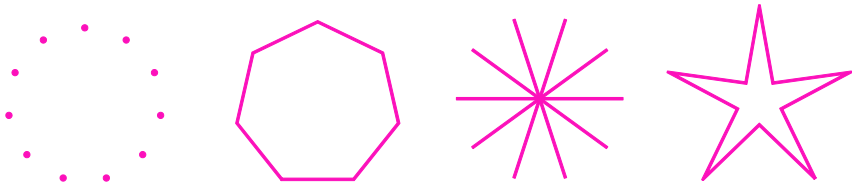
Hvězdicový n-úhelník vzniklý spojováním k-tých bodů budeme značit $\{n, k\}$. Tento tzv. *Schläfliho symbol* nese jméno švýcarského matematika Ludwiga Schläfliho (1814–1895), který se mimo jiné zabýval tzv. *pravidelnými polytopy*, tj. zobecněním pravidelných mnohoúhelníků a pravidelných mnohostěnů do vyšších dimenzí. Jeho práce [2] byla napsána roku 1852, ale publikována byla až roku 1901, tj. šest let po autorově smrti (více viz [3]).

Vznik hvězdicových mnohoúhelníků $\{6, 2\}$ a $\{7, 3\}$ je znázorněn na obr. 1 a 2. Lze na nich rovněž vidět, že kdybychom připustili možnost $\frac{n}{2} < k < n$,

bylo by $\{6,2\} = \{6,4\}$ a $\{7,3\} = \{7,4\}$. Je zřejmé, že by obecně platilo $\{n,k\} = \{n,n-k\}$, a proto není zapotřebí možnost $\frac{n}{2} < k < n$ v definici hvězdicového n-úhelníku uvažovat.

Někdy se pro dané n uvažuje rovněž možnost $k = 1$. V tomto případě spojujeme úsečkami všechny body v tom pořadí, v jakém jsou umístěny na (pomyslné) kružnici, a získáme *pravidelný n-úhelník*.

Existují přístupy, které při zavedení hvězdicového n-úhelníku připouštějí $k = 0$ a za hvězdicový mnohoúhelník $\{n,0\}$ považují pouze n bodů roviny, tj. vrcholy pravidelného n-úhelníku. Tento mezní případ se poté nazývá *diskrétní hvězdicový mnohoúhelník* (či zkráceně *diskrétní hvězda*) a hvězdicové mnohoúhelníky $\{n,k\}$, $k \geq 1$, se nazývají *nediskrétní*. V literatuře se setkáme i s možností, že je mezi hvězdicové mnohoúhelníky řazen (pro sudé n) případ $k = \frac{n}{2}$. Útvar $\left\{n, \frac{n}{2}\right\}$ je sjednocením $\frac{n}{2}$ „zdvojených“ úseček a nazývá se *hvězdička*.



Obr. 3 Útvary, které nejsou hvězdicovými n-úhelníky

V článku se budeme držet výše uvedené definice: ani diskrétní hvězdu, ani pravidelný n-úhelník, ani hvězdičku tedy nebudeme řadit mezi hvězdicové n-úhelníky. Symboly $\{n,0\}$, $\{n,1\}$, $\left\{n, \frac{n}{2}\right\}$ však k jejich označení používat budeme.[2)] Jestliže nebude výslovně specifikováno jinak, budeme n-úhelníkem $\{n,k\}$ rozumět jak pravidelný n-úhelník $\{n,1\}$, tak hvězdicový n-úhelník $\{n,k\}$, $2 \leq k < \frac{n}{2}$.

Raději upozorněme, že ne každý mnohoúhelník, který má tvar hvězdy s pravidelně rozmístěnými „cípy“, je hvězdicovým mnohoúhelníkem. Na obr. 3, na němž jsou zakresleny všechny tři výše uvedené případy útvarů, které za hvězdicové mnohoúhelníky považovat nebudeme, je navíc vpravo mnohoúhelník, který není hvězdicovým mnohoúhelníkem $\{5,2\}$, jak by se mohlo na první pohled zdát. Úsečky tvořící obvod tohoto mnohoúhelníku totiž neleží na spojnicích bodů umístěných na pomyslné kružnici.

[2)] Místo symbolu $\{n,1\}$ se v literatuře používá i zápis $\{n\}$.

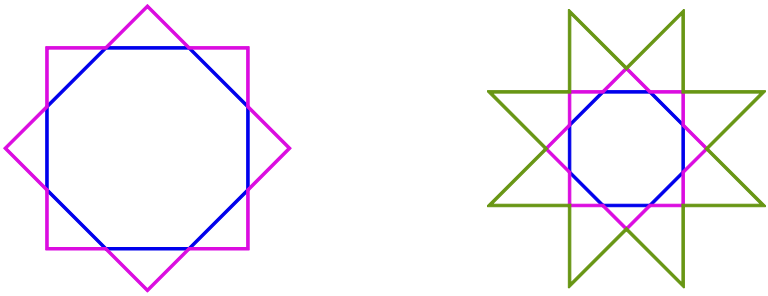
Jiný přístup k zavedení hvězdicových mnohoúhelníků

Než představíme některé vlastnosti hvězdicových mnohoúhelníků, uveďme ještě jejich jinou definici. Analogii níže uvedeného vymezení pojmu použil již ve 14. století Thomas Bradwardine (asi 1295–1349) ve svém textu [1]. Tento anglický teolog, matematik, fyzik a filozof byl prvním, který se hvězdicovými mnohoúhelníky zabýval systematicky. Před ním byla uvedená problematika předmětem zájmu jen sporadicky. Johannes Campanus z Novary (1220–1296) například krátce studoval hvězdicový pětiúhelník $\{5, 2\}$, tzv. *pentagram.*[3)] Později věnovali hvězdicovým mnohoúhelníkům pozornost Regiomontanus (vlastním jménem Johannes Müller, 1436–1476), Charles de Bovelles (též Carolus Bovillus, asi 1475–1567) či Johannes Kepler (1571–1630).

Definice 2

Hvězdicovým n-úhelníkem prvního řádu (řádu 1) rozumíme útvar, který vznikne protažením stran pravidelného n-úhelníku až do jejich průsečíků. Hvězdicový n-úhelník, který vznikne protažením stran hvězdicového n-úhelníku prvního řádu, nazveme *hvězdicový n-úhelník druhého řádu (řádu 2)*. Obecně *hvězdicový n-úhelník řádu $p + 1$* získáme výše uvedeným způsobem z hvězdicového n-úhelníku řádu p. Průsečíky protažených stran budeme nazývat *vrcholy* hvězdicového n-úhelníku.

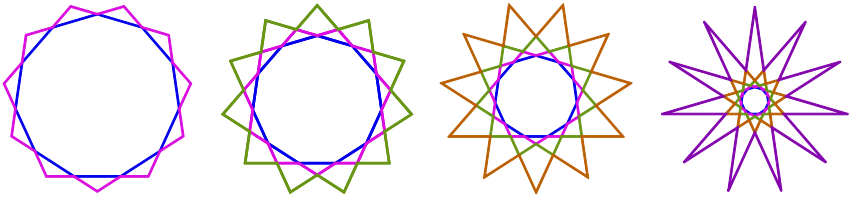
Vznik hvězdicových osmiúhelníků, resp. jedenáctiúhelníků, podle Bradwardinova přístupu je znázorněn na obr. 4, resp. 5. Z uvedených obrázků je rovněž zjevné, že pro dané n nelze tvořit hvězdicové mnohoúhelníky libovolných řádů. Otázku jejich existence budeme řešit níže.



Obr. 4 Hvězdicový osmiúhelník prvního a druhého řádu

[3)] Pentagram se jakožto symbol objevoval již ve starověkém Řecku.

Číslo n má zřejmě v obou definicích hvězdicového mnohoúhelníku stejný význam. Někoho možná napadne otázka, zda Bradwardinem zavedeným řád p hvězdicového n-úhelníku je roven číslu k v symbolu $\{n, k\}$. Odpověď je sice negativní, avšak vztah mezi nimi existuje, a to velmi triviální: $k = p + 1$. Zatímco k vyjadřuje *kolikátý bod* se má *spojit*, p sděluje, *kolik bodů* máme při spojování „*přeskočit*“. (Například na obr. 5 je na třetím místě zleva jedenáctiúhelník třetího řádu. Vznikl po třetím prodloužení stran „předchozích“ mnohoúhelníků. Současně však mohl být získán spojováním vrcholů, při němž vynecháváme tři body, tj. spojováním každého čtvrtého bodu.)



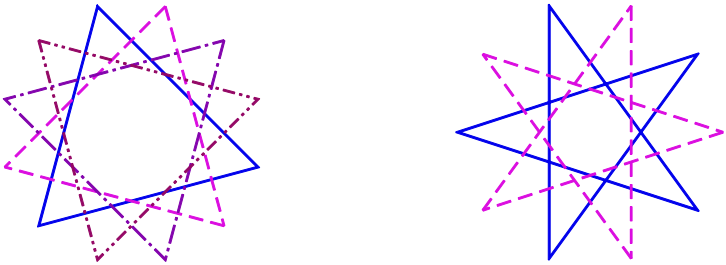
Obr. 5 Hvězdicový jedenáctiúhelník prvního až čtvrtého řádu

Jednoduché a složené hvězdicové n-úhelníky

Hvězdicové n-úhelníky můžeme rozdělit na *jednoduché* a *složené*. Jednoduché hvězdicové n-úhelníky vznikají v případě, že se nám podaří propojit – spojováním každého k-tého bodu – všechny body „jedním tahem“. Naopak při vzniku složených hvězdicových n-úhelníků se po určitém počtu kroků vrátíme do výchozího bodu, některé body zůstanou nespojeny a postup musíme zopakovat. Typickým případem složeného hvězdicového n-úhelníku je hvězdicový n-úhelník $\{n, k\}$, kde k dělí n. Takový složený hvězdicový n-úhelník $\{n, k\}$ je sjednocením k pravidelných $\frac{n}{k}$-úhelníků.

Na obr. 6 je nalevo hvězdicový dvanáctiúhelník $\{12, 4\}$, který je sjednocením čtyř rovnostranných trojúhelníků ($\frac{12}{4} = 3$). Složené však nejsou pouze hvězdicové mnohoúhelníky $\{n, k\}$, kde k dělí n. Na obr. 6 vpravo je hvězdicový desetiúhelník $\{10, 4\}$, který je složený ze dvou hvězdicových pětiúhelníků $\{5, 2\}$. Číslo 4 sice nedělí číslo 10, ale dělí číslo 20 (každý z pentagramů se utvoří po „dvojitém průchodu po kružnici“).

Pokusme se odvodit, z kolika a z jakých mnohoúhelníků je složen obecný hvězdicový mnohoúhelník $\{n, k\}$. Nejmenší společný násobek čísel n a k označme s a jejich největší společný dělitel d. Přesun z bodu na sousední bod ležící na (pomyslné) kružnici nazývejme *krok* (ke spojení bodu s k-tým bodem v pořadí tedy provedeme k kroků).



Obr. 6 Složené hvězdicové mnohoúhelníky $\{12, 4\}$, $\{10, 4\}$

Do výchozího bodu se při spojování každého k-tého bodu navrátíme právě po s krocích. Je dobře známo, že $sd = nk$. Složené hvězdicové mnohoúhelníky vznikají právě tehdy, když $s < nk$, tj. když $d > 1$. Hvězdicový mnohoúhelník je tedy složený (jednoduchý) právě tehdy, když jsou čísla n a k soudělná (nesoudělná).

Při spojování každého k-tého bodu provedeme s kroků právě tehdy, když spojíme $\frac{s}{k}$ bodů, tj. hvězdicový mnohoúhelník $\{n, k\}$ je složen z mnohoúhelníků (buď z pravidelných n-úhelníků, jestliže k dělí n, nebo z hvězdicových n-úhelníků, jestliže k nedělí n) majících $\frac{s}{k}$ vrcholů. Protože $s = \frac{nk}{d}$, je přitom

$$\frac{s}{k} = \frac{n}{d}.$$

Jelikož na vytvoření každého z těchto $\frac{n}{d}$-úhelníků je potřeba $\frac{n}{d}$ bodů z původních n bodů, je těchto mnohoúhelníků d. Protože vrcholem $\frac{n}{d}$-úhelníku je každý d-tý bod z původních n bodů, je každý k-tý bod na kružnici s n body každým $\frac{k}{d}$-tým bodem na kružnici s $\frac{n}{d}$ body.

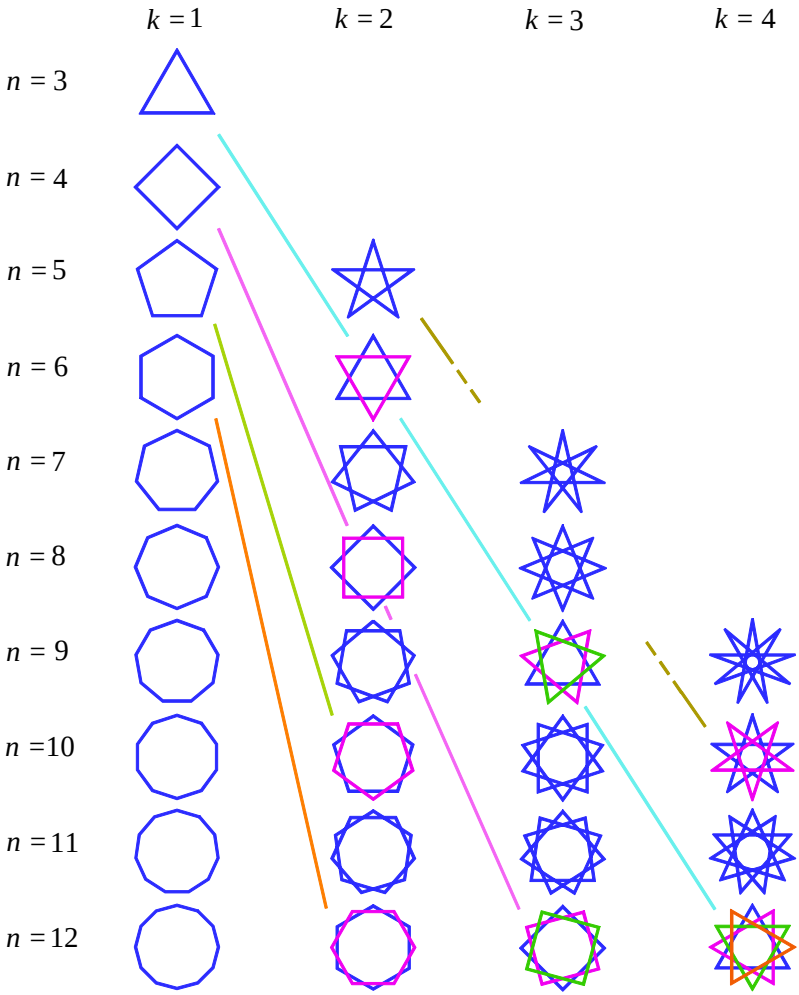
Celkově jsme tedy dokázali následující tvrzení:

Věta

Nechť $\{n, k\}$ je hvězdicový n-úhelník a nechť d je největší společný dělitel čísel n a k. Hvězdicový n-úhelník $\{n, k\}$ je složený, právě když n a k jsou čísla soudělná. V opačném případě je jednoduchý. Hvězdicový n-úhelník $\{n, k\}$ je složen z d mnohoúhelníků $\left\{\frac{n}{d}, \frac{k}{d}\right\}$.

Například hvězdicový dvacetičtyřúhelník $\{24, 9\}$ je složen ze tří osmiúhelníků $\{8, 3\}$, hvězdicový čtyřicetiúhelník $\{40, 12\}$ je složen ze čtyř desetiúhelníků $\{10, 3\}$. Hvězdicový n-úhelník $\{n, k\}$, který je jednoduchý (tedy $d = 1$), je „složen“ z jednoho n-úhelníku $\{n, k\}$. Z věty též plyne, že hvězdicový n-úhelník $\{n, k\}$, kde n je prvočíslo, je vždy jednoduchý.

Na obr. 7 je přehled pravidelných a hvězdicových n-úhelníků $\{n, k\}$ pro $n = 3, 4, \ldots, 12$ a $k = 1, 2, 3, 4$.



Obr. 7 Přehled mnohoúhelníků $\{n, k\}$

Složené hvězdicové mnohoúhelníky $\{6, 2\}$, $\{9, 3\}$, $\{12, 4\}$ jsou složené z rovnostranných trojúhelníků $\{3, 1\}$, hvězdicové mnohoúhelníky $\{8, 2\}$,

$\{12, 3\}$ se skládají ze čtverců $\{4, 1\}$, hvězdicový mnohoúhelník $\{10, 2\}$ je sjednocením pravidelných pětiúhelníků $\{5, 1\}$, hvězdicový mnohoúhelník $\{12, 2\}$ je vytvořen z pravidelných šestiúhelníků $\{6, 1\}$ a hvězdicový mnohoúhelník $\{10, 4\}$ je sjednocením pentagramů $\{5, 2\}$. Dále je na tomto obrázku vidět, že pro prvočíslo n jsou hvězdicové mnohoúhelníky $\{n, k\}$ vždy jednoduché.

Mnohý čtenář již zřejmě zpozoroval souvislost mezi mnohoúhelníky $\{n, k\}$ a zlomky n/k. Hvězdicový mnohoúhelník $\{n, k\}$ je jednoduchý právě tehdy, když je zlomek n/k v základním tvaru. Hvězdicové mnohoúhelníky $\{n_1, k_1\}$ a $\{n_2, k_2\}$ jsou složeny ze stejných pravidelných nebo z jednoduchých hvězdicových mnohoúhelníků $\{n_0, k_0\}$, $k_0 \geq 1$, jestliže základní tvar zlomků n_1/k_1 a n_2/k_2 je n_0/k_0. Pokud tedy platí

$$\frac{n_1}{k_1} = \frac{a \cdot n_0}{a \cdot k_0},$$

resp.

$$\frac{n_2}{k_2} = \frac{b \cdot n_0}{b \cdot k_0},$$

kde a, b jsou přirozená čísla, je mnohoúhelník $\{n_1, k_1\}$, resp. $\{n_2, k_2\}$, složen z a, resp. z b, mnohoúhelníků $\{n_0, k_0\}$. Například

$$\frac{30}{12} = \frac{15}{6} = \frac{10}{4} = \frac{5}{2},$$

přičemž

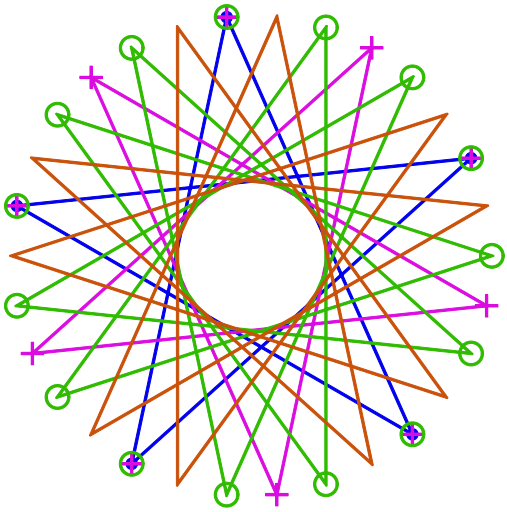
$$\frac{30}{12} = \frac{6 \cdot 5}{6 \cdot 2}, \quad \frac{15}{6} = \frac{3 \cdot 5}{3 \cdot 2}, \quad \frac{10}{4} = \frac{2 \cdot 5}{2 \cdot 2}.$$

Hvězdicový mnohoúhelník $\{30, 12\}$, resp. $\{15, 6\}$, resp. $\{10, 4\}$, je tedy sjednocením 6, resp. 3, resp. 2, jednoduchých hvězdicových mnohoúhelníků $\{5, 2\}$, tj. pentagramů. Všechny uvedené hvězdicové mnohoúhelníky lze nalézt na obr. 8. U mnohoúhelníku $\{5, 2\}$ přitom uvažujeme pouze vrcholy (a jejich spojnice), které jsou zvýrazněny vyplněným kroužkem, u mnohoúhelníku $\{10, 4\}$ jen vrcholy s křížkem, u mnohoúhelníku $\{15, 6\}$ vrcholy opatřené kružnicí, ale u mnohoúhelníku $\{30, 12\}$ vrcholy všechny.

Existence hvězdicových mnohoúhelníků

Všimněme si, že některá místa jsou na obr. 7 ponechána prázdná, neboť hvězdicové n-úhelníky řádu $k \geq \frac{n}{2}$ neuvažujeme. Z definice 1 vyplývá, že pro $n \geq 5$ existuje (až na podobnost) právě $\lceil \frac{n}{2} \rceil - 2$ hvězdicových n-úhelníků $\{n,\, k\}$ (a to pro $k = 2, 3, \ldots, \lceil \frac{n}{2} \rceil - 1$), kde $\lceil \frac{n}{2} \rceil$ značí horní celou část čísla $\frac{n}{2}$.

