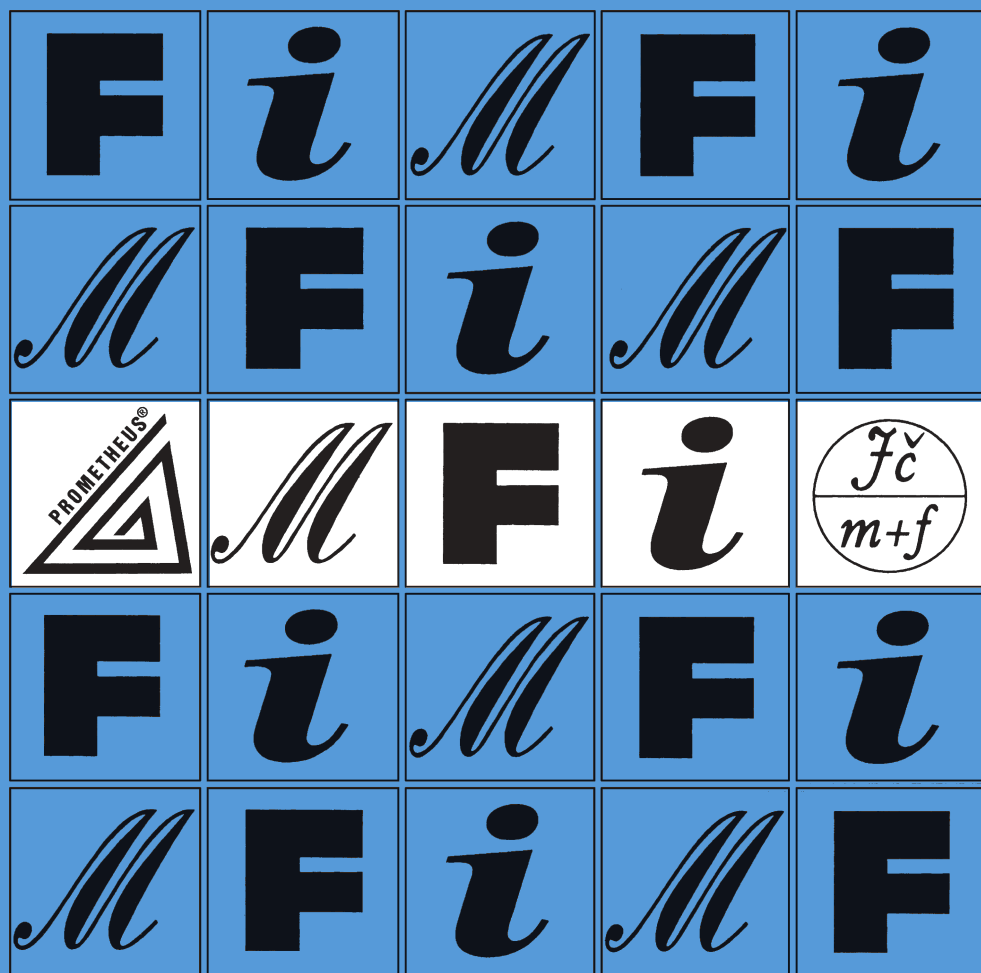


MATEMATIKA 5 FYZIKA INFORMATIKA

ČASOPIS PRO VÝUKU NA ZÁKLADNÍCH A STŘEDNÍCH ŠKOLÁCH



MATEMATIKA – FYZIKA – INFORMATIKA

Časopis pro výuku na základních a středních školách
Ročník XXVII (2018), číslo 5

Vydává Prometheus, spol. s r. o. ve spolupráci s Jednotou českých matematiků a fyziků

Redakce:

Oldřich Lepil – vedoucí redaktor a redaktor pro fyziku

Jaroslav Švrček – redaktor pro matematiku

Eduard Bartl – redaktor pro informatiku

Lukáš Richterek – redaktor WWW stránek

Redakční rada:

Pavel Calábek, Zdeněk Drozd, Radomír Halaš, Štěpán Hubálovský, Růžena Kolářová, Miluše Lachmannová, Pavel Leischner, Dana Mandíková, Oldřich Odvárko, Jarmila Robová, Bohuslav Rothanzl, Emanuel Svoboda, Jaromír Šimša, Pavel Tlustý, Pavel Töpfer, Bohumil Vybíral

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

<i>J. Polák:</i> Analogie v matematice a jejich didaktické využití	321
<i>V. Vaněk, P. Calábek, D. Nocar:</i> České stopy v Matematickém klokanovi	334
Zajímavé matematické úlohy	347

FYZIKA

<i>E. Hejmová:</i> Testování vědeckého myšlení	350
<i>Č. Kodejška:</i> Inovativní demonstrace druhého Newtonova zákona	359
<i>Z. Gibová:</i> Návrh pracovního listu k apletu na zákony zachování energie . . .	365

INFORMATIKA

<i>E. Bartl:</i> Moderní šifry II	373
---	-----

ZPRÁVY

<i>P. Calábek:</i> 12. střeoevropská matematická olympiáda	389
<i>P. Töpfer:</i> Mezinárodní olympiády v informatice v roce 2018	392
<i>D. Hrubý:</i> Seminář Matematika a fyzika ve škole	397
<i>L. Richterek:</i> Proč být učitelem fyziky	398

Analogie v matematice a jejich didaktické využití

JOSEF POLÁK

Fakulta aplikovaných věd ZČU v Plzni

Pojmem *analogie* (z řec. *analogia* = obdoba, podobnost) různých (netotožných) objektů, popř. jevů či situací se rozumí nalezení jejich podobných (spec. stejných) vlastností. Na základě shody jedné vlastnosti se usuzuje na shodu dalších vlastností. V tomto smyslu se s používáním analogií setkáváme nejen v běžném životě či v umění, ale zejména ve vědách humanitních (filozofii, logice, psychologii, právu, lingvistice), vědách přírodních (fyzice, chemii, biologii) i vědách technických (mechanice, elektrotechnice, stavebnictví) a speciálně v matematice. Analogie se používají nejen v matematice jako vědě, ale mají též specifický význam a využití ve vyučování matematiky, jehož didaktickými aspekty se budeme zabývat v tomto článku.

Pojem analogie v matematice, klasifikace analogií

Analogie matematických objektů je vztah mezi netotožnými matematickými objekty, které mají jisté vlastnosti podobné (spec. stejné). Obdobně se definují pojmy *analogie matematických systémů*, *analogie matematických situací* apod. Matematické objekty, jež jsou vzájemně ve vztahu matematické analogie, se nazývají *analogické matematické objekty*. S příklady se setkáváme prakticky ve všech matematických disciplínách. Typickými příklady jsou dvojice analogických planimetrických a stereometrických útvarů (podrobněji viz [12, str. 96]): čtverec – krychle, obdélník – kvádr, rovnoběžník – rovnoběžnostěn, trojúhelník – čtyřstěn, mnohoúhelník – mnohostěn, kruh – koule.

V matematice i dalších vědních oborech se lze setkat s rozlišováním různých druhů analogií. Z kognitivního (poznávacího) hlediska se rozlišují dva typy analogií:

Intuitivní analogie (heuristická analogie) je analogie získaná pouze na základě intuice, tj. pouhého bezprostředního vytušení (bez hlubšího zdůvodnění).

Strukturní analogie (syntaktická analogie) je analogie založená na zjištění určité podobnosti dvou *matematických struktur*, tj. množin matematických objektů s danými vlastnostmi.

Usuzování z analogie

V matematické logice se používají tři druhy *usuzování* (vytváření *úsudků*):

Deduktivní usuzování představuje vytváření logicky správných úsudků na základě výrokové logiky. V matematice je základem *dokazování* (*důkazů matematických vět*).

Induktivní usuzování je založené zpravidla na neúplné indukci. V matematice má charakter *heuristické (objevitelské) metody*, jež mnohdy může posloužit k formulaci věrohodných (pravděpodobně platných) *matematických hypotéz*.

Usuzování z (na základě) analogie má obvykle jednu z následujících dvou forem *heuristického úsudku*:

a) Premisy (předpoklady) úsudku:

Objekt (systém) A je analogický s objektem (systémem) B .

Objekt (systém) B má vlastnost v .

Závěr úsudku: Objekt (systém) A má pravděpodobně též vlastnost v .

b) Premisy (předpoklady) úsudku:

Výrok p je analogický k výroku q .

Výrok q je pravdivý.

Závěr úsudku: Výrok p je pravděpodobně též pravdivý.

Poznámka. Zakladatelem moderního pojetí heuristiky v matematice a vynikajícím propagátorem užití heuristických metod v didaktice matematiky byl maďarský matematik *George Pólya* [džordž pója] (1887–1985), který po mnoho let pedagogicky působil a vědecky tvořil v USA. Jeho knihy [1] a [2] se staly klasickými v oboru didaktického využití heuristických metod v matematice.

Při řešení matematických problémů heuristickými metodami je ovšem důležité si uvědomovat, že jejich výsledkem je vždy pouze vyslovení nějaké *matematické hypotézy*, jejíž pravdivost je pak nutné v další (deduktivní) části řešení buď *dokázat*, anebo *vyvrátit*. V této souvislosti v literatuře (např. v knize [2]) se dokládá na četných příkladech, že v historii matematiky vedlo vhodné použití metody analogie k zásadním objevům, ale její pouhé intuitivní užití svedlo vědce i k vyslovení nesprávných (nepravdivých) hypotéz. Viz např. [12, s. 283].

Základní didaktická využití analogií ve výuce matematiky

Z didaktického hlediska je užití analogií ve vyučování matematiky vhodné a užitečné zejména v těchto případech:

- při analogické formulaci matematických definic a vět,
- při objevování a vyšetřování nových matematických vlastností,
- při řešení analogických matematických úloh,
- k snadnějšímu a trvalejšímu zapamatování určitých analogických matematických poznatků.

Typické příklady didaktického využití analogií:

Analogické definice a věty, např. základní věty pro číselné rovnosti a nerovnosti, definice a věty o vlastnostech operací v různých číselných oborech, o úpravách rovnic a nerovnic, definice a věty pro aritmetické a geometrické posloupnosti, o rovnoběžnosti a kolmosti v rovině a v prostoru (přitom pro některé planimetrické věty analogické stereometrické věty neplatí), o míře geometrických útvarů v rovině a v prostoru, pro geometrická tělesa (hranol – válec, rotační válec – rotační kužel apod.), definice a věty pro kuželosečky (analogické geometrické definice a analytická vyjádření).

Analogická řešení typových úloh v algebře, geometrii (výpočetních i konstrukčních úloh), v kombinatorice aj. Specificky je analogie využívána při řešení gradovaných řetězců matematických úloh (viz [12, str. 104–108]).

Analogie jako užitečné heuristické strategie pro řešení matematických úloh

Heuristickými strategiemi (strategickými postupy) se nazývají obecné, popř. specifické heuristické (objevitelské) metody řešení matematických problémů (úloh), které se cílevědomě používají zejména při řešení složitějších matematických úloh (viz např. knižní publikace [8] a [12, str. 94–104]).

Strategií analogie (strategií založenou na analogii) je nazývána specifická heuristická strategie řešení matematické úlohy, jež spočívá v tom, že se nejprve řeší vhodná jednodušší (snadněji řešitelná) úloha, jejíž řešení je pak inspirací pro řešení dané analogické matematické úlohy.

V následujících dvou příkladech ilustrujících použití strategie analogie nejprve rozřešíme planimetrické úlohy, jejichž řešení nám pak budou inspirací pro řešení jistých náročnějších analogických stereometrických úloh.

Příklad 1

Planimetrická úloha: Je dán ostroúhlý trojúhelník ABC a libovolný bod P uvnitř tohoto trojúhelníku nebo na jeho hranici. Nechť K, L, M jsou po řadě paty kolmic z bodu P na strany BC, CA, AB a $|PK|, |PL|, |PM|$ jsou po řadě vzdálenosti bodu P od stran BC, CA, AB , $a = |BC|$, $b = |CA|$, $c = |AB|$ jsou délky těchto stran trojúhelníku ABC . Dokažte, že pak platí rovnost

$$a \cdot |PK| + b \cdot |PL| + c \cdot |PM| = 2S,$$

kde S je obsah trojúhelníku ABC .

Řešení. Pro vnitřní bod P trojúhelníku ABC je jeho obsah S roven součtu obsahů trojúhelníků PAB, PBC, PCA , tj. platí rovnost

$$\frac{1}{2} a \cdot |PK| + \frac{1}{2} b \cdot |PL| + \frac{1}{2} c \cdot |PM| = S$$

a odtud po vynásobení této rovnosti dvěma dostáváme dokazovanou rovnost. Speciálně pro bod P na hranici trojúhelníku ABC jsou příslušné výrazy na levé straně této rovnosti nulové.

Analogická stereometrická úloha: Je dán čtyřstěn $ABCD$ a libovolný bod P uvnitř tohoto čtyřstěnu nebo na jeho hranici. Nechť K, L, M, N jsou po řadě paty kolmic z bodu P na stěny ABC, BCD, CDA, ABD a $|PK|, |PL|, |PM|, |PN|$ jsou po řadě vzdálenosti bodu P od těchto stěn a S_1, S_2, S_3, S_4 jsou jejich obsahy. Dokažte, že pak platí rovnost

$$S_1 \cdot |PK| + S_2 \cdot |PL| + S_3 \cdot |PM| + S_4 \cdot |PN| = 3V,$$

kde V je objem čtyřstěnu $ABCD$.

Řešení. Pro vnitřní bod P čtyřstěnu $ABCD$ je jeho objem V roven součtu objemů čtyřstěnů $PABC, PBCD, PCDA, PABD$, tj. platí rovnost

$$\frac{1}{3} S_1 \cdot |PK| + \frac{1}{3} S_2 \cdot |PL| + \frac{1}{3} S_3 \cdot |PM| + \frac{1}{3} S_4 \cdot |PN| = 3V$$

a odtud po vynásobení této rovnosti třemi dostáváme dokazovanou rovnost. Speciálně pro bod P na hranici čtyřstěnu $ABCD$ jsou příslušné výrazy na levé straně této rovnosti nulové.

Příklad 2

Vivianiho věta: Je dán rovnostranný trojúhelník ABC a libovolný bod P uvnitř tohoto trojúhelníku nebo na jeho hranici. Nechtě K , L , M jsou po řadě paty kolmic z bodu P na strany BC , CA , AB , $a = |BC| = |CA| = |AB|$ je délka strany rovnostranného trojúhelníku ABC . Pak součet vzdáleností bodu P od stran trojúhelníku ABC je konstantní a platí rovnost

$$|PK| + |PL| + |PM| = h,$$

kde h je výška rovnostranného trojúhelníku ABC . Dokažte.

Důkaz této věty je speciálním případem řešení důkazové planimetrické úlohy z příkladu 1. Dokazovanou rovnost dostáváme speciálně pro rovnostranný trojúhelník ABC , kde $a = b = c$, $S = \frac{1}{2}ah$.

Poznámka. Vincenzo Viviani [vinčenco viviani] (1622–1703) byl italský fyzik a matematik, jehož učiteli, spolupracovníky a přáteli byli významní italští fyzikové a matematici Galileo Galilei (1564–1642) a Evangelista Torricelli (1608–1647). *Vivianiho větu* obsahuje jeho geometrická práce z roku 1659.

Analogická stereometrická věta k Vivianiho větě: Je dán pravidelný čtyřstěn $ABCD$ a libovolný bod P uvnitř tohoto čtyřstěnu nebo na jeho hranici. Nechtě K , L , M , N jsou po řadě paty kolmic z bodu P na stěny ABC , BCD , CDA , ABD , $|PK|$, $|PL|$, $|PM|$, $|PN|$ jsou po řadě vzdálenosti bodu P od těchto stěn, a je délka hrany pravidelného čtyřstěnu $ABCD$. Pak součet vzdáleností bodu P od stěn čtyřstěnu $ABCD$ je konstantní a platí rovnost

$$|PK| + |PL| + |PM| + |PN| = h,$$

kde h je výška pravidelného čtyřstěnu $ABCD$. Dokažte.

Důkaz této věty je speciálním případem řešení důkazové stereometrické úlohy z příkladu 1. Z něho speciálně pro pravidelný čtyřstěn $ABCD$, u něhož je $S_1 = S_2 = S_3 = S_4$, $V = \frac{1}{3}S_1h$, takže platí

$$S_1 \cdot (|PK| + |PL| + |PM| + |PN|) = 3 \cdot \frac{1}{3} S_1 h$$

a odtud plyne dokazovaná rovnost.

Příklad 3

Planimetrická úloha: V rovině je dán libovolný středově souměrný rovinný obrazec a bod $P \neq S$ (kde S je střed souměrnosti obrazce). Nalezněte přímkou p , která prochází bodem P a rozděluje daný obrazec na dva shodné geometrické útvary.

Řešení je velmi jednoduché. Protože rovinná středová souměrnost se středem S je shodné zobrazení, bezprostředně odtud plyne, že každá přímka procházející středem souměrnosti S daného obrazce jej rozdělí na dva shodné geometrické útvary. A tedy hledanou přímkou p je přímka PS (určená body P a S).

Analogická stereometrická úloha: V prostoru je dáno libovolné středově souměrné těleso a přímka p , která neprochází jeho středem souměrnosti S . Nalezněte rovinu ϱ , která prochází přímkou p a rozděluje dané těleso na dva shodné geometrické útvary.

Řešení je opět velice jednoduché: Protože také v prostoru středová souměrnost se středem S je shodné zobrazení, vyplývá odtud, že každá rovina procházející středem souměrnosti S daného obrazce jej rozdělí na dva shodné geometrické útvary. A tedy hledanou rovinou ϱ je rovina pS (určená přímkou p a bodem S).

Poznámka. G. Pólya v [1, str. 110] zdůrazňuje, že je vhodnější řešit takto formulovanou úlohu pro obecné středově souměrné těleso, než jen např. pro pravidelný osmistěn. Její řešení speciálně platí pro libovolný středově souměrný pravidelný mnohostěn.

Příklad 4

Pozoruhodné, i když málo známé, jsou *stereometrické analogie Pythagorovy věty a Thaletovy věty*, s nimiž se lze seznámit v zajímavém článku [9].

Užití analogií při řešení aplikačních úloh

Reálný svět a jeho zkoumání, jakož i veškeré lidské činnosti v něm jsou často natolik složité a bezprostředně těžko proveditelné, že vyžadují vytváření různých materiálních či abstraktních (myšlenkových, kognitivních) modelů. Připomeňme (viz [12, str. 111–114]):

Modelem daného objektu (resp. jevu, procesu, situace) nebo systému se rozumí jeho vhodná reprezentace (zastoupení, resp. zobrazení v širokém slova smyslu) se zachováním podstatných charakteristických vlastností.

Procesy vytváření, přeměňování a interpretování modelů se nazývají *modelování* či *simulace*. Velmi významným speciálním případem abstraktních modelů jsou matematické modely, tj. modely vyjádřené matematickými prostředky (např. rovnicemi nebo soustavami rovnic). Modelování užitím matematických modelů je nazýváno *matematické modelování*. Ve školské matematice se používají matematické modely při *matematizaci reálných situací* a *řešení aplikačních úloh*. Speciálně dvě nebo více aplikačních úloh, jež se řeší užitím stejného (resp. analogického) matematického modelu, se nazývají *analogické aplikační úlohy*.

Příklad 5

Fyzikální úloha o výpočtu průměrné rychlosti automobilu: Automobil ujel vzdálenost 210 km za 2,5 hodiny. Stanovte jeho průměrnou rychlost na celé trati.

Řešení. Při výpočtu průměrné rychlosti obecně nerovnoměrného pohybu automobilu vycházíme z její definice známé z fyziky. *Průměrná rychlost* nerovnoměrného pohybu tělesa („hmotného bodu“) na dráze s uražené za čas t je definována vzorcem

$$v_p = \frac{s}{t},$$

tj. je rovna rychlosti takového modelu rovnoměrného pohybu tělesa, při kterém by těleso urazilo stejnou celkovou dráhu s za tutéž dobu t . Odtud pro zadané numerické hodnoty dráhy $s = 210$ km a času $t = 2,5$ h dostáváme, že průměrná rychlost automobilu byla

$$v_p = \frac{210 \text{ km}}{2,5 \text{ h}} = 84 \text{ km} \cdot \text{h}^{-1}.$$

Poznámka. Protože průměrnou rychlost automobilu počítáme jako podíl ujeté dráhy s a doby t , za kterou byla ujeta, je zřejmé, že při každém zdržení, tj. prodloužení doby t , se průměrná rychlost sníží.

Analogická aplikační úloha o výpočtu průměrné spotřeby automobilu: Auto ujelo 420 km a spotřebovalo při tom 29 l benzínu. Jaká byla jeho průměrná spotřeba na 100 km?

Řešení. Vzhledem k tomu, že jízda automobilu je zpravidla nerovnoměrná, jeho spotřeba pohonných hmot (benzínu, nafty) je pak též nerovnoměrná v průběhu jízdy. Přitom *spotřebou motorového vozidla* se rozumí objem V spotřebované pohonné hmoty (paliva motoru) vyjádřený v litrech. Pro

vyjádření ekonomičnosti a cenové náročnosti provozu motorového vozidla je zaveden a používán údaj tzv. *průměrné spotřeby motorového vozidla* na 100 km jízdy. Jeho definice vychází z toho, že se skutečný (nerovnoměrný) pohyb vozidla nahradí modelem rovnoměrného pohybu vozidla se spotřebou V paliva přímo úměrnou dráze s ujeté vozidlem: $V = ks$, kde konstanta k je koeficient této přímé úměrnosti ($k = \frac{V}{s}$ představuje spotřebu paliva na 1 km). Spotřeba paliva na dráze 100 km je pak $\frac{V}{s} \cdot 100$ km. Na základě tohoto matematického modelu se pro spotřebu paliva při jeho skutečné (nerovnoměrné) jízdě vozidla zavádí pojem *průměrné spotřeby paliva na 100 km jízdy* takto: *Průměrná spotřeba V_p paliva motorového vozidla* (v litrech) na 100 km jízdy při jeho celkové spotřebě V (v litrech) na dráze s (v km) je definována vzorcem

$$V_p = \frac{V}{s} \cdot 100 \text{ km.}$$

(Lze ji též vyjádřit ve formě poměru $V_p : V = 100 \text{ km} : s$, tzv. trojčlenkou.) Odtud pro zadané numerické hodnoty dráhy automobilu $s = 420$ km a celkové spotřeby benzínu $V = 29$ l dostáváme, že průměrná spotřeba automobilu na dráze 100 km byla

$$V_p = \frac{29 \text{ l}}{420 \text{ km}} \cdot 100 \text{ km} \doteq 6,9 \text{ l.}$$

V článku [11] byl popsán a doporučen alternativní postup řešení této úlohy (a dalších numericky zadaných úloh) založený na užití „strategie analogie“. Stručně lze tento postup řešení vyjádřit takto: V daném numerickém zadání řešené úlohy se číselné údaje nahradí vhodnými jednoduššími („přátelštějšími“) čísly. Nalezne se řešení úlohy s tímto zjednodušeným číselným zadáním. V nalezeném algoritmu jejího řešení se nahradí pozměněné číselné údaje původními číselnými údaji a tím se určí řešení úlohy v původním znění. Takto pro výše zadanou slovní úlohu o průměrné spotřebě automobilu se v článku [11] nejprve řeší „analogická úloha“ se vhodně zjednodušeným číselným zadáním: Auto ujelo 200 km a spotřebovalo při tom 16 l benzínu. Jaká byla jeho průměrná spotřeba na 100 km? Výsledek řešení této úlohy je zřejmý – průměrná spotřeba auta na 100 km činí 8 litrů benzínu, přičemž podle [11] jeho výpočet se dá zrekonstruovat takto:

$$\frac{16}{\frac{200}{100}} = 8$$

a po návratu k původní úloze se ta vyřeší stejným způsobem:

$$\frac{\frac{29}{420}}{100} \doteq 6,9.$$

K tomuto postupu řešení připojme několik zásadních připomínek: Řešení úlohy pomocí analogie (založené na zjednodušení jejího číselného zadání) není žádnou její alternativní výpočetní metodou. Původní úloha i „analogická úloha“ jsou řešeny v podstatě toutéž výpočetní metodou. V případě úlohy o průměrné spotřebě auta na 100 km je metoda výpočtu založena na (výše popsaném) předpokladu přímé úměrnosti spotřeby auta a ujeté dráhy, přičemž výpočet průměrné spotřeby může být realizován různými ekvivalentními způsoby, např. užitím trojčlenky. Zápis výsledku výpočtu ve tvaru složeného zlomku je jen jedním z možných ekvivalentních vyjádření. Praktický výpočet řešení v „analogické úloze“ a v původní úloze se liší jen v tom, že zatímco v prvním případě se snadno provede z paměti, ve druhém případě se obvykle uskuteční s použitím kalkulátoru. Zároveň je třeba zdůraznit, že v aplikačních úlohách se mají výpočty provádět nikoliv jen s číselnými hodnotami údajů (veličin), ale s hodnotami veličin, tj. včetně jejich jednotek. A ve výuce fyziky jsou žáci vedeni k tomu, aby řešení fyzikálních úloh prováděli nejprve obecně a teprve poté do obecného výsledku dosazovali dané numerické hodnoty veličin.

Při řešení aplikačních úloh užitím strategie analogie je vždy nutné analyzovat úlohu nejen z matematického hlediska, ale též ji správně interpretovat z aplikačního hlediska. V následujícím příkladu ilustrativně ukážeme, jak užití analogie nesprávně z tohoto hlediska vede k chybnému řešení aplikační úlohy. Úlohy z tohoto příkladu jsou obsaženy v 8. upraveném vydání knižní publikace *Běloun, F. a kol.: Sbírka úloh z matematiky pro základní školu* (Prometheus, Praha 2010) v kapitole o slovních úlohách na str. 113–115, výsledky úloh jsou uvedeny na str. 245.

Příklad 6

Slovní úloha o směsi čajů: Ze dvou druhů čaje v ceně 160 Kč a 220 Kč za 1 kilogram se má připravit 20 kg směsi v ceně 205 Kč za 1 kilogram. Kolik kilogramů každého druhu čaje bude třeba smíchat?

