

MATEMATIKA

Důkazy a kalkuly

FRANTIŠEK KUŘINA

Pedagogická fakulta UHK, Hradec Králové

Tento příspěvek je volným pokračováním mého článku *Matematika a kalkuly* [1]. Chci v něm na několika z historie známých příkladech ukázat, že kalkuly vhodného typu mohou v některých případech nahradit důkazy založené na „chytřém“ nápadu. Kalkuly se tak mohou stát prostředkem jisté „demokratizace“ matematiky, neboť mohou zprostředkovat přechod od „matematiky pro experty“ k matematice pro „skoro všechny“. Na střední škole můžeme některé příklady v článku uváděné využít buď ke smysluplnému procvičování příslušných kalkulů, nebo k ilustraci různých přístupů k téže problematice.

1. Thaletova věta

Důkaz věty

Množina vrcholů všech pravých úhlů roviny, jejichž ramena procházejí danými body A , B , je kružnice s průměrem AB

můžeme po zavedení skalárního součinu vektorů „provést výpočet“ takto: v kartézské soustavě souřadnic podle obr. 1, kde $A[-r, 0]$, $B[r, 0]$, $X[x, y]$ je úhel AXB pravý, právě když pro skalární součin platí:

$$\overrightarrow{AX} \cdot \overrightarrow{BX} = 0, \quad (1)$$

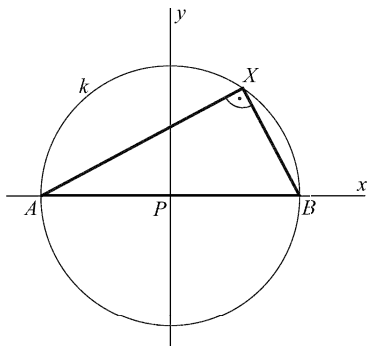
neboli

$$(x + r, y)(x - r, y) = 0. \quad (2)$$

To ovšem znamená, že souřadnice vrcholu X vyhovují rovnici

$$x^2 + y^2 = r^2 \quad (3)$$

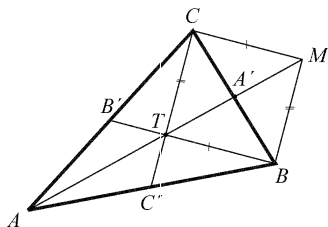
a leží tedy na kružnici s průměrem AB . Obráceně můžeme rovnost (3) upravit na tvar (1) a Thaletova věta je dokázána.



Obr. 1

2. Těžnice trojúhelníku

Věta o těžnicích trojúhelníku je součástí geometrie základní školy. Z řady důkazů této věty (pět jich uvádím v knize *Umění vidět v matematice* [2]) připomenu jeden, který zkonfrontuji s „důkazy výpočtem“.



Obr. 2

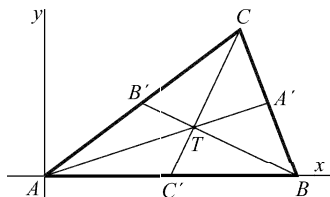
V trojúhelníku ABC jsou CC' a BB' těžnice, které se protínají v bodě T . Sestrojíme na přímce AT bod M tak, aby bod T byl středem úsečky AM (obr. 2). Protože je podle konstrukce $B'T$ střední příčka trojúhelníku AMC , je přímka $B'T = TB$ rovnoběžná s přímkou CM . Ze stejných důvodů je přímka CT rovnoběžná s přímkou MB (TC' je střední příčka trojúhelníku ABM). Čtyřúhelník $TBMC$ je tedy rovnoběžník, A' je střed strany BC a $|AT| = 2|A'T|$. Platí tedy:

V libovolném trojúhelníku procházejí těžnice jedním bodem, který dělí každou z nich v poměru 2 : 1.

Toto vyprávění, tento příběh, můžeme považovat za důkaz věty o těžišti trojúhelníku. Jeho jádrem byl nápad sestavit bod M popsaným způsobem.

Dovolím si zde osobní poznámku. V knize *Podivuhodný svět elementární matematiky* [3] jsem citovaný důkaz uvedl jako nový důkaz, který publikoval v roce 2004 jistý Američan. Tento důkaz však uvádí již *Eduard Čech* ve své učebnici z roku 1946 [4]. Stejný nápad se zrodil v různých dobách na různých místech.

Student, který zná základy analytické geometrie v rovině, může platnost věty o těžišti ověřit výpočtem. Vhodné je umístit trojúhelník do souřadnicového systému např. podle obr. 3 ($A[0, 0]$, $B[b, 0]$, $C[c, d]$) a vypočítat, že průsečíkem T přímk AA' , BB' prochází přímka CC' . To je příklad užití kalkulu analytické geometrie k důkazu věty o těžišti trojúhelníka.