Pokud postupujeme podle Bradwardinovy definice 2, snadno zjistíme, že nejmenším hvězdicovým n-úhelníkem prvního řádu je pentagram $\{5, 2\}$ a druhého řádu sedmiúhelník $\{7, 3\}$ (tedy i při Bradwardinově přístupu stačí uvažovat $n \geq 5$). Zjištění maximálního řádu $p = k - 1$ je již pro relativně malé p časově náročnější. Průsečíky protahovaných stran přestanou vznikat pro $p = \lceil \frac{n}{2} \rceil - 2$.



Obr. 8 Složený hvězdicový mnohoúhelník $\{30, 12\}$

V článku jsme se seznámili především s různými přístupy k definici hvězdicových mnohoúhelníků a představili souvislost složených hvězdicových mnohoúhelníků s konvexními pravidelnými n-úhelníky, resp. s jednoduchými hvězdicovými n-úhelníky. V následujícím čísle časopisu se budeme zabývat metrickými vlastnostmi těchto na pohled půvabných rovinných útvarů.

Literatura

[1] *Bradwardine, T.*: Geometria speculativa, Paris, 1495; anglický překlad: Molland, A. G.: Geometria Speculativa, Franz Steiner Verlag, Wiesbaden, Stuttgart, 1989.

[2] *Schläfli, L.*: Theorie des vielfachen Kontinuität, Aufträge der Denkschriften-Kommission der Schweizer naturforschender Gesellschaft, Zurcher & Furrer, 1901.

[3] *Stillwell, J.*: Příběh stodvacetistěnu v $\mathbb{R}^4$. Pokroky matematiky, fyziky a astronomie, roč. 46 (2001), s. 265–280.

Zajímavé matematické úlohy

Uveřejňujeme další část pravidelné rubriky Zajímavé matematické úlohy a uvádíme zadání další dvojice úloh. Řešení nových úloh 241 a 242 můžete zaslat nejpozději do 20. 3. 2019 na adresu: Redakce časopisu MFI, 17. listopadu 12, 771 46 Olomouc nebo také elektronickou cestou (pouze však v TEXovských verzích, příp. v MS Wordu) na emailovou adresu: *mfi@upol.cz*.

Úloha 241

Dokažte, že pro libovolná reálná čísla x, y, z platí nerovnost

$$x^2 + y^2 + z^2 + 1 \geq \frac{2}{3}\,(xy + yz + zx + x + y + z).$$

Kdy nastane rovnost?

Jaroslav Švrček

Úloha 242

Označme O střed kružnice opsané trojúhelníku ABC a V průsečík jeho výšek (ortocentrum). Předpokládejme, že kružnice $k(O, |OV|)$ protíná jeho výšky (jako přímky) z vrcholů A, B, C kromě bodu V po řadě v bodech $A' \neq V$, $B' \neq V$, $C' \neq V$. Dokažte, že trojúhelník $A'B'C'$ je podobný trojúhelníku ABC.

Šárka Gergelitsová

Dále uvádíme řešení úloh 237 a 238, jejichž zadání najdete ve čtvrtém čísle minulého (26.) ročníku našeho časopisu.

Úloha 237

Je dán pravoúhlý čtyřstěn $ABCD$ s pravými úhly při vrcholu D. Na jeho hranách AD, BD, CD uvažujme po řadě body X, Y, Z, pro něž platí

$$\frac{|AX|}{|XD|}+\frac{|BY|}{|YD|}+\frac{|CZ|}{|ZD|}=1.$$

Dokažte, že těžiště tohoto čtyřstěnu leží v rovině XYZ.

Řešení. Daný čtyřstěn umístíme do kartézské soustavy souřadnic $Oxyz$ tak, že bod D leží v počátku O a body A, B, C leží po řadě na kladných poloosách x, y, z. Nechť v této souřadnicové soustavě mají body následující souřadnice:

$$A[a,0,0],\ B[0,b,0],\ C[0,0,c],\ D[0,0,0],\ X[\xi,0,0],\ Y[0,\eta,0],\ Z[0,0,\zeta].$$

Protože body A, B, C leží na kladných poloosách, body X, Y, Z na příslušných hranách a podle zadání jsou vzdálenosti $|XD|$, $|YD|$ a $|ZD|$ nenulové, platí

$$0<\xi\le a,\quad 0<\eta\le b,\quad 0<\zeta\le c.$$

Podle zadání pak platí

$$1=\frac{|AX|}{|XD|}+\frac{|BY|}{|YD|}+\frac{|CZ|}{|ZD|}=\frac{a-\xi}{\xi}+\frac{b-\eta}{\eta}+\frac{c-\zeta}{\zeta}=\frac{a}{\xi}+\frac{b}{\eta}+\frac{c}{\zeta}-3.$$

Odtud plyne

$$\frac{a}{\xi}+\frac{b}{\eta}+\frac{c}{\zeta}=4. \tag{1}$$

Snadno ověříme, že body X, Y, Z leží v rovině

$$\frac{x}{\xi}+\frac{y}{\eta}+\frac{z}{\zeta}=1$$

(tzv. úsekový tvar roviny XYZ). Ukážeme, že v této rovině také leží těžiště T čtyřstěnu se souřadnicemi $T\left[\frac{1}{4}a,\frac{1}{4}b,\frac{1}{4}c\right]$. Užitím (1) platí

$$\frac{\frac{a}{4}}{\xi}+\frac{\frac{b}{4}}{\eta}+\frac{\frac{c}{4}}{\zeta}=\frac{1}{4}\left(\frac{a}{\xi}+\frac{b}{\eta}+\frac{c}{\zeta}\right)=\frac{1}{4}\cdot 4=1.$$

Poznámka. Jak si povšiml např. *Anton Hnáth*, pro řešení není potřeba podmínka kolmosti hran u vrcholu D. Tvrzení platí pro libovolný čtyřstěn, stačí uvažovat souřadnicovou soustavu (ne nutně kartézskou) s počátkem D tak, aby body A, B, C ležely na příslušných poloosách.

Správná řešení zaslali *Karol Gajdoš* z Trnavy, *Anton Hnáth* z Moravan, *Jozef Mészáros* z Jelky, *Martin Raszyk* z ETH Zürich, *Matěj Doležálek* z G v Humpolci, *Vít Jelínek*, *Josef Minařík* a *Štěpán Šmíd*, všichni z G v Brně, tř. Kpt. Jaroše, *Danil Koževnikov* z GJK v Praze 6, Parléřova, *Martin Raška* a *Jiří Škrobánek*, oba z WG v Ostravě-Porubě.

Úloha 238

Určete všechna celá čísla n, pro která je číslo

$$4n^2 - 9n + 16$$

druhou mocninou přirozeného čísla.

Pavel Calábek

Řešení. Označme m přirozené číslo, pro které platí

$$4n^2 - 9n + 16 = m^2.$$

Tuto rovnici upravíme do tvaru

$$\left(2n - m - \frac{9}{4}\right)\left(2n + m - \frac{9}{4}\right) + 16 = \frac{81}{16},$$

tedy

$$(8n - 4m - 9)(8n + 4m - 9) = -175.$$

Protože m je přirozené číslo, jsou obě čísla $8n - 4m - 9 < 8n + 4m - 9$ celá, jejich součin je záporné číslo, tedy platí

$$8n - 4m - 9 < 0 < 8n + 4m - 9.$$

Zbytek při dělení čtyřmi je u obou čísel roven 3, hledáme tak všechny rozklady čísla

$$-175 = -5^2 \cdot 7$$

na součin dvou celých čísel, která při dělení čtyřmi dávají zbytek 3. Vyhovují pouze rozklady uvedené v následující tabulce, ve které současně

dopočítáme hodnoty n a m řešením příslušné soustavy rovnic.

$8n-4m-9$	-25	-5	-1
$8n+4m-9$	7	35	175
n	0	3	12
m	4	5	22

Z tabulky jsou patrné všechny hodnoty celého čísla n, které vyhovují zadání. Jsou to čísla $n \in \{0, 3, 12\}$.

Správná řešení zaslali *Karol Gajdoš* z Trnavy, *Anton Hnáth* z Moravan, *František Jáchim* z Volyně, *Jozef Mészáros* z Jelky, *Martin Raszyk* z ETH Zürich, *Matěj Doležálek* z G v Humpolci, *Denisa Chytilová* a *Jana Pallová*, obě z GJŠ v Přerově, *Vít Jelínek*, *Josef Minařík* a *Štěpán Šmíd*, všichni z G v Brně, tř. Kpt. Jaroše, *Danil Koževnikov* z GJK v Praze 6, Parléřova, *Vojtěch Lanz* a *Vojtěch Lengál*, oba z GChD v Praze 5, Zborovská, *Jiří Náběl*ek a *Bára Tížková*, oba z GMK v Bílovci. *Vít Pískovský* z GOH v Ostravě-Porubě, *Martin Raška* a *Jiří Škrobánek*, oba z WG v Ostravě-Porubě a *Václav Steinhauser* z G v Dačicích.

Neúplné řešení zaslal *Tomáš Perutka* z G v Brně, tř. Kpt. Jaroše.

Pavel Calábek

FYZIKA

Netradiční experimenty s vázanými oscilátory

OLDŘICH LEPIL – ČENĚK KODEJŠKA

Přírodovědecká fakulta UP, Olomouc

Úvod

Poznatky o dějích ve vázaných oscilátorech mají klíčový význam pro výklad zásadního rozdílu mezi kmitáním izolovaného oscilátoru a dějů v lineární soustavě oscilátorů spojených vazbou, kterou se šíří vlnění. Pro izolovaný oscilátor je charakteristická jedna vlastní (rezonanční) frekvence určená parametry oscilátoru (např. hmotností a tuhostí u mechanického oscilátoru, popř. indukčností a kapacitou u elektromagnetického oscilátoru). Soustavou vázaných oscilátorů se může šířit vlnění o různé frekvenci a dochází k přenosu energie. Tyto děje jsou však podstatně složitější a o to významnější je jejich prezentace experimentem. Nové možnosti pro experimentální studium dějů ve vázaných oscilátorech a jejich názornou prezentaci podporovanou počítačovými programy ukážeme v další části příspěvku.

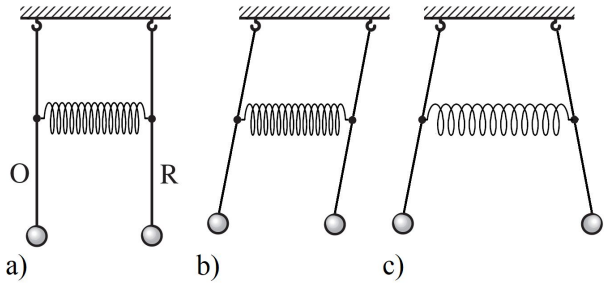
Mechanické vázané oscilátory

Většina učebnic fyziky se omezuje jen na výklad mechanických vázaných oscilátorů v podobě *spřažených kyvadel* (obr. 1a), která lze v praxi snadno realizovat. Experimentem se spřaženými kyvadly ukážeme, že se energie kmitání prvního kyvadla – *oscilátoru* postupně přenáší k druhému oscilátoru – *rezonátoru*. Tento děj se periodicky opakuje a v soustavě spřažených kyvadel vznikají rázy. Vznik rázů interpretujeme tak, že jde o superpozici

dvou módů kmitání, které se liší periodou. *Symetrický mód* odpovídá případu, kdy mají obě kyvadla v počátečním okamžiku stejnou počáteční fázi (obr. 1b). Při ní se vazba neprojeví a obě kyvadla kmitají se stejnou úhlovou frekvencí $\omega_1 = \omega_0$, jaká odpovídá vlastní frekvenci oscilátoru bez spřažení. Při antisymetrickém módu (obr. 1c) je počáteční fáze kyvadel opačná. Z názoru je zřejmé, že vlivem působení vazby budou kyvadla kmitat s kratší periodou, tedy s větší úhlovou frekvenci $\omega_2 > \omega_0$. Perioda kmitání závisí na velikosti vazebné síly, která je úměrná rozdílu výchylek obou kyvadel. Z teorie vyplývá (viz např. [1]), že symetrickému a antisymetrickému módu kmitání vázaných oscilátorů odpovídají úhlové frekvence

$$\omega_1 = \omega_0, \quad \omega_2 = \sqrt{\omega_0^2 + 2c},$$

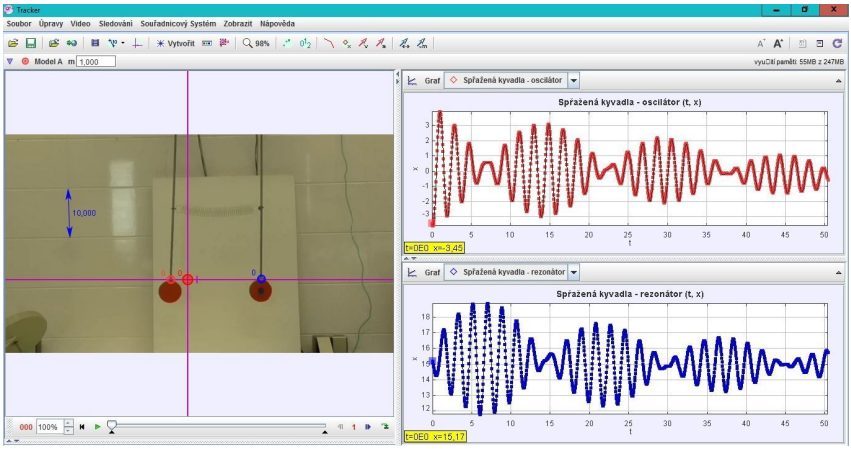
kde c je činitel vazby, který je v případě kyvadel spřažených pružinou úměrný její tuhosti. Čím větší je tedy činitel vazby, tím rychleji dochází k výměně energie mezi oscilátory a frekvence rázů je větší.



Obr. 1

• **Videoanalýza kmitání spřažených kyvadel**

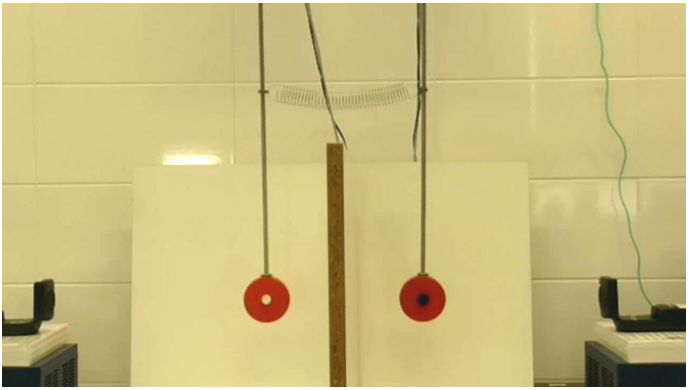
Časový diagram kmitání spřažených kyvadel můžeme poměrně jednoduše získat metodou videoanalýzy, která je dostupná i pro samostatnou práci žáků. Pro videoanalýzu mechanických pohybů existuje více programů, z nichž se jako nejvhodnější jeví program Tracker [I]. Analyzován byl obrazový záznam kmitání spřažených kyvadel fy PHYWE, určených pro klasické laboratorní cvičení. Obrazový záznam pořízený digitální kamerou má dobu trvání přibližně 1 min (1 260 snímků). Při frekvenci snímání 25 obr./s jde o posloupnost snímků s časovým krokem 0,04 s. Výsledek videoanalýzy je patrný z obr. 2.



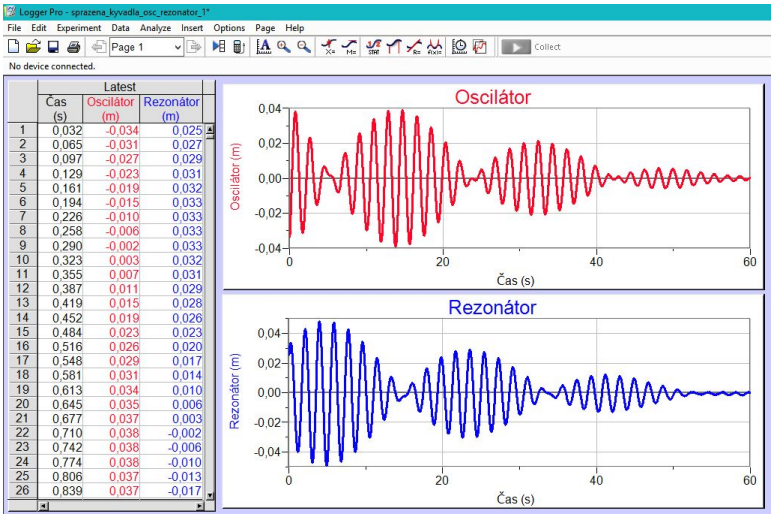
Obr. 2

• **Záznam kmitání spřažených kyvadel sonarem Vernier**

Další možností počítačem podporovaného experimentu se spřaženými kyvadly je využití měřicího systému Vernier, jehož součástí jsou senzory polohy a pohybu Motion Detector 2. Uspořádání experimentu se dvěma senzory je patrné z obr. 3. Aby nedocházelo k vzájemnému rušení současného záznamu kmitů oscilátoru i rezonátoru, byla mezi kyvadla umístěna přepážka. Získaná data byla analyzována programem Logger Pro [II] (obr. 4).



Obr. 3



Obr. 4

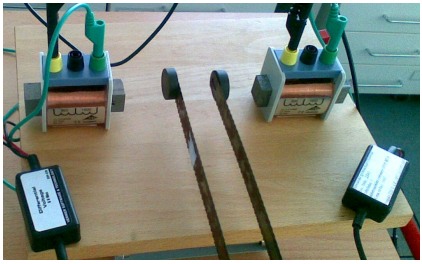
• **Záznam kmitání pružných pásků spřažených magneticky**

V učivu o kmitání je dána přednost pružinovému oscilátoru před kyvadlem. Demonstrace vázaných pružinových oscilátorů je obtížná a ve výuce se omezujeme jen na počítačové simulace. Snadno však ukážeme pružné kmity soustavy dvou ocelových pásků délky cca 30 cm, umístěných ve vzájemné vzdálenosti asi 3 cm. Vazbu zajišťují dva feritové magnety přichycené ke koncům pásků tak, že se navzájem odpuzují (obr. 5). Hmotnost magnetů ovlivňuje také frekvenci kmitání pásků. V blízkosti magnetů jsou umístěny cívky z rozkladného transformátoru (600 závitů, rovné jádro). Při pohybu magnetů se v cívkách indukuje napětí, které je sice funkcí rychlosti pohybu magnetů, ale časový diagram poskytuje informaci o kmitání obou oscilátorů. Potřebná data byla získána připojením senzorů napětí (DVP--BTA) a pro jejich zpracování byl použit program Logger Pro (obr. 6).

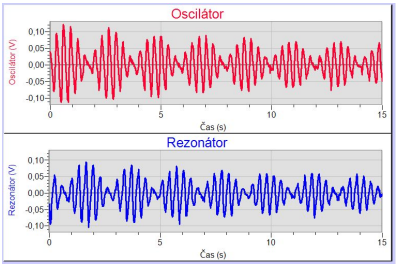
Elektromagnetické vázané oscilátory

K experimentu byly použity dva oscilační obvody LC tvořené cívkami s 600 závity s rovným jádrem a kondenzátory o kapacitě 1 μF. Cívky jsou umístěny na společné ose tak, že mezi jádry cívek je měnitelná vzduchová mezera o šířce přibližně 4 cm (obr. 7). Pro buzení elektrických kmitů v oscilátoru je použit poměrně originální postup, který se liší od způsobu,

jakým je rozkmitání oscilátoru popisováno ve většině učebnic fyziky (nabití kondenzátoru a jeho vybití připojením k cívce). Použili jsme obrácený postup, kdy cívkou protéká proud a po jeho přerušení vypínačem se v cívce indukuje dostatečně velké napětí. Tímto napětím se nabije kondenzátor a oscilátor se rozkmitá. K tomu stačí i malé připojené napětí např. z ploché baterie 4,5 V (podrobněji viz [2]).