Řešení. Označíme hledané hmotnosti prvního a druhého čaje po řadě m_1 , m_2 , jejich dané ceny za 1 kilogram $c_1 = 160$ Kč/kg, $c_2 = 220$ Kč/kg, hmotnost směsi $m_3 = 20$ kg a její cenu za 1 kilogram $c_3 = 205$ Kč/kg. Sestavíme soustavu dvou lineárních rovnic pro neznámé m_1 , m_2 , z nichž

první vyplývá z fyzikálního zákona zachování hmotnosti a druhá vyjadřuje, že součet celkových cen smíchávaných čajů má být roven celkové ceně jejich směsi:

$$\begin{aligned}m_1 + m_2 &= m_3, \\c_1 m_1 + c_2 m_2 &= c_3 m_3\end{aligned}$$

Řešením této soustavy rovnic dostáváme

$$\begin{aligned}m_1 &= \frac{c_2 - c_3}{c_2 - c_1} m_3, \\m_2 &= \frac{c_3 - c_1}{c_2 - c_1} m_3\end{aligned}$$

a odtud numericky po dosazení

$$\begin{aligned}m_1 &= \frac{1}{4} \cdot 20 \text{ kg} = 5 \text{ kg}, \\m_2 &= \frac{3}{4} \cdot 20 \text{ kg} = 15 \text{ kg}.\end{aligned}$$

Analogická úloha o slitině kovů: Ze dvou kovů s hustotami $7,4 \text{ g} \cdot \text{cm}^{-3}$ a $8,2 \text{ g} \cdot \text{cm}^{-3}$ máme připravit $0,5 \text{ kg}$ slitiny s hustotou $7,6 \text{ g} \cdot \text{cm}^{-3}$. Kolik gramů každého kovu je k tomu zapotřebí?

Řešení. Označíme hledané hmotnosti prvního a druhého kovu po řadě m_1 , m_2 , jejich hustoty $\rho_1 = 7,4 \text{ g} \cdot \text{cm}^{-3}$, $\rho_2 = 8,2 \text{ g} \cdot \text{cm}^{-3}$, hmotnost slitiny $m_3 = 500 \text{ g}$ a její hustotu $\rho_3 = 7,6 \text{ g} \cdot \text{cm}^{-3}$. V citované sbírce úloh byla sestavena pro neznámé m_1 , m_2 soustava dvou lineárních rovnic formálně analogického tvaru k rovnicím z předchozí úlohy:

$$\begin{aligned}m_1 + m_2 &= m_3, \\\rho_1 m_1 + \rho_2 m_2 &= \rho_3 m_3\end{aligned}$$

Řešením této soustavy rovnic pro neznámé m_1 , m_2 obdobně jako v předchozí úloze dostáváme

$$\begin{aligned}m_1 &= \frac{\rho_2 - \rho_3}{\rho_2 - \rho_1} m_3, \\m_2 &= \frac{\rho_3 - \rho_1}{\rho_2 - \rho_1} m_3\end{aligned}$$

a odtud numericky po dosazení

$$m_1 = \frac{3}{4} \cdot 500 \text{ g} = 375 \text{ g},$$

$$m_2 = \frac{1}{4} \cdot 500 \text{ g} = 125 \text{ g}.$$

Toto řešení (uvedené ve výsledcích sbírky úloh) je však chybné, protože pro slitiny (a pro roztoky) druhá z rovnic soustavy neplatí (nemá fyzikální smysl). Danou úlohu lze řešit prostředky školské matematiky pouze aproximativně tak, že druhou rovnici soustavy nahradíme přibližně platnou rovnicí pro objemy obou kovů a jejich slitiny V_1, V_2, V_3 :

$$m_1 + m_2 = m_3,$$

$$V_1 + V_2 = V_3, \text{ neboli } \frac{m_1}{\rho_1} + \frac{m_2}{\rho_2} = \frac{m_3}{\rho_3}.$$

Řešením této soustavy rovnic pro neznámé m_1, m_2 dostáváme

$$m_1 = \frac{\rho_1}{\rho_3} \cdot \frac{\rho_2 - \rho_3}{\rho_2 - \rho_1} m_3,$$

$$m_2 = \frac{\rho_2}{\rho_3} \cdot \frac{\rho_3 - \rho_1}{\rho_2 - \rho_1} m_3$$

a odtud numericky po dosazení

$$m_1 \doteq 365,13 \text{ g}, \quad m_2 \doteq 134,87 \text{ g}.$$

Užití strukturních analogií ve výuce matematiky

Nechť jsou dány množiny M_1, M_2 , jež mají po řadě odpovídající analogické vlastnosti v_1, v_2 čili jsou zadány dvě matematické struktury $(M_1, v_1), (M_2, v_2)$. Jestliže existuje vzájemně jednoznačné zobrazení f množiny M_1 na množinu M_2 , které zachovává jejich vlastnosti v_1, v_2 , pak toto zobrazení f se nazývá *izomorfní zobrazení* nebo krátce *izomorfismus* a $(M_1, v_1), (M_2, v_2)$ se nazývají *izomorfní matematické struktury* vzhledem k vlastnostem v_1, v_2 . Pokud vlastnosti v_1, v_2 jsou v jistém smyslu analogické, potom izomorfní matematické struktury $(M_1, v_1), (M_2, v_2)$ představují *strukturní analogie* mezi množinami M_1, M_2 .

Speciálně se rozlišují dva typy izomorfismů:

1. Je-li $v_1 = R_1$ a $v_2 = R_2$, kde R_1 a R_2 jsou po řadě určité (dané) relace mezi prvky množin M_1 a M_2 , pak jde o *izomorfismus f zachovávající relace R_1, R_2* .
2. Je-li $v_1 = O_1$ a $v_2 = O_2$, kde O_1 a O_2 jsou po řadě určité (dané) operace pro prvky množin M_1 a M_2 , pak jde o *izomorfismus f zachovávající operace O_1, O_2* .

V následujících dvou příkladech uvedeme některé významné izomorfismy (strukturní analogie), které nalézají široké uplatnění ve školské matematice.

Příklad 7

Izomorfismus (strukturní analogie) zachovávající relace:

$(\mathbb{R}, R_1)$ a $(\mathbb{E}_1, R_2)$ kde R_1 je relace uspořádání ($\leq$) na množině $\mathbb{R}$ (oboru reálných čísel) a R_2 je analogická relace uspořádání na množině $\mathbb{E}_1$ (eukleidovském prostoru dimenze 1, tj. přímce),

$(\mathbb{R}, d(a, b))$ a $(\mathbb{E}_1, d(A, B))$, kde $d(a, b) = |a - b|$ je metrika v $\mathbb{R}$ a $d(A, B) = |AB|$ je metrika v $\mathbb{E}_1$; na obou těchto izomorfismech je založeno geometrické znázorňování reálných čísel na *číselné ose*.

$(\mathbb{R}^2, d(a, b))$ a $(\mathbb{E}_2, d(A, B))$, kde $a = [a_1, a_2]$, $b = [b_1, b_2]$, $d(a, b) = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2}$ je metrika v $\mathbb{R}^2$ a $d(A, B) = |AB|$ je metrika v rovině $\mathbb{E}_2$.

$(\mathbb{R}^3, d(a, b))$ a $(\mathbb{E}_3, d(A, B))$, kde $a = [a_1, a_2, a_3]$, $b = [b_1, b_2, b_3]$, $d(a, b) = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2 + (a_3 - b_3)^2}$ je metrika v $\mathbb{R}^3$ a $d(A, B) = |AB|$ je metrika v rovině $\mathbb{E}_3$.

Ve všech uvedených případech izomorfismů f přitom platí $d(a, b) = d(AB)$, tj. zobrazení f jsou *izometrická* a pomocí této izometrie se přechází od geometrického prostoru $\mathbb{E}_n$ k jeho aritmetickému modelu $\mathbb{R}^n$ ($n = 1, 2, 3$, $\mathbb{R}^1 = \mathbb{R}$), což je využíváno v analytické geometrii při souřadnicovém vyjádření bodů v rovině, resp. v prostoru.

Příklad 8

Izomorfismus (strukturní analogie) zachovávající operace:

$(\mathbb{R}^+, \cdot)$ a $(\mathbb{R}, +)$, kde $\mathbb{R}^+$ je množina všech kladných čísel s operací násobení a $\mathbb{R}$ obor reálných čísel s operací sčítání; tento izomorfismus f zřejmě reprezentuje *logaritmickou funkci*.

$(\mathbb{C}, +)$ a $(G, +)$, kde $\mathbb{C}$ je obor komplexních čísel s operací sčítání a G je rovina se zavedenou kartézskou soustavou souřadnic bodů s definovanou

operací jejich sčítání; na tomto izomorfismu f je založeno geometrické znázorňování komplexních čísel v *Gaussově rovině* G .

$(\mathbf{V}_g, +)$ a $(\mathbf{V}_a, +)$, kde $\mathbf{V}_g$ je vektorový prostor geometrických vektorů v rovině, resp. v prostoru s definovanou operací sčítání a $\mathbf{V}_a$ je vektorový prostor aritmetických vektorů dimenze 2, resp. 3, tj. $\mathbf{V}_a = \mathbb{R}^2$, resp. $\mathbf{V}_a = \mathbb{R}^3$ s definovanou operací sčítání; tento izomorfismus f je využíván v analytické geometrii lineárních geometrických útvarů.

Literatura

- [1] *Pólya, G.*: How to Solve It – A new Aspects of Mathematical Methods. Princeton University Press, Princeton, 1945, 1957 (2. rozšířené vyd.), 2004, 2014. (Ruský překlad 1. vydání: Kak rešat' zadaču, Učpedgiz, Moskva 1961. Český překlad 2. vydání v reedici z r. 2014: Jak to řešit? – Překvapivé aspekty (nejen) matematických metod. MatfyzPress, Praha, 2016.)
- [2] *Pólya, G.*: Mathematics and Plausible Reasoning. Princeton University Press, Princeton, 1954. (Ruský překlad: Matematika i pravdopodobnyje rassuždenija. Nauka, Moskva, 1975.)
- [3] *Erdnišev, P. M.*: Srovnání a zobecnění při učení matematice. Učpedgiz, Moskva, 1960.
- [4] *Čerkasov, R. S., Stoljar, A. A. a kol.*: Metodika předpovídání matematiky. Obščaja metodika. Prosveščeniye, Moskva, 1985.
- [5] *Ženčáková, R.*: Užití analogie v matematice. Acta Univ. Palacki. Olomuc., Fakulta Pedagogická, Math. II, 1988.
- [6] *Odvárko, O. a kol.*: Metody řešení matematických úloh. SPN, Praha, 1990.
- [7] *Křemen, J.*: Modely a systémy. Academia, Praha, 2007.
- [8] *Kopka, J.*: Umění řešit matematické problémy. HAV, Praha, 2013.
- [9] *Švrček, J.*: Prostorové analogie dvou planimetrických vět. MFI, roč. 23 (2014), č. 2, s. 81–85.
- [10] *Polák, J.*: Didaktika matematiky – Jak učit matematiku zajímavě a užitečně. I. část Konkrétní didaktika matematiky. Nakladatelství Fraus, Plzeň, 2014.
- [11] *Eisenmann, P., Příbyl, J.*: Analogie – Užitečná heuristická strategie. Učitel matematiky, roč. 24 (2016), č. 3 (99).
- [12] *Polák, J.*: Didaktika matematiky – Jak učit matematiku zajímavě a užitečně. II. část: Obecná didaktika matematiky. Nakladatelství Fraus, Plzeň, 2016.

České stopy v Matematickém klokanovi

VLADIMÍR VANĚK – PAVEL CALÁBEK – DAVID NOCAR

Univerzita Palackého v Olomouci

Matematický klokan je jednou z nejznámějších mezinárodních matematických soutěží pro žáky ZŠ a SŠ. Tato soutěž se liší od ostatních matematických soutěží jako je například Matematická olympiáda, Pythagoriáda atd. v několika aspektech. Tím nejvýznamnějším je její struktura. Lze říci, že oproti výše zmíněným soutěžím probíhá pouze jednokolově v předem stanovený den. Dále se zde nehodnotí postup, případně nalezení „nejelegantnějšího“ řešení, ale pouze správný výsledek, který si navíc může soutěžící „tipnout“ z nabízených odpovědí A, B, C, D a E, z nichž *právě jedna* je správná. Většina žáků se s ní setkává již na prvním stupni ZŠ a pravidelně se jí účastní až do posledních ročníků střední školy. Soutěž je rozdělena do šesti kategorií dle věku účastníků.

Poprvé si mohou zasoutěžit již děti druhých a třetích tříd základních škol – kategorie Cvrček, dále pak následují kategorie Klokánek (4.–5. třída), Benjamín (6.–7. třída), Kadet (8.–9. třída) a na středních školách Junior (1. a 2. ročník, resp. ekvivalentní ročníky víceletých gymnázií) a Student (3. a 4. ročník). Zadání Cvrčka obsahuje 18 úloh a jeho časová dotace je 60 minut. Kategorie Klokánek, Benjamín a Kadet obsahují 24 úloh a je pro ně vyhrazeno 60 minut na řešení plus 15 minut na administraci testu. Středoškolské kategorie mají také 24 úloh a časovou dotaci 75 + 15 minut. Soubor soutěžních úloh je rozdělen na třetiny dle obtížnosti, za které žáci mohou získat po řadě 3, 4, resp. 5 bodů. V případě chybné odpovědi je jim jeden bod odečten, pokud úlohu neřeší neztrácejí žádný bod. O dosažitelných bodových ohodnoceních pojednává podrobněji článek [4]. Aby ani soutěžící, který nevyřeší žádnou úlohu správně, nedosáhl záporného výsledku, vstupuje do soutěže s 18 (Cvrček), resp. 24 body (ostatní kategorie). Další podrobnosti je možno najít na internetových stránkách soutěže www.matematickyklokan.net.

V přípravě budoucích učitelů se poměrně často setkáváme se situací, kdy se studenti domnívají, že Matematický klokan je soutěží regionální,

případně republikovou a její realizace se omezuje pouze na krátký časový úsek na začátku druhé třetiny měsíce března. V tomto článku bychom rádi uvedli vše na pravou míru a kromě historie celé mezinárodní soutěže se podívali i na několik vybraných úloh, kterými přispěli organizátoři z České republiky k jejímu celosvětovému úspěchu.

Historie Matematického klokana

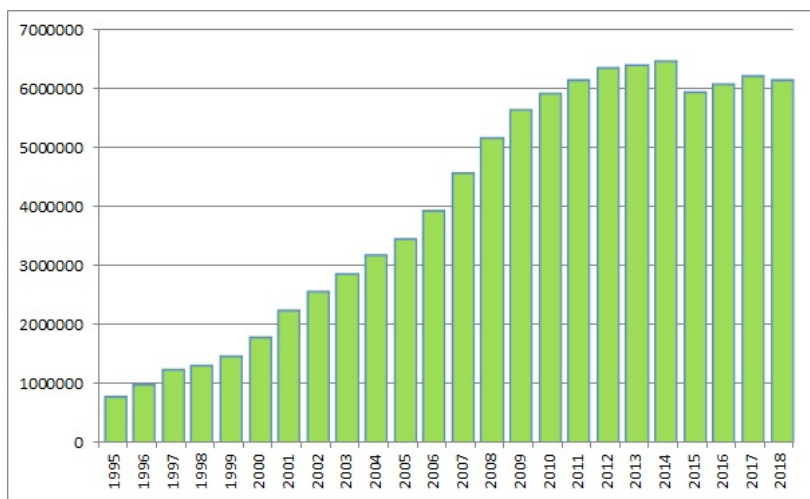
Na začátku 80. let představil australský učitel matematiky *Peter O'Halloran* na australských školách nový druh matematické soutěže, jejímž základním stavebním prvkem byl didaktický test s výběrem odpovědí. Na testové otázky bylo možno odpovídat jednotně pomocí počítače, jímž byl celý test také opravován a vyhodnocován, což znamenalo, že se současně mohly účastnit soutěže tisíce žáků napříč Austrálií a jediným omezením bylo připojení k internetu. Ihned v počátcích tak slavila soutěž velký úspěch.

V roce 1991 se dva francouzští učitelé (*André Deledicq* a *Jean Pierre Boudine*) rozhodli po vzoru australského kolegy založit ve Francii podobnou soutěž, kterou nazvali „Kangaroo“, čímž chtěli vzdát hold svým australským přátelům. V prvním ročníku se zúčastnilo 120 000 žáků ve věku 15–16 let. V následujících letech se soutěž otevřela i pro další věkové kategorie.

V červnu 1993 se v Paříži konalo setkání organizátorů francouzských matematických soutěží v rámci The World Federation of National Mathematics Competitions (WFNMC), kam byli pozváni také zástupci dalších evropských zemí. Zde byla mimo jiné představena soutěž Kangaroo. Účastníci konference byli ohromeni rostoucím zájmem žáků o tento typ soutěže (120 000 v roce 1991, 300 000 v roce 1992, 500 000 v roce 1993). Sedm evropských zemí – Bělorusko, Maďarsko, Nizozemsko, Polsko, Rumunsko, Rusko a Španělsko – převzalo myšlenku i způsob organizace a v květnu 1994 slavila nová soutěž ve všech zemích velký úspěch. Stále se však jednalo o individuální soutěže, které měly v jednotlivých zemích jiná zadání a také odlišný čas pro řešení. O měsíc později na zasedání Evropské rady ve Štrasburku valné shromáždění delegátů deseti evropských zemí rozhodlo o vytvoření asociace „Kangourou sans frontieres“ (Kangaroo without Frontiers, AKSF) s volenou radou 6 členů a s právním statutem registrovaným v Paříži. Tím byl odstartován globalizační proces celé soutěže a nastavena základní pravidla platná pro všechny participující země.

Již v prosinci 1995 byl v Eindhovenu připravován další ročník soutěže, společný (identický) na úrovni kategorie Kadet (13–14 let) pro všechny

země: byla stejná soutěžní zadání, časová dotace a soutěž se také konala ve všech zemích ve stejný den. Zajištění organizace, vyhodnocení soutěže i ocenění nejlepších řešitelů bylo ponecháno na jednotlivých zemích. Počínaje následujícím rokem byly již společně připravovány i ostatní věkové kategorie. V roce 1997 přijalo 21 zúčastněných zemí konečné nařízení, které přesně definuje finanční účast a pravidla soutěže, která mají být dodržována všemi zeměmi, jež se chtějí stát členy asociace Kangaroo without Frontiers. V současnosti je v asociaci registrováno 84 zemí z celého světa a soutěže se v roce 2018 ve všech kategoriích účastnilo 6 124 834 žáků.



Rozsáhlý a zajímavý je i seznam zemí AKSF: Albánie, Argentina, Arménie, Austrálie, Ázerbajdžán, Belgie, Bělorusko, Bolívie, Bosna a Hercegovina, Brazílie, Bulharsko, Chile, Filipíny, Kolumbie, Kostarika, Chorvatsko, Kypr, Česká republika, Dánsko, Dominikánská republika, Ekvádor, Estonsko, Etiopie, Finsko, Francie, Německo, Ghana, Řecko, Maďarsko, Indie, Indonésie, Írán, Irák, Izrael, Itálie, Jamajka, Jižní Korea, Kanada, Katalánsko, Kazachstán, Kosovo, Kyrgyzstán, Litva, Lotyšsko, Makedonie, Malajsie, Mexiko, Moldavsko, Mongolsko, Mosambik, Myanmar, Nigérie, Nizozemí, Norsko, Pákistán, Panama, Paraguay, Peru, Polsko, Portoriko, Portugalsko, Rakousko, Rumunsko, Rusko, Saudská Arábie, Singapur, Slovensko, Slovinsko, Spojené království, Srbsko, Španělsko, Švédsko, Švýcarsko, Tádžikistán, Tanzánie, Tunisko, Turecko, Ukrajina, Uruguay, USA, Uzbekistán, Venezuela, Vietnam, Zambie.

Historie českého Matematického klokana

Historie Matematického klokana v ČR se začala psát v roce 1994. Konference WFNMC se účastnili také dva členové katedry algebry a geometrie Přírodovědecké fakulty UP v Olomouci Josef Molnár a Jaroslav Švrček. Usoudili, že v ČR podobný typ soutěže chybí a tak byl Matematický klokan J. Molnárem na podzim roku 1994 na konferenci MAKOS2014 vyhlášen i v České republice. Prvního ročníku v roce 1995 se účastnily pouze vybrané školy především z území dnešního Olomouckého a Moravskoslezského kraje, přesto se zapojilo téměř 25 000 žáků v kategoriích Klokánek (4. a 5. třída ZŠ), Benjamín (6. a 7. třída ZŠ), Kadet (8. a 9. třída ZŠ), Junior (1. a 2. ročník SŠ) a Student (3. a 4. ročník SŠ). Všechny kategorie měly strukturu $10 + 10 + 10$ úloh a vyhrazený čas byl 75, resp. 90 minut (na SŠ). Změna nastala až v roce 2002, kdy se snížil počet úloh na dnešních $8 + 8 + 8$ a o tři roky později přibyla ještě kategorie Cvrček pro 2. a 3. třídu ZŠ se strukturou $4 + 4 + 4$.

V polovině letošního roku došlo pouze k administrativní úpravě, kdy nově nezastupuje Českou republiku v AKSF fyzická osoba (J. Molnár), ale osoba právnická (JČMF, pobočný spolek Olomouc), zastoupená Vladimírem Vaňkem.

V současné době tak soutěž pořádá pobočný spolek Olomouc Jednoty českých matematiků a fyziků ve spolupráci s Katedrou matematiky Pedagogické fakulty Univerzity Palackého v Olomouci kategorie Klokánek, garant: Martina Uhlířová, kategorie Benjamín, garant: David Nocar, kategorie Kadet, garant: Jitka Hodaňová a Katedrou algebry a geometrie Přírodovědecké fakulty Univerzity Palackého v Olomouci kategorie Junior, garant: Vladimír Vaněk a kategorie Student, garant: Pavel Calábek. Pro žáky 2. a 3. třídy základní školy byla u nás v roce 2005 zavedena kategorie Cvrček (v roce 2012 se stala řádnou mezinárodní kategorií, od roku 2013 má strukturu $6 + 6 + 6$ a časovou dotaci 60 minut), garant: Eva Nováková. Při organizaci soutěže dále pomáhají tzv. krajsí a okresní důvěrníci a samozřejmě učitelé na školách.

Do tří let od uvedení do ČR byl Matematický klokan zařazen mezi soutěže, které jsou plně hrazeny z Ministerstva školství, mládeže a tělovýchovy. Jsme jednou z 15 zemí, kde účastníci neplatí žádné „startovné“.

Tabulka 1 uvádí vývoj počtu účastníků soutěže Matematický klokan v České republice a potvrzuje zájem žáků o tuto soutěž. Matematický klokan tak bezvýhradně plní své největší poslání a tím je propagace matematiky mezi dětmi a mládeží.

Tabulka 1: Vývoj počtu účastníků soutěže Matematický klokan v ČR

	Cvr.	Klok.	Benj.	Kad.	Jun.	Stud.	Σ
1995		6 205	7 834	7 280	2 195	1 297	24 811
1996		18 522	30 819	27 262	6 148	3 938	86 689
1997		61 161	59 314	51 769	8 631	7 349	188 224
1998		62 963	67 417	57 653	11 580	8 484	208 097
1999		87 885	79 717	73 578	16 847	6 606	264 633
2000		95 426	87 304	81 893	20 384	10 319	295 326
2001		93 434	86 458	78 408	20 173	11 228	289 701
2002		99 204	86 785	81 440	20 479	10 428	298 336
2003		83 584	74 112	65 839	19 615	9 879	253 029
2004		78 275	75 609	68 324	17 345	9 729	249 282
2005	11 076	70 886	72 090	69 425	18 333	10 690	252 500
2006	46 832	66 799	69 739	69 104	18 003	9 947	280 424
2007	60 744	70 705	66 840	71 491	17 804	10 274	297 858
2008	70 942	74 668	64 995	69 734	19 101	10 191	309 631
2009	70 084	75 624	64 258	65 694	18 711	10 599	304 970
2010	78 291	81 737	66 731	63 412	18 711	9 646	318 528
2011	79 758	84 031	65 461	60 404	16 326	8 721	314 701
2012	84 221	87 324	67 750	61 010	15 021	8 987	324 313
2013	86 011	86 065	67 794	59 408	15 503	8 243	323 024
2014	97 478	94 528	69 635	61 244	15 479	7 900	346 264
2015	102 346	96 763	71 120	64 074	15 559	7 894	357 756
2016	109 187	105 668	74 113	62 953	16 002	8 115	376 038
2017	115 925	111 013	75 330	65 443	16 326	7 568	391 605
2018	115 120	117 232	80 227	66 405	15 233	7 051	401 268

Další zajímavostí může být porovnání počtu účastníků soutěže mezi Českou republikou a vybranými státy. Do srovnání jsme zařadili jednak naše nejbližší sousedy, ale také státy, které stály u počátků rozšíření soutěže do Evropy v roce 1994. Měly tak stejnou dobu na její propagaci mezi žáky. Uvádíme zde jednak absolutní hodnoty, které mají ovšem menší vypovídající hodnotu, neboť 400 000 účastníků v desetimilionové ČR nelze srovnat

se 400 000 účastníky například v Rusku, také počet obyvatel daného státu a poměrné zastoupení soutěžících ku počtu obyvatel v procentech (údaje byly převzaty z wikipedia.com).

Tabulka 2: Porovnání počtu účastníků soutěže mezi ČR a vybranými státy

stát	počet soutěžících	počet obyvatel	poměrné zastoupení
Francie	322 100	65 605 000	0,491 %
Rusko	1 159 571	142 423 773	0,814 %
Bělorusko	144 416	9 461 800	1,526 %
Maďarsko	39 314	9 957 731	0,395 %
Polsko	371 338	38 533 789	0,964 %
Rumunsko	17 321	19 043 767	0,091 %
Nizozemí	132 502	16 778 806	0,790 %
Španělsko	153 853	47 265 321	0,326 %
Česká republika	401 268	10 553 843	3,802 %
Slovensko	65 580	5 412 008	1,212 %
Německo	910 700	81 993 000	1,111 %
Rakousko	120 315	8 488 511	1,417 %

Relativní hodnoty řadí ČR na přední místa ve světě a pokud bychom porovnali naše výsledky se všemi členy asociace KSF, jsme na druhém místě. Předčili nás pouze soutěžící ze Slovinska, kterých bylo v letošním roce pouze 87 551, ale ve srovnání s populací jde o 4,235% zastoupení. O popularitě soutěže svědčí například fakt, že kategorie Klokánek se v roce 2018 účastnil téměř každý druhý žák čtvrté, resp. páté třídy ZŠ.