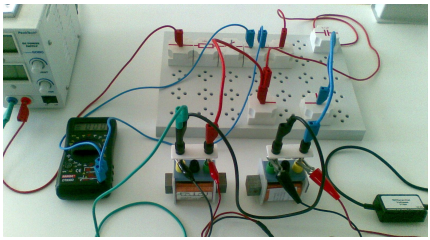


Obr. 5

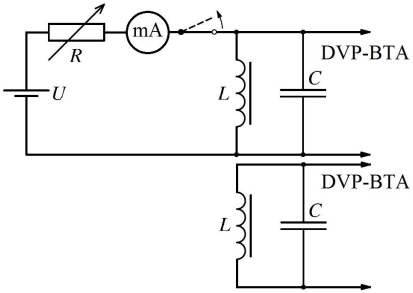


Obr. 6

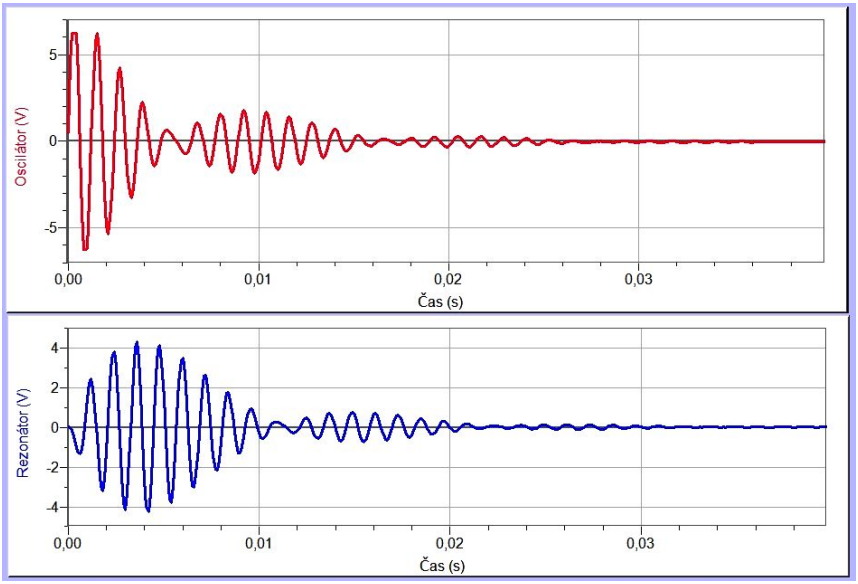
Schéma obvodu pro demonstraci kmitání vázaných oscilátorů s indukční vazbou je na obr. 8. Získaná data byla opět zpracována programem Logger Pro (obr. 9). Experimenty byly provedeny jak s indukčně, tak s kapacitně vázanými obvody (obr. 10; vazební kondenzátor C_v měl rovněž kapacitu 1 μF). Základním problémem této demonstrace je relativně velký odpor použitých cívek a tomu odpovídající tlumení kmitů. Činitel tlumení oscilačního obvodu $\delta = R/2L$, takže by bylo možné zmenšit ho zvětšením indukčnosti cívky. Ta však závisí na počtu závitů vinutí cívky, ale větší počet závitů má za následek zvětšení odporu vinutí cívky. Je tedy třeba volit kompromis mezi hodnotami L a R, popř. provést výběr cívky, která při experimentu vykazuje nejlepší výsledky.



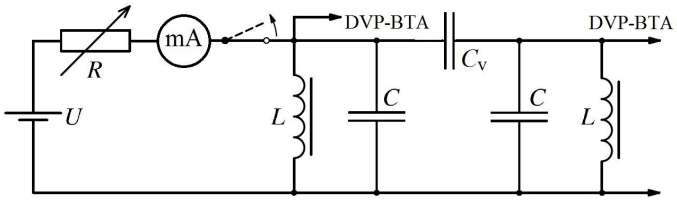
Obr. 7



Obr. 8



Obr. 9



Obr. 10

Modely kmitání vázaných oscilátorů

Současné počítačové technologie umožňují také vytvářet poměrně snadno interaktivní modely dějů ve vázaných oscilátorech, které jsme v předcházející části příspěvku studovali reálným experimentem. Východiskem těchto modelů jsou diferenciální rovnice popisující odpovídající děje. Jejich analytické řešení je pro středoškolskou výuku ovšem nedostupné. Dostatečně názorné řešení tohoto problému však představuje metoda dynamického modelování, založená na numerickém řešení diferenciálních rovnic [3].

Při modelování se uplatní také analogie mezi mechanickým a elektromagnetickým kmitáním. Jako příklady vázaných oscilátorů uvedeme pružinové oscilátory spřažené výchylkou a elektromagnetické oscilační obvody vázané indukční vazbou. Děje v těchto vázaných oscilátorech popisují následující rovnice:

Spřažené pružinové oscilátory	Oscilační obvody s indukční vazbou
$m\frac{\mathrm{d}^2y_1}{\mathrm{d}t^2} + b\frac{\mathrm{d}y_1}{\mathrm{d}t} + ky_1 + c(y_1 - y_2) = 0$	$L\frac{\mathrm{d}^2q_1}{\mathrm{d}t^2} + R\frac{\mathrm{d}q_1}{\mathrm{d}t} + \frac{q_1}{C} + M\frac{\mathrm{d}^2q_2}{\mathrm{d}t^2} = 0$
$m\frac{\mathrm{d}^2y_2}{\mathrm{d}t^2} + b\frac{\mathrm{d}y_2}{\mathrm{d}t} + ky_2 - c(y_1 - y_2) = 0$	$L\frac{\mathrm{d}^2q_2}{\mathrm{d}t^2} + R\frac{\mathrm{d}q_2}{\mathrm{d}t} + \frac{q_2}{C} + M\frac{\mathrm{d}^2q_1}{\mathrm{d}t^2} = 0$

Pro jednoduchost uvažujeme vázané oscilátory se stejnými parametry m (hmotnost), k (tuhost pružiny), popř. L (indukčnost cívky) a C (kapacita kondenzátoru). Tlumení oscilátorů určuje součinitel odporu b ovlivňující rychlost kmitání oscilátoru, popř. odpor R oscilačního obvodu, na němž závisí velikost proudu v obvodu. Veličina c je činitel vazby u mechanických oscilátorů a M je vzájemná indukčnost indukčně vázaných oscilátorů.

Dynamický model kmitání vázaných mechanických oscilátorů popisují rovnice (h je časový krok):

$$F_1 = m\frac{\mathrm{d}^2y_1}{\mathrm{d}t^2} = -ky_1 - bv_1 + c(y_1 - y_2)$$

$$F_2 = m\frac{\mathrm{d}^2y_2}{\mathrm{d}t^2} = -ky_2 - bv_2 - c(y_1 - y_2)$$

$$a_1 = \frac{F_1}{m}, \quad a_2 = \frac{F_2}{m}$$

$$v_{1,i+1} = v_{1,i} + a_1 \cdot h, \quad v_{2,i+1} = v_{2,i} + a_2 \cdot h$$

$$y_{1,i+1} = y_{1,i} + v_{1,i+1} \cdot h, \quad y_{2,i+1} = y_{2,i} + v_2 \cdot h$$

$$t_{i+1} = t_i + h$$

Poněkud složitější je model elektromagnetických vázaných oscilátorů. Poněvadž platí

$$\frac{\mathrm{d}^2q}{\mathrm{d}t^2} = \frac{\mathrm{d}i}{\mathrm{d}t}, \quad \frac{\mathrm{d}q}{\mathrm{d}t} = i, \quad R\frac{\mathrm{d}q}{\mathrm{d}t} = Ri = u_R, \quad \frac{q}{C} = u_c,$$

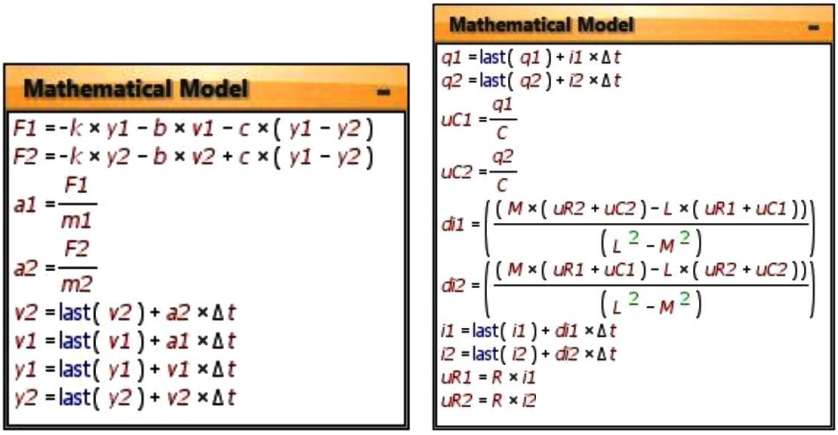
najdeme úpravou rovnic pro vázané elektromagnetické oscilátory přírůstky proudu di za časový krok dt:

$$\mathrm{d}i_1 = \frac{M(u_{R2} + u_{C2}) - L(u_{R1} + u_{C1})}{L^2 - M^2}$$

$$\mathrm{d}i_2 = \frac{M(u_{R1} + u_{C1}) - L(u_{R2} + u_{C2})}{L^2 - M^2}$$

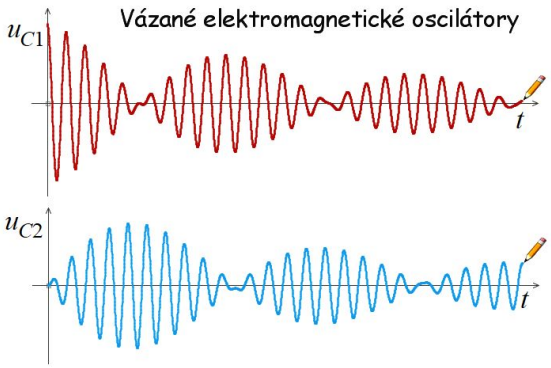
V modelu pak obdobně jako u mechanického oscilátoru určujeme hodnoty proudu v posloupnosti časových kroků. Časový diagram napětí u_{C1} a u_{C2} zobrazuje rázy kmitání obou vázaných oscilátorů.

Počítačový model popsaného děje lze vytvořit různými prostředky. Pro jednoduché modelování, které nevyžaduje znalost programovacího jazyka, jsme zvolili program Modellus 4.01 [III]. Matematické modely pro mechanické i elektromagnetické vázané oscilátory vytvořené tímto programem jsou na obr. 11. Podrobnější teoretický popis modelů viz [3].



Obr. 11

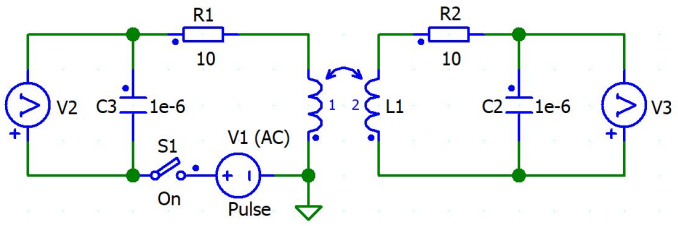
Pro ilustraci je na obr. 12 uveden výsledný časový diagram kmitání oscilátoru LC s parametry $L = 1$ H, $C = 10$ μF, $R = 5\ \Omega$, $M = 0{,}1$ H (menu *Parameters*). Časový krok $h = 0{,}2$ ms (v programu Modellus je časový krok označen Δt), $t_{\max} = 0{,}5$ s. Tyto hodnoty se nastavují v menu *Independent Variable*. Počáteční podmínky (*Initial Coditions*) jsou $q_1 = 10^{-4}$ C a ostatní veličiny (q_2, i_1, i_2) mají nulovou počáteční hodnotu.



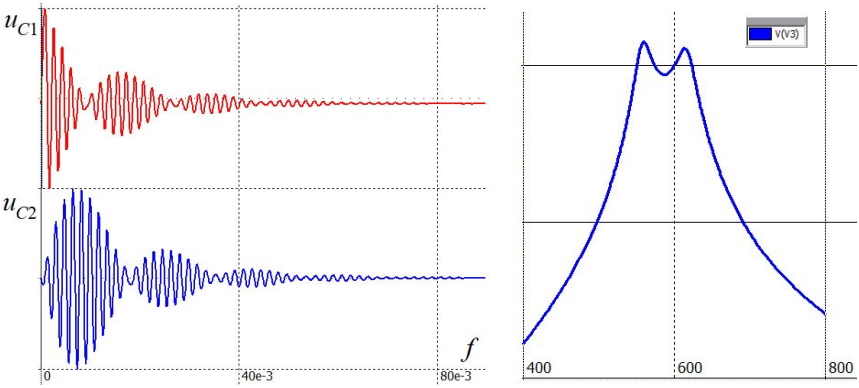
Obr. 12

Popsané modely jsou jednoduché a umožňují zkoumání dějů ve vázaných oscilátorech interaktivními změnami všech parametrů, popř. počátečních podmínek, což obvykle není možné u reálných experimentů. Je však obtížné vytvářet tímto jednoduchým postupem složitější systémy oscilátorů, jejichž popis diferenciálními rovnicemi ani není znám, nebo jejich řešení je příliš složité. Určitým problémem experimentů s vázanými oscilátory je také experimentální měření jejich frekvenční charakteristiky – *rezonanční křivky*. Prakticky nemožné je měření rezonanční křivky jednoduchých mechanických oscilátorů. U elektromagnetických oscilátorů můžeme rezonanční křivku získat klasickým měřením amplitudy kmitů při postupně rostoucí frekvenci (viz [1]). U vázaných oscilátorů toto měření ukáže, že soustava dvou vázaných oscilátorů na rozdíl od izolovaného oscilátoru má rezonanční křivku se dvěma extrémy. Tzn. vázané oscilátory mají dvě rezonanční frekvence, odpovídající symetrickému a antisymetickému módu kmitání.

Pro studium těchto složitějších systémů vázaných elektromagnetických oscilátorů a jejich frekvenčních charakteristik můžeme využít např. simulační program NL5 Circuit Simulator [IV]. V něm snadno vytvoříme schéma obvodu kreslením přímo na ploše monitoru a ihned můžeme zobrazit jak časový diagram kmitání v daném obvodu, tak jeho frekvenční charakteristiku. Tento program byl použit k simulaci všech zapojení s vázanými elektromagnetickými oscilátory. Jako ukázka je na obr. 13 je schéma soustavy indukčně vázaných oscilátorů a na obr. 14 jsou odpovídající časové diagramy kmitání oscilátorů a frekvenční charakteristika se dvěma charakteristickými rezonančními frekvencemi.

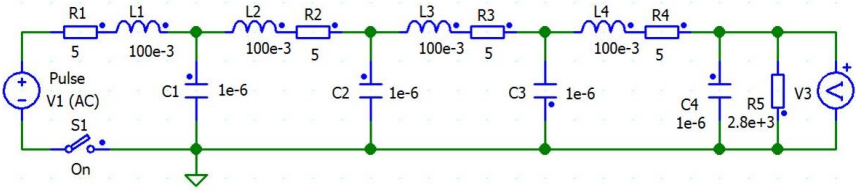


Obr. 13

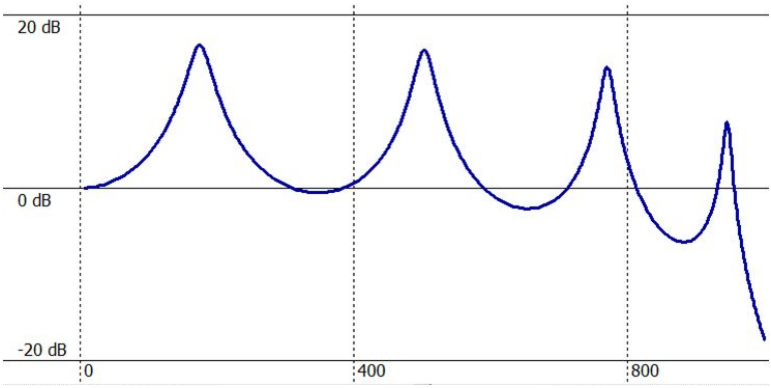


Obr. 14

Tímto programem byl také vytvořen řetězec čtyř kapacitně vázaných oscilátorů (obr. 15), jehož frekvenční charakteristika vykazuje odpovídající nárůst rezonančních maxim (obr. 16). To umožňuje při výuce dospět extrapolací tohoto případu na dlouhou řadu vázaných oscilátorů, čili k představě dvouvodičového vedení, kterým se může šířit postupná elektromagnetická vlna.



Obr. 15



Obr. 16

Literatura

[1] *Lepil, O.*: Příspěvek k metodice výkladu rezonančních jevů ve vázaných oscilátorech. In: Acta UP, Fac. Rer. Nat. Tom 15, 1964. Dostupné na: http://dml.cz/dmlcz/119814

[2] *Lepil, O., Látal, F.*: Experiment v učivu o kmitání elektromagnetického oscilátoru. MFI, roč. 22 (2013), č. 5, s. 344. Dostupné na: http://mfi.upol.cz/files/2205/mfi_2205_344_354.pdf

[3] *Lepil, O., Richterek, L.*: Dynamické modelování, Repronis, Ostrava, 2007. Dostupné na: http://ufm.sgo.cz/ke_stazeni.php

Software

[I] Tracker 4.97: <http://www.cabrillo.edu/~dbrown/tracker/>

[II] Logger Pro 3.14.1: <https://www.vernier.com/>

[III] Modellus 4.01: <http://modellus.fct.unl.pt/>

[IV] NL 5 Circuit Simulator: <http://nl5.sidelinesoft.com/>

Srovnání charakteristik tónového generátoru a zvukové karty PC

ČENĚK KODEJŠKA – LENKA MYSLIVCOVÁ – FRANTIŠEK HOŠEK – MATYÁŠ ROUHA

Gymnázium, Komenského 77, Nový Bydžov

Úvod

Cílem naší práce bylo prozkoumat různé vlastnosti a charakteristiky tónového generátoru a zvukové karty PC jako zdrojů střídavého napětí.

V experimentální části jsme se zabývali nejprve porovnáním charakteristik obou zdrojů a posléze experimenty uvedenými v [1], které jsme provedli s tónovým generátorem i zvukovou kartou PC. Nejprve jsme se zabývali otázkou, zda oba zdroje patří mezi tzv. tvrdé zdroje napětí, nebo jestli vykazují při zatížení výrazný pokles napětí. Současně jsme zkoumali závislost výstupního napětí zdroje na frekvenci proudu. Po přezkoumání těchto charakteristik jsme došli k závěru, že všechny výše uvedené zdroje lze považovat za tzv. měkké zdroje napětí a přistoupili jsme ke srovnání chování zdrojů v níže uvedených experimentech.

Prvním experimentem bylo měření indukčnosti cívky, druhým měření kapacity kondenzátoru, třetím frekvenční závislost kapacitance a induktance, čtvrtým ověření frekvenční závislosti sériového RLC obvodu a posledním ověření frekvenční závislosti paralelního RLC obvodu.

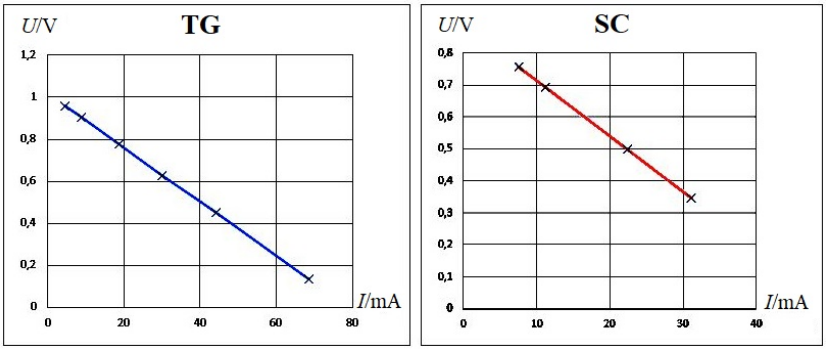
Ve všech případech jsme pomocí statistické analýzy v programu MS Excel na hladině statistické významnosti $\alpha = 0{,}05$ zjišťovali, jak se experimentální data liší od teoreticky vypočítaných. Kde to bylo možné, určili jsme i příslušnou nejistotu měření dané veličiny.

Voltampérové charakteristiky tónového generátoru a zvukové karty PC

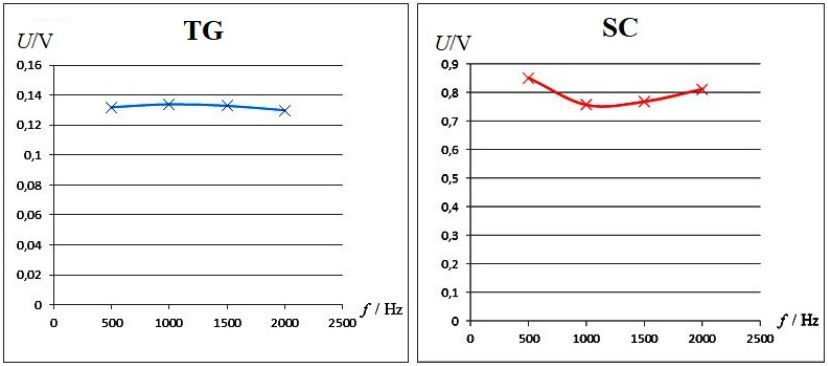
V první části popíšeme nejdříve voltampérové charakteristiky obou zdrojů a poté čtyři základní experimenty pro 3. ročník gymnázia, ve kterých jsme porovnávali tónový generátor BM 365 a zvukovou kartu notebooku. V následujícím textu budeme tónový generátor označovat zkratkou TG a zvukovou kartu počítače zkratkou SC.

Hodnoty zátěže byly voleny v případě TG 100 Ω, 500 Ω, 1 000 Ω, 2 000 Ω, 5 000 Ω a 10 000 Ω, u SC jsme zvolili hodnoty 8 Ω, 20 Ω, 60 Ω, 100 Ω. U obou zdrojů byla měření provedena pro frekvence 500 Hz, 1 000 Hz, 1 500 Hz a 2 000 Hz, které svým rozsahem pokrývají dostatečně interval frekvencí volených při experimentech.

Zatěžovací charakteristika TG, resp. SC, je na obr. 1 vlevo, resp. vpravo. Hodnota RZ v popisku obr. 2 představuje použitou zátěž.



Obr. 1 VA charakteristika TG (vlevo) a SC (vpravo) při frekvenci 1 000 Hz



Obr. 2 Frekvenční závislost výstupního napětí TG (vlevo) a SC (vpravo) pro $R_Z = 100\ \Omega$

Z grafu na obr. 2 vlevo plyne, že napětí je na námi zvoleném frekvenčním rozsahu konstantní a jeho velikost není volbou frekvence ovlivněna. Pomocí MS Excel jsme určili průměrnou hodnotu tohoto napětí a jeho nejistotu jako $U = (0{,}132 \pm 0{,}001)$ V.

V grafu na obr. 2 vpravo je vidět mírný pokles napětí pro frekvenci cca 1 200 Hz. Pomocí MS Excel jsme určili průměrnou hodnotu tohoto napětí a jeho nejistotu jako $U = (0{,}80 \pm 0{,}02)$ V. V měřicí technice se obvykle za hraniční hodnotu pro konstantní veličinu považuje nárůst nebo pokles veličiny o 3 dB, což odpovídá 1,4 násobku měřené hodnoty [2]. V našem případě se jedná maximálně o 1,025 násobek měřené hodnoty napětí, a proto považujeme i zvukovou kartu za zdroj napětí, který není frekvenčně závislý.

Měření kapacity kondenzátoru a indukčnosti cívky. Ověření frekvenční závislosti kapacitance a induktance pomocí TG a SC

Kondenzátor i cívka kladou střídavému proudu odpor, který nazýváme kapacitance X_C, resp. induktance X_L. Tyto veličiny jsou frekvenčně závislé a platí pro ně následující vztahy (1) a (2):

$$X_C = \frac{1}{2\pi f C} \tag{1}$$

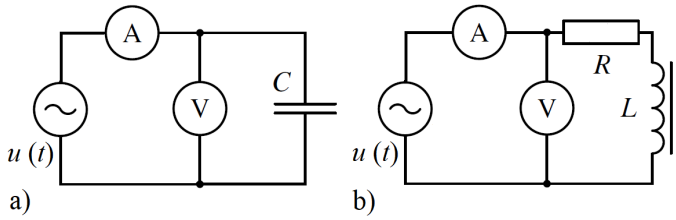
$$X_L = 2\pi f L \tag{2}$$

kde C je kapacita kondenzátoru, L je indukčnost cívky a f je frekvence střídavého proudu.

Pomůcky: multimetr VA18B (2 ks), svitkový kondenzátor 4,7 μF (3 ks), cívka $N = 600$, $L = 6$ mH, vodič jack 3,5 mm / 2 banánky, TG, PC (notebook), Visual Analyser, propojovací vodiče

Postup práce

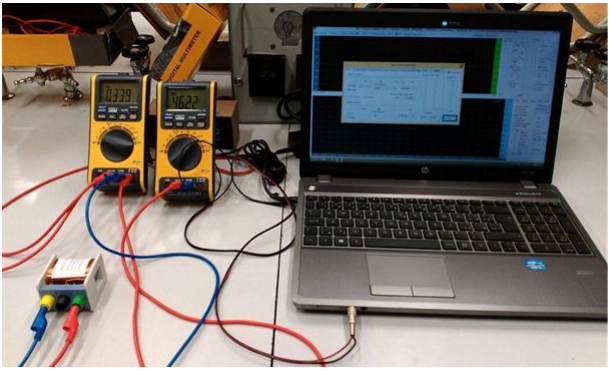
Schéma zapojení je na následujícím obr. 3.



Obr. 3 Schéma zapojení kondenzátoru (a) a cívky (b) – ověření frekvenční závislosti X_C a X_L

Uspořádání experimentu při měření indukčnosti a induktance je patrné z obr. 4, podobně postupujeme při měření kapacity a kapacitance.

Ve frekvenčním intervalu (100–2 000) Hz zvolíme rovnoměrně přibližně 20 frekvencí, které na TG generujeme nastavením frekvence jemným laděním na daném frekvenčním rozsahu a pomocí SC v programu Visual Analyser pomocí tlačítka *Wave*. V případě TG jsme nastavenou frekvenci vždy ověřili pomocí multimetru VA18B.



Obr. 4 Měření indukčnosti cívky a frekvenční závislosti induktance pomocí SC

Pro každou frekvenci změříme pomocí multimetrů VA18B proud a napětí, ze kterých pak můžeme vypočítat hodnotu kapacitance $X_C = U/I$, resp. induktance $X_L = U/I$. Vypočítané hodnoty zapíšeme do tabulky a vyneseme grafickou závislost kapacitance, resp. induktance na frekvenci. Grafy tvoříme pomocí programu MS Excel.

V druhé části výpočtů využijeme vztahy (1) a (2) k výpočtu kapacity kondenzátoru, resp. indukčnosti cívky. V případě určení kapacitance a kapacity kondenzátoru provedeme měření nejprve pro jeden kondenzátor s kapacitou $C_1 = 4{,}7$ μF a potom pro dva paralelně spojené kondenzátory s výslednou kapacitou $C_2 = 9{,}4$ μF.

Výběr námi naměřených hodnot pro výpočet kapacitance a kapacity kondenzátorů s využitím SC uvádíme v tabulce 1. Indexem 1 je označeno měření s kondenzátorem o kapacitě $C_1 = 4{,}7$ μF a indexem 2 měření s kondenzátorem o kapacitě $C_2 = 9{,}4$ μF.

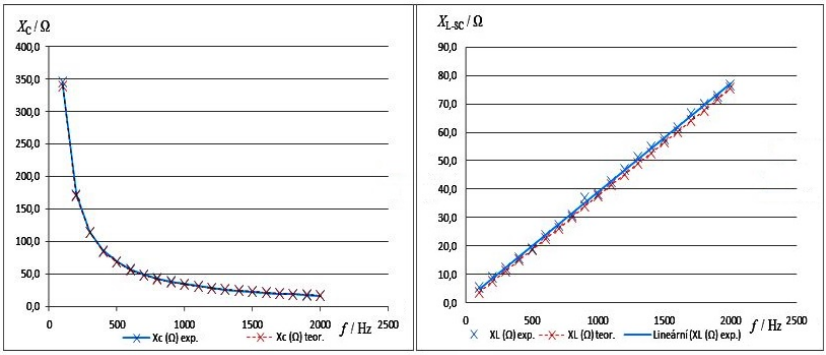
Průměrná hodnota kapacity kondenzátoru C_1 byla určena jako $C_{1TG} = (5{,}5 \pm 0{,}2)$ μF, pro kondenzátor C_2 jsme vypočítali hodnotu $C_{2TG} = (15 \pm 2)$ μF. Z grafu na obr. 5 vlevo je dobře patrný exponenciální pokles kapacitance v závislosti na frekvenci. Experimentálně naměřené hodnoty jsou vyznačeny modrými křížky, teoretické hodnoty kapacitance vypočítané ze vztahu (1) jsou zobrazeny červeně.

Tabulka 1 Měření kapacity kondenzátorů a frekvenční závislosti kapacitance s SC

f/Hz	U_1/V	I_1/mA	X_{C1}/Ω	C_1/μF	U_2/V	I_2/mA	X_{C2}/Ω	C_2/μF
100	1,177	3,41	345,2	4,6	1,171	6,99	167,5	9,5
500	0,960	14,03	68,4	4,7	0,867	26,00	33,3	9,6
1 000	0,774	22,82	33,9	4,7	0,587	35,42	16,6	9,6
1 500	0,690	30,95	22,3	4,8	0,448	41,32	10,8	9,8
2 000	0,636	38,72	16,4	4,8	0,377	47,25	8,0	10,0

Průměrná hodnota kapacity kondenzátoru C_1 byla určena jako $C_{1SC} =$ $= (4{,}71 \pm 0{,}02)$ μF, pro kondenzátor C_2 jsme vypočítali hodnotu $C_{2SC} =$ $= (9{,}68 \pm 0{,}03)$ μF. Obdobným způsobem jsme změřili indukčnost cívky s parametry $N = 600$, $L = 6$ mH a indukčnost cívky s $N = 12\,000$ a $L = 95$ mH.

Grafická závislost induktance na frekvenci proudu při měření SC je zobrazena na obr. 5 vpravo. Modře jsou znázorněny experimentálně naměřené hodnoty, červeně teoreticky vypočítané ze vztahu (2).



Obr. 5 Graf frekvenční závislosti kapacitance (vlevo) a induktance (vpravo) pomocí SC pro $C_1 = 4{,}7$ μF

Průměrná hodnota indukčnosti cívky L_{TG} měřené pomocí TG byla určena jako $L_{TG} = (6{,}4 \pm 0{,}1)$ mH, hodnota zjištěná pomocí SC je $L_{SC} = (6{,}2 \pm 0{,}2)$ mH. Relativní nejistota činila v případě TG 1,5 %, pro SC vychází relativní nejistota 3,2 %.

Rezonanční křivka paralelního obvodu RLC s TG a SC

Vzhledem k tomu, že v naší loňské práci [4] jsme se podrobně zabývali sériovým obvodem RLC, v této práci se pokusíme porovnat hodnoty získané pomocí TG a SC u paralelního obvodu RLC a v případě zvukové karty jsme ještě zkusili proměřit nadstavbu se zesilovačem Marshall na jejím výstupu.

Tímto experimentem ověřujeme známý vztah pro frekvenci oscilátoru LC, který platí jak pro sériové, tak i paralelní zapojení cívky a kondenzátoru. Vzhledem k tomu, že běžné školní laboratorní zdroje střídavého proudu pracují pouze s frekvencí 50 Hz, není klasickým způsobem možné tuto frekvenční závislost ověřit.

Z opakovaných měření kapacity kondenzátoru a indukčnosti cívky plyne, že digitální multimetr VA18B měří přesně v rozsahu 200 Hz – 2 000 Hz i mimo výrobcem udávaný frekvenční rozsah 40 Hz – 400 Hz. Frekvenci střídavého napětí pak dokáže měřit v rozsahu 10 Hz – 1 MHz.

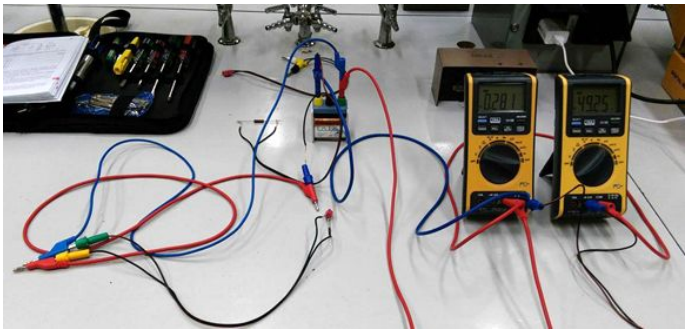
Pro vlastní frekvenci oscilátoru LC platí obecně známý Thomsonův vztah, který je shodný pro sériové i paralelní zapojení kondenzátoru o kapacitě C a cívky s indukčností L.

Pro impedanci paralelního obvodu RLC platí vztah, ze kterého plyne, že pro frekvenci střídavého proudu, která je rovna vlastní frekvenci f_0, je impedance obvodu největší.

Pomůcky: multimetr VA18B (2 ks), svitkový kondenzátor 4,7 μF (3 ks), cívka $N = 600$, $L = 6$ mH, rezistor $R = 135$ kΩ, propojovací vodiče, vodič jack 3,5 mm / 2 banánky, PC (notebook), TG, Visual Analyser

Postup práce

Uspořádání experimentu je patrné z obr. 6.



Obr. 6 Uspořádání experimentu – paralelní zapojení obvodu RLC

Voltmetr, cívku, rezistor i kondenzátor zapojíme paralelně. Voltmetrem měříme napětí na cívce a kondenzátoru.

Výstup TG i SC slouží jako zdroj střídavého napětí, které pomocí speciálního vodiče s konektorem jack 3,5 mm přivedeme na svorky paralelního obvodu RLC.

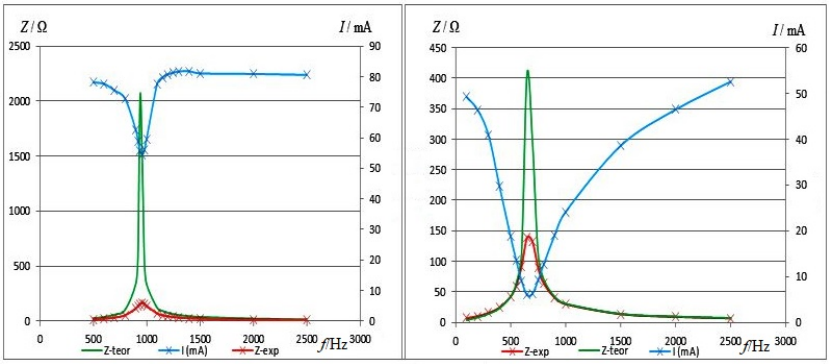
Jeden multimetr VA18B zapojíme jako ampérmetr, přičemž navolíme střídavý typ proudu (na displeji vlevo se objeví AC) a mA. Druhým multimetrem měříme velikost střídavého napětí na rezistoru, cívce a kondenzátoru.

Postupně zvyšujeme frekvenci od 100 Hz až do frekvence 2 500 Hz. V okamžiku, kdy zaznamenáme na ampérmetru největší hodnotu proudu, proměříme okolí této frekvence po cca 20 Hz.

Z naměřených hodnot napětí a proudu vypočítáme hodnotu impedance $Z = U/I$ a vyneseme do grafu závislost impedance na frekvenci. Nakonec se z grafu pokusíme určit rezonanční frekvenci f_0, která odpovídá největší hodnotě Z a porovnat ji s frekvencí získanou z Thomsonova vztahu.

Tabulka 2 uvádí měření provedené s využitím SC a kondenzátorem o kapacitě 9,4 μF. Hodnoty impedance Zteor jsou vypočítány ze vztahu pro impedanci paralelního obvodu RLC pro parametry $R = 135$ kΩ, $L = 6$ mH a $C = 4{,}7$ μF.

Z grafu na obr. 7 vlevo je dobře pozorovatelná shoda minima proudu a maxima impedance odpovídající hodnotě rezonanční frekvence $f_0 = 948$ Hz vypočítané z Thomsonova vztahu.



Obr. 7 Graf závislosti impedance a proudu na frekvenci paralelního obvodu RLC pro TG (vlevo) a SC (vpravo)

Z grafu na obr. 7 vpravo je dobře pozorovatelná shoda minima proudu a maxima impedance odpovídající hodnotě rezonanční frekvence $f_0 = 671$ Hz vypočítané z Thomsonova vztahu. I zde je patrný rozdíl mezi hodnotami teoretickými (zelená křivka) a experimentálními (červená křivka), zejména v okolí rezonanční frekvence.

Tabulka 2 Impedance paralelního obvodu RLC v závislosti na frekvenci SC pro $C = 9{,}4\ \mu\text{F}$

f/Hz	U/V	I/mA	Z/Ω	Z_{teor}/Ω
100	0,350	49,24	7	4
200	0,481	46,42	10	8
300	0,642	40,86	16	14
400	0,727	29,62	25	23
500	0,794	18,80	42	42
550	0,817	13,68	60	63
600	0,833	9,10	92	113
650	0,837	6,03	139	407
700	0,835	6,34	132	293
750	0,826	9,21	90	113
800	0,811	12,62	64	71
900	0,770	18,97	41	42
1 000	0,723	24,13	30	31
1 500	0,530	38,56	14	14
2 000	0,427	46,46	9	10
2 500	0,361	52,56	7	7

Podrobné statistické výsledky ze všech provedených měření jsou uvedeny v [5].

Závěr

V naší práci jsme se zabývali srovnáním různých charakteristik tónového generátoru BM 365 a zvukové karty notebooku a jejich využitím v různých experimentech pro 3. ročník.

Experimentálně naměřená data byla porovnána hodnotami predikovanými teorií a párově statisticky analyzována. Ze statistické analýzy jednoznačně vyplynulo, že použití zvukové karty jako zdroje sinusového napětí malé hodnoty ve všech provedených experimentech se na hladině statistické významnosti $\alpha = 0{,}05$ poskytuje experimentální hodnoty, které se statisticky významně neliší od teorie.

V případě tónového generátoru jsme dospěli k podobnému závěru s výjimkou paralelního RLC obvodu, kde se hodnoty statisticky významně liší. Dalším zjištěním je, že použití zesilovače na výstupu zvukové karty přineslo horší výsledky, než měření pouze s SC.

Závěrem můžeme konstatovat, že zvuková karta je plnohodnotnou náhradou tónového generátoru a lze ji úspěšně používat při školních fyzikálních experimentech.

Poděkování

Autoři děkují všem studentům zapojeným do výzkumu. Výzkum je podpořen z prostředků projektu No. CZ.02.3.68/0.0/0.0/16_011/0000669 (PŘÍRodovědné Oborové Didaktiky A praktikující učitel). Projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

Literatura

[1] *Lepil, O.*: Fyzika pro gymnázia, Elektřina a magnetismus, Prometheus, Praha, 2011.

[2] Elektronika, teoretické základy, praktické zapojení, kap. Decibely, [online]. [cit. 2017-02-27].
Dostupné z: http://elnika.sweb.cz/mereni/decibely.htm

[3] Cvičení ze statistiky IV., [online]. [cit. 2017-02-27].
Dostupné z: http://ulb.upol.cz/praktikum/statistika4.pdf

[4] *Myslivcová, L., Hošek, F., Rouha, M.*: Náhrada tónového generátoru pomocí zvukové karty PC, Středoškolská odborná práce, Nový Bydžov, 2016.

[5] *Myslivcová, L., Hošek, F., Rouha, M.*: Srovnání charakteristik tónového generátoru a zvukové karty PC, [Středoškolská odborná práce], Nový Bydžov, 2017, [online]. [cit. 2017-04-29].
Dostupné z: http:/www.sclpx.eu/clanky/SOC_2017_final.pdf

Nedostatek aprobovaných učitelů fyziky na západě Čech: bude hůř

MARIE MOLLEROVÁ – JIŘÍ KOHOUT – LUKÁŠ FEŘT – PAVEL MASOPUST

Fakulta pedagogická, Západočeská univerzita v Plzni

Kolik aprobovaných učitelů fyziky na školách v České republice vlastně chybí? Jaká bude další budoucnost předmětu fyzika na školách? Jaká je situace na vysokých školách připravujících budoucí učitele fyziky? Tyto i jiné otázky si kladou nejen akademičtí pracovníci vysokých škol, ale i ředitelé základních a středních škol. Je tato situace skutečně tak závažná, že by potřebovala řešit? A kde a od koho vůbec získat skutečné a potřebné počty aprobovaných učitelů fyziky?

Dá se tušit, že situace ohledně počtu aprobovaných učitelů fyziky rozhodně nebude nikterak růžová. Přeci jen se jedná o jeden z náročnějších předmětů v přípravě budoucích učitelů, a ani samotní studenti už na základních a především středních školách nemají fyziku příliš v oblibě [1]. Tak proč se rozhodnout pro studium učitelství fyziky? Proč zasvětit svůj život učitelské profesi? Odpovědí je spousta a co učitel, to jiný názor. Obecně jdou ale učitelství fyziky studovat lidé, které tento obor baví (pro ostatní by to zřejmě bylo dost velké utrpení), a kteří jsou současně ochotni své poznatky předávat dál. Člověka prostě tento obor musí bavit. Ale... Na druhou stranu může časem přijít značné rozčarování, které člověka donutí učitelskou profesi opustit. Jednak je to prakticky mizivá vidina profesního růstu, nízké finanční ohodnocení práce učitelů, nízká autorita ze strany žáků (a často i rodičů), a samozřejmě možnost uplatnit se v jiném oboru a mít více času i peněz [2]. A tak se nemůžeme divit, že je počet zájemců o studium učitelství fyziky menší a menší a že počet aprobovaných učitelů fyziky celkově rok od roku klesá.

Snahy o zjištění počtu učitelů fyziky

Otázkou počtu aprobovaných učitelů se zabýval a stále zabývá *doc. RNDr. Leoš Dvořák, CSc.* z Matematicko-fyzikální fakulty UK v Praze,

který vystoupil na konferenci „Moderní trendy v přípravě učitelů fyziky 7“ s příspěvkem Příprava učitelů fyziky v ČR [3, s. 27–37]. V něm se mimo jiné zabýval právě otázkou počtu aprobovaných fyzikářů a počtem studentů na fakultách připravujících budoucí učitele tohoto oboru. Na základě sebraných dat od vysokých škol poté zjistil, že za posledních pět let absolvovalo na těchto fakultách zhruba 300 studentů, což je zhruba 60 absolventů učitelství fyziky za rok. Počet učitelů fyziky, kteří ročně opouštějí školství a musí být nahrazeni, řešil jako Fermiho úlohu (úloha kde rychle a přibližně, ale kvalifikovaně, odhadujeme nějakou kvantitu) a došel k hrubému odhadu, že ročně by bylo třeba mít cca 150 nových učitelů fyziky, tedy mnohem více, než je současný stav. Účastníci konference se shodli, že pro fakulty připravující učitele i další odborníky je nanejvýš důležité mít k dispozici tvrdá data o počtech a věkové struktuře učitelů fyziky tak, abychom se nemuseli opírat pouze o rámcové odhady, jež mohou být zatíženy velkou chybou.