Matematický klokan v průběhu roku

Jak už bylo v úvodu naznačeno, mohlo by se zdát, že Matematický klokan je jednodenní záležitostí, kdy vše proběhne v třetí pátek měsíce března. To je ovšem pouze vyvrcholení. Příprava každého ročníku probíhá průběžně celý rok. Postupně se ustálilo následující schéma. Nejprve v období července a srpna organizátoři ze všech zemí předkládají individuálně na zabezpečeném serveru návrhy tzv. „klokanských“ úloh, a to v anglickém jazyce. Ty by měly splňovat následující podmínky:

- jsou přiměřené věku řešitelů,
- musejí zaujmout, být motivující,
- nejedná se o typicky školské úlohy,
- pro jejich řešení není potřeba znalosti složitého matematického aparátu, stačí školské znalosti a dobrý nápad, tzn. existuje velmi krátké a elegantní řešení,
- na jejich vyřešení postačí nejvýše 5 minut, tříbodové je možné většinou řešit tzv. „z hlavy“,
- lze je formulovat jako úlohu s výběrem odpovědi,
- zadání musí být jednoznačné a co nejkratší.

V průběhu září probíhá tzv. rating, kdy jednotlivé země mohou hodnotit navržené úlohy (v každé kategorii se obvykle objeví 120–250 návrhů úloh). Hodnotí se náročnost úlohy, přiměřenost vzhledem ke kategorii a bodovému přiřazení, „klokanskost“, tedy vhodnost pro soutěž. Ke každé úloze lze také dopsat komentář, zda v dané zemi již mají žáci dostatečné znalosti pro její řešení, případně návrh na její upřesnění.

V říjnu pak vybraný člen asociace uspořádá pětidenní setkání zástupců všech zemí spolu se zasedáním valného shromáždění Asociace Kangaroo without frontiers. Primárním účelem setkání je výběr konkrétních úloh pro jednotlivé soutěžní kategorie. Zpravidla se vybírá 30 úloh plus 5 náhradních (v kategorii Cvrček 24). Při výběru se přihlíží jednak k ratingu, ale také k učebním osnovám jednotlivých zemí. Jde o to, aby žáci stejného věku a stejného stupně vzdělání nedostali typy příkladů na učivo, které se ještě neučili. Žáci by tedy nebyli schopni takové příklady vyřešit a vůči vrstevníkům z jiných států by byli znevýhodněni. Proto má každá země možnost vypustit či změnit některé úlohy, a tím se vyhnout zmíněnému problému. Úlohy jsou seřazeny dle obtížnosti a zástupci anglicky mluvících zemí provedou jazykovou korekturu. Poslední den setkání je věnován administrativním záležitostem asociace a vybere se země, která bude pořádat další setkání o dva roky později.

Do konce listopadu probíhá (mezinárodně) především grafická úprava jednotlivých úloh tak, aby každoročně k 1. prosinci byla soutěžní zadání ve finální anglické podobě. Mnoho zemí tak má již na začátku prosince úlohy připraveny. U nás je ještě nutné úlohy přeložit do českého jazyka, o což se starají garanti jednotlivých kategorií, případně je potřeba upravit i obrazy, které se v úlohách objevují tak, aby vyhovovaly českým pravidlům a zvykům.

Zpravidla v polovině ledna je pořádán čtyřdenní workshop Klokani v Jeseníkách, kde skupina učitelů ZŠ a SŠ a pořadatelů z Univerzity Palackého připravuje finální verzi českého zadání Matematického klokana. Důraz je kladen na správnou formulaci jak z pohledu matematického a lingvistického, tak z pohledu porozumění úloze vzhledem k věku řešitele. Všechny úlohy se znovu přepočítávají a kontroluje se i vhodnost distraktorů. Z oficiální mezinárodní sady třiceti úloh je vybrána sestava 24 úloh (u kategorie Cvrček 18 ze 24 úloh). Do poloviny února zapracují garanti připomínky a soutěžní zadání jsou tak připravena pro distribuci na jednotlivé školy, která probíhá dva až tři týdny před konáním samotné soutěže. Správné výsledky jsou pak zveřejněny až v odpoledních hodinách v den konání soutěže.

Jakmile proběhne soutěžní den (je stanoven centrálně), na všech školách začíná období oprav a vyhodnocení. V tomto čase je využita struktura okresních a krajských důvěrníků a především práce učitelů na školách. Ti nejprve opraví jednotlivé úlohy v rámci tříd, resp. školy. Informace o počtu řešitelů a nejlepších řešitelích zasílají okresnímu důvěrníkovi, který sbírá údaje ze všech zapojených škol v bývalých okresech. Vybere z nich nejlepší řešitele a data předává krajskému důvěrníkovi, který je zpracuje v rámci kraje a odešle do konce května vedení soutěže na Univerzitu Palackého. Zde dojde k vyhodnocení soutěže za celou republiku a zveřejnění výsledků, připraví se diplomy i věcné ceny a vše se odešle vítězům ještě před koncem školního roku. V tuto dobu již autoři úloh vkládají své návrhy na další ročník soutěže Matematický klokan.

V některých zemích se v průběhu prázdnin ještě pořádají tábory nejlepších řešitelů, které jsou tematicky zaměřeny na řešení zajímavých matematických problémů. Česká republika sama žádný takový tábor nepořádá (na druhou stranu nevybírá startovné), ale pravidelně vysílá vybrané řešitele na mezinárodní tábor pořádaný organizátory Matematického klokana v Německu.

České stopy

Hlavním cílem organizátorů při mezinárodním setkání je vybrat co nejlepší sestavu úloh, které odpovídají znalostem a vědomostem řešitelů. Přitom ovšem v dobrém probíhá mezi jednotlivými zeměmi další soutěž o to, kolik jimi navržených úloh se nakonec dostane do finální verze zadání. Jsou zde udělovány diplomy ve třech disciplínách: nejvíce zaslaných návrhů, nejvíce vybraných úloh a nejlepší poměr mezi počtem vybraných a zaslaných

úloh. Právě v této poslední disciplíně jsme v roce 2018 získali bronzovou medaili.

Soutěžní úlohy s výběrem odpovědí, mezi něž se řadí i ty klokanské, lze řešit v podstatě následujícími způsoby:

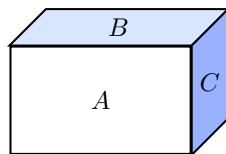
- Tipem s pravděpodobností 20 % na úspěch – samozřejmě se nejedná námi preferovaný způsob. Proto se snažíme v rámci úloh přiřazovat správné výsledky distraktorům A, B, C, D a E tak, aby celkové rozložení správných výsledků bylo co nejobecnější. Podrobněji o strategii tvorby odpovědí a s nimi spojené statistice bude pojednávat článek, který bude publikován v některém z následujících vydáních MFI.
- Správným vyřešením úlohy.
- Postupným vyzkoušením jednotlivých distraktorů a nalezením toho vyhovujícího – nelze využít u všech typů úloh.
- Eliminací nesprávných/nevyhovujících distraktorů na základě dalších atributů – např. pomocí rozměru (jednotek objemu, obsahu apod.), viz následující úlohu.
- Využitím znalosti, že správná odpověď je právě jedna. Eliminací nesprávných distraktorů, které se navzájem nevylučují.

Student (2018, 9)

Obsahy stěn kváдру na obrázku jsou A , B , C .

Vypočítejte jeho objem.

- (A) ABC (B) $2(A + B + C)$
 (C) $\sqrt{AB + BC + CA}$ (D) $\sqrt[3]{ABC}$
 (E) $\sqrt{ABC}$



Komentář: Pro jednoduché řešení si stačí uvědomit, že obsah je uváděn v jednotkách čtverečních a objem v jednotkách krychlových. Hledejme proto z nabízených distraktorů ty, které budou odpovídat jednotkám krychlovým. Můžeme vyloučit odpověď (A), prostý součin obsahů (jednotka na šestou), ale také (B), (C) a (D), neboť všechny výpočty vedou na výsledky s jednotkami čtverečními. Správně tak může být pouze odpověď (E).

České úlohy v Matematickém klokanovi

Z desítek vybraných úloh českých autorů uvedme jen některé z posledních let. Tyto úlohy je možno řešit často různými způsoby.

Junior (2018, úloha č. 21, autor J. Švrček)

Každé z celých čísel 1, 2, 3, 4, 5, 6 napíšeme právě do jednoho pole tabulky 2×3 (dva řádky, tři sloupce). Kolika různými způsoby lze čísla zapsat do této tabulky tak, aby součet čísel v každém řádku a v každém sloupci byl dělitelný třemi?

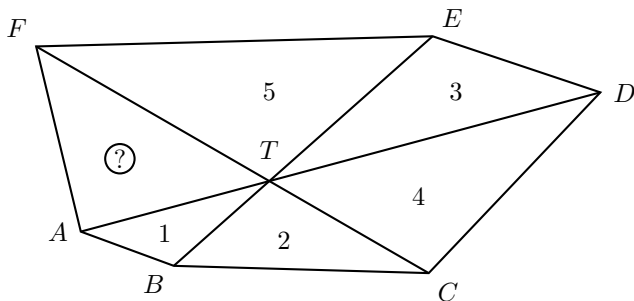
- (A) 36 (B) 42 (C) 45 (D) 48 (E) jiné číslo

Řešení: Vzhledem k požadavku dělitelnosti součtu čísel v jednotlivých sloupcích třemi, může být ve sloupci s 1 pouze 2 nebo 5. Obdobně s 2 pouze 1 nebo 4, s 3 jen 6 atd. Chceme-li do prázdné tabulky umístit např. 1, můžeme to udělat právě *šesti* způsoby. Do stejného sloupce pak můžeme umístit jen 2 nebo 5, tedy máme *dvě* možnosti. Zvolme 2. Číslo 3 lze do prázdných políček umístit *čtyřmi* způsoby a spolu s ním může být v příslušném sloupci pouze číslo 6. Pozice zbývajících čísel je pak určena jednoznačně. Podle kombinatorického pravidla součinu je pak počet možných rozmístění čísel roven $6 \cdot 2 \cdot 4 = 48$.

Student (2001, úloha č. 30, autor J. Švrček)

Úhlopříčky AD , BE , CF konvexního šestiúhelníku $ABCDEF$ se protínají ve společném bodě T . Jestliže čísla v trojúhelnících udávají jejich obsah, pak obsah trojúhelníku FAT je:

- (A) $\frac{6}{5}$ (B) 3 (C) $\frac{10}{3}$ (D) $\frac{24}{5}$ (E) jiný



Řešení: Nechť P_{XYZ} znamená obsah trojúhelníku XYZ . Potom platí

$$P_{ABT} = \frac{|AT| \cdot |BT| \sin \angle ABT}{2}, \quad P_{DET} = \frac{|DT| \cdot |ET| \sin \angle DET}{2},$$

$$P_{BCT} = \frac{|BT| \cdot |CT| \sin \angle BCT}{2}, \quad P_{EFT} = \frac{|ET| \cdot |FT| \sin \angle EFT}{2},$$

$$P_{CDT} = \frac{|CT| \cdot |DT| \sin |\sphericalangle CD|}{2}, \quad P_{FAT} = \frac{|FT| \cdot |AT| \sin |\sphericalangle FA|}{2},$$

přitom

$$|\sphericalangle AB| = |\sphericalangle DE|, \quad |\sphericalangle BC| = |\sphericalangle EF| \quad \text{a} \quad |\sphericalangle CD| = |\sphericalangle FA|.$$

Proto

$$P_{ABT} \cdot P_{CDT} \cdot P_{EFT} = P_{BCT} \cdot P_{DET} \cdot P_{FAT}.$$

Odtud již snadno určíme

$$P_{FAT} = \frac{1 \cdot 4 \cdot 5}{2 \cdot 3} = \frac{10}{3}.$$

Student (2018, úloha č. 22, autor P. Calábek)

Kolik reálných řešení má rovnice

$$||4^x - 3| - 2| = 1?$$

(A) 2

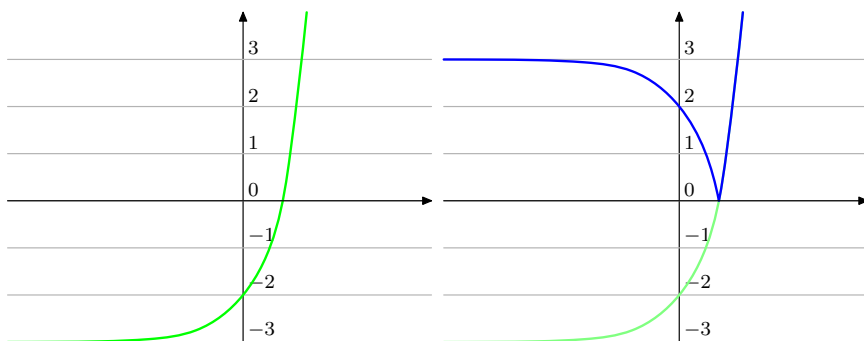
(B) 3

(C) 4

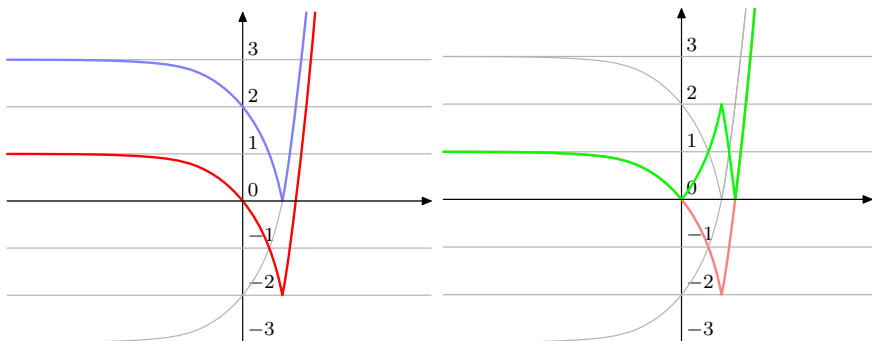
(D) 5

(E) 6

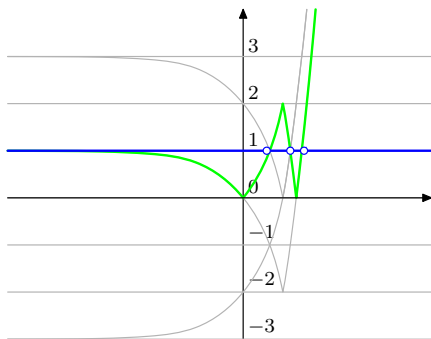
Řešení: Úlohu můžeme řešit graficky. Postupně sestavujeme graf funkce na levé straně. Zeleně je znázorněn na následujícím obrázku graf funkce $4^x - 3$. Na dalším obrázku je modrý graf funkce $|4^x - 3|$.



Vertikálním posunutím sestavíme červený graf funkce $|4^x - 3| - 2$. A konečně zelený graf funkce $||4^x - 3| - 2|$.



Zadanou úlohu nyní řešíme graficky (přímka $y = 1$ je znázorněna modře) a vidíme, že úloha má právě tři řešení.



Jiné řešení: Z rovnice

$$||4^x - 3| - 2| = 1$$

plyne

$$|4^x - 3| = 2 \pm 1,$$

proto

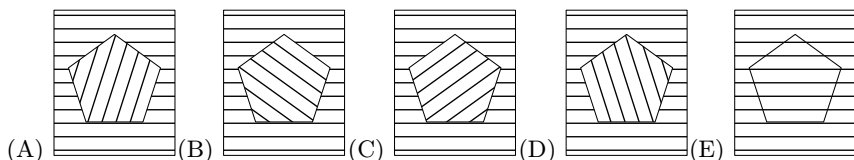
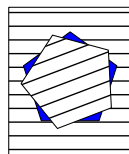
$$4^x = 3 \pm (2 \pm 1) \in \{0, 2, 4, 6\}.$$

Jelikož $4^x > 0$, mají tyto rovnice právě tři řešení:

$$x_1 = \log_4 2 = \frac{1}{2}, \quad x_2 = \log_4 4 = 1, \quad x_3 = \log_4 6 \doteq 1,292.$$

Student (2018, úloha č. 16, autor P. Calábek)

Z linkovaného listu papíru jsme vystřihli pravidelný pětiúhelník. V každém kroku jej otočíme proti směru hodinových ručiček kolem jeho středu o 21° . Na obrázku vpravo je situace po prvním kroku. Který obrázek znázorňuje situaci, kdy pětiúhelník poprvé zapadne do vystřiženého otvoru?



Řešení: Pravidelný pětiúhelník zapadne do vystřiženého otvoru, právě když se otočí o celý násobek pětiny plného úhlu, tedy o celý násobek 72° . Do vystřiženého otvoru zapadne poprvé, pokud se otočí (ve stupňové míře) o nejmenší společný násobek $72 = 2^3 \cdot 3^2$ a kroku $21 = 3 \cdot 7$, tedy o úhel (ve stupňové míře)

$$2^3 \cdot 3^2 \cdot 7 = 504 = 360 + 144.$$

Pravidelný pětiúhelník tak vykoná jednu plnou otáčku a poté se otočí ještě o 144° . Když poprvé pětiúhelník zapadne do do vystřiženého otvoru, bude situace vypadat jako na obrázku (B).

Literatura

- [1] *Association Kangourou sans Frontières* [online]. Paříž, 2018 [cit. 3.9.2018]. Dostupné z: <http://aksf.org/>
- [2] *Matematický klokan* [online]. Olomouc, 2018 [cit. 10.9.2018]. Dostupné z: <http://www.matematickyklokan.net/>
- [3] *Mathematical Kangaroo* [online]. Paříž, 2018 [cit. 20.8.2018]. Dostupné z: <https://ksf-support.org/Private/Default.aspx>
- [4] Švrček, J.: Bodové zisky v Matematickém klokanovi. Rozhledy matematicko-fyzikální, roč. 78 (2001), č. 3.

Zajímavé matematické úlohy

Uveřejňujeme další část pravidelné rubriky Zajímavé matematické úlohy a uvádíme zadání další dvojice úloh. Řešení nových úloh 249 a 250 můžete zaslat nejpozději do 20. 1. 2019 na adresu: Redakce časopisu MFI, 17. listopadu 12, 771 46 Olomouc nebo také elektronickou cestou (pouze však v $\text{\TeX}$ ovských verzích, příp. v MS Wordu) na emailovou adresu: mfi@upol.cz.

Úloha 249

V rámci městského tanečního festivalu vstoupilo i pět dívčích tanečních kroužků: hanácký, valašský, romský, slovenský a ukrajinský. Vystoupení se velmi líbila, ale nešlo o soutěž. Jitka s Bětkou si však řekly, že si stanoví výsledné pořadí alespoň pro sebe. Začaly tím, že hanácký kroužek dají výš než valašský, a rovněž že romský dají výš než ukrajinský. V této chvíli je opusťme.

Stanovte, kolik je možných různých výsledných pořadí za těchto dvou zadaných podmínek, jestliže navíc uvážíme, že na některých místech může být i více než jeden kroužek.

Stanislav Trávníček

Úloha 250

Uvnitř čtverce $ABCD$ leží bod P , pro který platí $|AP| = 1$, $|BP| = 2$ a $|CP| = 3$. Dokažte, že bod P' souměrně sdružený s bodem P podle přímky AB leží na kružnici opsané čtverci $ABCD$.

Jozef Mészáros

Dále uvádíme řešení úloh 245 a 246, jejichž zadání najdete ve třetím čísle tohoto (26.) ročníku našeho časopisu.

Úloha 245

Určete všechny funkce $f: \mathbb{R} \rightarrow \mathbb{R}$, které pro všechna reálná čísla x vyhovují rovnici

$$f(2x) + f(-2x) = x(f(3x) + x^3).$$

József Kalinowski (Kalety)

Řešení. Dosazením $x = 0$ dostaneme $2f(0) = 0$, tedy $f(0) = 0$. Nechť t je libovolné nenulové reálné číslo. V dané funkcionální rovnici položíme

nejprve $x = t$ a poté $x = -t$, dostaneme

$$\begin{aligned}f(2t) + f(-2t) &= t(f(3t) + t^3), \\f(-2t) + f(2t) &= -t(f(-3t) - t^3).\end{aligned}$$

Jelikož levé strany obou rovnic jsou stejné, dostaneme porovnáním jejich pravých stran po vydělení nenulovým číslem t rovnost $-f(3t) = f(-3t)$. Jelikož tato rovnost platí pro libovolné reálné číslo t (užitím již dokázaného $f(0) = 0$), plyne odtud, že funkce f je lichá.

Levá strana zadané rovnice je tak rovna 0 a proto pro $x \neq 0$ platí

$$f(3x) = -x^3,$$

což opět spolu s $f(0) = 0$ dává, že pro všechna reálná čísla x platí

$$f(x) = -\frac{1}{27}x^3. \quad (1)$$

Zkouškou snadno ověříme, že tato funkce je opravdu řešením dané funkcionální rovnice.

Tedy existuje jediná funkce f mající dané vlastnosti, je to funkce 1.

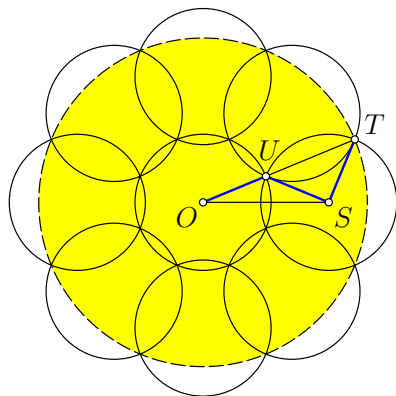
Správná řešení zaslali *Karol Gajdoš* z Trnavy, *Anton Hnáth* z Moravan, *Jozef Mészáros* z Jelky, *Vojtěch David* z WG v Ostravě-Porubě, *Matěj Doležálek* z G v Humpolci, *Viktor Fukala* a *Jakub Petr*, oba z GJK v Praze 6, *Parléřova*, *Karel Chwistek* z MG v Opavě, *Dalibor Kramář* z G v Brně-Řečkovcích, *Adam Křivka* z CMGaSOPŠ v Brně, *Tomáš Křížák* z GMK v Bílovci, *Karolína Kučerová* z G v Českém Krumlově, *Lucie Kundratová* z GaJŠ ve Zlíně, *Tomáš Sourada* z G v Žamberku a *Petr Zahradník* z GaSOŠDVŠ v Ústí nad Labem.

Úloha 246

Kruhový terč s průměrem 12 zasáhlo 10 šípů. Rozhodněte, zda vzdálenost mezi každou dvojicí šípů může být aspoň 5.

Pavel Calábek

Řešení. Kolem kruhu s vhodně zvoleným průměrem d rovnoměrně rozmístíme 8 s ním shodných kruhů dle obrázku tak, aby pokrývaly celý terč s průměrem 12. Pokud ukážeme, že $d < 5$, budou podle Dirichletova principu aspoň dva z 10 šípů ležet uvnitř téhož kruhu a tedy jejich vzdálenost bude menší než 5.



Nyní nerovnost $d < 5$ dokážeme. Označme podle obrázku O střed terče a současně střed středního kruhu, S střed jednoho z krajních kruhů a U průsečík jejich hranic. Tento průsečík leží současně na hranici s ním sousedícího kruhu a druhý průnik jejich hranic označme T . Ze symetrie podle přímky OU plyne, že body O , U a T leží na téže přímce. Navíc platí $|OU| = |US| = |ST| = \frac{1}{2}d$. Z rovnoměrnosti rozmístění plyne, že velikost úhlu SOU je $\frac{1}{2,8} 360^\circ = 22,5^\circ$, tedy velikost vnitřního úhlu při vrcholu U proti základně OS rovnoramenného trojúhelníku OUS je 145° a rovnoramenný trojúhelník UST je tak pravoúhlý. Odtud již plyne

$$\frac{1}{2}12 = |OT| = |OU| + |UT| = \frac{1}{2}d + \frac{1}{2}\sqrt{2}d = \frac{1}{2}(1 + \sqrt{2})d.$$

Dokazovaná nerovnost $d < 5$ je tak ekvivalentní po řadě s nerovnostmi

$$12 < (1 + \sqrt{2})5 = 5 + 5\sqrt{2},$$

$$7 < 5\sqrt{2},$$

$$7^2 = 49 < 50 = 2 \cdot 5^2.$$

Protože poslední nerovnost platí, dokázali jsme, že pokud terč zasáhne alespoň deset šípů, vzdálenost mezi některými dvěma bude menší než 5.

Správná řešení zaslali *Jozef Mészáros* z Jelky, *Matěj Doležálek* z G v Humpolci, *Viktor Fukala* a *Jakub Petr*, oba z GJK v Praze 6, *Parléřova*, *Dalibor Kramář* z G v Brně-Řečkovících, *Adam Křivka* z CMGaSOPŠ v Brně, *Karolína Kučerová* z G v Českém Krumlově, *Lucie Kundratová* z GaJŠ ve Zlíně a *Tomáš Sourada* z G v Žamberku.

Neúplné řešení zaslal *František Jáchim* z Volyně.

Pavel Calábek

Testování vědeckého myšlení

EVA HEJNOVÁ

Přírodovědecká fakulta UJEP, Ústí nad Labem

Současné diskuse o výsledcích českých žáků v různých národních a mezinárodních šetřeních (viz např. testování žáků 5. a 9. ročníků, které provádí Česká školní inspekce; mezinárodní šetření TIMSS a PISA) vedou odbornou i laickou veřejnost k úvahám o cílech vzdělávání i jejich změnách. S ohledem na velké množství nových informací se ukazuje jako nezbytné přenést důraz od získávání poznatků na osvojování obecných principů myšlení, označovaných také jako metakognitivní kompetence [1]. Právě přírodovědné vzdělávání umožňuje učiteli předkládat takové problémy, při jejichž řešení si žáci mohou přirozeně osvojovat metody vědeckého zkoumání, které zahrnují např. vytváření a testování hypotéz, získávání a interpretaci dat, posuzování výsledků experimentování a formulování závěrů.