Z pozice předsedy Fyzikální pedagogické společnosti JČMF se Dvořák na základě usnesení účastníků zmíněné konference snažil v letech 2015 až 2017 získat od MŠMT příslušné informace. Výsledky tohoto úsilí shrnul na další konferenci „Moderní trendy v přípravě učitelů fyziky 8“ v příspěvku Dva roky snah o získání počtu učitelů fyziky [4]. Bohužel i přes veškeré sliby ze strany MŠMT se žádných relevantních dat nedočkal, což bylo zdůvodněno tím, že získávání těchto údajů by vedlo k dalšímu zvýšení administrativní zátěže škol. Mohl tak uvést jen „odhady“ založené na základě vyplněných dotazníků sebraných z naprosto mizivého počtu škol. Na jejich základě interpolací určil počet chybějících učitelů fyziky na základních školách v ČR na zhruba jedenáct set. Na SŠ poté chybí odhadem šest set fyzikářů. Jedná se však skutečně jen o odhad s velmi malou vypovídací hodnotou, z něhož zároveň není vzhledem k absenci informací o věkové struktuře fyzikářů patrné, jak se bude situaci vyvíjet do budoucna.

Cíle a metodologie výzkumného šetření

Na základě všech těchto informací jsme se rozhodli pro vlastní průzkum ohledně počtu aprobovaných učitelů fyziky na základních školách. Průzkum byl proveden pro dva kraje, Plzeňský a Karlovarský, jelikož se jedná o spádové regiony, kde se nejčastěji uplatňují absolventi FPE ZČU. Pro oba kraje jsme získali kompletní seznam všech základních škol,[1)] z něhož byly následně vyškrtnuty malotřídní školy, na nichž se fyzika nevyučuje.

[1)] viz http://www.atlasskolstvi.cz/zakladni-skoly

Samotný výzkum pak zahrnoval několik vzájemně souvisejících částí:

1. Analýzu ŠVP jednotlivých škol s cílem získat představu o tom, v jakém rozsahu je fyzika vyučována a jaká je posloupnost tematických celků.
2. Telefonické rozhovory s řediteli škol vedené s cílem získat informace o aprobovanosti a věkové struktuře učitelů fyziky, a rovněž o příčinách případného nedostatku učitelů fyziky.
3. Výzkum zaměřený na absolventy ZŠ týkající se především toho, jak je fyzika na základní škole bavila a jak často učitelé do výuky zařazovali pokusy.

V rámci telefonických rozhovorů jsme se ptali ředitelů škol na tři základní otázky: Máte výuku fyziky vedenou aprobovaným učitelem? Do jaké věkové skupiny patří vyučující fyziky? Máte problém pro vaši školu sehnat aprobovaného fyzikáře, a pokud ano, proč tomu tak je? Zároveň byl všem dotazovaným vysvětlen pojem aprobovaný učitel, protože tento termín se často zaměňuje s pojmem kvalifikovaný učitel. Aprobovaného učitele chápeme v tomto výzkumu ve shodě s Dvořákovým výzkumem následovně [4]:

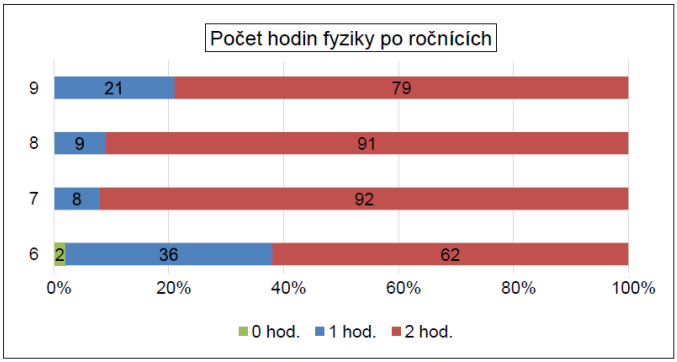
1. Absolvent učitelství fyziky pro základní a střední školy v magisterském studijním programu.
2. Absolvent učitelství jiných všeobecně vzdělávacích předmětů + oboru Fyzika v programu celoživotního vzdělávání (studium k rozšíření odborné kvalifikace).
3. Absolvent magisterského neučitelského studijního oboru (tedy i inženýrského) se zaměřením na fyziku + doplňujícího pedagogického studia.

Díky nečekaně velké ochotě ředitelů se nám podařilo získat informace ze 114 základních škol v Plzeňském kraji a 65 v Karlovarském kraji, což tvoří přibližně 98 % škol příslušného typu v těchto regionech.

Pro získání komplexní představy a zjištění souvislostí mezi aprobovaností učitelů a vnímáním výuky žáky jsme provedli rovněž výzkum zaměřený na to, jak absolventy ZŠ pokračující ve studiu na SŠ výuka bavila a jak časté v ní byly pokusy z jednotlivých oblastí fyziky. Do výzkumu se zapojilo celkem 107 studentů 1. ročníku Střední průmyslové školy dopravní v Plzni, kteří přišli z 58 škol Plzeňského a Karlovarského kraje, jež byly zahrnuty do výzkumné studie.

Rozsah a obsah výuky na základních školách

Fyzika je v současné době zařazena do výukové oblasti Člověk a příroda, která je spolu s přírodopisem, chemií a zeměpisem dotována 22 hodinami. Je na každé škole, kolik hodin pro výuku fyziky vyčlení. Na 49 % základních škol je fyzika vyučována v 7 hodinách napříč 6.–9. ročníkem, na 37 % škol v 8 hodinách a na 13 % škol v 6 hodinách. Nejčastější rozvržení hodin je v modelu 2+2+2+2 (37 % škol), 2+2+2+1 (15 % škol) a 1+2+2+2 (25 % škol). Jen na jediné škole jsme zaznamenali situaci, že celkem byla fyzika dotována pouze pěti hodinami (ve skladbě 1+2+1+1). Srovnání s výsledky celorepublikového výzkumu z let 2002–2004 [5, s. 26–29] ukazuje, že se rozsah výuky fyziky na základních školách v posledních více než 10 letech prakticky nezměnil, počty hodin jsou však stále na podstatně nižší úrovni, než by si učitelé fyziky přáli. Varující je velmi malý počet půlených hodin (alespoň jednu půlenou hodinu fyziky od 6. do 9. ročníku má dle našeho výzkumu ve sledovaných regionech méně než 10 % škol). Rostoucí počet dětí ve třídách především ve městech a příměstských oblastech pak výrazně komplikuje realizaci komplexnějších laboratorních prací.



Obr. 1 Počet hodin fyziky v jednotlivých ročnících ZŠ v Plzeňském a Karlovarském kraji

Z hlediska obsahu výuky fyziky dle ŠVP se naprostá většina škol drží posloupnosti dle klasických učebnic.[2)] Odlišnosti se objevují především na školách bez aprobovaného učitele fyziky a budou diskutovány dále. Z hlediska rozdělení výukových témat do jednotlivých ročníků je zajímavé, že

[2)] Sady učebnic fyziky od nakladatelství Prometheus a Fraus, které jsou v západních Čechách nejrozšířenější.

množství učiva uvedené v ŠVP ve většině případů nezávisí na zvolené hodinové dotaci pro daný ročník (1 nebo 2 hodiny). Zvláště výrazný je tento efekt v 6. ročníku, kdy je pouze jednohodinová dotace poměrně častá (36 % škol). Pravděpodobně to souvisí s přirozenou snahou probrat z organizačních důvodů učivo uvedené v učebnici pro daný ročník, může to však vést k tomu, že dojde k uspěchání důležitých úvodních partií fyziky.

Aprobovanost učitelů v Plzeňském kraji

Veškeré získané informace jsou pro lepší přehlednost upraveny do tabulek a grafů a rozděleny do sekcí podle dvou zkoumaných krajů. Nejprve tedy situace v Plzeňském kraji. Dle vyjádření ředitelů vyučuje fyziku na ZŠ v Plzeňském kraji celkem 178 učitelů na 114 školách. Přitom 117 učitelů je aprobovaných a alespoň jednoho aprobovaného fyzikáře má 77 škol (67,5 %), 37 (32,5 %) nikoliv. Detailní informace po okresech jsou uvedeny v Tabulce 1.

Tabulka 1: Přehled škol v jednotlivých okresech Plzeňského kraje

Okres	Celkový počet ZŠ	ZŠ s alespoň jedním aprobovaným učitelem Fy	ZŠ bez jediného aprobovaného učitele Fy	Průměrný věk aprobovaných učitelů fyziky
Plzeň-město	26	21 (81 %)	5 (19 %)	40
Plzeň sever	21	11 (52 %)	10 (48 %)	51
Plzeň jih	13	9 (69 %)	4 (31 %)	39
Rokycany	10	7 (70 %)	3 (30 %)	40
Tachov	12	7 (58 %)	5 (42 %)	50
Domažlice	12	10 (83 %)	2 (17 %)	44
Klatovy	20	12 (60 %)	8 (40 %)	50

Podle přehledu v tabulce se může zdát, že na tom některé okresy Plzeňského kraje nejsou vůbec špatně, ale opak je pravdou. Stačí se podívat na věk aprobovaných učitelů a situace už se nezdá tak optimistická. Například okres Domažlice je na tom v současné době dobře, ale v tomto okrese je na 10 školách, kde je výuka vedena aprobovaným učitelem, polovina vyučujících ve věkové skupině 50+. Úplně nejhorší situace je v okrese Tachov, v okrese Plzeň-sever (z 11 škol s aprobovaným učitelem fyziky jsou na

čtyřech vyučující v důchodovém věku) a v okrese Klatovy (z 12 škol s aprobovaným učitelem fyziky jsou na dvou vyučující v důchodovém věku a na 6 školách ve věkové skupině 50+). Komplexní přehled o věkové struktuře učitelů fyziky v Plzeňském kraji nabízí obr. 2, z něhož plyne, že desetina učitelů fyziky je již v důchodovém věku.

Obr. 2 Věkové složení aprobovaných fyzikářů v Plzeňském kraji

Aprobovanost učitelů v Karlovarském kraji

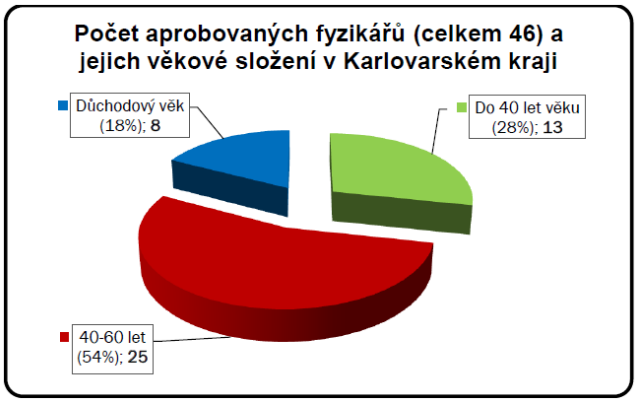
V Karlovarském kraji je situace bohužel ještě horší. Podle vyjádření ředitelů vyučuje fyziku na ZŠ v Karlovarském kraji celkem 101 učitelů na 65 školách. Přitom pouze 46 učitelů (45,5 %) je aprobovaných a alespoň jednoho aprobovaného fyzikáře má 35 škol (53,8 %), 30 (46,2 %) nikoliv.

Tabulka 2: Přehled škol v jednotlivých okresech Karlovarského kraje

Okres	Celkový počet ZŠ	ZŠ s alespoň jedním aprobovaným učitelem Fy	ZŠ bez jediného aprobovaného učitele Fy	Průměrný věk aprobovaných učitelů fyziky
Karlovy Vary	24	14 (58 %)	10 (42 %)	50
Cheb	20	13 (65 %)	7 (35 %)	46
Sokolov	21	8 (38 %)	13 (62 %)	50

Situace v jednotlivých okresech je popsána v Tabulce 2. Z ní je patrné, že nejhorší stav je v okrese Sokolov. Z osmi aprobovaných učitelů jsou dva již v důchodovém věku a dva těsně před dosažením důchodového věku. Ve

výhledu několika let tak bude v tomto okrese situace velmi tíživá. Rozdělení z hlediska věkových skupin je pak uvedeno na obr. 3. Z něj je patrné, že téměř pětina aprobovaných učitelů fyziky v kraji je již v důchodovém věku a přesluhuje.



Obr. 3 Věkové složení aprobovaných fyzikářů v Karlovarském kraji

Příčiny neaprobovanosti a její dopady na výuku

Podle ředitelů je příčin, proč nemohou sehnat aprobovaného fyzikáře, hned několik. Za zmínku stojí ty prakticky totožně zmiňované na všech základních školách:

1. Útěk do jiných sektorů (typicky z důvodu nedostatečného finančního ohodnocení).
2. Prestiž učitelského povolání.
3. Nízká autorita ze strany žáků.
4. Náročnost studia na fakultách připravujících učitele fyziky.

Dopad na výuku fyziky s, resp. bez aprobovaného učitele byl poznat hned v několika důležitých aspektech:

1. Změna posloupnosti výuky vedoucí k nelogičnostem (analýza ŠVP vedla ke zjištění, že mnohdy jsou vyučovány Newtonovy zákony před tématem Pohyb a klid těles, někdy dokonce došlo k zařazení aplikované mechaniky tekutin (vodní motory) před dynamiku, která je zařazena před kinematikou...).

2. Dle informací získaných během rozhovorů od ředitelů škol dochází k častému střídání učitelů.
3. Žáky více baví výuka vedená aprobovaným učitelem fyziky (výzkum mezi žáky prokázal statisticky významně lepší výsledky pro školy mající plně aprobované fyzikáře – p-hodnota příslušného statistického testu byla 0,004).
4. Častější zařazování experimentů do výuky na školách s aprobovanými fyzikáři (výzkum mezi žáky ukázal, že průměrná míra experimentování v hodinách fyziky byla u škol s plně aprobovanými fyzikáři 3,42 bodu z možných 8, zatímco v případě úplné neaprobovanosti to bylo jen 2,83 bodu; p-hodnota testu byla 0,097, což naznačuje statistickou významnost na hladině 0,1).
5. Ze škol majících aprobované fyzikáře odchází větší procento žáků na gymnázia.[3)]

Celkově výsledky našeho výzkumu naznačují, že aprobovanost zde hraje podstatnou roli a není možné akceptovat občas se objevující argument, že diplom nehraje roli a neaprobovaní učitelé učí stejně či dokonce lépe než ti aprobovaní.

Závěr

Podle věkové struktury aprobovaných fyzikářů v obou krajích lze předpokládat, že kritická situace nastane na základních školách během pěti až deseti let. Středními školami se tento výzkum nezabýval, nicméně je důvod se domnívat, že na nich jsou učitelé fyziky v průměru ještě starší a problém zde tudíž nastane rovněž. Nedostatek kvalifikovaných učitelů fyziky je problémem, se kterým se potýká většina vyspělých zemí,[4)] přičemž např. v USA je v tomto ohledu špatná situace již po dobu mnoha desítek let [6]. Na rozdíl od nás však je zpravidla k dispozici ucelená statistika toho, kolik učitelů fyziky chybí a díky znalosti věkové struktury je poměrně jasné i to, jak se bude situace vyvíjet v dalších letech. Pokládáme proto za nutné,

[3)] Zde může hrát podstatnou roli to, že méně aprobovaných učitelů fyziky je ve venkovských oblastech, kde je procento žáků hlásících se na gymnázia zpravidla nižší než ve městech. Samotná role aprobovaných fyzikářů spočívající potenciálně ve schopnosti vést žáky k logickému myšlení potřebnému při přijímacích zkouškách tak není jednoznačná a bylo by třeba ji prokázat/vyvrátit v dalším výzkumu.

[4)] Viz přehled uvedený na http://www.air.org/sites/default/files/downloads/report/Creating-Coherence-Teacher-Shortage-Debate-June-2016.pdf

aby podobná evidence týkající se nejen fyzikářů vznikla i v ČR. Obavy, že by se jednalo o neúměrné navýšení administrativní zátěže, pokládáme za neopodstatněné, protože jde o informace, které školy stejně shromažďují a stačilo by je přenést do vhodné databáze. K prosazení této iniciativy pak pokládáme za důležité, aby se k Fyzikální pedagogické společnosti JČMF přidaly další zainteresované organizace jako Asociace děkanů pedagogických fakult či asociace ředitelů různých typů škol. Společně by pak měly vytvořit dostatečný tlak na příslušné orgány vedoucí k tomu, aby se touto problematikou konečně začaly systematicky zabývat.

Poděkování

Výzkum byl podpořen projektem OP VVV Didaktika – Člověk a příroda A (CZ.02.3.68/0.0/0.0/16_011/0000665).

Literatura

[1] *Höfer, G., a kol.*: Výuka fyziky v širších souvislostech – názory žáků. [cit. 6. 8. 2017]. Dostupné na: https://kdf.mff.cuni.cz/vyzkum/materialy/vyuka_fyziky_v_sirsich_souvislostech.pdf

[2] *Danielková, D.*: Analýza faktorů pracovní spokojenosti zaměstnanců školství. Bakalářská práce. Univerzita Karlova, Praha. [cit. 6. 8. 2017]. Dostupné na: https://is.cuni.cz/webapps/zzp/download/130007019

[3] *Dvořák, L.*: Příprava učitelů fyziky v ČR – Úvod do diskuze o stávajícím stavu a možnostech budoucího vývoje. In: Moderní trendy v přípravě učitelů fyziky 7. Sborník z konference. Vydavatelství ZČU, Plzeň, 2016.

[4] *Dvořák, L.*: Dva roky snah o získání počtu učitelů fyziky. Příspěvek přednesený na konferenci Moderní trendy v přípravě učitelů fyziky 8 dne 21. 4. 2017.

[5] *Höfer, G., Svoboda, E.*: Postoje učitelů základních a středních škol k výuce fyziky. MATFYZPRESS, Praha, 2008.

[6] *Hniličková-Fenclová, J.*: Snahy o sjednocení a zkvalitnění přípravy učitelů fyziky v USA. Pokroky matematiky, fyziky a astronomie, roč. 14 (1969), s. 221–226.

INFORMATIKA

Moderní šifry I

EDUARD BARTL

Přírodovědecká fakulta UP, Olomouc

Série článků o šifrování se snaží přiblížit problematiku moderních šifrovacích metod čtenáři se základními znalostmi středoškolské matematiky. První díl série vykládá základní principy asymetrického šifrování a bezpečné výměny tajného klíče. Text směřuje k vysvětlení šifry, které se říká RSA a která v současné době hraje důležitou roli při zabezpečení komunikace na Internetu i v dalších souvisejících oblastech, například v elektronickém podpisu. V této sérii tak nahlédneme pod pokličku objevům, které se podílely na prudkém rozvoji Internetu; jen těžko si lze totiž představit, že by byl Internet používaný v takové míře jako je tomu dnes, kdyby jeho uživatelé neměli solidní možnost ochránit svoje soukromé údaje a soukromou komunikaci.

Co se Eva nesmí dozvědět

Existuje mnoho způsobů, jak utajit citlivou informaci. Některé způsoby utajení jsou velmi jednoduché (například substituční nebo transpoziční šifra), jiné jsou naopak značně složité (například šifrovací stroj Enigma; ten byl dokonce kvůli své složitosti po nějakou dobu považován za nerozluštitelný). Přestože se tyto šifry zdají být rozdílné, scénář, jímž se řídí, je stále stejný. Zkusme si ho ve stručnosti popsat.

Na začátku jsou dva lidé, kteří si potřebují sdělit nějakou důvěrnou zprávu; tuto důvěrnou zprávu obyčejně nazýváme *otevřeným textem*. Odesilateli zprávy se v kryptografii zpravidla říká *Alice*, příjemce bývá pojmenován jako *Bob*. Aby Alice zajistila utajení této zprávy, tak ji zašifruje a pak pošle Bobovi. V tento okamžik nijak neřešíme, jestli je zpráva poslána

prostřednictvím pošty (ať už klasické nebo elektronické), telegrafu nebo nějakým jiným způsobem. Pouze předpokládáme, že způsob přenosu zprávy nijak nezaručuje její utajení (proto také Alice před odesláním zprávu zašifrovala). Do hry tak může vstoupit třetí osoba, která má možnost bez velkého úsilí zašifrovanou zprávu obdržet a na šifru takzvaně zaútočit; to znamená, může se pokusit ze zašifrované zprávy získat zprávu původní. Této třetí osobě se v knížkách o kryptografii často říká *Eva*.[1)] Bob v určitém okamžiku zašifrovanou zprávu přijme a dešifruje ji, čímž obdrží onu důvěrnou informaci od Alice. Všimněme si dobře, že ani Alice ani Bob nemají možnost zjistit, jestli skutečně došlo k Evině pokusu o útok. Protože jsou však paranoidní, tak útok předpokládají a snaží se použít natolik bezpečné šifrování, aby se Evě útok nezdařil.

V první polovině 20. století bylo konstruktérům šifer jasné, že by bezpečnost šifer neměli zakládat na utajení toho, jak šifry fungují.[2)] Princip fungování šifer[3)] se totiž utajuje jen velmi obtížně. Stačí, aby jeden z konstruktérů buď z vlastních pohnutek nebo proto, že byl nějakým způsobem donucen, princip Evě vyzradil a ta pak může nerušeně číst šifrovanou komunikaci, aniž by si toho byli Alice s Bobem vědomi.

Princip fungování šifry se proto zpravidla zveřejňuje. Je ovšem zřejmé, že musí existovat *něco*, co musí být drženo v tajnosti a co zajistí, že se Evě nepodaří zašifrovanou zprávu rozluštit. Čtenář se jistě dovtípí, že tím, co je potřeba držet v tajnosti, je nějaká podoba *tajného klíče*. Tento klíč musí být známý pouze Alici a Bobovi, Eva ho nesmí získat; pomocí něj totiž Alice provádí šifrování a Bob dešifrování.

Šifrování a dešifrování pod drobnohledem

Pokusme se nyní vše vysvětlit podrobněji. Šifrování a dešifrování se v kryptografii popisuje *matematickými funkcemi*. Matematickou funkci, která realizuje šifrování, budeme označovat písmenem e (využijeme prvního písmene anglického slova *encipher*, které znamená *šifrovat*) a budeme ji nazývat *šifrovací funkce*. Tato funkce „vyrobí“ z nějakého znaku x ote-

[1)] Patrně proto, že výslovnost anglické varianty tohoto jména – *Eve* – je [i:v]. Je tedy stejná jako výslovnost začátku anglického slova *eavesdrop* [i:vz.dra:p], což znamená *tajně naslouchat*.

[2)] Je historicky doloženo memorandum německých kryptografů pracujících na zlepšování šifrovacího stroje Enigma, které říká, že „při posuzování bezpečnosti šifry se předpokládá, že nepřítel má šifrovací stroj k dispozici“ [4].

[3)] Principem fungování šifry rozumíme postup, jakým tato šifra „vyrobí“ z otevřeného textu zašifrovanou zprávu a naopak.

vřeného textu a nějakého tajného klíče k určitý znak y zašifrovaného textu, což stručně zapisujeme jako

$$y = e(x, k).$$

Matematickou funkci, která popisuje dešifrování, budeme označovat písmenkem d (opět zde využijeme prvního písmene anglického slova: *decipher* znamená *dešifrovat*) a budeme ji nazývat *dešifrovací funkce*. Funkce d, jak můžeme čekat, z nějakého znaku y zašifrovaného textu a nějakého tajného klíče k „vyrobí“ příslušný znak x otevřeného textu. To může být opět stručně zapsáno jako

$$x = d(y, k).$$

Funkce e a d jsou přitom navrženy tak, že pokud Alice použije funkci e k zašifrování znaku x pomocí klíče k a získá tak znak y, pak Bob dešifrováním y pomocí téhož klíče k musí získat původní znak x. Musí tedy platit

$$d(e(x, k), k) = x.$$

Funkcím, které splňují tuto podmínku, se říká *inverzní*.[4)]

Dobře si všimněme, že co se šifrování a dešifrování týče, mají Alice a Bob stejné schopnosti. To znamená, že stejně jako Alice může šifrovat zprávu a Bob ji pak dešifrovat, může naopak Bob nějakou zprávu zašifrovat a Alice ji dešifrovat. Z tohoto pohledu je tedy vztah Alice a Boba symetrický a každému šifrování, které se vyznačuje touto vlastností, se proto říká *symetrické šifrování*.

Pro lepší pochopení si vše ukážeme na jednoduchém příkladu. Znaky otevřeného textu musí být nejprve vhodným způsobem kódovány, to znamená, převedeny na čísla, se kterými funkce e a d (a potažmo i počítač) umějí pracovat. Vhodné by bylo použít známé ASCII kódování,[5)] pro naše účely však bude bohatě stačit následující jednoduché kódování: písmeno `a` budeme kódovat číslem 0, písmeno `b` číslem 1, písmeno `c` číslem 2 atd. Nebudeme přitom uvažovat českou diakritiku (písmena s háčky, čárkami nebo kroužky) ani interpunkční znaménka (čárky, tečky, středníky,

[4)] S tímto pojmem se setkáváme na střední škole při výuce reálných funkcí jedné reálné proměnné – například na intervalu $\langle 0, \infty)$ je kvadratická funkce inverzní k funkci druhá odmocnina.

[5)] ASCII je zkratkou z American Standard Code for Information Interchange, což znamená „americký standardní kód pro výměnu informací“. ASCII umožňuje kódovat 128 znaků, například mezera je kódována číslem 32, malé písmeno `a` je kódováno číslem 97 a tak podobně.

závorky, uvozovky apod.); potřebovat budeme pouze (viditelnou) mezeru ␣, kterou budeme kódovat číslem 26. Kódování je přehledně znázorněno v tab. 1.

znak	`a`	`b`	`c`	`d`	...	`y`	`z`	␣
kódové číslo	0	1	2	3	...	24	25	26

Tab. 1 Jednoduché kódování písmen abecedy a mezery ␣.

Uvažovat budeme jednoduchou posouvací šifru; tajným klíčem k je číslo určující posunutí abecedy zašifrovaného textu vůči abecedě otevřeného textu. Šifrovací funkce e je pak definována následujícím způsobem:

$$e(x, k) = x + k, \tag{1}$$

kde x je jedno z čísel od 0 do 26 kódující znak otevřeného textu. Předpokládejme, že se Alice s Bobem shodnou na tajném klíči $k = 5$ a že Alice bude chtít zašifrovat písmeno `b`. Nejprve si z tab. 1 zjistí kód tohoto písmene (číslo 1) a pak již může vypočítat hodnotu funkce e:

$$e(x, k) = e(1, 5) = 1 + 5 = 6.$$

Z téže tabulky pak Alice zjistí, jaké písmeno se kóduje číslem 6. Dojde tedy k závěru, že písmeno otevřeného textu `b` se šifruje písmenem `G` (v literatuře o kryptografii bývá zvykem psát otevřený text malými písmeny, kdežto zašifrovaný text velkými písmeny). Pozornému čtenáři jistě neunikne, že takto definovaná šifrovací funkce nepracuje zcela správně. Pokud by totiž Alice potřebovala šifrovat znak, jenž se kóduje číslem 22 nebo vyšším, pak by se přičtením čísla 5 dostala mimo rozsah tab. 1. Toto „přetečení“ se dá naštěstí snadno odstranit tak, že se začne počítat od začátku.[6)] Například písmeno `y` kódované číslem 24 se tak bude šifrovat písmenem `C` kódovaným číslem 2.

Jak již dobře víme, dešifrovací funkce d je inverzní k šifrovací funkci e, platí tedy

$$d(y, k) = y - k, \tag{2}$$

kde y je jedno z čísel od 0 do 26 kódující znak zašifrovaného textu. Samozřejmě zde musíme vyřešit „podtečení“ v případě, že dešifrujeme písmena kódovaná číslem 4 nebo menším. To se však dělá podobným trikem jako v případě „přetečení“. Můžeme tak snadno ověřit, že písmena `G` a `C` se pomocí funkce d dešifrují zpět na písmena `b` a `y`.

[6)] Využijeme takzvanou *modulární aritmetiku*. Podrobně se k tomuto „kruhovému počítání“ vrátíme v příštím díle.

Nejde-li to silou, pak to půjde ještě větší silou

Jednoduché symetrické šifry, o kterých byla doposud řeč, se v dnešní době nedají k praktickému šifrování použít – jsou nevhodné k šifrování e-mailových zpráv, k zabezpečení komunikace mezi bankou a klientem a podobně. Důvod je nasnadě. Ve chvíli, kdy na scénu vstoupily moderní počítače, zmíněné šifry přestaly být bezpečné. Pokud totiž Eva zachytí zašifrovanou zprávu, může rychle pomocí počítače zkoušet různé klíče a skončit ve chvíli, kdy obdrží nějaký smysluplný text. Pokud je zašifrovaná zpráva dostatečně dlouhá, tak si může být jistá, že je tento smysluplný text hledanou zprávou. Tomuto způsobu získání tajného klíče se říká *útok hrubou silou*. Pojmenování je to vskutku příhodné; Eva nemusí vymýšlet nic složitého, stačí hrubou silou „kácet“ jeden klíč za druhým.

Čtenáře jistě napadne, že by pro zajištění bezpečnosti stačilo zvětšit počet klíčů natolik, že by Evě i nejrychlejším počítačem trvalo příliš dlouho projít všechny možné kombinace klíčů. Dostatečná délka tajných klíčů a potažmo i dostatečně velký počet různých klíčů je skutečně jedním ze základních požadavků, které musí moderní šifry splňovat.[7)] Například šifra AES[8)] používá klíče, které mají, pokud je zapíšeme v binární podobě, délku až 256 bitů (to znamená, že tajným klíčem je posloupnost nul a jedniček a délka této posloupnosti je až 256). Počet všech klíčů je tedy $2^{256} \doteq 1{,}158 \cdot 10^{77}$, což je skutečně obrovské číslo.[9)]

Mohlo by se zdát, že bezpečné moderní šifry s dlouhým klíčem vyřešily problém se zabezpečením komunikace. Zdaleka tomu tak není. Dokonce i šifra AES trpí jedním zásadním nedostatkem. Představme si následující situaci: Alice, Bob a Charlie spolu potřebují (každý s každým) zabezpečeně komunikovat. Například tedy Alice si potřebuje posílat zprávy s Charliem tak, aby je Bob (a kdokoliv jiný) nemohl číst. Použijí k tomu šifru AES nebo jinou dostatečně bezpečnou šifru. Kolik tajných klíčů si musí mezi

[7)] Zdůrazněme, že dostatečně velký počet klíčů nezaručuje, že je daná šifra skutečně bezpečná. K šifrám, jako je substituční šifra nebo Vigenèrova šifra, existují velmi chytré metody, jak rychle najít tajný klíč bez použití hrubé síly (v případě substituční šifry stačí použít frekvenční analýzu, u Vigenèrovy šifry je nejprve potřeba zjistit délku bloku). Moderní bezpečné šifry musí být odolné i vůči těmto metodám.

[8)] AES je zkratkou z anglického názvu Advanced Encryption Standard. Jedná se o takzvanou blokovou šifru, která byla zavedena roku 2001 a dnes je využívaná zejména v protokolu WPA2 definujícím komunikaci a zabezpečení v bezdrátových Wi-Fi sítích. Tuto šifru také využívá známý program pro internetovou telefonii – Skype.

[9)] Pro srovnání: počet atomů ve viditelném vesmíru se odhaduje na 10^{80}.

sebou vyměnit?[10] Snadno se dopočítáme, že pouze 3 – jeden tajný klíč si musí vyměnit Alice s Bobem, jeden Alice s Charliem a jeden Charlie s Bobem. Pokud do své skupiny přiberou ještě jednoho účastníka, řekněme kupříkladu Davida, pak již budou potřebovat 6 klíčů. Jak bude vypadat situace, pokud skupina bude mít obecně n účastníků? Protože každé dvojici ze skupiny přiřazujeme jiný klíč (přičemž nezáleží na pořadí účastníků v dané dvojici), můžeme počet klíčů v závislosti na počtu účastníků vyjádřit kombinačním číslem

$$\binom{n}{2} = \frac{n!}{(n-2)! \cdot 2!} = \frac{n \cdot (n-1)}{2}.$$

Například pro skupinu o tisíci účastnících tedy celkem potřebujeme

$$\frac{1\,000 \cdot 999}{2} = 499\,500 \text{ klíčů.}$$

Vidíme tedy, že počet tajných klíčů roste s počtem účastníků dosti rychle. To klade velké nároky na *správu klíčů*: klíče je nejprve potřeba vytvořit, účastníci si je musí vyměnit a poté bezpečným způsobem uložit. A právě ve výměně tajných klíčů tkví hlavní nevýhoda symetrických šifer (tedy i šifry AES). Tato výměna totiž musí probíhat opět zabezpečeně. Jestliže by se Evě podařilo během výměny tajný klíč získat, tak by mohla nerušeně číst jakoukoliv zprávu tímto klíčem zašifrovanou.

Jakým způsobem bezpečnou výměnu klíčů vyřešit? Lákavá možnost by mohla být následující: pokud se chce Alice domluvit s Bobem na nějakém tajném klíči, tak ho může jednoduše zašifrovat (třeba s využitím téže šifry, kterou se chystají zabezpečit samotnou komunikaci). Tím se ale zjevně problém nevyřeší, pouze odsune na jinou úroveň; pro zašifrování tajného klíče se totiž Alice a Bob musí bezpečně domluvit na dalším tajném klíči.

Přibližně do 60. let 20. století, tedy v dobách, kdy šifrování zpráv používala především armáda nebo vládní organizace dané země, se výměna klíčů řešila celkem jednoduše. Komunikující strany se buď osobně setkaly a klíč si vyměnily nebo si zajistily nějakého důvěryhodného kurýra a ten jim výměnu tajného klíče zprostředkoval. Přestože není toto řešení zrovna ideální, v minulosti fungovalo celkem uspokojivě. Situace se však zcela zásadně změnila v okamžiku, kdy se začaly ve větší míře používat počítače

[10] V anglicky psané literatuře se často používá termín *key exchange*, proto budeme také mluvit o *výměně klíče*. Víme však, že klíč pro šifrování i dešifrování je tentýž, takže bychom měli tuto výměnu spíše chápat jako *vzájemné sdělení klíče*. Proto se také můžeme setkat s příhodným označením *key distribution – distribuce klíče*.

v soukromé sféře a pro firmy i běžné uživatele vyvstala nutnost zabezpečit svoji vlastní komunikaci. Osobní setkání komunikujících stran za účelem výměny klíče se stalo prakticky neproveditelné a použití důvěryhodného kurýra příliš zdlouhavé a finančně nákladné. Bylo tedy nezbytně nutné najít nějaký jiný způsob bezpečné výměny tajných klíčů, který by obstál i v nových podmínkách nebo vymyslet zásadně jiný způsob šifrování, který by výměnu klíčů vůbec nevyžadoval.

Bezpečná výměna klíče

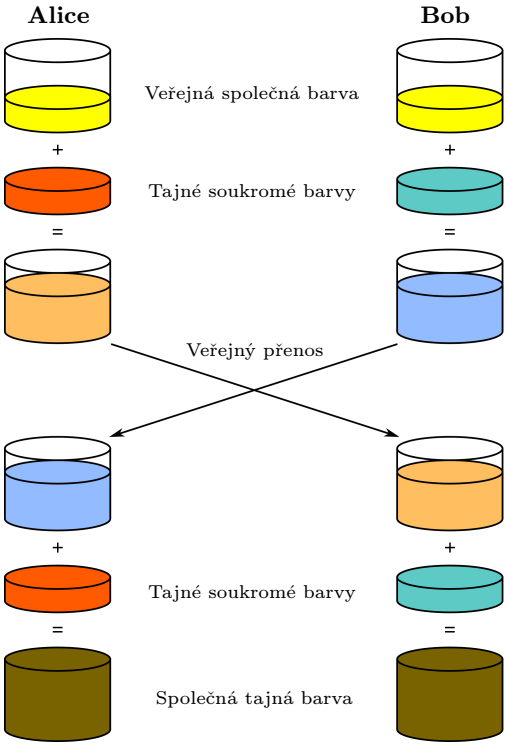
Povězme si nejprve něco o první možnosti – o bezpečné výměně tajného klíče. S velmi zajímavým řešením přišli američtí informatici Ralph Merkle, Whitfield Diffie a Martin Hellman. Tato metoda byla publikována roku 1976 [1], o dvacet let později však vyšlo najevo, že byla objevena již na začátku sedmdesátých let Jamesem Ellisem, Cliffordem Cocksem a Malcolmem Williamsonem. Tito kryptografové ovšem na svůj objev přišli v rámci své práce v britské vládní zpravodajské a špionážní organizaci GCHQ (Government Communications Headquarters) a nemohli tak svůj objev zveřejnit.

Pokusíme se Diffieho–Hellmanovu–Merklovu výměnu klíče (jak je často nazývána) vysvětlit na příkladu, který by byl sice v praxi těžko použitelný, dobře však demonstruje popisovaný princip. Představíme si totiž, že tajným klíčem nebude nějaké číslo, jak tomu bylo doposud, ale bude jím plechovka s barvou určitého odstínu. Bezpečnost šifrování tedy bude založena na obtížnosti uhádnout odstín této barvy.

Postup výměny tajné barvy je znázorněn na obr. 1. Tento obrázek je rozdělen do dvou sloupců, v levém jsou zobrazeny barvy, jež má k dispozici Alice v jednotlivých krocích výměny, v pravém sloupci jsou pak uvedeny barvy, které získává v jednotlivých krocích Bob. Barva, na které se Alice a Bob potřebují dohodnout, je hnědá, zobrazená vespod obrázku.

Proces výměny začne tím, že se Alice a Bob dohodnou na nějaké společné barvě; na obrázku je tato barva zobrazena na prvním řádku, jedná se tedy o žlutou barvu. Tato společná barva může být zvolena náhodně a Alice a Bob se na ní mohou dohodnout nezabezpečeně. Je tedy lhostejno, zdali se Eva dozví, že se jedná o žlutou barvu či nikoliv. V dalším kroku (zachyceném na druhém řádku obrázku) si Alice i Bob zvolí svoji vlastní tajnou barvu. V našem případě si Alice zvolila červenou barvu, Bob zelenou barvu. Svoji vlastní tajnou barvu si Alice i Bob mohou zvolit náhodně, je však nezbytně nutné, aby obě tyto tajné barvy zůstaly utajené. Poté

Alice smíchá společnou žlutou barvu se svojí tajnou barvou (červenou) a stejně tak Bob smíchá společnou barvu se svojí tajnou barvou (zelenou). Smícháním získají novou barvu – Alice béžovou, Bob modrou.



Obr. 1 Diffieho–Hellmanova–Merklova výměna tajného klíče (zdroj: Wikipedia https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange)

V dalším kroku si Alice a Bob tyto smíchané barvy vymění (výměna může proběhnout nezabezpečeně). Alice tedy obdrží modrou barvu, Bob béžovou; na obrázku je tento moment zachycen na čtvrtém řádku. Posledním krokem je přidání tajné barvy do takto vyměněné barvy: Alice smíchá červenou barvu s modrou, získá tak hnědou barvu, Bob smíchá zelenou barvu s béžovou a získá také hnědou barvu.

Jak je možné, že Alice i Bob získají na konci výměny stejnou barvu? Zdůvodnění je snadné a pozorný čtenář je jistě uviděl v průběhu čtení předchozích dvou odstavců. Stačí sledovat, jakým způsobem „cestuje“ schéma-

tem společná barva zvolená na začátku:

1. společná (žlutá) barva na straně Boba byla nejprve smíchána s Bobovou tajnou barvou (zelenou), pak byla poslána na stranu Alice, kde byla smíchána s její tajnou barvou (červenou);
2. společná (žlutá) barva na straně Alice byla smíchána s její tajnou barvou (červenou), poslána Bobovi, který ji smíchal se svojí tajnou barvou (zelenou).

Jak můžeme vidět, v obou dvou případech byla společná (žlutá) barva smíchána s oběma tajnými barvami (červenou a zelenou). Jediný rozdíl mezi body 1 a 2 je v tom, že jsou tajné barvy přidány v opačném pořadí. Výsledek smíchání však musí být totožný, v našem příkladě je jím hnědá barva.

Můžeme si také všimnout, že pokud bude Eva odposlouchávat komunikaci mezi Alicí a Bobem, pak získá společnou (žlutou) barvu a barvy, které vznikly přidáním tajných barev do této společné barvy (modrou a béžovou). Bez znalosti aspoň jedné z tajných barev však nikdy nedospěje k výsledné (hnědé) barvě, která představuje tajný klíč.

Jak bylo řečeno v úvodu této sekce, zvolený příklad s mícháním barev by byl v praxi nepoužitelný. Ve skutečné Diffieho–Hellmanově–Merklově výměně klíče se proto nemíchají barvy, ale jistým způsobem se „míchají“ čísla. V tento okamžik je nad naše znalosti vysvětlit toto „míchání“ čísel podrobně, v příštím díle ovšem požadované znalosti získáme a k Diffieho–Hellmanově–Merklově výměně klíče se ještě krátce vrátíme.

Zámek, který se zamyká jedním a odemyká jiným klíčem

Přejděme nyní k šifrování, které výměnu tajného klíče vůbec nepotřebuje. Začneme tím, že se zkusíme podívat na symetrické šifrování trochu jinýma očima: Alice chce poslat zprávu Bobovi, napíše ji tedy na papír a zamkne ji do skříňky. Zamčení zprávy do skříňky odpovídá jejímu zašifrování. Pro jednoduchost předpokládáme, že skříňka je nerozbitná, a že je možné ji otevřít pouze použitím (jediného) správného klíče. Tento klíč je vlastně tajným klíčem, o kterém jsme se bavili doposud. Alice po uzamčení pošle skříňku Bobovi třeba obyčejnou poštou. Pro Evu nemusí být obtížné skříňku během její cesty od Alice k Bobovi získat, pokud ji však získá, tak ji bez klíče neotevře (leda, že by vyráběla klíče různých tvarů a zkoušela, jestli jeden z nich zámek neodemkne). Naopak Bob, jakožto právoplatný příjemce, musí mít možnost skříňku otevřít (tedy zprávu dešifrovat). Musí

mít proto k dispozici kopii stejného klíče, jako má Alice. Na podobě tajného klíče se však Alice s Bobem musí nějak domluvit, čímž se vracíme k problému výměny klíče.