Pokud učitel potřebuje otestovat úroveň vědeckého myšlení svých žáků nebo studentů, může využít *Lawsonův test vědeckého uvažování*, který je dostupný i v české verzi (viz [2, s. 182–191]). Tento test jsme zadali 165 žákům 9. ročníků základních škol a jedné kvarty víceletého gymnázia v Ústeckém kraji. V článku prezentujeme výsledky našeho výzkumu, poukazujeme na nízkou úroveň dovedností vědeckého myšlení u testované skupiny žáků a navrhuje možné způsoby nápravy námi zjištěných skutečností.

Co je to vědecké myšlení?

Vědeckým myšlením obvykle rozumíme soubor dovedností, jež vytvářejí určitou hierarchii a navzájem spolu úzce souvisejí v tom smyslu, že osvojení nižší dovednosti je obvykle předpokladem k osvojení vyšší dovednosti [3]. Patří k nim např. dovednost klást si a rozpoznat otázky, které je možno zodpovědět pomocí vědeckého zkoumání; dovednost formulovat

a ověřovat hypotézy; vyvozovat závěry ze získaných poznatků a kriticky hodnotit cizí závěry; dovednost zobecňovat a předpovídat budoucí jevy na základě současných znalostí; komunikovat získané poznatky atd. Protože se jedná o obecné dovednosti, lze je snadno využít nejen v jiných vědních disciplínách, ale i v běžných životních situacích, kdy je třeba se umět uváženě rozhodovat.

Vědecké myšlení si žáci nejlépe osvojují prostřednictvím induktivního způsobu vyučování, který je základem různých konstruktivisticky orientovaných metod. Ty stavějí především na vlastních aktivitách žáka, které často v menší, či větší míře kopírují práci vědce [4]. Důležité při tom je, aby se žáci naučili, co odlišuje vědecké myšlení od běžného přemýšlení a uvažování. Základní postupy vědecké práce si mohou žáci konkrétně osvojovat prostřednictvím určitých činností zaměřených na rozvíjení tzv. *science process skills*, které Minářechová [4] označuje jako způsobilosti vědecké práce. American Association for the Advancement of Science [5] formulovala v roce 1989 třináct těchto dovedností, které rozdělila na základní, mezi něž zařadila pozorování, měření, třídění, kvantifikace, usuzování, předpovídání, hledání vztahů a komunikaci; a vyšší (integrované) dovednosti, mezi něž patří interpretace (výklad), kontrola proměnných, definování, tvorba hypotéz a experimentování. Tento soubor představuje široce přenositelné dovednosti, které odrážejí to, jak skuteční vědci pracují. Výzkumy navíc ukázaly (viz např. [6]), že rozvoj výše uvedených dovedností (způsobilostí vědecké práce) má trvalý vliv i na rozvoj dovedností potřebných k učení jednotlivým předmětům (např. matematice, cizímu jazyku apod.).

Pro hodnocení vědeckého myšlení se v minulosti používaly různé nástroje (např. *Group Assessment of Logical Thinking Test* (GALT), *Test of Logical Thinking* (TOLT) atd.) [7]. Největší popularitu mezi výzkumníky i učiteli si pro svoji snadnou administraci získal Lawsonův test vědeckého uvažování (*Lawson's Classroom Test of Scientific reasoning* (LCTSR)) [8], který byl vytvořen na konci 70. let.

Metodologie výzkumu

V tomto článku uvádíme některé dílčí výsledky společného výzkumu, který byl realizován v roce 2017 ve spolupráci katedry fyziky a matematiky Přírodovědecké fakulty Univerzity J. E. Purkyně v Ústí nad Labem [9]. Dále uváděné výsledky se týkají vědeckého myšlení, které bylo testováno pomocí Lawsonova testu. V našem výzkumu jsme použili jeho český překlad [2, s. 182–191] a na základě výzkumů [10] jsme provedli drobnou úpravu u položek 8a a 8b.

Verze Lawsonova testu, kterou jsme použili, zahrnuje 12 párových otázek (tj. celkem 24 testových položek) se stoupající náročností. Každá z dvojice položek se skládá z otázky, po níž následuje druhá část úlohy, ve které žák vybírá zdůvodnění své odpovědi, kterou zvolil v první části úlohy.

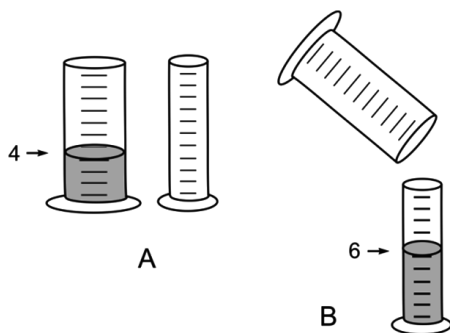
Lawsonův test umožňuje hodnotit vědecké myšlení v několika oblastech:

1. zachování hmotnosti (položky 1, 2) a vytlačeného objemu (položky 3, 4),
2. poměrové myšlení (položky 5, 6, 7, 8),
3. identifikace a kontrola proměnných (položky 9, 10, 11, 12, 13, 14),
4. pravděpodobnostní myšlení (položky 15, 16, 17, 18),
5. korelační myšlení (položky 19, 20),
6. kombinační myšlení (položky 21, 22, 23, 24).

Níže uvádíme příklady dvou párových položek z testu (5–6, 7–8), které byly zaměřeny na poměrové myšlení a u nichž jsme u testované skupiny žáků zaznamenali vůbec nejnižší úspěšnost (úlohy a obrázky jsou převzaty z [2, s. 184]).

Testové úlohy 5 a 6

5. Na obrázku jsou zobrazeny široký a úzký válec. Na válcích jsou značky ve stejných vzdálenostech od sebe. Do širšího válce je nalita voda po 4. značku (viz A). Když je voda přelita do úzkého válce, vystoupí po 6. značku (viz B). Oba válce jsou vylity (není znázorněno) a pak je do širokého válce nalita voda po 6. značku.



Jak vysoko vystoupí voda, když ji přelijeme do prázdného úzkého válce?

- a. Asi k 8. značce.
- b. Asi k 9. značce.
- c. Asi k 10. značce.
- d. Asi k 12. značce.
- e. Žádná z předchozích odpovědí není správná.

6. protože

- a. Odpověď nelze určit ze zadaných informací.
- b. V prvním případě stoupala o 2 značky, takže opět vystoupí o 2 značky.
- c. Pro každé 2 značky v širokém válci stoupne o 3 značky v úzkém.
- d. Druhý válec je užší.
- e. Vodu musíme do válců skutečně nalít a pozorovat, co se stane.

Testové úlohy 7 a 8

7. Nyní nalijeme vodu do úzkého válce (popsaného výše v bodě 5) k 11. značce. Jak vysoko voda vystoupí, když ji přelijeme do prázdného širokého válce?

- a. Asi na $7\frac{1}{2}$ (polovinu nad 7. značku).
- b. Asi k 9. značce.
- c. Asi k 8. značce.
- d. Asi k $7\frac{1}{3}$ (třetinu nad 7. značku).
- e. Žádná z předchozích odpovědí není správná.

8. protože

- a. Poměry musí zůstat stejné (tj. pro každé 3 značky v úzkém válci odečteme 2 v širším).
- b. Vodu musíme do válců skutečně nalít a pozorovat, co se stane.
- c. Odpověď nelze určit ze zadaných informací.
- d. Předtím byla výška o 2 nižší, tak musí být zas o 2 nižší.
- e. První válec je širší.

Správně odpovědi jsou 5b, 6c, 7d, 8a.

Co se týče hodnocení testu, za každou dvojici z úloh 1 až 22 mohl žák získat dva body, pokud zároveň zvolil správnou odpověď na otázku a správné odůvodnění své odpovědi. Odpovědi na úlohy 23 a 24 byly hodnoceny nezávisle, tj. žák mohl získat jeden bod za správně zodpovězenou otázku nebo za správné odůvodnění. Možná zdůvodnění u některých otázek vycházejí

z častých miskoncepcí, které byly mnohými výzkumy identifikovány (viz např. [11, 12]).

Podle celkového dosaženého skóre je možné testované žáky rozdělit do tří vývojových úrovní ([2, s. 108]):

- první vývojová úroveň (konkrétně operační): 0–8 bodů,
- druhá vývojová úroveň (přechodná): 9–16 bodů,
- třetí vývojová úroveň (formálně operační): 17–24 bodů.

Na základě zahraničních výzkumů [10] by se zhruba polovina žáků 9. ročníku měla nacházet na druhé vývojové úrovni.

Výzkumný soubor

Náš výzkumný soubor zahrnoval 165 žáků ve věku 14–15 let z osmi tříd 9. ročníku základní školy a jedné kvarty víceletého gymnázia. Všechny školy se nacházely v Ústeckém kraji (konkrétně v Ústí nad Labem, Děčíně, Litoměřicích a Teplicích). Na základě známek z českého jazyka, matematiky a fyziky, které měli žáci na pololetním vysvědčení školního roku 2016/17, lze říci, že ve výzkumném souboru byli zahrnuti žáci nadprůměrní, průměrní i podprůměrní. Aritmetický průměr známek z českého jazyka byl 2,3 se standardní odchylkou 0,96, v matematice 2,3 se standardní odchylkou 0,98 a ve fyzice 2,1 se standardní odchylkou 0,94.

Výsledky a diskuse

V Tabulce 1 uvádíme výsledky Lawsonova testu pro testovanou skupinu žáků. V jednotlivých sloupcích tabulky je uveden maximální možný bodový zisk a průměrný bodový zisk za úlohy v dané oblasti, směrodatná odchylka a průměrná úspěšnost žáků v dané oblasti (v procentech) vypočtená jako podíl průměrného bodového zisku a maximálního počtu bodů, které bylo možné v dané oblasti získat.

Úlohy zaměřené na zachování hmotnosti a vytlačeného objemu patří v testu k těm nejjednodušším. Ověřují správné vytvoření základních konceptů, na základě nichž si pak děti mohou budovat složitější mentální modely (např. model atomu). Lze tedy očekávat, že v řešení těchto úloh budou testovaní žáci nejúspěšnější. To se sice potvrdilo, nicméně z výsledků uvedených v Tabulce 1 je zřejmé, že žáci v průměru dosáhli pouze přibližně dvou třetin maximálního bodového zisku. Bodové zisky jednotlivých žáků však vykazují značný rozptyl, což poukazuje na skutečnost,

že značné procento žáků dobře nerozumí ani těmto základním pojmům (konkrétně se jedná přibližně o 19 % žáků 9. ročníku, kteří získali za tyto úlohy 0 bodů).

Poměrové myšlení patří k základním dovednostem, které jsou u dětí rozvíjeny již na 1. stupni základní školy. Úlohy v testu, jejichž úplné zadání jsme uvedli výše, byly zaměřeny na porozumění jednoduchým i složeným úměrám. V procesu učení je poměrové myšlení považováno za fundamentální dovednost, která představuje nezbytný základ pro úspěšné zvládnutí matematiky i přírodních věd [13]. V této oblasti byli žáci v naší testované skupině nejméně úspěšní, 113 žáků ze 165 (tj. 68,5 %) nevyřešilo správně ani jednu úlohu. Domníváme se, že toto zjištění ukazuje na nezvládnutí základních matematických dovedností, což může mít zásadní vliv na porozumění dalším matematickým konceptům.

Tabulka 1 Základní charakteristiky testované skupiny žáků v jednotlivých oblastech vědeckého myšlení

Oblasti vědeckého myšlení	Maximální počet bodů za úlohy v oblasti	Průměrný bodový zisk za úlohy v oblasti	Směrodatná odchylka	Průměrná úspěšnost (%)
1. Zachování hmotnosti a vytlačeného objemu	4	2,6	1,5	64,8
2. Poměrové myšlení	4	0,9	1,4	22,0
3. Identifikace a kontrola proměnných	6	1,4	1,8	24,2
4. Pravděpodobnostní myšlení	4	1,4	1,6	34,3
5. Korelační myšlení	2	0,6	0,9	29,0
6. Kombinační myšlení	4	1,1	1,0	27,5
Součet	24	8,0	-	-

Identifikace a kontrola proměnných zahrnuje zejména dovednost identifikovat proměnné a vztahy mezi nimi. Je to důležitá složka v přírodovědném zaměřeném výzkumu, která je předpokladem pro objevení nebo zkonstruování nějakého nového poznatku [14]. Pro ověření této dovednosti je do testu zařazen největší počet úloh (tři párové položky), což podtrhuje důraz kladený na tuto oblast. Při řešení těchto úloh dosáhli žáci druhé nejnížší úspěšnosti a zároveň byl v této oblasti zaznamenán vůbec největší rozptyl v bodových ziscích u jednotlivých žáků. Na základě získaných dat jsme zjistili, že přibližně 51 % žáků 9. ročníků nevyřešilo správně ani jednu úlohu.

Úlohy z testu zaměřené na pravděpodobnostní myšlení jsou založeny na klasické definici pravděpodobnosti, tj. pravděpodobnost nějakého náhodného jevu je definována jako poměr případů příznivých danému jevu ke všem možným případům, které mohou nastat. Předpokladem správného vyřešení těchto úloh je i dobrá úroveň poměrového myšlení. V této oblasti přibližně polovina žáků (53 %) nevyřešila správně ani jednu úlohu, což může souviset s jejich špatnými výsledky v oblasti poměrového myšlení.

Korelačnímu myšlení byla v testu věnována pouze jedna párová otázka, která využívala jednoduchý kontext počítání myši s různými znaky pocházejícími z určité oblasti. Tato úloha má úzký vztah k poměrovému i pravděpodobnostnímu myšlení, konkrétně k tzv. podmíněné pravděpodobnosti (tj. jestliže existuje korelace mezi počtem případů náhodného jevu A a náhodného jevu B, pravděpodobnost jevu A může ovlivňovat pravděpodobnost jevu B a naopak). Podobný typ úloh je pro naše žáky nezvyklý, což může výrazněji ovlivňovat i úspěšnost žáků v této oblasti, párovou položku (úlohy 19 a 20) nevyřešili více jak dvě třetiny žáků.

Kombinační myšlení obsahuje prvky ze všech předchozích oblastí, v testu jsou mu věnovány poslední dvě párové položky, které by měly patřit k těm nejobtížnějším. Jsou náročné nejen po obsahové stránce, ale kladou vysoké nároky i na čtenářskou gramotnost. Překvapivě v nich však testovaná skupina žáků dosáhla lepších výsledků než v „nižších“ oblastech (např. v oblasti poměrového myšlení a v oblasti identifikace a kontroly proměnných).

Pokud srovnáme výsledky žáků 9. ročníků s výsledky, které uvádějí zahraniční výzkumy [10], lze konstatovat, že naši žáci dosáhli výrazně horších výsledků zejména v prvních třech oblastech (zachování hmotnosti a vytlačeného objemu, poměrovém myšlení a identifikaci a kontrole proměnných), přičemž nejslabší výsledky jsme zaznamenali zejména v případě poměrového myšlení.

V českém prostředí lze uvést srovnání naší testované skupiny žáků se skupinou studentů učitelství pro 1. stupeň ZŠ, jejichž úroveň vědeckého myšlení byla také zjišťována pomocí Lawsonova testu [15, s. 72]. Při tomto srovnání se překvapivě ukazuje, že výsledky žáků 9. ročníků jsou vesměs ve všech oblastech lepší, než je tomu u budoucích prvostupňových učitelů, což je skutečně alarmující zjištění. Další srovnání nabízí také výzkum, který provedla Dvořáková [2, s. 111], jež zadávala Lawsonův test svým žákům v 9. ročníku. Průměrný bodový zisk 14, 8 bodu, kterého její žáci dosáhli, lze považovat za velmi dobrý výsledek, a to i ve srovnání s testovanými skupinami středoškolských studentů, jejichž výsledky ve své práci také

uvádí. Úspěch svých žáků Dvořáková připisuje zejména způsobu vedení výuky, ve které hraje velmi podstatnou roli experimentování, jež žákům dává dostatek podnětů k rozvoji vědeckého uvažování.

Základům vědeckého myšlení se učí žáci v českých školách zejména v rámci přírodovědně orientovaných oborů. Je však otázkou, do jaké míry se při tom učitelé vědomě a také systematicky zaměřují na osvojování zásad vědeckého myšlení. V českém vzdělávacím prostředí již existují některé iniciativy jednotlivých učitelů a pedagogických odborníků (např. [2, 16]) i různých sdružení (např. [17]) a projektů [18], které předkládají v praxi vyzkoušené metody, kterými je možné rozvíjet a hodnotit dovednosti vědeckého myšlení.

K rozvoji vědeckého myšlení nepochybně přispívá i badatelsky orientovaná výuka ([4, 19]), která je zaměřena na praktické aktivity a na výuku týkající se věcí a jevů spojených s reálným, každodenním životem. Navíc se tato cesta ukazuje jako vhodný způsob pro rozvoj klíčových kompetencí i v rámci nižšího primárního vzdělávání [20]. Právě badatelsky orientovaná výuka umožňuje vytvářet a rozvíjet schopnosti a dovednosti žáků hledat a objevovat, zkoumat, lépe porozumět vědeckých pojmům, objevovat vědecké principy atd. Považujeme proto za velmi důležité, aby učitelům byla v tomto směru poskytnuta konkrétní podpora např. ve formě seminářů, metodických materiálů, příkladů dobré praxe apod.

Závěr

V našem příspěvku jsme chtěli ukázat, jakým způsobem lze zjišťovat úroveň vědeckého myšlení žáků. V našem výzkumu jsme využili Lawsonův test vědeckého uvažování, který je dobře použitelný i pro studenty středních a vysokých škol. Výsledky testování ukázaly nízkou úroveň osvojení dovedností vědeckého myšlení u žáků na konci základní školy, a to zejména v oblasti poměrového myšlení a v oblasti identifikace a kontroly proměnných.

Protože jednotlivé testované oblasti nejsou nezávislé, ale vytvářejí hierarchii, tj. úspěšné zvládnutí dovedností vyšší úrovně předpokládá zvládnutí dovedností nižší úrovně, může mít podstatná část žáků závažné problémy s přechodem na třetí (formálně-operační) úroveň myšlení. Mnohé zahraniční výzkumy navíc ukazují, že rozvoj vědeckého myšlení přirozeně podporuje i rozvoj klíčových dovedností, které žáci mohou uplatnit jak v jiných oblastech vzdělávání, tak i ve svém dospělém životě.

Literatura

- [1] *Stuchlíková, I., Mareš, J.*: Rozvoj metakognitivních kompetencí žáků – otevřený úkol. *Pedagogika*, roč. (2014), č. 3, s. 267–269.
- [2] *Dvořáková, I.*: Fyzikální vzdělávání žáků a učitelů v projektu Heuréka (Dizertační práce). Univerzita Karlova, Praha, 2011. Dostupné z: <http://kdf.mff.cuni.cz/lide/dvorakova/Disertace.pdf>
- [3] *Hejnová, E., Hejna, D.*: Rozvoj vědeckého myšlení žáků prostřednictvím přírodovědného vzdělávání. *Scientia in educatione*, roč. 7 (2016), č. 2, s. 2–17.
- [4] *Minárechová, M.*: História induktívneho prístupu v prírodovednom vzdelávaní v USA a jeho súčasná reflexia na Slovensku. *Scientia in educatione*, roč. 5 (2014), č. 1, s. 2–19.
- [5] *American Association for the Advancement of Science*. Project 2061: Science for all Americans. AAAS, Washington, 1989.
- [6] *Shayer, M., Adey, P. S.*: Accelerating the development of formal thinking in middle and high school students IV: three years after a two-year intervention. *Journal of Research in Science Teaching*, roč. 30 (1993), č. 4, s. 351–366.
- [7] *Bao, L., Xiao, Y., Koenig, K., Han, J.*: Validity of the Lawson classroom test of scientific reasoning. *Physical Review Physics Education Research*, roč. 14 (2018), č. 2, 020106.
- [8] *Lawson, A. E.*: The development and validation of a classroom test of formal reasoning. *Journal of Research in Science Teaching*, roč. 15 (1978), č. 1, s. 11–24.
- [9] *Cihlář, J., Eisenmann, P., Hejnová, E., Přibyl, J.*: Pupils' abilities to solve problems in mathematics and physics and their school performance. In: Fejfar, J., Fejfarová, M., Flégl, M., Houška, M., Husák, J., Krejčí, I., Urbancová, H. (eds.): *ERIE 2018 (Efficiency and Responsibility in Education)*. Zemědělská univerzita, Praha, 2018, s. 29–35.
- [10] *Han J.*: Scientific Reasoning: Research, Development, and Assessment (Dizertační práce). The Ohio State University, Ohio, 2013.
- [11] *Driver, R., Squires, A., Rushfords, P., Wood-Robinson, V.*: Making Sense of Secondary Science. Routledge Falmer, New York, 2003.
- [12] *Stepans, J.*: Targeting Students' Science Miskonceptions. Showboard, Inc., Tampa, 2003.
- [13] *Roth, W. M., Milkent, M. M.*: Factors in the Development of Proportional Reasoning Strategies by Concrete Operational College Students. *Journal of Research in Science Teaching*, roč. 28 (1991), č. 6, s. 553–566.
- [14] *Dean, D., Kuhn, D.*: Direct instruction vs. discovery: the long view. *Science Education*, roč. 91 (2007), č. 3, s. 384–397.

- [15] Nováková, A., Chytrý, V., Říčan, J.: Vědecké myšlení a metakognitivní monitorování studentů učitelství pro 1. stupeň základní školy. *Scientia in educatione*, roč. 9 (2018), č. 1, s. 66–80.
- [16] Bělecký, Z.: Vzdělávací strategie 7. Dostupné z: <http://www.ucitel-ske-listy.cz/2010/01/zdenek-belecky-serial-vzdelavaci.09.html>
- [17] Kolektiv autorů: Průvodce pro učitele badatelsky orientovaným vyučováním. Sdružení Tereza, Praha, 2013. Dostupné z: http://www.zsmltu.cz/dum/BOV/BOV/DATA/01_PRUVODCE_PRO_UCITELE/00_PR%D9VODCE_CELA_KNIHA/01_Pruvodce_pro_ucitele.pdf
- [18] <https://kdf.mff.cuni.cz/heureka/>
- [19] Papáček, M.: Badatelsky orientované přírodovědné vyučování – cesta pro biologické vzdělávání generací Y, Z a alfa? *Scientia in educatione*, roč. 1 (2010), č. 1, s. 33–49.
- [20] Janoušková, S. a kol.: Přírodovědná gramotnost v primárním a raném období primárního vzdělávání jako prostředek zvýšení zájmu o studium přírodovědných a technických oborů. *Scientia in educatione*, roč. 5 (2014), č. 1, s. 36–49.

Inovativní demonstrace druhého Newtonova zákona

ČENĚK KODEJŠKA

Přírodovědecká fakulta UP, Olomouc

Ověření druhého Newtona zákona patří mezi základní demonstrační experimenty prvního ročníku gymnázia. Problémem tohoto experimentu je volba vhodné působící síly, která uděluje danému tělesu určité zrychlení. Klasické uspořádání se vzduchovou dráhou je většinou obtížně realizovatelné z důvodu malé přesnosti naměřených hodnot.

Uspořádání experimentu s vozíčkovou dráhou a vozíkem, který je přes kladku urychlován zavěšeným závažím, naráží zase na problém výsledného vztahu pro zrychlení vozíku, který není závislý pouze na hmotnosti vozíku m_1 , ale i na hmotnosti závaží m_2 , jak ukazuje následující vztah (1), a to i

v případě, že zanedbáme tření ($f = 0$), [1]:

$$a = \frac{g(m_2 - fm_1)}{m_1 + m_2} \quad (1)$$

Zrychlení je podle druhého Newtonova zákona definováno vztahem (2)

$$a = \frac{F}{m}, \quad (2)$$

kde F je síla působící na těleso a m je hmotnost tělesa.

Potřebujeme tedy experiment zrealizovat takovým způsobem, aby hnací síla byla přímo součástí vozíku, u kterého navíc musíme mít možnost měnit jeho hmotnost. Po několika různých zkušebních pokusech s různými typy pohonů jsme dospěli pouze k jedinému reálně možnému experimentálnímu uspořádání, jehož jednoduchost provedení a použité pomůcky zvyšují atraktivitu tohoto experimentu.

Příprava experimentu

Jako zdroj síly jsme použili elektromechanický pohon autíčka auto-dráhy, kterou jsme napájeli různým napětím. Protože velikost napájecího napětí je přímo úměrná síle vyvinuté elektromotorkem, můžeme tímto způsobem demonstrovat závislost velikosti zrychlení na působící síle. Na autíčko jsme pak pomocí modelíny dokázali připevnit ocelové válečky o hmotnostech 50 g a 100 g a při konstantním napájecím napětí pak ověřit i závislost velikosti zrychlení na hmotnosti autíčka. Jedinou nevýhodou tak zůstává pořizovací cena použitých pomůcek, která činí přibližně 800 Kč. Vliv třecích sil jsme zanedbali.



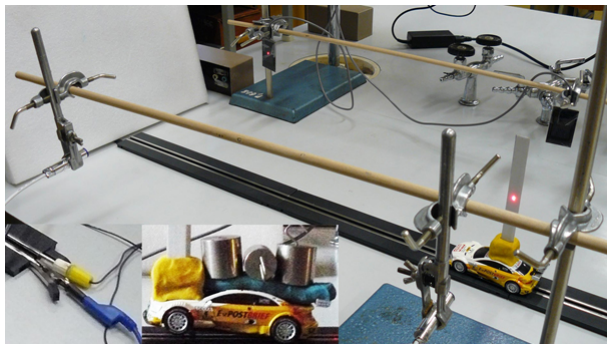
Obr. 1 Autíčko s kartonovým přerušovačem – ověření 2. Newtonova zákona

Pohybuje-li se autíčko se zrychlením, můžeme ve dvou různých okamžicích zaznamenat dvěma optickými branami (stereogatem) průchod papírového přerušovače. Pomocí jeho konstantní šířky pak můžeme vypočítat hodnoty okamžité rychlosti v_1 , v_2 autíčka při průchodu první, resp. druhou optickou branou z jednoduchého vztahu $v_n = d/t_n$, kde d je šířka přerušovače (v našem případě $d = 1 \text{ cm} = 0,01 \text{ m}$), t_n je čas, za který přerušovač projde n -tým monogatem.

K provedení experimentu budeme potřebovat následující pomůcky: dvě optické brány, laboratorní zdroj napětí, papírový přerušovač, 4 ks rovinky autodráhy o délce 30 cm, autíčko autodráhy o hmotnosti 92 g (včetně modelíny a papírového přerušovače), modelína, několik závaží 50 g a 100 g, stativový materiál, tlumící deska.

Experimentální provedení

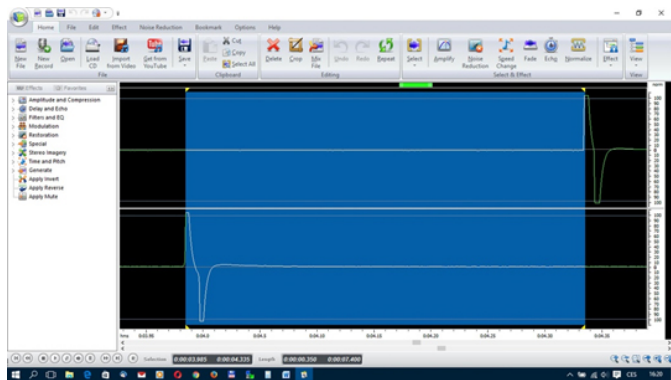
Uspořádání experimentu je na obr. 2. V levé dolní části obrázku je detail připojení napájecího napětí pomocí krokosvorky a upraveného banánu a detail upevnění přídatných závaží pomocí modelíny. Jednotlivé díly autodráhy propojíme do roviny o délce 120 cm, kterou připojíme pomocí vodičů k laboratornímu zdroji napětí. Na autíčko upevníme pomocí modelíny papírový přerušovač a za dojezdový díl autodráhy umístíme tlumící destičku z molitanu nebo podobného materiálu, která zabráni případnému poškození autíčka. Stereogate připojíme na mikrofonní vstup počítače.



Obr. 2 Uspořádání experimentu

Při ověřování závislosti zrychlení na působící síle použijeme autíčko bez přídatného závaží a měníme pouze velikost napájecího napětí v rozmezí 6 V – 12 V. Autíčko pouštíme stále ze stejné pozice a necháme ho projet

oběma optickými branami. Pomocí programu Free Audio Editor (FAE) určíme časy průchodu papírového přerušovače prvním a druhým monogatem, ze kterých určíme hodnoty okamžitých rychlostí v_1 a v_2 . Dále ve FAE změříme celkový čas Δt průchodu autíčka mezi prvním a druhým fotogatem (obr. 3) a nakonec vypočítáme hodnotu zrychlení ze vztahu $a = \Delta v / \Delta t$, kde $\Delta v = v_2 - v_1$. Naměřené hodnoty zapíšeme do tabulky a na závěr vytvoříme graf závislosti zrychlení autíčka na napájecím napětí, které je přímo úměrné síle působící na autíčko.

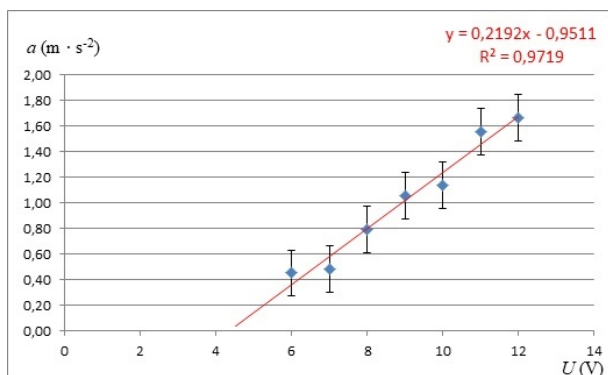


Obr. 3 Náhled signálu ve FAE

Námi naměřené hodnoty jsou uvedeny v tabulce 1 a grafická závislost zrychlení na působící síle je na obr. 4.

Tabulka 1 Měření zrychlení autíčka v závislosti na působící síle (napájecím napětí)

$\frac{U}{V}$	$\frac{t_1}{s}$	$\frac{t_2}{s}$	$\frac{v_1}{m \cdot s^{-1}}$	$\frac{v_2}{m \cdot s^{-1}}$	$\frac{\Delta v}{m \cdot s^{-1}}$	$\frac{\Delta t}{s}$	$\frac{a}{m \cdot s^{-2}}$
6	0,016	0,012	0,625	0,833	0,21	0,461	0,45
7	0,014	0,011	0,714	0,909	0,19	0,400	0,49
8	0,012	0,009	0,833	1,111	0,28	0,350	0,79
9	0,011	0,008	0,909	1,250	0,34	0,323	1,06
10	0,011	0,008	0,909	1,250	0,34	0,300	1,14
11	0,010	0,007	1,000	1,429	0,43	0,275	1,56
12	0,009	0,007	1,111	1,538	0,43	0,256	1,67



Obr. 4 Graf závislosti zrychlení autíčka na působící síle (napájecím napětí)

Ve druhé části experimentu ponecháme konstantní velikost napájecího napětí a zvyšujeme velikost hmotnosti autíčka přidáváním závaží na autíčko. Opět určíme pro každou hmotnost autíčka jeho zrychlení a sestojíme graf závislosti zrychlení na hmotnosti autíčka.

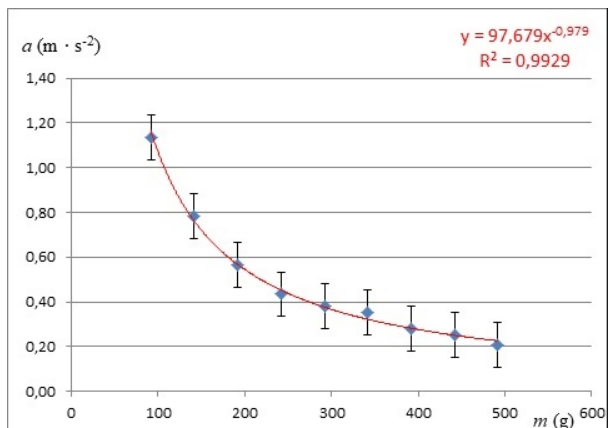
Námi naměřené hodnoty jsou uvedeny v tabulce 2 a grafická závislost zrychlení na hmotnosti vozíku pro napájecí napětí $U = 10 \text{ V}$ je na obr. 5.

Tabulka 2 Měření zrychlení autíčka v závislosti na jeho hmotnosti pro $U = 10 \text{ V}$

$\frac{m}{\text{g}}$	$\frac{t_1}{\text{s}}$	$\frac{t_2}{\text{s}}$	$\frac{v_1}{\text{m} \cdot \text{s}^{-1}}$	$\frac{v_2}{\text{m} \cdot \text{s}^{-1}}$	$\frac{\Delta v}{\text{m} \cdot \text{s}^{-1}}$	$\frac{\Delta t}{\text{s}}$	$\frac{a}{\text{m} \cdot \text{s}^{-2}}$
92	0,011	0,008	0,909	1,250	0,34	0,300	1,14
142	0,014	0,010	0,714	1,000	0,29	0,364	0,78
192	0,015	0,011	0,667	0,909	0,24	0,428	0,57
242	0,018	0,013	0,556	0,769	0,21	0,492	0,43
292	0,019	0,014	0,526	0,714	0,19	0,495	0,38
342	0,022	0,015	0,455	0,667	0,21	0,600	0,35
392	0,025	0,017	0,400	0,588	0,19	0,670	0,28
442	0,026	0,018	0,385	0,556	0,17	0,671	0,25
492	0,027	0,019	0,370	0,526	0,16	0,742	0,21

Z grafu lineární regresní funkce na obr. 4, která je vyznačena červenou barvou, je dobře vidět lineární závislost zrychlení na působící síle. Stejně tak na obr. 5 je dobře pozorovatelná hyperbolická křivka nepřímé

úměrnosti mezi zrychlením a hmotností autíčka. Hodnota exponentu této regresní křivky je $-0,979 \doteq -1$, což odpovídá vztahu (2).



Obr. 5 Graf závislosti zrychlení autíčka na jeho hmotnosti

V článku jsme se zabývali inovací experimentálního ověření zákona síly, při kterém jsme k demonstraci využili pro žáky atraktivní pomůcky jako je autodráha a počítač.

Pomocí dvou optických bran sestavených z laserového ukazovátka a solárního článku jsme zaznamenali průchod autíčka a v programu FAE určili časy průchodu jednotlivými branami i celkový čas pohybu.

Experimentálně naměřené hodnoty potvrdily jak lineární závislost zrychlení na působící tažné síle, tak hyperbolický pokles zrychlení v závislosti na hmotnosti autíčka.

Závěrem lze konstatovat, že demonstrace druhého Newtonova zákona pomocí výše uvedených jednoduchých pomůcek umožňuje žákům rychlé pochopení probírané látky a učitelům fyziky snadnou demonstraci tohoto zákona, než provedení klasickým způsobem pomocí vzduchové nebo vozíčkové dráhy. Současné využití ICT při této demonstraci posiluje také mezipředmětové vazby a zvyšuje pro žáky atraktivitu demonstračního experimentu.

Literatura

- [1] Horáková, R.: Pohyb soustavy těles spojených vláknem. Studijní text pro řešitele FO, (2014) [online]. Dostupné z: <http://fyzikalniolympiada.cz/texty/pohyb.pdf>

Návrh pracovného listu k apletu na zákony zachovania energie

ZUZANA GIBOVÁ

Fakulta elektrotechniky a informatiky, Technická univerzita v Košiciach, SLOVENSKO

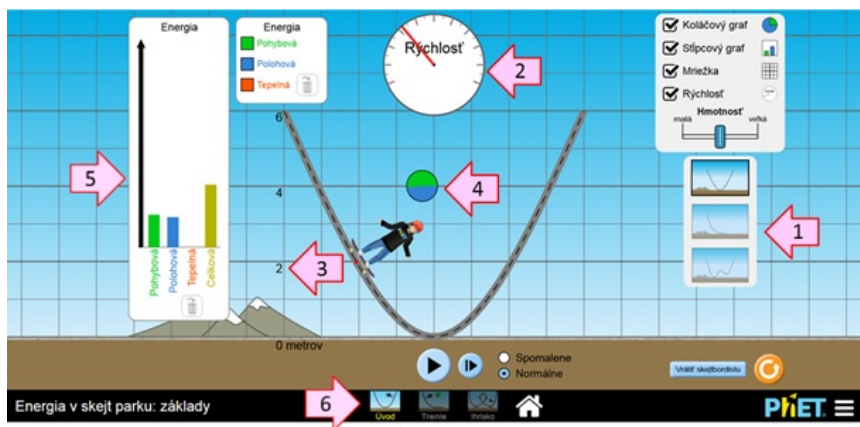
Úvod

Vo výučbe fyziky sa bežne používajú aplety, ktoré umožňujú demonštrovať rôzne javy, deje a zákonitosti v závislosti od rôznych počiatočných podmienok. Na internete je možné nájsť veľa fyzikálnych apletov. Väčšina z nich obsahuje popis ako aplet funguje a čo demonštruje. Aby výučba s apletmi bola efektívna, je vhodné k apletom vytvoriť pracovný list, ktorý by obsahoval inštrukcie k používaniu apletov a otázky a úlohy pomocou ktorých žiaci pochopia demonštrované javy. V opačnom prípade, ak žiaci nevedia čo majú pomocou apletu sledovať a aké majú nastaviť podmienky, unikne im fyzikálna podstata javov a zamerajú sa len na technickú stránku apletu [1]. V článku je prezentovaný pracovný list vytvorený k apletu, ktorý demonštruje zákony zachovania energie a príslušné premeny energie v ideálnych a reálnych podmienkach.

Popis apletu

Pracovný list bol vytvorený k apletu Energia v skejt parku zo zdroja [2].

Aplet demonštruje pohyb skejtbordistu na troch rôznych rampách (obr. 1), ktoré je možné voliť v pravej časti apletu (1). Okrem toho zobrazuje rýchlosť skejtbordistu (2), jeho polohu (výšku nad povrchom zeme – 3), koláčový (4) a stĺpcový (5) diagram energii pri jeho pohybe. Polohu a hmotnosť skejtbordistu je možné meniť. Aplet má tri úrovne (6). Prvá úroveň (Úvod) je zameraná na demonštrovanie zmien energii pri pohybe skejtbordistu a zákona zachovania mechanickej energie, teda pri ideálnych podmienkach. Druhá úroveň (Trenie) umožňuje nastaviť ľubovoľnú hodnotu trenia a pozorovať ako dochádza ku stratám energie a k premenám energie skejtbordistu za reálnych podmienok. V tejto úrovni je možné demonštrovať zákon zachovania energie.



Obr. 1 Aplet Energia v skejt parku

Tretia úroveň (ihrisko) umožňuje vytvárať vlastnú rampu na skejt a pozorovať tie isté zákony a deje ako v predchádzajúcich úrovniach.



Obr. 2 Ovládanie apletu

Ovládanie apletu je na obr. 2. Aplet možno spustiť a zastaviť (1), krokovať (2), spomaliť (3), obnoviť aplet na pôvodné podmienky (5) a vrátiť skejtbordistu do počiatočnej polohy (4).

Pracovný list

Pracovný list je navrhnutý na použitie druhej úrovne apletu (trenie) na prvej z rámp (U rampe).

Je zameraný

- na zopakovanie a upevnenie pojmov kinetická energia, potenciálna energia, mechanická energia, celková energia,
- demonštrovanie a pochopenie zákona zachovania mechanickej energie,
- demonštrovanie a pochopenie zákona zachovania energie,
- pochopenie premien energií skejtbordistu pri pohybe na rampe,
- ukázanie vplyvu trenia na pohyb, premeny a straty energií,
- ukázanie vplyvu zmeny hmotnosti na celkovú energiu.

Pracovný list pozostáva z troch častí (obr. 3). V úvode obsahuje inštrukcie k nastaveniu počiatočných podmienok, ktoré umožnia demonštrovať očakávané fyzikálne javy a zákonitosti. V druhej časti pracovný list obsahuje otázky na zopakovanie a pochopenie pojmov a zákonov. Žiaci si odpovede na otázky zapisujú do pracovného listu na základe pozorovania pohybu skejtbordistu na aplete, najprv bez zobrazenia rýchlosti a energie skejtbordistu. Správnosť svojich odpovedí si overujú opäť pomocou apletu, kde sú už zobrazované rýchlosť a energie skejtbordistu pomocou stĺpcových grafov. Tretia časť obsahuje úlohy, pri riešení ktorých žiaci použijú aplet.

Pracovný list k apletu Energia v skejt parku

Otvorte si aplet Energia v skejt parku – trenie do nového okna zo zdroja:
https://phet.colorado.edu/sims/html/energy-skate-park-basics/latest/energy-skate-park-basics_sk.html



V pravej časti apletu vyberte U rampu. Nastavte nasledovné počiatočné podmienky:
Zaškrtnite políčko: Mriežka. **Nastavte** hmotnosť na polovičnú hodnotu. **Trenie nastavte** na žiadne.
 Pomocou myši uchopte skejtbordistu a položte ho na U rampu do výšky 4 m a spustite aplet. Pozorujte pohyb skejtbordistu. Aplet môžete kedykoľvek zastaviť, spomaliť alebo sledovať po krokoch.

Odpovedzte na nasledujúce otázky:

Predpokladajte, že hladina nulovej potenciálnej energie je na povrchu zeme.

1. V ktorom bode svojej trajektórie (na U rampe) má skejtbordista len potenciálnu (polohovú) energiu?
2. V ktorom bode svojej trajektórie (na U rampe) má skejtbordista len kinetickú (pohybovú) energiu?
3. V ktorom bode svojej trajektórie (na U rampe) má skejtbordista nenulovú kinetickú aj potenciálnu energiu?
4. Ako je daná celková energia skejtbordistu v bode 0 m, 2 m a 4 m nad zemou? Čo platí pre mechanickú energiu v týchto miestach?

Pri overení správnosti odpovedí použite aplet. Nastavte nasledovné počiatočné podmienky:
Zaškrtnite políčka: Mriežka, stĺpcový diagram, rýchlosť. **Nastavte** hmotnosť na polovičnú hodnotu. **Trenie nastavte** na žiadne.
 (Sledujte ako sa mení rýchlosť a jednotlivé energie v stĺpcovom grafe.)

Riešte nasledujúce príklady:

Skejtbordista začína svoj pohyb na U rampe vo výške 4 m. Hmotnosť skejtbordistu je 80 kg. Predpokladajte, že hladina nulovej potenciálnej energie je na povrchu zeme. Riešte najprv všeobecne, potom dosadzte konkrétne hodnoty. Pri riešení použite aj aplet, ktorý môžete kedykoľvek zastaviť, spomaliť alebo sledovať po krokoch.

Obr. 3 Ukážka pracovného listu k apletu

1. Inštrukcie k apletu

Otvorte si aplet Energia v skejt parku zo zdroja [2].

Zvoľte úroveň Trenie. V pravej časti apletu vyberte U rampu. Nastavte nasledovné počiatočné podmienky:

Zaškrtnite políčko: Mriežka. Nastavte hmotnosť na polovičnú hodnotu. Trenie nastavte na žiadne.

Pomocou myši uchopte skejtbordistu a položte ho na U rampu do výšky 4 m a spustite aplet. Pozorujte pohyb skejtbordistu. Aplet môžete kedykoľvek zastaviť, spomaliť alebo sledovať po krokoch.

2. Otázky

Odpovedzte na nasledujúce otázky:

Predpokladajte, že hladina nulovej potenciálnej energie je na povrchu zeme.

1. V ktorom bode svojej trajektórie (na U rampe) má skejtbordista len potenciálnu (polohovú) energiu?

.....

2. V ktorom bode svojej trajektórie (na U rampe) má skejtbordista len kinetickú (pohybovú) energiu?

.....

3. V ktorom bode svojej trajektórie (na U rampe) má skejtbordista nenulovú kinetickú aj potenciálnu energiu?

.....

4. Ako je daná celková (mechanická) energia skejtbordistu vo výške 0 m, 2 m, a 4 m nad zemou? Čo platí pre mechanickú energiu v týchto miestach?

.....

5. Do akej maximálnej výšky vystúpi skejtbordista na pravej strane U rampy, ak svoj pohyb začína na ľavej strane U rampy vo výške 5 m? Akú rýchlosť bude dosahovať na pravej a ľavej strane U rampy vo výške 3 m? Vysvetlite prečo.

.....

Pri overení správnosti odpovedí použite aplet. Nastavte nasledovné počiatočné podmienky:

Zaškrtnite políčka: Mriežka, stĺpcový diagram, rýchlosť. Nastavte hmotnosť na polovičnú hodnotu. Trenie nastavte na žiadne. (Sledujte ako sa mení rýchlosť a jednotlivé energie v stĺpcovom grafe.)

6. Zmeňte počiatočné podmienky. Nastavte trenie na polovičnú hodnotu. Zaškrtnite políčko: Mriežka. Nastavte hmotnosť na polovičnú hodnotu. Pomocou myši uchopte skejtbordistu a položte ho na U rampu do výšky 4 m a spustite aplet.

a) Pozorujte pohyb skejtbordistu. Do akej výšky vystúpi na pravej strane U rampy po prvom prechode najnižšou polohou?

b) Aká bude jeho rýchlosť v najnižšom bode po jednom prejdení U rampy?

c) Pozorujte pohyb skejtbordistu až do zastavenia. Ako je daná jeho celková energia na začiatku jeho pohybu? Ako je daná jeho celková energia na konci pohybu? Aká je jeho mechanická energia na začiatku a na konci pohybu? Vysvetlite.

Pri overení správnosti odpovedí použite aplet. Nastavte nasledovné počiatočné podmienky:

Zaškrtnite políčka: Mriežka, stĺpcový diagram, rýchlosť. Nastavte hmotnosť na polovičnú hodnotu. Trenie nastavte na polovičnú hodnotu. (Sledujte ako sa mení rýchlosť a jednotlivé energie v stĺpcovom grafe.)

3. Úlohy

Skejtbordista začína svoj pohyb na U rampe vo výške 4 m. Hmotnosť skejtbordistu je 80 kg. Predpokladajte, že hladina nulovej potenciálnej energie je na povrchu zeme. Riešte najprv všeobecne, potom dosadzte konkrétne hodnoty. Pri riešení použite aj aplet, ktorý môžete kedykoľvek zastaviť, spomaliť alebo sledovať po krokoch.

1. Vypočítajte celkovú energiu skejtbordistu, ktorú dosahuje na začiatku pohybu vo výške 4 m nad zemnou.

2. Vypočítajte maximálnu rýchlosť, ktorú pri svojom pohybe dosahuje. (Overte svoj výpočet pomocou apletu. Ukazovateľ rýchlosti má hlavné dieliky delené po 2 m/s.)

3. Určte kinetickú energiu vo výške 3 m.

4. Pomocou apletu určte, v akej výške bude potenciálna energia skejtbordistu rovná kinetickej energii. Potvrďte výsledok aj výpočtom.

5. Zmeňte hmotnosť skejtbordistu (zväčšite potom zmenšite) vzhľadom na pôvodnú hodnotu hmotnosti. Pomocou apletu určte, aká bude jeho maximálna rýchlosť pre všetky zvolené hmotnosti. Aká bude potenciálna a kinetická energia skejtbordistu v rôznych výškach pre všetky zvolené hmotnosti. Výsledky potvrďte aj výpočtom pre hmotnosti 50 kg, 70 kg, 100 kg.

6. Vypočítajte aká bude strata energie po jednom prejazde U rampy, ak predpokladáme vplyv trenia na pohyb skejtbordistu (nastavte trenie na aplete na polovičnú hodnotu). Skejtbordista začína svoj pohyb na U rampe vo výške 4 m. Hmotnosť skejtbordistu je 80 kg. Predpokladajte, že hladina nulovej potenciálnej energie je na povrchu zeme.

Výsledky:

1. $E = mgh_{\max} = 80 \cdot 10 \cdot 4 \text{ J} = 3\,200 \text{ J}$

2. $v_{\max} = \sqrt{2gh_{\max}} = 8,94 \text{ m/s}$, z apletu $v_{\max} = 8,9 \text{ m/s}$

3. $E_{k3} = mgh_{\max} - mgh_3 = (3\,200 - 80 \cdot 10 \cdot 3) \text{ J} = 800 \text{ J}$

4. $mgh_{\max} = 2mgh \rightarrow h = \frac{1}{2}h_{\max} = 2 \text{ m}$, z apletu $h = 2 \text{ m}$

5. Zmena hmotnosti ovplyvní hodnotu potenciálnej a kinetickej energie. Na aplete sa to prejaví rôznou výškou stĺpcového grafu, ktorý zobrazuje príslušnú energiu. Čím väčšia je hmotnosť, tým väčšia je príslušná energia. Pre $m = 50 \text{ kg}$ závisí potenciálna energia od výšky podľa vzťahu $E_p = mgh = (50 \cdot 10) h$ a kinetická energia závisí od rýchlosti podľa vzťahu $E_{pk} = \frac{1}{2}mv^2 = 25v^2$. Hodnota maximálnej rýchlosti nezávisí od hmotnosti skejtbordistu, vyplýva to zo vzťahu $v_{\max} = \sqrt{2gh_{\max}}$. Dosahuje rovnaké maximálne rýchlosti pre rôzne hmotnosti.

6. Po jednom prechode U rampy vystúpi skejtbordista do maximálnej výšky $h_{1\max} = 3 \text{ m}$ (na pravej strane U rampy) pri zvolenej hodnote trenia. Potom použitím zákona zachovania energie $E = E_k + E_p + E_s = \text{konš.}$

Strata energie je

$$E_{s1} = mgh_{\max} - mgh_{1\max} = (3\,200 - 80 \cdot 10 \cdot 3) \text{ J} = 800 \text{ J}.$$

Aplikácia vo výučbe

Výučba s prezentovaným pracovným listom bola realizovaná na numerických cvičeniach z fyziky na Fakulte elektrotechniky a informatiky Technickej univerzity v Košiciach. Vyučovanie prebiehalo v tradičnej triede s tabuľou, kde bol k dispozícii jeden počítač s dataprojektorom a plátnom. Preto bol aplet premietaný na plátno a ovládaný učiteľom. Všetci študenti mali vlastný pracovný list, do ktorého si zapisovali odpovede na otázky. Potom nasledovala spoločná kontrola správnosti odpovedí pomocou apletu. Početnosť správnych odpovedí sa zisťovala zdvihnutím rúk študentov. Riešenie úloh prebiehalo spoločné s použitím apletu, ktoré bolo doplnené o riešenie úloh podobného typu z predpísanej zbierky úloh. Výučba trvala 1,5 hod., z toho pomocou apletu asi polovicu času. V skupinách bolo okolo 25 študentov.

Výučba s navrhovaným pracovným listom môže prebiehať aj v malých skupinách v počítačovej miestnosti, kde na jedného študenta pripadá jeden počítač. V tomto prípade je učiteľ vo funkcii koordinátora činnosti študentov a ich poradcom.

Ďalšie možnosti

Aplety je možné používať v ľubovoľnej časti výučby (motivácia, výklad učiva, aplikácia učiva, zopakovanie). Máme skúsenosť s ich používaním na prednáškach, na cvičeniach a v rámci domácej prípravy [3]. Je dôležité, aby ku každej poznávacej činnosti mali študenti pripravený pracovný list. K prednáškam majú študenti k dispozícii pracovné listy na stránke vyučujúcej, kde sa k nim môžu po prednáške a v rámci prípravy na skúšku vrátiť [4]. Uvádzam niekoľko príkladov pracovných listov na rôzne výučbové činnosti:

- motivácia
<http://people.tuke.sk/zuzana.gibova/aplet8.htm>
- výklad nového učiva
<http://people.tuke.sk/zuzana.gibova/files/aplet-rychlostt.pdf>
- aplikácia učiva
<http://people.tuke.sk/zuzana.gibova/files/aplet-priamo-iare-pohyby.pdf>
<http://people.tuke.sk/zuzana.gibova/files/aplet-zrychleniet.pdf>
- domáca úloha
<http://people.tuke.sk/zuzana.gibova/ApletEnergia2.pdf>

V rámci domácej prípravy boli aplety s pracovným listom použité v externej forme výučby, kde mali študenti vypracovať semestrálne zadanie s riešením úloh pomocou apletov. Návrh úloh nájdete na [5].

Efektivita výučby

Použitie apletu na zákony zachovania energie na numerických cvičeniach z fyziky na Fakulte elektrotechniky a informatiky Technickej univerzity v Košiciach bolo zámerne, pretože študenti na zápočtových písomkách pri riešení podobných úloh dosahovali zle výsledky. Navyše, sa na cvičeniach riešili úlohy, v ktorých teleso padalo voľným pádom alebo bolo vrhnuté zvislo nahor, vždy len za ideálnych podmienok.