Otázka tedy zní: nebylo by možné zkonstruovat skříňku s naprosto novým typem zámku, který by se zamykal jedním, ale odemykal zcela jiným klíčem? Bob by byl jediným vlastníkem klíče pro odemykání zámku (dešifrování zprávy), proto se tomuto klíči říká *soukromý*. Klíč určený pro zamykání zámku (šifrování zpráv) by mohl Bob komukoliv poskytnout, třeba tak, že by na svých webových stránkách zveřejnil detailní popis jeho tvaru. Alice (nebo kdokoliv jiný, kdo by chtěl Bobovi poslat zprávu) by si podle návodu klíč vyrobila o mohla ho použít pro uzamčení zprávy. Tento klíč se proto nazývá *veřejný*.

Celý vtip tkví v tom, že rozdělením tajného klíče na klíč soukromý a veřejný tak naprosto odpadá nepohodlná, nákladná a nebezpečná[11)] správa tajných klíčů.

Tomuto způsobu šifrování se často říká *šifrování s veřejným klíčem* nebo také *asymetrické šifrování*. U zrodu asymetrických šifer opět stáli, nám už známí, Whitfield Diffie a Martin Hellman.

Zbývá tedy nějakou konkrétní šifru s veřejným klíčem zkonstruovat. Pokud bychom zůstali u našeho mechanického příměru se skříňkou uzamykatelnou jedním klíčem a odemykatelnou druhým (jiným) klíčem, tak taková konstrukce překvapivě existuje a je velmi jednoduchá. Jedná se o skříňku, která se sama uzamkne pouhým zaklapnutím dvířek. Veřejný klíč sice nemá fyzickou podobu – v tomto případě je jím znalost toho, jak dvířka zaklapnout – to však na podstatě věci nic nemění. Klíč, který skříňku odemyká, musí být vlastněn pouze zamýšleným příjemcem skříňky, a je tedy výše zmíněným soukromým klíčem.[12)]

Tímto jednoduchým nápadem jsme však problém zdaleka nevyřešili. Přenést ho do světa počítačového šifrování (to znamená, najít vhodnou šifrovací a dešifrovací funkci) totiž není vůbec snadné a informatikům trvalo poměrně dlouhou dobu, než se jim to podařilo.

Na začátku stálo jedno důležité pozorování. Zamknutí skříňky pomocí veřejného klíče (zaklapnutí dvířek) a odemknutí skříňky pomocí soukro-

[11)] Nebezpečná v tom smyslu, že kurýr nemusí být tak důvěryhodný, jak se Alice s Bobem domnívali a že tedy může tajný klíč vyzradit.

[12)] Ještě jednodušším příkladem takového systému je obyčejná poštovní schránka. Kdokoliv do ní může vhodit dopis, ale pouze pověřený zaměstnanec pošty má (soukromý) klíč, kterým se schránka odemyká. Poštovní schránka tak realizuje bezpečný přesun dopisu mezi odesilatelem a poštou.

mého klíče je snadno a rychle proveditelnou akcí. Odemknutí skříňky pouze se znalostí veřejného klíče (se znalostí, jak zaklapnout dvířka) je však velmi obtížné. Stejně tak šifra, kterou se snažíme zkonstruovat, by měla vypadat tak, že šifrování pomocí veřejného klíče a dešifrování pomocí soukromého klíče by mělo být jednoduché a rychlé; dešifrování se znalostí veřejného klíče by však mělo být obtížné, v ideálním případě nemožné.

Převedeno do řeči matematických funkcí, které takovou šifru popisují, to znamená, že:

1. pro zvolené číslo x a veřejný klíč k_e[13)] musí být výpočet hodnoty šifrovací funkce $y = e(x, k_e)$ snadný;
2. pokud budeme znát zašifrované číslo y a soukromý klíč k_d, tak výpočet původní hodnoty $x = d(y, k_d)$ musí být také snadný;
3. výpočet čísla x pouze ze znalosti zašifrovaného čísla y a veřejného klíče k_e – jinými slovy, výpočet takového x, aby platilo $y = e(x, k_e)$ – musí být obtížný.

Protože je výpočet hodnoty šifrovací funkce e „v jednom směru“ (bod 1) snadný a „v opačném směru“ (bod 3) obtížný, je taková šifrovací funkce nazývána *jednosměrnou funkcí*. K původní hodnotě x se tak můžeme dostat pouze s využitím soukromého klíče (bod 2), kterému se proto někdy říká *zadní vrátka*.

Dokážeme najít vhodného kandidáta jednosměrné funkce se zadními vrátky? Pokusme se nejprve zamyslet třeba nad funkcí

$$e(x, k_e) = k_e \cdot x.$$

Veřejným klíčem k_e bude například číslo 2. Ptáme se tedy, jestli funkce, která danému x přiřadí číslo $2x$, splňuje podmínky kladené na jednosměrnou funkci. Výpočet v jednom směru (tedy výpočet dvojnásobku zadaného čísla) je jistě snadný a rychlý. Výpočet v opačném směru (tedy vydělení zadaného čísla dvěma) je ovšem také rychlý. Čtenář by mohl namítnout, že pro obrovská čísla násobení a dělení rychlé není. Zde však *rychlost výpočtu* chápeme následujícím způsobem: pro násobení a dělení máme k dispozici

[13)] Zopakujme si, že uvažujeme dva klíče – jeden veřejný určený pro šifrování, druhý soukromý určený pro dešifrování. Tyto klíče je potřeba ve výpočtech nějakým způsobem odlišit, proto již nemůžeme používat jediný symbol k. Index e v symbolu k_e je opět odvozen od slova *encipher*, česky *šifrovat*. Čtenář se jistě dovtípí, že soukromý klíč budeme značit symbolem k_d.

postup, pomocí kterého jsme schopni daný výpočet úspěšně provést v několika krocích tak, že zvětšováním zadaných čísel počet těchto kroků *nebude dramaticky růst*. Tímto postupem[14)] je známé násobení a dělení „v ruce“, jak jsme se mu naučili na základní škole. Zmíněná funkce tedy není jednosměrná a pro konstrukci šifry s veřejný klíčem je tedy nepoužitelná.

Zkusme jinou funkci, řekněme

$$e(x, k_e) = x^{k_e}.$$

Za veřejný klíč opět zvolíme číslo 2. Pokud tedy šifrujeme nějaké konkrétní číslo x, pak pouze vypočítáme hodnotu druhé mocniny čísla x, čímž získáme zašifrované číslo y. Výpočet druhé mocniny (to znamená, násobení čísla sebou samým) je – jak už dobře víme – rychle proveditelné. Jestliže naopak chceme získat ze zadaného zašifrovaného čísla y jemu odpovídající číslo x, musíme vypočítat druhou odmocninu čísla y. Výpočet druhé odmocniny je však opět možné provést poměrně rychle například s pomocí *metody bisekce*.[15)]

Nalezení vhodného kandidáta jednosměrné funkce se zadními vrátky se zdá být obtížné. Ve skutečnosti jsme se však druhým, výše uvedeným příkladem k tomuto kandidátovi přiblížili – je jím opravdu funkce $e(x, k_e) = x^{k_e}$, na umocnění se ovšem musíme podívat pohledem takzvané *modulární aritmetiky*, které jsme se lehce dotkli při vysvětlování „přetečení“ při sčítání v rovnici (1). Zmíněná funkce se často nazývá RSA funkcí, protože stojí v samotném základu asymetrického šifrování RSA.

Stručné zdůvodnění, proč je RSA funkce vhodným kandidátem je takové, že modulární aritmetika se chová oproti běžně používané aritmetice velmi nepravidelně. Abychom však tomuto zdůvodnění byli schopni lépe porozumět, bude nutné podrobněji si vysvětlit, jak vlastně modulární aritmetika funguje. Příští díl tedy začneme vysvětlením modulární aritmetiky; poté budeme moci přejít k vysvětlení šifrování RSA a k některým jeho aplikacím (například v elektronickém podpisu).

[14)] V informatice takovému postupu říkáme *algoritmus*.

[15)] Této metodě se také někdy říká *metoda půlení intervalu*. V rychlosti (a značně zjednodušeně) si ji popíšeme na následujícím příkladu. Chceme vypočítat $\sqrt{576}$. Začneme tím, že výsledek odhadneme, řekněme, že jím bude číslo 21. Druhá mocnina z 21 je 441, což je méně než požadovaných 576. Odhad proto zvětšíme, třeba na číslo 26. To je však příliš, protože 26^2 je 676. Odhad tedy zmenšíme, například na číslo 24, což už je správný výsledek. Poznamenejme, že ve skutečnosti se čísla nehádají, ale stanovují jako prostředek intervalu daného hodnotami vypočtenými v předchozím kroku. Zvídavého čtenáře odkážeme na knihu od Donalda Knutha [2].

Literatura

[1] *Diffie, W., Hellman, M.*: New directions in cryptography. IEEE Transactions on Information Theory, roč. 22 (1976), č. 6, s. 644–654.

[2] *Knuth, D. E.*: The Art of Computer Programming, Volume 3: Sorting and Searching. Addison-Wesley, 1998.

[3] *Levy, S.*: Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age. Penguin Books, 2001.

[4] *Singh, S.*: Kniha kódů a šifer: Tajná komunikace od starého Egypta po kvantovou kryptografii. Argo, Dokořán, 2003.

Dva základní šifrovací principy

MIROSLAV KOLAŘÍK

Přírodovědecká fakulta UP, Olomouc

Ukážeme si základní principy ze zajímavé a stále se rozvíjející oblasti informatiky – z kryptologie.[1)] Kryptologie zahrnuje kryptografii a kryptoanalýzu. Kryptografie se zabývá metodami utajení (říkáme také šifrováním) obsahu zpráv; toto utajení se provádí tak, že se zpráva převede do podoby, která je srozumitelná pouze zamýšlenému příjemci. Kryptoanalýza se zabývá luštěním zašifrovaných zpráv (dešifrováním).

První kryptografické metody se objevily už ve starověkém Řecku a až do začátku 20. století byly založené na jednoduchých principech. Představíme si dva základní šifrovací principy: substituci a transpozici. Jedná se o jednoduché a přitom zásadní šifrovací metody, které se využívají i u moderních kryptografických metod, jako jsou například DES nebo AES. Šifrovací principy demonstrujeme na několika jednoduchých příkladech, které mohou být použity při výuce na základních a středních školách.

Substituční šifry

Jako první se budeme věnovat substituci, neboli záměně (náhradě). Začneme pěkně zvolna jednoduchým příkladem. Představme si situaci, že

[1)] Kryptologie je naukou o metodách utajování zpráv i o tom, jak zašifrované zprávy luštit (dešifrovat).

chceme zašifrovat text „INFORMATIKA JE SUPER“. Použijeme k tomu následující tabulku, ve které snadno najdeme všechna písmena anglické abecedy, a jak je zašifrovat. Jednoduše, horní písmeno z každého pole tabulky zašifrujeme písmenem ležícím pod ním (ve stejném poli), přičemž mezeru neměníme.

A	B	C	D	E	F	G	H	I
G	N	O	C	S	W	L	Z	F
J	K	L	M	N	O	P	Q	R
V	A	K	H	R	U	Q	B	Y
S	T	U	V	W	X	Y	Z	
T	X	E	D	M	P	I	J	

Například písmeno I zašifrujeme jako F, podobně písmeno N zašifrujeme jako R a text „INFORMATIKA JE SUPER“ zašifrujeme na text „FRWUYHGXFAG VS TEQSY“. Pro jednoduchost budeme v příkladech vynechávat háčky, čárky a také kroužky. Proto v tabulkách uvádíme pouze písmena anglické abecedy.

Opusťme naši první tabulku a podívejme se na jiný způsob, jak lze nahradit anglická písmena pomocí posloupnosti symbolů, tentokrát tvořených tečkami a čárkami.

A	B	C	D	E	F	G	H	I
.-	-...	-.-.	-..	.	..-.	--.	....	..
J	K	L	M	N	O	P	Q	R
.---	-.-	.-..	--	-.	---	.--.	--.-	.-.
S	T	U	V	W	X	Y	Z	
...	-	..-	...-	.--	...-	-.--	--..	

S využitím druhé tabulky a dohody, že jednotlivá písmena od sebe oddělíme symbolem | (přičemž mezery vynecháme), zakódujeme text „INFORMATIKA“ na tvar „|..|-.|...-.|---|.-.|--|.-|-|..|-.-|.-|“. Pozorný čtenář jistě poznal Morseovu abecedu. Ano, i na morseovku je možné nahlížet jako na substituční šifru.[2)] Toto kódování vymyslel ame-

[2)] Morseovu abecedu však nepoužíváme proto, abychom zprávu utajili, ale pouze *kódovali*, tedy převedli do tvaru, se kterým umí pracovat dané technické zařízení. V případě Morseova kódu je tímto zařízením elektrický telegraf.

rický vynálezce, malíř a sochař Samuel Morse. Ten také uskutečnil v roce 1844 první telegrafické spojení mezi Washingtonem a Baltimorem. Znaky zvolil tak, aby v angličtině nejfrekventovanějším písmenům odpovídaly nejkratší sekvence teček a čárek. Na podobné optimalizaci, kdy nejčastěji používaným znakům je přiřazen nejkratší kód, je založeno také tzv. Huffmanovo kódování, viz např. [1].

Písmena můžeme nahrazovat i nepísmennými symboly, třeba obrázky nebo čísly. Jako ukázka poslouží následující tabulka, ve které jsou písmena anglické abecedy nahrazena jednoduchými obrázky a také je jim přiřazena odpovídající číselná hodnota tzv. ASCII kódu.

A	B	C	D	E	F	G	H	I
♣	☺	★	♯	©	♠	⊗	⇳	∗
65	66	67	68	69	70	71	72	73
J	K	L	M	N	O	P	Q	R
•	⊛	□	☾	≺	♡	≻	Φ	☹
74	75	76	77	78	79	80	81	82
S	T	U	V	W	X	Y	Z	
⊞	⋈	◎	☻	Θ	⇜⇝	§	♢	
83	84	85	86	87	88	89	90	

S využitím této tabulky převedeme slovo „ALGORITMUS“ na „♣□⊗♡☹∗⋈☾◎⊞“ a na číslo „65767179827384778583“. Samozřejmě můžeme nahrazovat i nepísmenné symboly (čísla, mezery, atd.) libovolnými symboly. Však také (volně řečeno) v informatice se pro počítač vše převádí na posloupnosti nul a jedniček.

Jak substituční šifru dešifrovat?

Podívejme se nyní, jak lze jednoduchou substituční šifru dešifrovat. Využijeme toho, že některá písmena se obvykle vyskytují častěji než jiná. Třeba v angličtině se mnohem častěji objeví písmeno E než písmeno Z. My se zaměříme podrobněji na češtinu. Typický výskyt písmen v běžném (dostatečně dlouhém) českém textu rozdělíme do následujících tří skupin:

- nejčastější výskyt (více než pět procent): E, A, O, I, L, N, S, T,
- běžný výskyt (mezi třemi a pěti procenty): D, K, M, P, R, U, V, Z,

- nejméně častý výskyt (méně než tři procenta): Q, X, W, F, G, B, C, H, J, Y.

Dělení je bez diakritiky (nerozlišujeme mezi E, É a Ě, atp.). Nejčastěji se v českém jazyce vyskytují samohlásky E, A a O, všechny s více než osmiprocentní pravděpodobností. Nejméně časté jsou pak souhlásky Q, X, W, F a G s méně než $\frac{1}{4}$procentní pravděpodobností výskytu. Jak lze takové pravděpodobnosti získat? Můžete si to vyzkoušet sami. Sežeňte si český, dostatečně dlouhý text. Čím delší, tím lepší, řekněme, s minimálně desetitisíci znaky. Poté zjistěte výskyty jednotlivých písmen a uvidíte, že to bude hodně podobné s rozdělením výše. Budeme-li nyní dešifrovat nějaký český, jednoduchou substitucí zašifrovaný text, můžeme s výhodou frekvenční analýzu použít. Můžete si to promyslet na konkrétní úloze. Jak bývá zvykem, budeme nyní psát písmena otevřeného (vyluštěného) textu malá a písmena zašifrovaného textu velká.

Úkol 1

Dešifrujte následující text:
ICM ZHVYNAM YJLJYJ YNRYH EN UNZDM UGLJWAN UFMY U IJYSF DNFNCG DNFM ENWAJYZMUGDM VZJUG. ASICMQZSW ENWAJIMVDNAAGKL VZJU EN UNZDM DSZJ, ANFANZN ICNWZJFQG S VIJEQG S S M. VASWAJ YSQ XCFG HLJWANDN ANQYNCS IMVDNAS. WSZN VN DHFNDN FSDNCMY YCNXS AS WUJEMKN IMVDNA S UGHFMY YJLJ, FN ANQYNCN EVJH KSVYN S ANQYNCN VN ANUGVQGYHEM UHXNK. ASVZNWAN KNZQJUN WJZHVYNAM XGUS LJWAN CGKLZN, ICJYJFN ZFN VASWAJ WJIZAJUSY KLGXNEMKM IMVDNAS KNZGKL VZJU.

Řešení. Víme, že jde o český text (bez diakritiky), který byl zašifrován substitucí. Přestože je krátký, získáme frekvenční analýzu všech jednotlivých symbolů. Výsledek absolutní četnosti všech 356 písmenných znaků je znázorněn v následující tabulce.

A	B	C	D	E	F	G	H	I
27	0	12	14	9	13	15	9	11
J	K	L	M	N	O	P	Q	R
27	10	9	21	53	0	0	9	1
S	T	U	V	W	X	Y	Z	
23	0	16	18	14	5	21	19	

Nejčastěji se v šifrovém textu vyskytuje písmeno N, je to tedy horký kandidát na písmeno e v otevřeném textu. Hodně často se vyskytují i písmena A, J a S. Písmeno A se v jednom slově v šifře vyskytuje dvakrát za sebou, nabízí se proto, že by se v otevřeném textu mohlo jednat o písmeno n. Písmeno S se v šifrovém textu vyskytuje několikrát jako samotné jednopísmenné slovo, bude se proto v otevřeném textu nejspíše jednat o písmeno a. Nahradíme-li v šifrovaném textu tato tři písmena a podíváme se na mezivýsledek, snadno odhadneme, že často se vyskytující J bude v otevřeném textu samohláska, nejspíše o. Dostáváme tak slibný mezivýsledek a můžeme pokračovat dále.

Samozřejmě se občas stane, že nějaké písmeno (nějaká písmena) netipneme hned správně. Později ale začnou vycházet nesmysly, což nás přirozeně navede na změnu tak, aby výsledná zpráva dávala smysl. Celý otevřený text vypadá takto: *pri lusteni tohoto textu je velmi vyhodne vzit v potaz mezery mezi jednotlivymi slovy. napriklad jednopismennych slov je velmi malo, neznele predlozky a spojky a a i. snadno tak brzy uhodneme nektera pismena. dale se muzeme zamerit treba na dvojice pismen a vyuzit toho, ze nektere jsou caste a nektere se nevyskytuji vubec. nasledne celkove dolusteni byva hodne rychle, protoze lze snadno doplnovat chybejici pismena celych slov.*

Níže je uvedena tabulka, převádějící písmena šifrového textu (velká) na písmena otevřeného textu (malá). Čtyři písmena nebyla použita (jsou u nich uvedeny otazníky), konkrétně: f, g, q, w, což dobře koresponduje s frekvenční analýzou českého jazyka.

Poznamenejme, že pro ztížení dešifrování substitučních zpráv bývá zvykem psát text bez interpunkce, po pěti znacích oddělených mezerou. Tento zvyk se používá od poloviny 19. století a souvisí s telegrafováním, kde se platilo za slovo, přičemž průměrná délka slov u většiny evropských jazyků je právě pět znaků. Pro názornost, začátek šifrového textu z prvního úkolu by vypadal takto: ICMZH VYNAM YJLJY JYNRY HENUN atd.

A	B	C	D	E	F	G	H	I
n	?	r	m	j	z	y	u	p
J	K	L	M	N	O	P	Q	R
o	c	h	i	e	?	?	k	x
S	T	U	V	W	X	Y	Z	
a	?	v	s	d	b	t	f	

Transpoziční šifry

Dalším základním šifrovacím principem je šifrování pomocí transpozice (přesunu). Opět začneme ukázkovým příkladem.

Mějme text „TRANSPOZICE SPOČÍVÁ VE ZMĚNĚ POŘADÍ ZNAKŮ DLE URČITÉHO PRAVIDLA“. Z daného textu odstraníme interpunkci a mezery a napíšeme jej do tabulky o sedmi sloupcích. Poznamenejme, že počet sloupců můžeme zvolit náhodně (s ohledem na délku textu).