Z dotazníkového prieskumu vyplynulo, že sa študentom výučba s použitím apletu páčila. Bola viac atraktívnejšia, názorná, viac si zapamätali. Výsledky zápočtových písomiek potvrdili, že sa zvýšila správnosť riešenia podobných úloh.

Zvýšenie úspešnosti riešenia úloh pomocou apletov za použitia pracovného listu potvrdzuje aj náš prieskum uskutočnený u študentov v externej forme výučby. Súčasne sa ukázalo, že použitie apletov pri riešení semestrálneho zadania viedlo k lepšiemu pochopeniu vzťahov medzi teóriou a praxou študentmi [6].

Výsledky viacerých našich dotazníkových prieskumov uskutočnených medzi študentmi denného štúdia poukazujú na to, že výučba s použitím apletov je pre nich atraktívnejšia a pracovné listy k apletom sú pre nich jasne a zrozumiteľne vytvorené [7].

Záver

Aplety sú vhodným vyučovacím prostriedkom, pomocou ktorého sa výučba stáva atraktívnejšou a názornejšou. Ak je pri výučbe s apletmí používaný pracovný list, stáva sa výučba efektívnejšou. Viaceré výskumy skúmajúce integráciu apletov do výučby technických a prírodovedných predmetov uvedené v [8] potvrdzujú, že aplikácia apletov vo výučbe prispieva k dosiahnutiu vyššej úrovne kognitívnych vedomostí študentov, vedie študentov k lepšiemu pochopeniu vzťahov medzi teóriou a praxou, podporuje záujem študentov o preberanú problematiku a pomáha zvyšovať motiváciu študentov.

Literatura

- [1] Rakovská, M.: Modelovanie fyzikálneho poznávania prostredníctvom apletov. In: DIDFYZ 2004, s. 288–292.
- [2] https://phet.colorado.edu/sims/html/energy-skate-park-basics/latest/energy-skate-park-basics_sk.html
- [3] Gibová, Z., Fričová, O., Hutníková, M.: Applets in physics teaching. In: 19th Conference of Czech and Slovak Physicists. Košice, 2017, s. 89–90.
- [4] <http://people.tuke.sk/zuzana.gibova/prednasky---materialy.html>
- [5] <http://people.tuke.sk/olga.fricova/zadania.htm>
- [6] Fričová, O., Hutníková, M., Gibová, Z.: Interaktívne aplety vo výučbe fyziky. In: Výskumné a edukačné aktivity na katedrách fyziky technických univerzít. Bratislava, 2008, s. 43–46.
- [7] Gibová, Z., Fričová, O., Hutníková, M.: Aplety vo vyučovaní fyziky. Obzory MFaI, 39 (2010), č. 2, s. 45–50.
- [8] Žlvecký, M., Gabriška, D.: Motion capture as an extension of web-based simulation. Applied Mechanics and Materials, 513–517, (2014), s. 827–833.

Moderní šifry II

EDUARD BARTL

Přírodovědecká fakulta UP, Olomouc

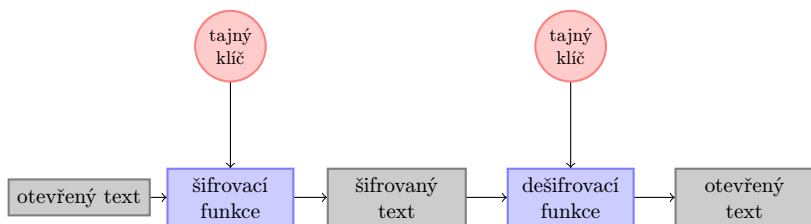
Předchozí díl série článků o šifrování byl zakončen výkladem jedno-
směrných šifrovacích funkcí se zadními vrátky. Tyto funkce jsou důležité
proto, že pomocí nich jsme schopni realizovat asymetrické šifrování. V zá-
věru jsme si řekli, že pro další výklad bude užitečné seznámit se s takzvanou
modulární aritmetikou. Tato aritmetika se od běžné aritmetiky v ledačem
liši, v tomto pokračování se ji proto pokusíme podrobně vysvětlit. Dále se
vrátíme k asymetrickému šifrování, vysvětlíme si, jak funguje šifra RSA a
jak se používá v praktických aplikacích (například v elektronickém pod-
pisu). Článek je doplněn dvěma řešenými úkoly, na kterých si může čtenář
ověřit pochopení textu.

Na úvod krátké opakování

V předešlém dílu jsme si ukázali princip asymetrického šifrování. Než
se podíváme na slíbenou modulární aritmetiku, kterou budeme potřebovat
pro podrobný výklad asymetrické šifry RSA, zopakujeme si, jak asymet-
rické šifrování funguje a jaký je jeho vztah k symetrickému šifrování.

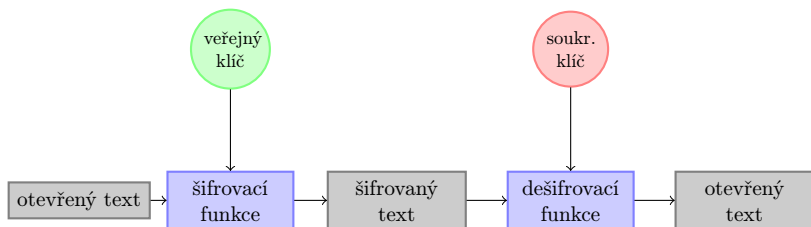
Princip symetrického šifrování můžeme znázornit pomocí diagramu na
obr. 1. Podstatné na symetrickém šifrování je skutečnost, že odesílatel
(Alice) i příjemce (Bob) disponují stejným klíčem, pomocí kterého Alice
zašifruje otevřený text a Bob pomocí něj zašifrovaný text opět dešifruje.
Pokud nějaká třetí osoba (Eva) získá tento klíč, může dešifrovat libovolnou
zachycenou zprávu. Z tohoto důvodu je nutné tento klíč udržet v tajnosti.
Proto je tento klíč nazýván *tajným*.

Problematické na symetrickém šifrování je zejména to, že se Alice i
Bob musí na tajném klíči dohodnout. Tento problém velmi elegantně řeší



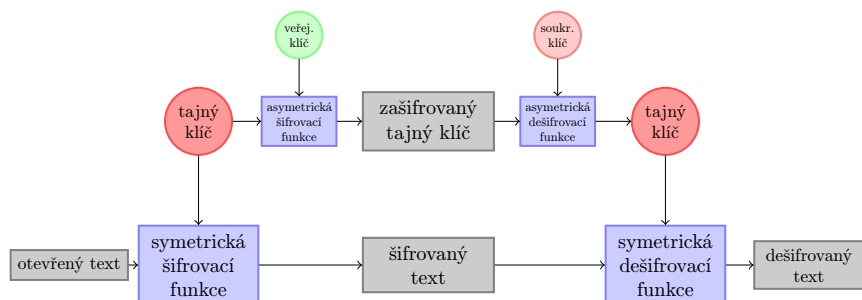
Obr. 1 Schéma symetrického šifrování

asymetrické šifrování, jehož princip je schematicky ukázán na obr. 2. Tento způsob šifrování již nepoužívá jediný klíč, ale používá klíče dva – jeden k šifrování, druhý k dešifrování. Klíč určený k šifrování může být zveřejněn (proto se mu také říká *veřejný klíč*), naopak klíč určený k dešifrování musí být udržen v soukromí (na což poukazuje jeho název – *soukromý klíč*). Přestože jsou tyto dva klíče různé, existuje mezi nimi určitý vztah. Veřejný klíč musí být snadno a rychle odvoditelný ze soukromého klíče; odvodit soukromý klíč z veřejného však musí být velmi obtížné, časově neschůdné. Právě tomuto vztahu bude v tomto dílu věnována pozornost.



Obr. 2 Schéma asymetrického šifrování

Připomeňme také krátce, že v praktických aplikacích se oba přístupy – symetrické šifrování a asymetrické šifrování – vhodným způsobem kombinuje. Šifrování dat se provádí symetricky, asymetrické šifrování se používá pouze pro výměnu tajného klíče tak, jak ukazuje schema na obr. 3. Tento přístup se volí proto, že symetrické šifrovací algoritmy jsou řádově rychlejší než asymetrické. Tím, že se objemná data šifrují symetricky a krátký tajný klíč asymetricky, je tak celý šifrovací proces významným způsobem urychlen.

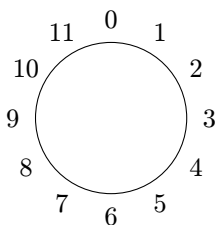


Obr. 3 Použití asymetrického šifrování při výměně tajného klíče

Počítání v kruhu

Pokračujme nyní ve slíbeném výkladu modulární aritmetiky. Této aritmetice se někdy říká *hodinová aritmetika*. Příklad s hodinami je trefný a umožní nám rychle pochopit podstatu věci.

Představme si klasický hodinový ciferník, jenž ukazuje čas v dvanácti-hodinovém cyklu. Tento ciferník však mírně upravíme: místo, aby ukazoval hodiny od 1 do 12, bude ukazovat hodiny od 0 do 11. Číslo od 1 do 11 tedy zůstanou na svých místech, pouze číslo 12 nahradíme číslem 0, jak můžeme vidět na obr. 4. Tato změna nikterak neovlivní způsob počítání, na který jsme zvyklí; cyklus je stále dvanáctihodinový, pouze budeme *dvanácté* hodině říkat *nultá* hodina.



Obr. 4 Dvanáctihodinový ciferník

Počítání na takovém ciferníku je nám dobře známé. Pokud například dvouhodinové divadelní představení začíná v 11 hodin, pak jeho konec (počítáno v dvanáctihodinovém cyklu) není v 13 hodin, ale v 1 hodinu,

můžeme tedy napsat $11 \oplus 2 = 1$; pro operaci sčítání v hodinové aritmetice jsme zvolili symbol $\oplus$, abychom ji odlišili od operace sčítání $+$, kterou běžně používáme.¹⁾

Jak by se dala popsat operace sčítání $\oplus$ v hodinové aritmetice pomocí běžného sčítání $+$? Podle předchozího příkladu se začátkem a koncem divadelního představení by se mohlo zdát, že jakmile dojde běžným součtem k „přetečení“, tak jednoduše od výsledku odečteme číslo 12, čímž se vrátíme zpět na číslo zobrazitelné na ciferníku. Mohli bychom tedy napsat:

$$11 \oplus 2 = 11 + 2 - 12 = 1.$$

Takto pojatá definice operace $\oplus$ však nebude fungovat vždy. K „přetečení“ totiž může dojít několikanásobně, odečtení čísla 12 pak k návratu na ciferník nepomůže. Například u součtu $11 \oplus 16$ musíme číslo 12 odečíst dvakrát:

$$11 \oplus 16 = 11 + 16 - 2 \cdot 12 = 3.$$

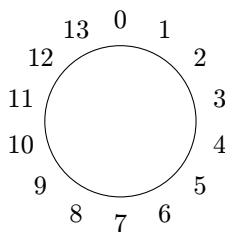
Čtenář již možná tuší, že správnou definici operace $\oplus$ pomocí operace $+$ je možné vyslovit s použitím *zbytku po celočíselném dělení*: součet $a \oplus b$ je roven zbytku po vydělení běžného součtu $a + b$ číslem 12. Skutečně, $11 + 16 = 27$; tento součet vydělíme číslem 12, podílem je pak 2, zbytek je 3. Platí tedy $11 \oplus 16 = 3$, jak jsme ostatně viděli výše. Operace odečítání se definuje obdobně: rozdíl $a \ominus b$ je roven zbytku po vydělení běžného rozdílu $a - b$ číslem 12.

Je celkem zřejmé, že operace $\oplus$ a $\ominus$ se dají jednoduše zobecnit i pro *ciferníky s jiným počtem cifer než je 12*. Jediný rozdíl bude v tom, že budeme uvažovat zbytek po dělení číslem, které udává počet cifer na ciferníku. Tomuto počtu se v hodinové aritmetice říká *modul* (proto této aritmetice říkáme modulární).

Pokud tedy bude mít ciferník například 14 cifer, jak můžeme vidět na obr. 5, pak dopadnou součty $11 \oplus 2$ a $11 \oplus 16$ zcela jinak. Konkrétně dostaneme, že $11 \oplus 2 = 13$, protože $11 + 2 = 13$ děleno 14 je 0, zbytek je 13. Dále pak můžeme psát, že $11 \oplus 16$ je opět 13, poněvadž $11 + 16 = 27$ děleno 14 je 1, zbytek je 13.

Protože hodnota modulu určuje, jakým číslem v definici operace $\oplus$ a $\ominus$ dělíme, bude jistě praktické dát tuto hodnotu jasně najevo. Uděláme to tak, že ji napíšeme do indexu symbolů $\oplus$ a $\ominus$. Budeme tedy například

¹⁾Kolečko v symbolu $\oplus$ nám bude připomínat, že se jedná o sčítání v modulární aritmetice – tedy o „sčítání v kruhu“.



Obr. 5 Čtrnáctihodinový ciferník

psát:

$$\begin{aligned} 11 \oplus_{12} 2 &= 1, \\ 11 \oplus_{12} 16 &= 3, \\ 11 \oplus_{14} 2 &= 13, \\ 11 \oplus_{14} 16 &= 13. \end{aligned}$$

Tím se vracíme zpět ke vztahům z předchozího dílu, které definují šifrovací a dešifrovací funkci posouvací šifry. Při výkladu této šifry jsme se domluvili na kódování dané tabulkou 1. Pracujeme tedy s čísly x , y a k ,

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

Tabulka 1 Jednoduché kódování písmen abecedy a mezery ␣

která mohou nabývat celkem 27 hodnot, konkrétně hodnot 0 až 26. Zmíněnou šifrovací funkci e a dešifrovací funkci d posouvací šifry můžeme – teď již zcela správně – napsat následující způsobem:

$$e(x, k) = x \oplus_{27} k, \quad (1)$$

$$d(y, k) = y \ominus_{27} k. \quad (2)$$

Pro úplnost dodejme, že operace výpočtu zbytku po celočíselném dělení je natolik užitečná, že se vyskytuje snad ve všech vyšších programovacích jazycích. Například v jazyce C je možné tento zbytek vypočítat pomocí operátoru `%`. Šifrovací funkci (1) posouvací šifry bychom tedy mohli definovat tak, jak ukazuje následující programový kód:

```

/* sifrovací funkce posouvací sifry */
short encipher(short x, short k)
{
    return (x + k) % 27;
}

```

Pro další výklad bude potřeba zamyslet se nad tím, jak v modulární aritmetice fungují i jiné operace, konkrétně nám půjde o násobení, umocnění a dělení. Pro tyto tři operace budeme používat po řadě symboly $\odot$, $\oslash$ a $\oslash$ (opět s dolním indexem určujícím modul, jak uvidíme za chvíli).

U prvních dvou zmíněných operací není celkem co řešit, situace je totiž analogická se sčítáním a odečítáním. Násobek $a \odot_n b$ je tak roven zbytku po vydělení čísla $a \cdot b$ číslem n . Proto například platí $3 \odot_{10} 5 = 5$. Podobně jednoduché je i umocnění: $a \oslash_n b$ je zbytek po vydělení čísla a^b číslem n ; lehce tak například zjistíme, že $2 \oslash_{10} 6 = 4$.

Vypočítat podíl v modulární aritmetice ovšem tak přímočaré není. V běžné aritmetice definujeme dělení pomocí násobení, platí totiž například, že 20 děleno 5 je totéž jako 20 krát $\frac{1}{5}$. Obecně můžeme napsat, že b děleno a je rovno součinu b a „převrácené“ hodnoty k číslu a (samozřejmě za předpokladu, že a nebude nula). K tomu, abychom převedli tuto myšlenku do modulární aritmetiky, musíme dobře porozumět tomu, co se myslí zmíněnou převrácenou hodnotou k danému číslu.

Převrácená hodnota k číslu a je takové číslo, které vynásobeno (ať už zleva nebo zprava) číslem a dá jedničku.²⁾ V běžné aritmetice je převrácenou hodnotou k číslu 5 skutečně zlomek $\frac{1}{5}$, protože

$$5 \cdot \frac{1}{5} = \frac{1}{5} \cdot 5 = 1.$$

Podobně v modulární aritmetice definujeme podíl $b \oslash_n a$ jako součin $b \odot_n A$, kde A značí převrácenou hodnotu k číslu a . Otázkou ovšem je, jestli k číslu a převrácená hodnota A existuje, a pokud ano, jak ji vypočítat.³⁾

Zkusme si situaci představit na jednoduchém příkladu. Budeme uvažovat modulární aritmetiku s modulem $n = 12$, to znamená, obvyčejně

²⁾Jedničku proto, že právě jednička se při násobení chová *neutrálně*, to znamená, že nemění výsledek součinu. Přesněji řečeno, pro jedničku a libovolné nenulové číslo a platí, že $a \cdot 1 = 1 \cdot a = a$.

³⁾Nezapomeňme, že v modulární aritmetice nemáme žádné zlomky. Převráceným číslem k číslu 5 jistě nebude $\frac{1}{5}$ už proto, že žádné takové číslo v modulární aritmetice (na ciferníku) nemáme.

hodiny s dvanáctihodinovým cyklem, které vidíme na obr. 4. Ptáme se, jestli k číslu 3 existuje převrácená hodnota. Formulováno v řeči hodin se tedy ptáme, jestli se poskládáním několika čtvrt hodinovek dostaneme na pět minut po celé (číslo 1). Na první pohled je jasné, že se nám to nepodaří. Pomocí čtvrt hodiny (čísla 3) se dostaneme pouze na půl hodinu (číslo 6), na tři čtvrtě hodiny (číslo 9) nebo na celou (číslo 0). K číslu 3 tedy převrácená hodnota neexistuje. Podobně dopadneme i s čísly 2, 4 a 6 – ani k nim neexistuje převrácená hodnota. Můžeme tedy snadno vyzorovat, že pokud nějaké číslo *dělí modul beze zbytku*, pak k tomuto číslu neexistuje převrácená hodnota.

Právě navržené kritérium však není úplné, protože neříká, jak to dopadne v případě, kdy dané číslo *nedělí modul beze zbytku*. Tak například k číslu 9, které nedělí modul 12 beze zbytku, také neexistuje převrácená hodnota. Důvodem je, že tři čtvrtě hodiny (číslo 9) je poskládána ze tří čtvrt hodin (čísel 3), ke kterým, jak už víme, převrácená hodnota neexistuje. Celkem tedy můžeme vyslovit následující tvrzení:

Tvrzení 1.

K danému číslu existuje převrácená hodnota, právě když je největším společným dělitelem tohoto čísla a modulu jednička (to znamená, toto číslo je s modulem nesoudělné).

Pokud převrácená hodnota k danému číslu existuje, pak se dá vypočítat takzvaným rozšířeným Euklidovým algoritmem. Tento algoritmus zde nebudeme popisovat, pro účely tohoto výkladu plně postačí, když vyzkoušíme všechny možné kombinace. V předchozím příkladu s dvanáctihodinovým ciferníkem tak dojdeme například ke zjištění, že převrácená hodnota k číslu 5 je opět číslo 5, protože $5 \odot_{12} 5 = 1$ (neboli $5 \cdot 5$ děleno 12 dává zbytek 1), viz také tabulka 2.

a	0	1	2	3	4	5	6	7	8	9	10	11
A	–	1	–	–	–	5	–	7	–	–	–	11

Tabulka 2 Převrácená hodnota A k číslu a v modulární aritmetice s modulem 12

Abychom počítání v modulární aritmetice dostatečně zažili, vyzkoušíme si na závěr této sekce několik jednoduchých příkladů. Vypočtěme následující příklady (výsledky jsou uvedeny na konci tohoto článku):

$$15 \ominus_{17} (10 \oplus_{17} 14 \oplus_{17} 0) = ?$$

$$14 \odot_{25} 24 = ?$$

$$3 \otimes_9 3 = ?$$

$$20 \oslash_6 5 = ?$$

$$10 \oslash_{10} 5 = ?$$

Nalezli jsme konečně jednosměrnou funkci?

Na konci předchozího dílu jsme prozradili, že kandidátem na jednosměrnou funkci se zadními vrátky je umocnění v modulární aritmetice. Nyní, když modulární aritmetiku docela dobře ovládáme, jsme schopni tuto funkci přesně popsat. Je-li tedy x číslo, které šifrujeme, k_e veřejný klíč a n modul, pak můžeme psát:

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

V dalším výkladu budeme uvažovat nějaké konkrétní nastavení – veřejným klíčem k_e bude číslo 2 a pro modul bude platit $n = 10$ (počítat tedy budeme na ciferníku s deseti ciframi). Šifrovací funkce pak vypadá takto:

$$e(x, 2) = x \otimes_{10} 2. \quad (3)$$

Dále předpokládejme, že zašifrované číslo, které se podaří Evě získat, je číslo 9. Důvod, proč šifrovací funkce založená na běžném umocnění, tedy $e(x, 2) = x^2$, není jednosměrnou funkcí, jsme objasnili už v předchozím dílu. Zopakujme si, že číslo x , pro které platí, že $9 = x^2$ můžeme rychle získat metodou půlení intervalu: Nejprve zkusíme x uhádnout; řekněme, že prvním pokusem bude $x = 4$. Jelikož je ale 4^2 větší než požadované zašifrované číslo 9, odhad čísla x musíme zmenšit. Druhým pokusem tedy bude $x = 2$. Pokud tuto hodnotu dosadíme do šifrovací funkce, získáme 2^2 , což je naopak menší číslo než 9. Dále zkusíme $x = 3$, čímž se dostáváme ke správnému výsledku.

Pokud bychom chtěli stejnou metodu využít i ve světě modulární aritmetiky, narazíme na značné obtíže. Začneme-li stejným počátečním odhadem $x = 4$ a dosadíme-li tento odhad do šifrovací funkce (3), obdržíme číslo $4 \otimes_{10} 2 = 6$ (zbytek po vydělení čísla 4^2 číslem 10 je 6). Dostali jsme výsledek, který je menší než požadované zašifrované číslo 9. Metoda půlení intervalu v tomto případě říká, že je potřeba odhad zvýšit. My ovšem

víme, že správným výsledkem je číslo menší, konkrétně $x = 3$, protože $3 \otimes_{10} 2 = 9$.

Můžeme tedy vyzorovat, že to, co dělá z šifrovací funkce $e(x, k_e) = x \otimes_n k_e$ dobrého kandidáta na jednosměrnou funkci je schopnost modulární aritmetiky (tím, že se počítání děje v kruhu) zamíchat výsledky umocnění $x \otimes_n k_e$ pro různé hodnoty x a zároveň však výpočet tohoto výsledku nijak nekomplikovat. To znamená, že je výpočet jedním směrem snadný, v opačném směru však obtížný, což je přesně to, co požadujeme po jednosměrné funkci.

Šifra RSA

Skutečnosti, že je funkce $e(x, k_e) = x \otimes_n k_e$ vhodným kandidátem na jednosměrnou funkci, si všiml v sedmdesátých letech 20. století americký informatik Ronald Rivest, který v té době pracoval v laboratoři počítačových věd na Massachusettském technologickém institutu.⁴⁾ Při hledání této funkce a při zamítání nevhodných kandidátů mu byli nápomocni jeho dva kolegové z téže laboratoře, Adi Shamir a Leonard Adleman. Roku 1977 tak společně publikovali článek, ve kterém navrhli asymetrickou šifru založenou právě na zmíněné funkci, která se dnes nazývá RSA (název je zkratkou iniciál jmen autorů). Nedávno však vyšlo najevo, že stejnou šifru navrhl už roku 1973 anglický kryptograf Clifford Cocks. Je to tentýž Clifford Cocks, který „předběhl“ Ralpha Merkleho, Whitfielda Diffieho a Martina Hellmana v objevu bezpečné výměny klíče (byla o tom řeč v předchozím dílu). V tomto smyslu se historie zopakovala.

Ušli jsme dlouhou cestu, abychom byli schopni, aspoň v prvním přiblížení, šifru RSA popsat. Pustíme se tedy do toho. Šifrovací a dešifrovací funkce šifry RSA vypadají takto:

$$e(x, k_e) = x \otimes_n k_e, \quad (4)$$

$$d(y, k_d) = y \otimes_n k_d. \quad (5)$$

Šifrovací funkci je, nám dobře známé, umocnění v modulární aritmetice. Veřejným klíčem je exponent k_e spolu s modulem n .⁵⁾ Soukromým klíčem je pak exponent k_d . Všimněme si dobře, že dešifrovací funkce je také

⁴⁾Massachusetts Institute of Technology, známý spíše pod zkratkou MIT, je prestižní soukromou americkou univerzitou, která se do dějin informatiky i jiných oborů zapsala mnohými významnými objevy a vynálezy. Svědčí o tom už fakt, že mezi absolventy MIT je více než 70 laureátů Nobelovy ceny.

⁵⁾V předchozím dílu, ve kterém jsme se bavili obecně o asymetrickém šifrování, jsme

založena na umocnění, stejně jako šifrovací funkce. O umocnění víme, že jej umíme rychle vypočítat. Umíme tedy rychle vypočítat hodnotu $y \otimes_n k_d$; exponent k_d proto představuje zadní vrátka, o kterých jsme mluvili v předchozím dílu.

Zbývá zodpovědět otázku, jak zvolit čísla k_e , n a k_d , aby vše správně fungovalo. V následujících odstavcích si proto uvedeme podrobný popis šifrovacího a dešifrovacího procesu. Šifrovací proces probíhá v těchto krocích:

1. Bob, který figuruje jako příjemce, si nejprve zvolí dvě prvočísla. Označme si tato prvočísla jako p a q . Dále vypočítá jejich součin. Tento součin si označíme písmenem n , platí tedy $n = p \cdot q$. Číslo n bude modulem v modulární aritmetice, na které jsou založeny výpočty hodnot šifrovací a dešifrovací funkce.

2. Dále Bob vypočítá číslo, které se zpravidla označuje jako $\phi(n)$, a pro které platí

$$\phi(n) = (p - 1) \cdot (q - 1).$$

Poznamenejme, že hodnota $\phi(n)$ udává počet čísel, která jsou menší než n a která jsou s n nesoudělná.

3. V dalším kroku si Bob zvolí číslo k_e . Tato volba může být náhodná, důležité pouze je, aby k_e a $\phi(n)$ byla nesoudělná čísla.
4. Čísla k_e a n Bob zveřejní.
5. Alice může získat veřejný klíč. Zprávu, kterou chce Bobovi odeslat, nějakým způsobem zakóduje do posloupnosti čísel.⁶⁾ Tuto posloupnost čísel pak rozdělí na stejně dlouhé bloky takovým způsobem, že pro každé číslo tvořící daný blok, bude platit, že je mezi 0 a $n - 1$ (to z toho důvodu, že se šifrování i dešifrování provádí v modulární aritmetice s modulem n).

za veřejný klíč uvažovali pouze jedno číslo. Skutečnost, že veřejný klíč šifry RSA je složen ze dvou částí, exponentu k_e a modulu n , však myšlenku asymetrického šifrování nijak nenarušuje. Je zjevné, že obě komunikující strany musí vědět, který modul mají ve svých výpočtech použít, proto musí být n také zveřejněno.

⁶⁾Toto kódování může být celkem libovolné. Pouze musí být zajištěno, aby Bob používal stejné kódování.

6. Alice pak postupně zašifruje všechny bloky pomocí šifrovací funkce a veřejného klíče složeného z čísel k_e a n . Pokud je tedy x číslo odpovídající danému bloku, pak vypočítá $e(x, k_e) = x \otimes_n k_e$.

7. Na závěr Alice odešle Bobovi takto vypočtená zašifrovaná čísla.

Dešifrovací proces je pak proveden v těchto krocích:

1. Bob obdrží zašifrovaná čísla.

2. Poté vypočítá převrácenou hodnotu k_d k číslu k_e s využitím modulu $\phi(n)$.⁷⁾ Proč je využito jako modul právě číslo $\phi(n)$ je spíše technickým (i když pro správné fungování RSA významným) detailem; zdůvodněním se tedy nebudeme zabývat.

3. Pokud je y jedno ze zašifrovaných čísel, pak Bob použije dešifrovací funkci a vypočítá tak $d(y, k_d) = y \otimes_n k_d$. Je možné ukázat, že takto vypočtené číslo $d(y, k_d)$ je stejné jako číslo x , které Alice zašifrovala.

Ukažme si šifrovací proces na následujícím příkladu. Předpokládejme prvočísla $p = 71$ a $q = 47$. Z těchto hodnot vypočítáme:

$$n = p \cdot q = 71 \cdot 47 = 3337,$$

$$\phi(n) = (p - 1) \cdot (q - 1) = 70 \cdot 46 = 3220.$$

Číslo k_e , které je součástí veřejného klíče, zvolíme rovno 79. Tato volba je v pořádku, protože čísla 79 a 3220 jsou nesoudělná (jediným společným dělitelem těchto čísel je jednička). V modulární aritmetice s modulem 3220 proto existuje k číslu $k_e = 79$ převrácená hodnota. Prozradíme, že touto převrácenou hodnotou je $k_d = 1019$, jelikož $79 \odot_{3220} 1019 = 1$ ($79 \cdot 1019$ děleno 3220 dává zbytek roven 1).

Zprávu, kterou chceme zašifrovat převedeme nějakým způsobem na posloupnost čísel. Dejme tomu, že tato posloupnost vypadá třeba takto:

1235371029471

Tuto posloupnost musíme rozdělit na stejně dlouhé bloky tak, že každý blok bude menší než $n = 3337$. Rozdělení tedy provedeme následovně:

123|537|102|947|001

⁷⁾ Zde se nám jasně vyjevil důvod, proč jsme požadovali, aby byla čísla k_e a $\phi(n)$ nesoudělná. Tato podmínka totiž zajistí, že převrácená hodnota k číslu k_e skutečně existuje.

Každé číslo pak samostatně zašifrujeme pomocí vztahu (4), například tedy první dvě čísla zašifrujeme na hodnoty:

$$e(123, 79) = 123 \odot_{3337} 79 = 1433,$$

$$e(537, 79) = 537 \odot_{3337} 79 = 1385.$$

Celkem pak dostaneme posloupnost zašifrovaných čísel:

$$14331385323022411$$

Šifrování RSA si může čtenář samostatně vyzkoušet prostřednictvím následujícího úkolu (řešení je opět uvedeno na konci článku). Alice poslala Bobovi zašifrovanou zprávu, ve které uvedla místo jejich plánované schůzky. K utajení zprávy se rozhodla použít šifru RSA s modulem $n = 33$. K zakódování textu zprávy použila následující tabulku:

a	b	c	d	e	f	g	h	i	j
00	01	02	03	04	05	06	07	08	09
k	l	m	n	o	p	q	r	s	t
10	11	12	13	14	15	16	17	18	19
u	v	w	x	y	z	␣	.	,	:
20	21	22	23	24	25	26	27	28	29
+	-	@							
30	31	32							

Protože je modul malý, rozdělila posloupnost čísel (kódujících zprávu) na dvojice. K šifrování si zvolila exponent $k_e = 7$. Zašifrovanou posloupnost čísel převedla pomocí zmíněné tabulky opět na znaky a obdržela tak následující text:

HAF,UIHCMFHAMQGNCVFVFULUMU.:CD

Jak zní původní zpráva? V úloze figuruje skutečně velmi malý modul. V této souvislosti musíme udělat dvě důležité poznámky o bezpečnosti šifry RSA:

1. Kvůli malému modulu musela Alice rozdělit posloupnost čísel na dvojice, takže vlastně šifrovala každé písmeno zprávy samostatně. Důsledkem toho je, že se například písmeno **a** vždy zašifruje na jeden a týž znak. Tím ovšem z RSA udělala obyčejnou substituční

(i když asymetrickou) šifru. Pokud by zvolila větší modul a mohla tak rozdělit posloupnost na větší bloky, tak ke zmíněnému problému nedošlo. Pro účely našeho příkladu jsme malý modul zvolili záměrně, abychom se nezahltili náročnými numerickými výpočty.

2. Záměrně jsme v zadání úlohy neuvedli, z jakých prvočísel je modul $n = 33$ složen. Bez těchto prvočísel nejsme schopni vypočítat exponent k_d . Řešitel této úlohy se proto ocitl v roli poněkud žárlivé Evy, které se podařilo zachytit zašifrovanou zprávu, a pokouší se ji s maximálním nasazením dešifrovat. Příklad je samozřejmě nastaven tak, aby se dal rozklad modulu n lehce uhádnout. Docházíme tak k jednomu důležitému závěru: bezpečnost šifry RSA není založena pouze na jednosměrnosti šifrovací funkce, ale také na obtížnosti rozkladu čísla na součin prvočísel. O tomto problému byla napsána spousta tlustých knih a mnoho vynikajících informatiků a matematiků si láme hlavu nad tím, jestli existuje nějaká rychlá metoda, která by tento rozklad byla schopná získat a to i v případě, že je rozkládané číslo hodně velké. Prozatím je toto hledání neúspěšné.

Vidíme tedy, že pro bezpečné použití šifry RSA je nutné, aby byl modul skutečně hodně velkým číslem. Ve výše uvedené úloze byl modul směšně malý, v praktických aplikacích se v dnešní době používají moduly, které mají, zapsány v binárním tvaru, délku od 1024 do 4096 bitů.

Dost dobré soukromí

V předchozím dílu jsme vyzdvihli všechny výhody asymetrického šifrování oproti šifrování symetrickému. Existuje však jedna vlastnost symetrických šifer, za kterou asymetrické šifry značně pokulhávají. Symetrické šifry jsou totiž založeny na jednoduchých matematických operacích; zašifrovat zprávu symetricky je proto vždy o něco rychlejší než zašifrovat ji asymetricky (například pomocí RSA). Tento malý rozdíl v rychlosti se pochopitelně zvětšuje při šifrování dlouhých zpráv. Pokud budeme chtít šifrovat objemné multimediální soubory, tak tento rozdíl může komplikovat plynulost komunikace.

Nedostatečnou rychlostí asymetrických šifer se zabýval americký programátor Philip R. Zimmermann, který si položil jednoduchou otázku: nebylo by možné zkombinovat symetrickou a asymetrickou šifru tak, aby byly zvýrazněny výhody a naopak potlačeny nevýhody obou těchto typů šifrování? V devadesátých letech 20. století vytvořil Zimmermann program,

ve kterém tuto kombinaci jednoduchým způsobem zrealizoval. Tento program, který nazval PGP (z angličtiny Pretty Good Privacy – dost dobré soukromí, jak je uvedeno v názvu této sekce), funguje následovně.

Šifrování zprávy, která může být značně objemná, je prováděno rychlou symetrickou šifrou. Symetrická šifra, jak víme, používá pouze jeden tajný klíč, který si musí Alice s Bobem vyměnit. Tato výměna je však slabým článkem komunikace, tajný klíč totiž může být odhalen. Pro výměnu tajného klíče však můžeme použít bezpečnou asymetrickou šifru, která problémem výměny klíče netrpí. Jako symetrickou šifru použil Zimmermann šifru zvanou IDEA, jako asymetrickou šifru použil právě RSA.

Podobným způsobem jako v programu PGP je šifra RSA použita pro šifrování tajného klíče v protokolu SSH. Tímto protokolem se v současné době ve velké míře zajišťuje bezpečnost komunikace na Internetu.

Na závěr se podepíšeme

Ukázali jsme si různé metody utajení obsahu zpráv. Šifrování má však i výrazně jiné použití – stojí v základu takzvaného elektronického podpisu, který v elektronické komunikaci nahrazuje klasický, ručně psaný podpis. V závěru si proto tuto problematiku stručně popíšeme.

Připojení elektronického podpisu k dané zprávě by mělo zejména zajistit následující dvě skutečnosti: *autentičnost* – Bob by měl být schopen ověřit, kdo zprávu podepsal a odeslal; *nepopiratelnost* – Alice by neměla mít možnost popřít, že zprávu podepsala.

Vidíme, že autentičnost i nepopiratelnost zajišťuje v klasické komunikaci vlastnoruční podpis jednoduše tím, že rukopis každého člověka je jedinečný. Jak ovšem tuto jedinečnost přenést do světa elektronické komunikace? Autentičnost je v elektronické komunikaci realizována použitím takzvaného *digitálního certifikátu*.⁸⁾ Nepopiratelnost je pak možné zajistit, možná trochu překvapivě, pomocí šifry RSA (nebo pomocí jiné asymetrické šifry). Stačí pouze vyměnit roli veřejného a soukromého klíče. Pro šifrování proto použijeme soukromý klíč a pro dešifrování naopak klíč veřejný. Pokud totiž Alice zašifruje zprávu soukromým klíčem,⁹⁾ jejímž

⁸⁾ Více informací o digitálních certifikátech a certifikačních autoritách, které tyto certifikáty vydávají a zaručují se za jejich správnost, je možné najít třeba na stránkách Wikipedie.

⁹⁾ Ve skutečnosti se nešifruje celá zpráva, ale pouze její „výťah“, který má oproti podepisované zprávě malou velikost. Tento výťah se získává tak, že se na zprávu aplikuje takzvaná *kryptografická hashovací funkce*.

je jediným vlastníkem, pak nemůže popřít, že jej podepsala. Na druhou stranu má Bob, nebo kdokoliv jiný, možnost zprávu dešifrovat, podobně jako u vlastnoručně psaného podpisu má kdokoliv možnost si tento podpis přechytit.

Jak jsme si ukázali, se šifrou RSA se setkáváme (zejména kvůli Internetu) dnes a denně, aniž by si toho byla většina uživatelů vědoma. Je historickou zajímavostí, že v době, kdy Ronald Rivest, Adi Shamir a Leonard Adleman pracovali na článku popisujícím princip fungování této šifry, Adleman navrhnul, aby nebyl uveden mezi autory. Domníval se totiž, že se bude jednat v jeho životě o nejméně významnou práci, na které se podílel...

Řešení úkolů

1. Řešení prvních čtyřech příkladů je následující:

$$15 \ominus_{17} (10 \oplus_{17} 14 \oplus_{17} 0) = 8,$$

$$14 \odot_{25} 24 = 11,$$

$$3 \oslash_9 3 = 0,$$

$$20 \oslash_6 5 = 4.$$

Poslední příklad $(10 \oslash_{10} 5)$ nemá řešení, protože k číslu 5 neexistuje převrácená hodnota (5 není nesoudělné s modulem 10).

2. Nejprve je potřeba rozložit modul $n = 33$ na součin prvočísel. Na první pohled je vidět, že tato prvočísla jsou $p = 3$ a $q = 11$. Dále vypočítáme hodnotu

$$\varphi(n) = (p - 1) \cdot (q - 1) = 2 \cdot 10 = 20.$$

Soukromý klíč k_d je převrácenou hodnotou veřejného klíče $k_e = 7$, přičemž modulem je hodnota $\varphi(n) = 20$. Snadno zjistíme, že $k_d = 3$.

Kryptogram

HAF,UIHCMFHAMQGNCFVFULUMU.:CD

zakódujeme pomocí tabulky uvedené v zadání na posloupnost čísel

07 00 05 28 20 08 07 02 12 05 07 00 12 16 06

13 02 05 21 05 20 11 20 12 20 26 29 02 03

Tato čísla budeme postupně dosazovat za y do vztahu pro dešifrování:

$$y \oplus_{33} 3.$$

Obdržíme tak posloupnost čísel

13 00 26 07 14 17 13 08 12 26 13 00 12 04 18

19 08 26 21 26 14 11 14 12 14 20 02 08 27

Dekódováním těchto čísel se konečně dostaneme k otevřenému textu:

`na_hornim_namesti_v_olomouci.`

Literatura

- [1] Whitfield Diffie and Martin Hellman 1976. New directions in cryptography. *IEEE Transactions on Information Theory*. 22 (6): 644–654.
- [2] Steven Levy 2001. *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*. Penguin Books.
- [3] Simon Singh 2000. *Kniha kódů a šifer: Tajná komunikace od starého Egypta po kvantovou kryptografii*. Argo, Dokořán.

ZPRÁVY

12. středoevropská matematická olympiáda



Dvanáctý ročník Středoevropské matematické olympiády (MEMO) se konal ve dnech 27. srpna až 2. září 2018 v polském městě Bielsko-Biala. Soutěže se zúčastnilo 66 žáků, mimo deseti tradičních zemí České republiky, Chorvatska, Litvy,

Maďarska, Německa, Polska, Rakouska, Slovenska, Slovinska a Švýcarska se soutěže zúčastnili jako hosté také soutěžící z Ukrajiny. Každou zemi reprezentovala šestice žáků nematuritních ročníků středních škol, kteří se letos nezúčastnili Mezinárodní matematické olympiády.

České reprezentační družstvo bylo sestaveno na základě výsledků ústředního kola kategorie A 67. ročníku české MO. Nominováni byli dva vítězové a čtyři úspěšní řešitelé. Byli jimi *Jonáš Havelka* z G v Českých Budějovicích, *Jírovcová 8*, *Dalibor Kramář* z G v Brně-Rečkovcích, *Josef Minařík* z G v Brně, *tř. Kpt. Jaroše*, *Magdaléna Mišinová* z G v Praze 6, *J. Keplera*, *Jana Pallová* z GJŠ v Přerově, a *Tomáš Souřada* z G v Žamberku. Vedoucím české delegace byl *RNDr. Pavel Calábek, Ph.D.*, z Přírodovědecké fakulty Univerzity Palackého v Olomouci, jeho zástupcem a pedagogickým vedoucím byl *doc. RNDr. Zbyněk Šír, Ph.D.* z Matematicko-fyzikální fakulty Univerzity Karlovy v Praze.

Zatímco den po příjezdu se soutěžící seznamovali s historií a současností Bielska-Biala a připravovali se na soutěž, vedoucí družstev tvořící mezinárodní *jury* po vyčerpávajících jednáních vybrali 12 úloh (4 pro soutěž jednotlivců a 8 pro soutěž družstev), přeložili je do národních jazyků a připravili systém jejich hodnocení. Všechna pracovní jednání *jury* a vlastní soutěž probíhala na místní Humanitně-technické univerzitě. Ve středu 29. srpna proběhla soutěž jednotlivců a o den později i soutěž družstev. První den měli soutěžící na vypracování řešení 5 hodin čistého času, každý příklad byl ohodnocen nejvýše 8 body. Druhý den řešila jednotlivá reprezentační družstva společně osm úloh, opět po dobu pěti hodin a každý příklad byl ohodnocen opět nejvýše 8 body. Jako třetí úloha v soutěži družstev byla zařazena i česká úloha, jejímž autorem byl *Josef Tkadlec*. Dva následující dny po soutěži byl pro soutěžící připraven poznávací program po Krakově a okolních polských Beskydech. Vedoucí družstev mezitím opravili žakovská řešení a zkoordinovali jejich hodnocení. Po uzavření koordinací stanovila *jury* závěrečná pořadí obou soutěží a bodové hranice pro udělení medailí.

Večer 1. září se na zámku v Bielsku-Biala konal závěrečný slavnostní ceremoniál, kde organizátoři vyhlásili výsledky. V soutěži jednotlivců bylo osm soutě-

žících, kteří získali plný počet bodů, ohodnoceno zlatými medailemi (Polsko 3, Maďarsko 2, po jedné získalo Chorvatsko, Německo a Ukrajina), dalších dvanáct soutěžících získalo stříbrné medaile a šestnáct soutěžících bronzové medaile. Navíc 17 žáků obdrželo čestná uznání za úplné vyřešení aspoň jedné soutěžní úlohy. Je potěšitelné, že se mezi oceněnými byli i čeští žáci. *Magdaléna Mišinová* obsadila se ziskem 17 bodů dělené 34. místo a získala bronzovou medaili, *Josef Minařík* (15 b.) a *Jana Pallová* (14 b.) získali čestná uznání. V porovnání s minulými léty jsou tyto výsledky nepříliš uspokojivé a útěchou nemůže být ani 8. místo v soutěži družstev, i když oproti loňsku jsme se o dvě místa polepšili.

V soutěži družstev zvítězila Ukrajina (62 bodů), následována Chorvatskem (60 b.) a Německem (59 b.). České družstvo získalo 27 bodů a obsadilo 8. místo. Uvedme na závěr pro představu počty zlatých, stříbrných a bronzových medailí, které vybojovala jednotlivá družstva v soutěži jednotlivců:

Česká republika (0–0–1), Chorvatsko (1–1–4), Litva (0–0–0), Maďarsko (2–1–2), Německo (1–1–1), Polsko (3–3–0), Rakousko (0–0–1), Slovensko (0–3–2), Slovinsko (0–0–2), Švýcarsko (0–0–1), Ukrajina (1–3–2).

Zájemci mohou získat podrobnější informace na internetových stránkách soutěže: <http://www.memo2018.abel.bielisko.pl/>

Na závěr uvádíme zadání všech dvanácti soutěžních úloh, za úlohou je uvedena navrhuji země.

Soutěž jednotlivců

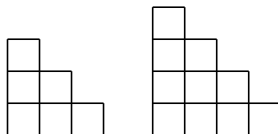
29. srpna 2018

1. Označme $\mathbb{Q}^+$ množinu všech kladných racionálních čísel a uvažujme $\alpha \in \mathbb{Q}^+$. Určete všechny funkce $f: \mathbb{Q}^+ \rightarrow (\alpha, +\infty)$ takové, že pro všechna $x, y \in \mathbb{Q}^+$ platí

$$f\left(\frac{x+y}{\alpha}\right) = \frac{f(x) + f(y)}{\alpha}.$$

(Rakousko)

2. Následující dva obrazce sestávající po řadě ze 6 a 10 jednotkových čtverců nazveme *schůdky*.



Uvažujme tabulku 2018×2018 složenou z 2018^2 buněk, z nichž každá je jednotkovým čtvercem. Odstraníme libovolné dvě buňky z jednoho řádku. Dokažte, že zbytek tabulky nelze rozstříhat (po stranách buněk) na schůdky (libovolně otočené).

(Ukrajina)

3. Nechť ABC je ostroúhlý trojúhelník, kde $|AB| < |AC|$. Označme D patu jeho výšky z vrcholu A . Dále označme R a Q po řadě těžiště trojúhelníků ABD a ACD . Nechť P je takový bod úsečky BC , že $P \neq D$ a body P , Q , R a D leží na téže kružnici. Dokažte, že se přímky AP , BQ a CR protínají ve společném bodě. (Slovensko)

4. a) Dokažte, že pro libovolné přirozené číslo m existuje celé číslo $n \geq m$ takové, že

$$\left\lfloor \frac{n}{1} \right\rfloor \cdot \left\lfloor \frac{n}{2} \right\rfloor \cdot \dots \cdot \left\lfloor \frac{n}{m} \right\rfloor = \binom{n}{m}. \quad (*)$$

- b) Označme $p(m)$ nejmenší celé číslo $n \geq m$, které vyhovuje rovnici (*). Dokažte, že platí $p(2018) = p(2019)$.

Poznámka: Pro reálné číslo x značí $\lfloor x \rfloor$ největší celé číslo, které nepřevyšuje x . (Slovensko)

Soutěž družstev

30. srpna 2018

1. Nechť pro kladná reálná čísla a , b , c platí $abc = 1$. Dokažte, že platí

$$\frac{a^2 - b^2}{a + bc} + \frac{b^2 - c^2}{b + ca} + \frac{c^2 - a^2}{c + ab} \leq a + b + c - 3.$$

(Polsko)

2. Nechť $P(x)$ je mnohočlen stupně $n \geq 2$ s racionálními koeficienty, který má n různých reálných kořenů tvořících aritmetickou posloupnost. Dokažte, že mezi nimi lze nalézt dva, které jsou zároveň dvěma kořeny nějakého mnohočlenu stupně 2 s racionálními koeficienty. (Rakousko)

3. Tlupa pirátů se pohádala, a teď každý z nich míří pistolemi na další dva piráty. Postupně jsou všichni v určitém pořadí jeden po druhém vyvoláni. Jestliže vyvolaný pirát žije, vystřelí na oba piráty, na které mířil (a to i v případě, že jsou již mrtví). Každá střela je okamžitě smrtící. Po vyvolání všech pirátů zjistíme, že jich bylo zastřeleno právě 28.

Dokažte, že i kdyby piráti byli vyvoláni v jakémkoliv jiném pořadí, bylo by jich zastřeleno aspoň 10. (Česká republika)

4. Pro přirozené číslo n uvažujme přirozená čísla $u_1, u_2, \dots, u_n$ nepřevyšující 2^k pro některé přirozené číslo $k \geq 3$. *Reprezentací* nezáporného celého čísla t rozumíme takovou posloupnost nezáporných celých čísel $a_1, a_2, \dots, a_n$, že platí

$$t = a_1 u_1 + a_2 u_2 + \dots + a_n u_n.$$

Dokažte tvrzení: Pokud má nezáporné celé číslo t nějakou reprezentaci, pak má také reprezentaci, ve které je méně než $2k$ z čísel $a_1, a_2, \dots, a_n$ nenulových.
(*Polsko*)

5. Nechť ABC je ostroúhlý trojúhelník, kde $|AB| < |AC|$. Označme D patu jeho výšky z vrcholu A . Body B' a C' leží po řadě na polopřímkách AB a AC tak, že body B', C' a D leží na téže přímce a body B, C, B' a C' leží na téže kružnici se středem O . Označme M střed úsečky BC a H průsečík výšek trojúhelníku ABC . Dokažte, že $DHMO$ je rovnoběžník. (*Slovensko*)

6. Uvažujme trojúhelník ABC . Osa jeho vnitřního úhlu ABC protíná stranu AC v bodě L a dále kružnici opsanou trojúhelníku ABC v bodě $W \neq B$. Kolmý průmět bodu K na přímku AW označme L . Kružnice opsaná trojúhelníku BLC dále protíná přímku CK v bodě $P \neq C$. Přímky BP a AW se protínají v bodě T . Dokažte, že platí $|AW| = |WT|$. (*Ukrajina*)

7. Definujme posloupnost přirozených čísel $a_1, a_2, a_3, \dots$ takto:

$$a_1 = 1 \text{ a pro každé přirozené číslo } k \text{ je } a_{k+1} = a_k^3 + 1.$$

Dokažte, že pro všechna prvočísla p tvaru $3\ell + 2$, kde ℓ je celé nezáporné číslo, existuje takové přirozené číslo n , že p dělí a_n . (*Polsko*)

8. Celé číslo n nazveme *slezské*, jestliže existují přirozená čísla a, b a c tak, že

$$n = \frac{a^2 + b^2 + c^2}{ab + bc + ca}.$$

a) Dokažte, že existuje nekonečně mnoho celých slezských čísel.

b) Dokažte, že existuje přirozené číslo, které není slezské.

(*Německo*)

Organizací příštího (13.) ročníku soutěže, který se uskuteční koncem srpna 2019, byla pověřena Česká republika.

Pavel Calábek

Mezinárodní olympiády v informatice v roce 2018



Naši nejlepší řešitelé Matematické olympiády kategorie P (programování) se každoročně účastní dvou mezinárodních soutěží v informatice a programování. V roce 2018 se nejprve v první polovině srpna konala v polské Varšavě Středoevropská olympiáda v informatice CEOI 2018 (Central European Olympiad in Informatics), na začátku září se potom v japonském

městě Tsukuba uskutečnila celosvětová Mezinárodní olympiáda v informatice IOI 2018 (International Olympiad in Informatics).

Reprezentační družstva pro obě mezinárodní olympiády v informatice jsme v dřívějších letech sestavovali pouze na základě výsledků dosažených v ústředním kole příslušného ročníku Matematické olympiády – kategorie P. V posledních dvou letech jsme pro výběr reprezentantů využili třídenní výběrové soustředění, na které jsme pozvali všechny úspěšné řešitele ústředního kola MO kategorie P. Soustředění se konalo v dubnu v prostorách Matematicko-fyzikální fakulty UK v Praze a mělo podobný charakter, jako mají mezinárodní olympiády. Studenti na něm tedy řešili pouze praktické úlohy na počítačích. Rozbory soutěžních úloh následující po každém soutěžním dnu posloužily navíc jako příprava na účast v dalších programátorských soutěžích. Při výběru reprezentantů se počítaly výsledky dosažené v ústředním kole MO-P a na tomto výběrovém soustředění. Na celosvětovou olympiádu IOI jsme vybrali družstvo sestavené ze čtyř nejlepších řešitelů bez ohledu na ročník jejich studia. Na středoevropskou soutěž CEOI jezdí tradičně další čtyři studenti, kteří ještě nejsou v maturitním ročníku a navíc splňují nižší věkový limit určený pravidly soutěže. Těmto mladším reprezentantům se účast na CEOI stává významným zdrojem zkušeností, které často využijí při své účasti v dalších ročnících národních i mezinárodních programátorských soutěží.