T	R	A	N	S	P	O
Z	I	C	E	S	P	O
C	I	V	A	V	E	Z
M	E	N	E	P	O	R
A	D	I	Z	N	A	K
U	D	L	E	U	R	C
I	T	E	H	O	P	R
A	V	I	D	L	A	

K zašifrování nyní stačí psát zprávu po jednotlivých sloupcích. Dostaneme tak text ve tvaru „TZCMAUIARIIEDDTVACVNILEINEAEZE HDSSVPNUOLPPEOARPAOOZRKCR“, který je na první pohled nesrozumitelný. Provedli jsme transpozici tak, že jsme ponechali původní písmena a jen změnili jejich pozice. Abychom ztížili možnost dešifrovat text, vyzkoušíme psát sloupce v různém pořadí. Použijeme k tomu nějaké sedmipísmenné slovo, řekněme „TELEFON“. Abecední pořadí písmen ve slově „TELEFON“ nám určí, který sloupec budeme psát první, který druhý atd. V našem příkladu budeme psát nejprve druhý sloupec a po něm hned čtvrtý, protože se pojí s písmenem E. Další v abecedě je písmeno F, a proto přepíšeme pátý sloupec, dále je písmeno L a tedy třetí sloupec, atd. Dostaneme tak text „RIIEDDTVNEAEZEHDSSVPNUOLACVNILEIO OZRKCRPPEOARPATZCMAUIA“.

Jinou možností je přepsat písmena z tabulky dle určitého vzoru, třeba podle tvaru spirály. Začneme-li vlevo nahoře a vydáme se směrem dolů a dále pak po obvodu (jak ukazují čísla v následující tabulce), obdržíme text ve tvaru „TZCMAUIAVIDLARCKRZOOPSNARIIEDDTEHOPRAOEP SECVNILEUNPVAEZ“.

1	26	25	24	23	22	21
2	27	44	43	42	41	20
3	28	45	54	53	40	19
4	29	46	55	52	39	18
5	30	47	56	51	38	17
6	31	48	49	50	37	16
7	32	33	34	35	36	15
8	9	10	11	12	13	14

Napsání textu pozpátku je dalším jednoduchým příkladem transpoziční šifry. Nebo třeba psaní nejprve písmen na lichých pozicích, pak na sudých pozicích. Příkladem je také tzv. skytalé. Tento historický šifrovací princip využívá válce a pásku papíru (dříve pergamenu). Páska papíru se postupně namotá na válec a až je namotaná napíše se na ni (ve směru osy válce) vzkaz. Po odmotání jsou písmena na pásce přemístěna a text se stává (na první pohled) nesrozumitelným. Nejrychleji se zpráva vyluští namotáním na válec o stejném průměru, jako měl původní válec. K dešifrování lze použít i kužel, na který se páska namotá, a poté se po něm posouvá do té doby, než se objeví smysluplné slovo. Tento druh šifrování používali Sparťané během válek.

Další hodně jednoduchou šifru, která přepisuje písmenka „cik-cak“ si demonstrujeme na tabulce s dvěma řádky a jedenácti sloupci. Samozřejmě pro jiné rozměry není těžké šifrovací algoritmus adekvátně pozměnit.

1	21	3	19	5	17	7	15	9	13	11
22	2	20	4	18	6	16	8	14	10	12

Zprávu nejprve přepíšeme po řádcích. Čísla v tabulce udávají pořadí přepisu jednotlivých písmen zprávy. Budeme-li chtít zašifrovat konkrétní zprávu „ENIGMA JE SIFROVACI STROJ“, tak ji nejprve po řádcích zapíšeme do tabulky.

E	N	I	G	M	A	J	E	S	I	F
R	O	V	A	C	I	S	T	R	O	J

Poté text dle „cik-cak“ postupu jednoduše přepíšeme na „EOIAMIJT SOFJIRESACGVNR“ a zašifrovaný text je hotový.

Jako poslední jednoduchou ukázku transpoziční šifry uvedeme zašifrování textu „ENIGMA JE STROJ“ pomocí tabulky o rozměrech 13×4 polí. Text napíšeme předem dohodnutým způsobem, například jako v následující tabulce, a poté jej přepíšeme po jednotlivých řádcích.

E						J						J
	N				A		E				O	
		I		M				S		R		
			G						T			

V našem případě obdržíme šifrový text ve tvaru „EJJNAEOIMSRGT“.

Otočná mřížka

Nyní se zaměříme na tzv. Fleissnerovu otočnou mřížku. Tuto transpoziční šifru popsal jako první Fleissner von Wostrowitz v roce 1881. K šifrování a dešifrování se používá pomůcka: čtvercová tabulka, ve které jsou na vybraných místech vystřihnuty malé čtverce. Například v následující tabulce velikosti 5×5 jsme čísly vyznačili vystřižené (malé) čtverce.

1				
				2
			3	
	4			5
		6		

Čtverce se vystřihují tak, aby se při postupné rotaci celého velkého čtverce (doprava o 90, 180 a 270 stupňů) vystřižené (malé) čtverce nikdy nepřekryly. Text zprávy se pak postupně vpisuje do vystřižených (malých) čtverců a po jejich zaplnění se mřížka otočí o 90 stupňů směrem doprava. S naší ukázkovou otočnou mřížkou tak můžeme zašifrovat zprávu o 24 symbolech. Jejich umístění znázorňují čísla 1 až 24 v následující tabulce. Prostřední políčko zůstalo prázdné a nebude se využívat. Šifrový text vytvoříme jednoduše tak, že jej čteme po jednotlivých řádcích.

1	19	13	20	7
14	8	21	15	2
9	16		3	22
17	4	10	23	5
24	11	6	12	18

Ukažme si postup na konkrétním příkladě. Chceme zašifrovat zprávu ve tvaru „NOTEBOOK – PŘENOSNÝ POČÍTAČ“. Použijeme k tomu výše uvedenou pomocnou otočnou mřížku velikosti 5×5. Po doplnění textu (bez mezer a diakritiky) obdržíme tuto tabulku:

N	O	N	C	O
O	K	I	S	O
–	N		T	T
Y	E	P	A	B
C	R	O	E	P

Nyní již lehce vytvoříme šifrový text. Přepsáním po jednotlivých řádcích dostáváme „NONCOOKISO–NTTYEPABCROEP“.

Pochopení principu otočné mřížky si můžete ověřit na následujícím úkolu. Šifrový text vznikl pomocí Fleissnerovy otočné mřížky velikosti 4×4. Napovíme, že v každém řádku mřížky je právě jeden vystřižený (malý) čtverec.

Úkol 2

Získejte heslo z následujících 16 písmen: „EOHSBLIEOMSJLVET“.

Řešení. Víme, že šifrový text vznikl pomocí Fleissnerovy otočné mřížky velikosti 4×4. Z nápovědy také víme, že v každém řádku mřížky je právě jedno vystřižené políčko. Uspořádáme-li šifrový text do mřížky obdržíme následující:

E	O	H	S
B	L	I	E
O	M	S	J
L	V	E	T

V prvním řádku bude počáteční písmeno otevřeného textu. Víme, že ve druhém řádku najdeme druhé písmeno otevřeného textu, ve třetím řádku bude třetí písmeno otevřeného textu a ve čtvrtém řádku najdeme čtvrté písmeno otevřeného textu. Otevřený text má být smysluplný, což nám hodně slepých cest eliminuje. Například vybereme-li E z prvního řádku, nebudeme vybírat E z druhého řádku, protože by otevřený text začínající písmeny „EE“ nedával smysl. Podobně můžeme s velkou jistotou okamžitě vyloučit trojice „OIJ“, „SLJ“, „EBM“. Při určování prvních čtyř písmen otevřeného textu je určitě užitečné pracovat s principem šifry – s otáčením mřížky vždy po sepsání čtveřice písmen. Například, vybereme-li jako první písmeno otevřeného textu písmeno O, nebo H, tak víme, která další tři písmena nebudou na druhé, třetí a čtvrté pozici v otevřeném textu. Podaří-li se nám správně určit první čtyři písmena, máme celý klíč k šifře, neboť tak známe polohu všech čtyř vystřižených políček v naší mřížce. Po těchto úvahách lze poměrně rychle získat otevřený text: „HESLEMJESLOVOBIT“. Správnou odpovědí je tedy slovo „BIT“.

Závěr

Představili jsme si dva základní šifrovací principy: SUBSTITUCI při které se znaky otevřeného textu nahrazují šifrovými symboly a TRANSPOZICI, kde se mění pořadí znaků otevřeného textu. Oba tyto principy se používají i v dnešní době – jejich vhodnou kombinací vznikají silné šifry. Dalším šifrovacím principem je například steganografie (ukrývání zpráv). Úkolem steganografie je skrýt samotnou existenci zpráv. Ke steganografickým metodám patří použití neviditelného inkoustu, nenápadné vyznačení písmen v jinak nezávadném textu, ukrytí znaků otevřeného textu na domluvených pozicích, ukrytí zprávy v obrázku na internetu, použití mikroteček apod. Pomocí počítače lze informaci ukrýt, například do obrázku, do audiosignálu, do videa. Ale o tom třeba někdy příště.

Literatura

[1] *Bartl, E.*: Teorie informace, MFI, roč. 24 (2015), č. 3, s. 219–228.

ZPRÁVY

11. středoevropská matematická olympiáda

Dějištěm 11. ročníku Středoevropské matematické olympiády (MEMO), která se konala 21. – 27. srpna 2017, byl litevský Vilnius. Soutěže se tradičně zúčastnilo 60 soutěžících z deseti středoevropských zemí (Švýcarska, Německa, Slovinska, Chorvatska, Maďarska, Slovenska, Rakouska, Polska, České republiky a pořádající Litvy), ale kromě nich také šestice žáků z hostujícího Běloruska. Každou zemi reprezentovali žáci, kteří v uplynulém školním roce nematurovali.

České reprezentační družstvo bylo složeno ze dvou vítězů a čtyř úspěšných řešitelů ústředního kola 66. ročníku v kategorii A. Byli jimi: *Filip Svoboda* (3/4 G Brno, Elgartova), *Radek Olšák* (6/8 Mensa G, Praha), *Josef Minařík* (6/8 G Brno, Kpt. Jaroše), *Matěj Doležálek* (6/8 G Humpolec), *Tomáš Perutka* (7/8 G Brno, Kpt. Jaroše) a *Jiří Škrobánek* (7/8 WG Ostrava-Poruba). Vedoucím české delegace a jejím zástupcem v jury byl *Michal Rolínek, PhD.,* z IST Austria ve Vídni, pedagogickým vedoucím družstva byl *Mgr. Radek Horenský, Ph.D.,* z Gymnázia Šternberk.

Den před soutěží vybrala po vyčerpávajících jednáních mezinárodní jury všech 12 soutěžních úloh, tedy čtyři do individuální soutěže a osm do soutěže týmů. Individuální soutěž se konala 23. srpna, týmová soutěž proběhla dne následujícího. Soutěžní prostory, jakož i zázemí pro jednání jury, poskytla matematicko-fyzikální fakulta místní univerzity.

Následující dva dny po soutěži jednotlivců probíhala koordinace soutěžních úloh za přítomnosti vedoucích národních týmů. Každá soutěžní úloha byla přitom hodnocena nejvýše 8 body. Soutěžící se mezitím se svými místními průvodci vydali na nedaleký hrad Trakai, na prohlídku vilniuského energeticko-technologického muzea a dalšího dne také do etnografického muzea ve vesničce Rumšiškes nedaleko Kaunasu. Poslední den si užili zábavy ve Vichy aqua parku ve Vilniusu.

Nyní k výsledkům. V soutěži jednotlivců bylo letos uděleno 7 zlatých, 10 stříbrných a 18 bronzových medailí, v soutěži týmů pak po jedné sadě každého druhu. Z hlediska české výpravy lze považovat za přijatelné výsledky individuální. Největšího úspěchu, stříbrné medaile, dosáhl *Matěj Doležálek*, jemuž smolně o jediný bod utekla medaile zlatá. Dva bronzové zásahy zaznamenali *Josef Minařík* a *Filip Svoboda*. Poslední z našich oceněných studentů *Radek Olšák* odjel s čestným uznáním. Výkon českého družstva v týmové soutěži už tak podařený nebyl, výsledkem bylo sdílené předposlední místo.

Podrobnější informace doplněné o fotogalerie ze soutěže mohou zájemci nalézt na oficiálních stránkách 11. MEMO (memo2017.lmnsc.lt).

Na závěr uvádíme texty všech soutěžních úloh.

Soutěž jednotlivců
(23. srpna 2017)

Příklad I–1

Určete všechny funkce $f\colon \mathbb{R} \to \mathbb{R}$ takové, že

$$f(x^2 + f(x)f(y)) = xf(x + y)$$

platí pro všechna reálná čísla x a y.

(Slovensko)

Příklad I–2

Ať $n \geqslant 3$ je kladné celé číslo. Označení n vrcholů, n stran a vnitřku pravidelného n-úhelníka pomocí $2n+1$ různých

celých čísel nazveme *memořádné*, jestliže platí následující podmínky:

(a) Každá strana je označena číslem rovným aritmetickému průměru čísel označujících její koncové body.

(b) Vnitřek je označen číslem rovným aritmetickému průměru všech n čísel označujících vrcholy.

Určete všechna $n \geqslant 3$, pro něž existuje memořádné označení pravidelného n-úhelníka využívající $2n+1$ po sobě jdoucích celých čísel.

(Česká republika)

Příklad I–3

Označme P průsečík úhlopříček CE a BD konvexního pětiúhelníku $ABCDE$. Ukažte, že platí-li $|\sphericalangle PAD| = |\sphericalangle ACB|$ a $|\sphericalangle CAP| = |\sphericalangle EDA|$, pak středy kružnic opsaných trojúhelníkům ABC a ADE leží na přímce s bodem P.

(Slovensko)

Příklad I–4

Určete nejmenší možnou hodnotu výrazu $|2^m - 181^n|$, v němž m a n jsou kladná celá čísla.

(Německo)

Soutěž družstev
(24. srpna 2017)

Příklad T–1

Určete všechny dvojice polynomů (P, Q) s reálnými koeficienty takové, že rovnost

$$P(x + Q(y)) = Q(x + P(y))$$

platí pro všechna reálná čísla x a y.

(Polsko)

Příklad T–2

Určete nejmenší reálnou konstantu C takovou, že nerovnost

$$|x^3 + y^3 + z^3 + 1| \leqslant C|x^5 + y^5 + z^5 + 1|$$

platí pro všechna reálná čísla x, y a z splňující $x + y + z = -1$.

(Rakousko)

Příklad T–3

Na každém políčku tabulky 2017×2017 je žárovka, která je buďto zapnutá, nebo vypnutá. Žárovku nazveme *šeroslepou*, pokud má sudý počet zapnutých sousedů. Jaký je nejmenší možný počet šeroslepých žárovek?

(Dvě žárovky považujeme za sousední, pokud jimi obsazená políčka sdílí hranu.)

(Rakousko)

Příklad T–4

Ať $n \geqslant 3$ je kladné celé číslo. O posloupnosti $P_1, P_2, \ldots, P_n$ navzájem různých bodů v rovině řekneme, že je *správná*, pokud žádné tři z nich neleží v přímce, lomená čára $P_1P_2 \ldots P_n$ neprotíná samu sebe a pro každé $i = 1, 2, \ldots, n-2$ je trojúhelník $P_iP_{i+1}P_{i+2}$ orientovaný proti směru hodinových ručiček. Pro každé celé číslo $n \geqslant 3$ určete největší celé číslo k s následující vlastností: Lze najít n po dvou různých bodů $A_1, A_2, \ldots, A_n$ v rovině, pro něž existuje k různých permutací

$$\sigma\colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$$

takových, že $A_{\sigma(1)}, A_{\sigma(2)}, \ldots, A_{\sigma(n)}$ je správná.

(Lomená čára $P_1P_2 \ldots P_n$ sestává z úseček $P_1P_2, P_2P_3, \ldots, P_{n-1}P_n$.)

(Polsko)

Příklad T–5

Nechť ABC je ostroúhlý trojúhelník splňující $|AB| > |AC|$ s kružnicí opsanou k. Označme M střed kratšího oblouku BC kružnice k a D průsečík polopřímek AC a BM. Dále ať E ($E \neq C$) je průsečík osy úhlu ACB s kružnicí opsanou trojúhelníku BDC. Předpokládejme, že E leží uvnitř trojúhelníku ABC a lze najít společný bod N přímky DE a kružnice k takový, že E je středem úsečky DN.

Ukažte, že N je středem úsečky I_BI_C, kde I_B a I_C jsou středy kružnic připsaných trojúhelníku ABC postupně ke stranám AC a AB.

(Chorvatsko)

Příklad T–6

Kružnici k se středem O je vepsán ostroúhlý trojúhelník ABC, v němž

$$|AB| \neq |AC|.$$

Ke kružnici k sestrojme tečny v bodech B a C a jejich průsečík označme D. Dále protněme přímky AO a BC v bodě E, označme M střed úsečky BC a N $(N \neq A)$ průsečík přímky AM s kružnicí k. Konečně sestrojme bod F $(F \neq A)$ na kružnici k tak, aby body A, M, E a F ležely na jedné kružnici. Ukažte, že přímka FN půlí úsečku MD.

(Slovensko)

Příklad T–7

Určete všechna celá $n \geqslant 2$ taková, že čísla $0, 1, \ldots, n-1$ lze seřadit do posloupnosti $x_0, x_1, \ldots, x_{n-1}$ tak, aby součty

$$x_0,\ x_0 + x_1,\ \ldots,\ x_0 + x_1 + \ldots + x_{n-1}$$

dávaly navzájem různé zbytky po dělení n.

(Polsko)

Příklad T–8

Pro celé číslo $n \geqslant 3$ definujeme posloupnost $\alpha_1, \alpha_2, \ldots, \alpha_k$ jako posloupnost exponentů v prvočíselném rozkladu

$$n! = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k},$$

kde $p_1 < p_2 < \ldots < p_k$ jsou prvočísla. Určete všechna celá čísla $n \geqslant 3$, pro něž je $\alpha_1, \alpha_2, \ldots, \alpha_k$ geometrická posloupnost.

(Rakousko)

Následující (12.) ročník MEMO se bude konat na základě oficiálního pozvání v roce 2018 v Polsku.

Radek Horenský

České družstvo na 11. MEMO. Zleva Mgr. Radek Horenský, Ph.D., Tomáš Perutka, Filip Svoboda (bronzová medaile), Matěj Doležálek (stříbrná medaile), Radek Olšák (čestné uznání), Josef Minařík (bronzová medaile), Jiří Škrobánek, Michal Rolínek, PhD.

LITERATURA

Simon Singh: Kniha kódů a šifer. Utajování od starověkého Egypta po kvantovou kryptografii

Druhá kniha britského autora zřejmě indického původu předčí jeho první knihu Velká Fermatova věta. Autor je vzděláním fyzik, který pracoval pro BBC, a věnuje se popularizaci vědy. Kniha líčí tajemnou a utajovanou historii kryptografii, tedy vědy o šifrování dokumentů a boj kryptologů, kteří se snaží prolomit šifry. Autor prokázal značné schopnosti literární i popularizační a také zúročil dlouhou přípravu, kterou věnoval napsání knihy. Líčí osudy vědců, kteří se věnovali šifrování i dešifrování a vývoj šifrování od jednoduché záměny množiny znaků, kdy každému znaku je jednoznačně přiřazen právě jeden znak stejné abecedy, tedy tzv. monoalfabetické šifry po kvantovou kryptografii.

Kniha vyšla v roce 2017 v 2. vydání v nakladatelství Dokořán a ARGO, Praha. Na její úrovni se v českém překladu podíleli oba překladatelé –Petr Koubský, Dita Eckhardtová a odborný lektor překladu, přední český kryptolog Vlastimil Klíma. Kniha je krásná po literární a obsahové i formální stránce a designu a čte se jedním dechem. Mohu ji doporučit každému, kdo se zajímá nejen o šifrování, ale o historii vědy nebo společnosti obecně. Autor zařadil také kapitolu o luštění starověkých písem, tedy o rozluštění egyptských hieroglyfů, které rozluštili Thomas Young a Jean Francois Champollion, kteří použili tzv. Rosettskou desku, která obsahovala zápis v řečtině, démotickém písmu a hieroglyfech. Mnohem složitější bylo rozluštění tzv. minojského lineárního B písma. Při něm použili vědci jen dedukci, neboť neměli žádné vodítko ani nevěděli, v jakém jazyku jsou destičky napsány. Nejzajímavější byla kapitola o druhé světové válce, jejíž kryptologické objevy byly třicet let utajovány. Tato historie je známa z dokumentárních televizních seriálů nebo z filmu Kód Navajo. Chybí mi kapitola o sovětské kryptografii, která je zřejmě ještě utajována.

Jako matematik bych přivítal něco víc o matematických základech asymetrického šifrování. Vzhledem k tomu, že je kniha určena širokému okruhu čtenářů, nebylo to asi možné. Předností knihy je rozsáhlý seznam literatury a webových stránek. Autor zařadil také soutěž pro čtenáře v luštění šifer, která byla v originálu ohodnocena cenou 10 000 liber. V Česku vyšla také výborná kniha Simona Garfinkela PGP – Báječné soukromí, která obsahuje historii asymetrického šifrování a popis programu Phila Zimmermanna PGP. Také tuto knihu i program, který sám používám, mohu čtenářům doporučit.

Karel Vašíček