Studenti vybraní k účasti na IOI a CEOI se na svoji soutěž každoročně připravují na týdenním přípravném soustředění. Soustředění označované jako CPSPC (Czech-Polish-Slovak Preparation Camp) je společné pro řešitele informatických olympiád z Čech, Polska a Slovenska a tyto tři země se také střídají v jeho pořádání. Letošní ročník CPSPC se konal na začátku července na Slovensku na Fakultě matematiky, fyziky a informatiky Univerzity Komenského v Bratislavě.

Středoevropská olympiáda v informatice CEOI 2018 probíhala ve dnech 12. až 18. srpna 2018 v Polsku v hlavním městě Varšavě. Byl to jubilejní 25. ročník této regionální soutěže mladších středoškoláků. Soutěž se konala v prostorách Fakulty matematiky, informatiky a mechaniky Varšavské univerzity, účastníci byli ubytováni v nedalekém hotelu Reduta Ibis. Měli jsme velmi kvalitní a příjemné ubytování, jehož velkou výhodou byla i možnost dojít pěšky na univerzitu. Celkem soutěžilo 55 studentů ze 13 zemí. Vedle osmi tradičních účastnických středoevropských států (Česká republika, Chorvatsko, Maďarsko, Německo, Polsko, Rumunsko, Slovensko, Slovinsko) přijeli navíc jako hosté soutěžící z Ázerbájdžánu, Gruzie, Itálie, Rakouska a Švýcarska. Tyto země se účastní CEOI poměrně často, ale protože se nepodílejí na střídavém pořádání olympiády, musí si svoji účast sami vždy uhradit. Jako obvykle se zúčastnilo také druhé družstvo z pořadatelské země.

České reprezentační družstvo bylo tvořeno těmito studenty:

Jan Kaifer, student gymnázia Jana Keplera v Praze

Jiří Kalvoda, student gymnázia na tř. Kpt. Jaroše v Brně

Radek Olšák, student Mensa gymnázia v Praze

Petr Zahradník, student gymnázia dr. V. Šmejkal v Ústí nad Labem

Vedoucími české delegace na CEOI 2018 byli doc. RNDr. Tomáš Pitner, Ph.D. z Fakulty informatiky Masarykovy univerzity v Brně a doc. RNDr. Pavel Töpfer, CSc. z Matematicko-fyzikální fakulty Univerzity Karlovy v Praze.

Vlastní soutěž se jako vždy odehrávala v průběhu dvou soutěžních dnů. V každém dni soutěžící řešili tři náročné algoritmické úlohy, na jejichž vyřešení měli pět hodin času. Večer před soutěží vedoucí všech delegací společně schválili soutěžní úlohy navržené pořadatelskou zemí, upravili podle potřeby jejich formulace a přeložili je pak do mateřského jazyka svých studentů. Čeští studenti tedy dostali jak anglickou, tak i českou verzi zadání úloh.

Každý soutěžící pracuje na přiděleném osobním počítači s nainstalovaným soutěžním prostředím, které umožňuje vyvíjet a testovat programy a odesílat je k vyhodnocení. Správnost vypracovaných programů organizátoři testují v průběhu soutěže pomocí předem připravené sady testovacích dat, každý test je navíc omezen časovým limitem. Tím je zajištěna nejen kontrola správnosti výsledků, ale pomocí časových limitů se také odliší kvalita použitého algoritmu. Při testování každé úlohy se používají sady testovacích dat různé velikosti, takže teoreticky správné řešení založené na neefektivním algoritmu zvládne dokončit včas výpočet pouze pro některé testy – pro ty menší a jednodušší. Takové řešení je potom ohodnoceno částečným počtem bodů. Krátce po odevzdání vypracovaného programu do vyhodnocovacího systému se soutěžící dozví hodnocení svého řešení a má pak ještě možnost opravit ho a odevzdat znovu. Jedná se o podobný systém, jaký používáme v posledních letech u nás v Matematické olympiádě kategorie P pro praktické úlohy domácího a ústředního kola.

Místní organizátoři zpříjemnili všem účastníkům olympiády pobyt v Polsku několika zajímavými doprovodnými akcemi. Hned první den po slavnostním zahájení a seznámení se soutěžním prostředím jsme měli možnost projít si centrum Varšavy s profesionálními průvodci. Součástí této procházky byla i návštěva vyhlídkové věže známého varšavského Paláce kultury a sportu. Mezi oba soutěžní dny byl zařazen jednodenní odpočinek s celodenním výletem. Každý účastník si mohl podle svého zájmu zvolit buď šestnáctikilometrový sjezd nedaleké řeky na kánoích, nebo autokarový poznávací zájezd, který navštívil rodiště známého polského hudebního skladatele Fryderyka Chopina v obci Żelazowa Wola, architektonicky zajímavý kostel Brochów a zámek Nieborów s barokními zahradami. V závěrečném dnu po skončení soutěže jsme pak ještě společně navštívili Koperníkovo středisko vědy ve Varšavě.

Poslední den našeho pobytu v Polsku proběhlo také slavnostní zakončení soutěže s vyhlášením výsledků. Každá ze soutěžních úloh byla hodnocena maximálně 100 body, takže celkově bylo teoreticky možné získat až 600 bodů. To se tentokrát nikomu nepodařilo – nejvyššího hodnocení 565 bodů dosáhli dva soutěžící, jeden z Polska a druhý z Rumunska. Úspěšnější polovina soutěžících dostává na

CEOI medaili, přičemž zlaté, stříbrné a bronzové medaile se rozdělují v přibližném poměru 1 : 2 : 3. Na CEOI 2018 bylo uděleno 5 zlatých, 9 stříbrných a 14 bronzových medailí. Středoevropská olympiáda v informatice je soutěží jednotlivců, žádné pořadí zúčastněných zemí v ní není vyhlášováno.

Naši reprezentující dosáhli následujících výsledků:

30.	Jan Kaifer	239 bodů
32.	Jiří Kalvoda	204 bodů
35.	Radek Olšák	200 bodů
47.	Petr Zahradník	127 bodů

Nikdo z našich studentů tedy nezískal žádnou medaili.

Veškeré informace o soutěži, texty soutěžních úloh i podrobné výsledky všech soutěžících lze nalézt na Internetu na adrese <https://ceoi2018.pl/>. Následující 26. ročník Středoevropské olympiády v informatice CEOI 2019 se bude konat v Bratislavě na Slovensku. Konkrétní datum zatím nebylo stanoveno, soutěž proběhne pravděpodobně začátkem srpna někdy před datem konání celosvětové olympiády IOI 2019.



IOI 2018 JAPAN
TSUKUBA, IBARAKI

Také Mezinárodní olympiáda v informatice IOI 2018 měla letos kulaté výročí. Její třicátý ročník se konal ve dnech 1. – 8. září 2018 v japonském městě Tsukuba v prefektuře Ibaraki vzdáleném asi 50 kilometrů od hlavního města Tokio. Akci organizovala University of Tsukuba ve spolupráci s městem Tsukuba, japonským ministerstvem školství, kultury, sportu, vědy a techniky a dalšími organizacemi, a podpořila ji účastí na slavnostním zahájení i vnučka současného císaře, princezna Kako Akišino.

Soutěž probíhala ve sportovní hale Tsukuba Capio, doprovodný program a zasedání komisí pak v blízkém mezinárodním kongresovém centru. V sousedícím hotelu byli také ubytováni vedoucí všech delegací a hosté, zatímco soutěžící bydleli na poměrně vzdálených kolejích výzkumné organizace KEK. Oproti jiným ročníkům tak program pro soutěžící zahrnoval i mnoho autobusových přesunů.

Letošní olympiády se zúčastnilo celkem 335 soutěžících z rekordních 87 zemí celého světa, mimo soutěž navíc ještě druhé družstvo pořádající země. Naše české družstvo mělo následující složení:

Pavel Hudec, absolvent Gymnázia Jiřího Gutha-Jarkovského v Praze 1

Michal Jireš, student Gymnázia F. M. Pelcla v Rychnově nad Kněžnou

Martin Kurečka, absolvent Gymnázia na tř. Kpt. Jaroše v Brně

Josef Minařík, student Gymnázia na tř. Kpt. Jaroše v Brně

Vedoucími české delegace na IOI 2018 byli jmenováni doc. Mgr. Zdeněk Dvořák, Ph.D. a Bc. Václav Rozhoň, oba z Matematicko-fyzikální fakulty Univerzity Karlovy v Praze.

Vlastní soutěž se konala jako obvykle ve dvou dnech, oddělených jedním od-

počinkovým dnem. Průběh soutěže i způsob hodnocení úloh je na IOI stejný, jako na CEOI. Oproti CEOI letošní novinkou v pravidlech IOI bylo, že soutěžící během soutěže dostávají průběžně informaci o tom, kolik bodů celkově získali ostatní soutěžící za jednotlivé úlohy. Tyto údaje by měly slabším účastníkům poskytnout informaci o tom, která z úloh je nejsnazší.

Pro všechny účastníky olympiády byl kromě samotné soutěže připraven i bohatý doprovodný program, v jehož rámci měli účastníci možnost navštívit několik zajímavých míst v blízkosti Tsukuby: Warp station Edo (areál, v němž se natáčí filmy z japonského středověku), expozici japonské vesmírné agentury JAXA, svatyni Isosaki, akvárium Aqua World Oarai a park Hitachi.

Každá ze šesti soutěžních úloh je hodnocena maximálně 100 body, takže celkem bylo možné získat až 600 bodů. Letošním absolutním vítězem se stal student Benjamin Qi z USA, který získal 499 bodů. Na rozdíl od CEOI, při IOI se rozdělují medaile podle dosažených bodů na základě přesně stanovených pravidel. Někteří z medailů obdrží nejvýše polovina účastníků soutěže, přičemž zlaté, stříbrné a bronzové medaile se rozdělují v poměru 1:2:3 s ohledem na to, aby soutěžící se stejným bodovým ziskem získali stejnou medaili. Na letošní IOI bylo uděleno celkem 167 medailů, z toho 29 zlatých, 55 stříbrných a 83 bronzových.

Výsledky našich soutěžících:

87.	Josef Minařík	269 bodů	bronzová medaile
111.	Pavel Hudec	244 bodů	bronzová medaile
133.	Michal Jireš	220 bodů	bronzová medaile
252.	Martin Kurečka	92 bodů	

Zisk tří bronzových medailů je pro nás určitým zhoršením oproti předchozím letům, například loni získali naši soutěžící na IOI jednu zlatou, jednu stříbrnou a dvě bronzové medaile. I tak nás ale dosažený medailový zisk řadí přibližně do poloviny celkového pořadí zúčastněných zemí. Mezinárodní olympiáda v informatice je výhradně soutěží jednotlivců a oficiální pořadí zúčastněných zemí v ní není vyhlašováno. Nejúspěšnější zemí se čtyřmi zlatými medailami se tentokrát stala Čína, dalšími nejúspěšnějšími zeměmi byla Korea (tři zlaté a jedna stříbrná medaile) a USA (tři zlaté a jedna bronzová medaile). Slovenské družstvo získalo v letošním roce stejně jako my tři bronzové medaile.

Podrobné informace o soutěži i texty soutěžních úloh lze nalézt na Internetu na adrese <https://ioi2018.jp/>, kompletní výsledková listina je k dispozici na webové stránce se statistikami <http://stats.ioinformatics.org/results/2018>. Další ročníky Mezinárodní olympiády v informatice se budou konat v Ázerbájdžánu (2019), v Singapuru (2020), v Egyptě (2021) a Indonésii (2022). Pořadatelé příští mezinárodní olympiády v informatice z Ázerbájdžánu na místě pozvali všechny delegace zúčastněné na IOI 2018, aby se zúčastnily také následujícího 31. ročníku soutěže. Proběhne v hlavním městě Baku v srpnu 2019.

Pavel Töpfer

Seminář Matematika a fyzika ve škole

Ve dnech 21.–23. srpna 2018 proběhl v Jevíčku 2. ročník konference *Matematika a fyzika ve škole*. Do Jevíčka přijelo 56 účastníků, většinou středoškolských učitelů matematiky a fyziky. Slavnostní zahájení konference proběhlo za přítomnosti starosty města Jevíčka Dušana Pávka, dipl. um. a ředitele gymnázia Mgr. Jiřího Janečka. V úvodu účastníci vyslechli dvě skladby na klavír a housle v podání žáků ZUŠ z Jevíčka a Boskovic. Organizátorem konference byla Komise pro vzdělávání učitelů matematiky a fyziky JČMF, pobočný spolek JČMF Olomouc, Přírodovědecká fakulta UP Olomouc a Gymnázium Jevíčko. Na konferenci byly prosloveny následující přednášky:

$\mathbb{R} + A + D + Y + \dots$

(Jiří Bouchala, FEI VŠB, Ostrava),

Některé problémy našeho školství

(Eduard Fuchs, PřF MU, Brno),

Připravované revize RVP pro předškolní, základní a střední vzdělávání

(Jaroslav Fidrmuc, NÚV, Praha),

O méně obvyklých způsobech řešení nelineárních rovnic na střední škole

(Aleš Kobza, Gymnázium, kpt. Jaroše, Brno),

Může být inkluze exkluzivní?

(Josef Molnár, PřF UP, Olomouc),

Nanotechnologie, které už dnes mění náš svět

(Jakub Navařík, PřF UP, Olomouc),

Antropický princip

(Jan Novotný a Jindřiška Svobodová, PedF MU, Brno),

Zrakové klamy

(František Pluháček, PřF UP, Olomouc),

Problematika výuky matematiky v odborném vzdělávání

(Miroslav Staněk, SŠ André Citroëna, Boskovice),

Permutační pohádka

(Jaromír Šimša, PřF MU, Brno),

Vzdělávání učitelů – klid nebo klid před bouří?

(Iva Stuchlíková, PedF JU, České Budějovice),

Matematika a její aplikace

(Eva Zelendová, NÚV, Praha).

Zástupci firmy Casio pak účastníkům představili možnosti využití kalkulačů Classwiz ve vyučování, díky tomu si mnozí přítomní odvezli i dárek v podobě nové kalkulačky. Největší zájem vyvolala problematika přípravného vzdělávání učitelů, nový systém akreditací a připravovaná revize Rámcových vzdělávacích

programů. V rámci diskuze vystoupili rovněž zástupci CERMATU, kteří podali informace o vývoji kolem připravovaných změn maturitní zkoušky.

Pro účastníky konference byl také připraven kulturní program. V úterý to byla procházka večerním Jevíčkem s výkladem o historii a současnosti Jevíčka doplněná výstupem na městskou věž, večer si připravili sami účastníci konference hudební vystoupení v restauraci *Na Dvorku*. Společenský večer se konal ve středu v prostorách restaurace hotelu *Morava*. K dobré náladě zahrál účastníkům jazzový septet.

Lze říci, že konference byla dobře připravena jak po stránce odborné, tak společenské. Poděkování patří všem, kteří se na její přípravě a průběhu podíleli – za Přírodovědeckou fakultu UP a pobočný spolek JČMF v Olomouci Josefu Molnárovi a Lukáši Richterkovi, za Komisi pro vzdělávání učitelů matematiky a fyziky JČMF jejímu předsedovi Aleši Trojánkovi, za Gymnázium v Jevíčku jeho řediteli Jiřímu Janečkovi a jeho spolupracovníkům.

Dag Hrubý

Proč být učitelem fyziky

To je název semináře, který uspořádala dne 26. října 2018 katedra experimentální fyziky Přírodovědecké fakulty Univerzity Palackého a pobočný spolek Jednoty českých matematiků a fyziků v Olomouci u příležitosti 85. narozenin *doc. RNDr. Oldřicha Lepila, CSc.* První příspěvek na semináři, který přednesl sám jubilant, měl název *Jak jsem se stal učitelem fyziky* s podtitulem *Osobnosti a motivy, které nejvíce ovlivnily můj profesní život* (obr. 1).



Obr. 1

V době studia na Přírodovědecké fakultě MU v Brně v letech 1951–1955 to byl *prof. Václav Truneček*, který vzbudil jubilantův zájem především o elektroniku, a *dr. Marta Chytilová*, s níž po studiích spolupracoval mnoho let v didaktice fyziky. Prvním pracovištěm *doc. Lepila* byla jedenáctiletá střední všeobecně vzdělávací škola v tehdejší Gottwaldově (dnes Gymnázium Zlín – Lesní čtvrť), kde velmi dobře vybavený kabinet umožnil věnovat se zejména demonstračním

periodických dějů pomocí osciloskopu. Blízkost atelierů Krátkého filmu dala jubilantovi příležitost k tvorbě výukových filmů. Po přechodu na Přírodovědeckou fakultu UP v Olomouci v roce 1963 se doc. Lepil stal nejbližším spolupracovníkem jednoho ze zakladatelů české didaktiky fyziky *prof. Josefa Fuky* a na řešení problémů didaktiky fyziky spolupracoval s kolegy *dr. Milanem Bednaříkem* a *doc. Miroslavou Šírokovou*. Z jejich spolupráce vznikla řada publikací, především učebnic fyziky a sbírek fyzikálních úloh.

V příspěvku doc. Lepila byla oceněna spolupráce s matematicko-fyzikální fakultou UK v Praze, s připomenutím společných publikací s *prof. Emilem Kašparem*, *prof. Jaroslavem Vachkem* a stále trvající bohatá spolupráce s *prof. Emanuelem Svobodou*. Osobností, která ovlivnila profesní život jubilanta, byl také *dr. Přemysl Šedivý*, učitel gymnázia J. K. Tyla v Hradci Králové, s nímž spolupracoval nejen na úspěšné učebnici pro gymnázia *Elektřina a magnetismus*, ale i v oblasti pomůcek pro výuku fyziky. V závěru vystoupení doc. Lepil uvedl několik experimentů z jeho starších prací, které jsou vhodnými náměty pro inovaci s použitím současných měřicích počítačových systémů.

Další příspěvek přednesla *doc. RNDr. Alena Šolcová, Ph.D.*, předsedkyně Jednoty českých matematiků a fyziků, na téma *Matematické a fyzikální metody doby pozdně barokní a osvěcený jezuita Josef Stepling* (obr. 2). Podala charakteristiku podmínek v 18. století, od nichž se odvíjelo dílo Josefa Steplinga (1717–1778) a zmínila Steplingův vztah k Olomouci. Stepling zde studoval v letech 1735–1738 filozofii a po dalším studiu ve Štýrském Hradci se do Olomouce ještě krátce vrátil. Uveden byl příspěvek Steplinga k rozvoji astronomických pozorování, měření času slunečními hodinami a další souvislosti při experimentálním studiu statické elektřiny a paprskové optiky.



Obr. 2

Experimentální ráz mělo vystoupení *RNDr. Čenka Kodejšky, Ph.D.*, nazvané *Induktor za stovku a jeho využití*. S jednoduchým zdrojem vysokého napětí před-

vedl několik demonstrací výbojů v plynech a ve vzduchu. Obdobný ráz měl příspěvek *doc. RNDr. Zdeňka Drozda, Ph.D.*, který společně s *RNDr. Danou Mandíkovou, CSc.* v příspěvku *Několik rad zkušenějšímu kolegovi* předvedl celou sérii převážně motivačních experimentů z různých oblastí fyziky (obr. 3). Experimentální část semináře doplnilo vystoupení *doc. RNDr. Josefa Hubeňáka, CSc.*, v němž na téma *Fyzika s úsměvem* prezentoval sérii vtipných kreseb charakterizujících osobnosti fyziky a humorné veršíky vycházející z fyzikálních zákonů.



Obr. 3

Závěr semináře byl zaměřen na výsledky práce *doc. Lepila* v didaktice fyziky. *Prof. RNDr. Emanuel Svoboda, CSc.* v příspěvku *Lepilova didaktika fyziky (včera, dnes a zítra)* shrnul dlouhodobou spolupráci s jubilantem jak v didaktice fyziky, tak v činnosti Fyzikální pedagogické sekce JČMF a poukázal i na současnost spojenou s aktuálními pracemi na elektronickém doplňku společné publikace *Přehledu středoškolské fyziky*. *Prof. RNDr. Erika Mechlová, CSc.* v příspěvku *Kompetence učitele fyziky a role* *doc. RNDr. Oldřicha Lepila, CSc.* vymezila obecně sedm základních kompetencí učitele fyziky, které pak na základě dlouholeté spolupráce aplikovala na osobnost jubilanta. Závěrečný příspěvek přednesl zástupce šéfredaktorky nakladatelství Prometheus *PaedDr. Bohuslav Rothanzl*, který charakterizoval spolupráci *doc. Lepila* s nakladatelstvím od jeho vzniku v roce 1993 v oblasti učebnicové tvorby, která se netýká jen přípravy učebnic fyziky a sbírek úloh, ale např. také recenzní činnosti. Druhou oblastí spolupráce je funkce vedoucího redaktora časopisu *Matematika–fyzika–informatika*, který *doc. Lepil* s podporou nakladatelství založil a vede ho až do současného 27. ročníku.

Lukáš Richterek

MATEMATIKA – FYZIKA – INFORMATIKA
Časopis pro výuku na základních a středních školách
Ročník XXVII (2018)

MATEMATIKA

P. Leischner: Polibky kružnic: Philip Beecroft (s. 1) – *I. Chajda*: Matematika hrou (s. 9) – *M. Štěpánová*: Hvězdicové mnohoúhelníky (s. 13) – *M. Štěpánová*: Metrické vlastnosti hvězdicových mnohoúhelníků (s. 81) – *Z. Vrba*: Zlatý řez v jedné úloze 67. MO (s. 90) – *V. Zlámal*: O důkazech konkurentnosti přímek v rovině (s. 161) – *J. Vančura*: Využití Khan Academy pro zadávání a hodnocení domácích úkolů (s. 169) – *T. Gavala, S. Lukáč*: Diagnostika žiackych miskoncepcii v pravdepodobnosti (s. 180) – *P. Leischner*: Thébaultův problém 3887 (s. 241) – *P. Thustý, I. Krech*: O jedné úloze z AIME (s. 251) – *T. Hanusová, M. Štěpánová*: Leonardův dráp a Leonardovo zrcadlo (s. 256) – *J. Polák*: Analogie v matematice a jejich didaktické využití (s. 321) – *V. Vaněk, P. Calábek, D. Nocar*: České stopy v Matematickém klokanovi (s. 334) – Zajímavé matematické úlohy (s. 22, 96, 192, 268, 347)

FYZIKA

O. Lepil, Č. Kodejška: Netradiční experimenty s vázanými oscilátory (s. 26) – *Č. Kodejška, L. Myslivcová, F. Hošek, M. Rouha*: Srovnání charakteristik tónového generátoru a zvukové karty PC (s. 37) – *M. Mollerová, J. Kohout, L. Feřt, P. Masopust*: Nedostatek aprobovaných učitelů fyziky na západě Čech: bude hůř (s. 46) – *Č. Kodejška, J. Říha, S. Ganci*: Experimentální ověření rovnováhy atmosférického tlaku a hydrostatického tlaku ve válci (s. 99) – *D. Mandíková*: Zkoumáme ohřívání a chladnutí (s. 110) – *E. Svoboda*: Dekadické a binární předpony používané ve fyzice a ve výpočetní technice (s. 122) – *B. Vybíral, J. Kříž*: PRÆMIUM BOHEMIÆ 2017 ve zlatě (s. 126) – *R. Polma*: 50 let Mezinárodní fyzikální olympiády (1967–2017) (s. 134) – *O. Lepil*: Elektromagnetická indukce v obvodu s cívkou (s. 197) – *P. Adámek, P. Varnuška*: Jednoduché elektronické obvody s možným univerzálním použitím (s. 206) – *L. Břízová, M. Křížová, J. Šlégr*: Demonstrační mikrovlnný radiometr pro školní použití (s. 216) – *O. Lepil*: Nové vydání učebnice Mechanické kmitání a vlnění (s. 267) – *V. Štefl*: Keplerovy zákony ve výuce fyziky na gymnáziu (s. 278) – *Č. Kodejška, J. Říha*: Obecné řešení Buquoyovy úlohy (s. 288) – *E. Hejnová*: Testování vědeckého myšlení (s. 350) – *Č. Kodejška*: Inovativní demonstrace druhého Newtonova zákona (s. 359) – *Z. Gibová*: Návrh pracovního listu k apletu na zákony zachování energie (s. 365)

INFORMATIKA

E. Bartl: Moderní šifry I (s. 55) – *M. Kolařík*: Dva základní šifrovací principy (s. 67) – *P. Töpfer*: Mosty (Úlohy z MO kategorie P, 36. část) (s. 139) – *I. Nagyová*: Jak počítal první programovatelný počítač? (s. 149) – *Z. Tkáčová*: Projektové vyučování v informatice (s. 223) – *M. Tomáš*: Kontroverzní popularita simulační hypotézy (s. 231) – *L. Benediktová*: iBooks Author ve výuce na základní škole (s. 291) – *J. Frank, V. Vrbík*: Jedno méně obvyklé užití programu GeoGebra (s. 300) – *E. Bartl*: Moderní šifry II (s. 373)

ZPRÁVY

R. Horenský: 11. střeoevropská matematická olympiáda (s. 77) *L. Richterek*: Celostátní kolo FO 2018 (s. 158) – *J. Švrček*: Ústřední kolo 67. ročníku MO (kategorie A) (s. 238) – *P. Töpfer*: Ústřední kolo 67. ročníku MO (kategorie P) (s. 306) – *M. Rolínek, J. Tkadlec*: Dvě stříbra a dva bronzky z IMO 2018 (s. 308) – *J. Švrček, J. Zhouf*: EGMO 2018 v Itálii (s. 312) – *P. Calábek*: 12. střeoevropská matematická olympiáda (s. 389) – *P. Töpfer*: Mezinárodní olympiády v informatice v roce 2018 (s. 392) – *D. Hrubý*: Seminář Matematika a fyzika ve škole (s. 397) – *L. Richterek*: Proč být učitelem fyziky (s. 398)

LITERATURA

K. Vašíček: Simon Singh: Kniha kódů a šifer. Utajování od starověkého Egypta po kvantovou kryptografii (s. 80) – Recenze knihy Martiny Bečvářové a kol. Matematika ve středověké Evropě (s. 318)