Obr. 3

S užitím formálního kalkulu s body a vektory jako uspořádanými dvojicemi reálných čísel můžeme ovšem postupovat takto:

$$A + \frac{2}{3}\overrightarrow{AA'} = B + \frac{2}{3}\overrightarrow{BB'} = C + \frac{2}{3}\overrightarrow{CC'} = \frac{1}{3}(A + B + C), \quad (4)$$

neboť

$$A' = \frac{1}{2}(B + C), \quad \frac{2}{3}\overrightarrow{AA'} = \frac{2}{3}(A' - A) = \frac{1}{3}B + \frac{1}{3}C - \frac{2}{3}A, \quad (5)$$

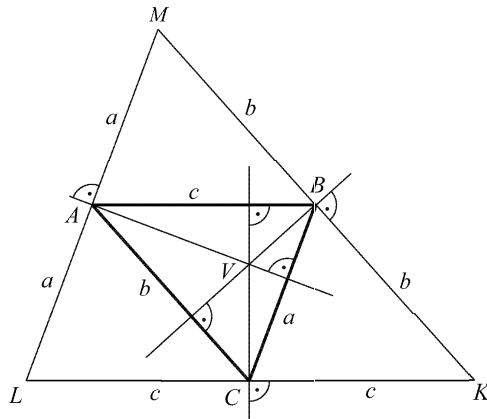
$$A + \frac{2}{3}\overrightarrow{AA'} = \frac{1}{3}(A + B + C). \quad (6)$$

Uvedené důkazy kalkulací spočívaly na rutinních výpočtech, které nevyžadovaly žádný zvláštní nápad.

3. Výšky trojúhelníku

Věta o průsečíku výšek trojúhelníku se v našich učebnicích obvykle opírá o myšlenku interpretovat výšky trojúhelníku jako osy stran jiného trojúhelníku následujícím způsobem.

Vedeme-li každým z vrcholů trojúhelníku ABC přímkou rovnoběžnou s protilehlou stranou, jsou průsečíky těchto přímek vrcholy trojúhelníku na obr. 4 označeného KLM , jehož osy stran jsou výškami trojúhelníku ABC (čtyřúhelníky $ABCL$, $ABKC$, $ACBM$ jsou totiž rovnoběžníky). Střed kružnice opsané trojúhelníku KLM je průsečík výšek trojúhelníku ABC .

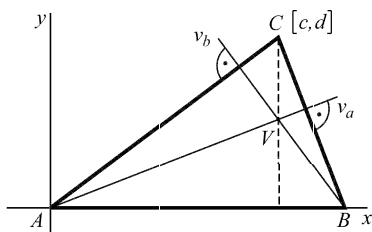


Obr. 4

To je příběh výšek trojúhelníku, jak ho pojal podle publikace [5] *Carl Friedrich Gauss* (1777 – 1855).

Metodou klasické analytické geometrie můžeme větu o průsečíku výšek dokázat výpočtem. Stačí ověřit, že průsečík přímek, v nichž leží výšky v_a , v_b (v označení podle obr. 5) má první souřadnici c .

Elegantněji můžeme dokázat větu o průsečíku výšek pomocí vektorového počtu, jak je uvedeno např. v učebnici ([6], s. 45).

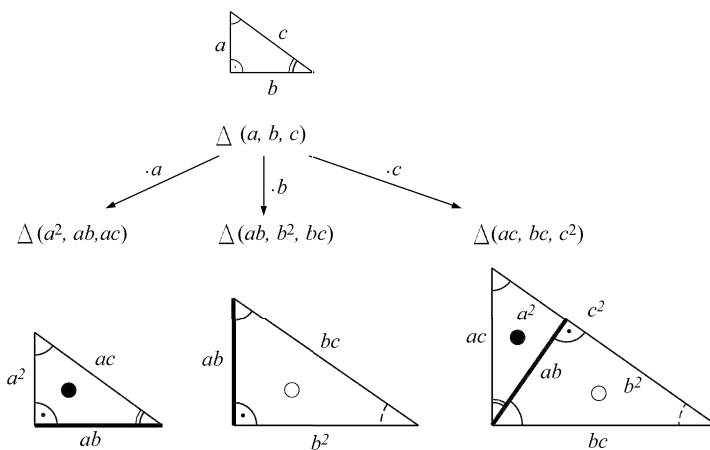


Obr. 5

4. Věta Pythagorova a její zobecnění

Důkazů Pythagorovy věty je známo velké množství. Zde uvedeme jeden méně známý, jehož autor je *Frank Burke* (citováno z knihy [7]). Důkaz má početně-konstruktivní charakter a nenašel jsem ho v reprezentativní publikaci [8].

Zvětšíme-li strany a , b , c pravoúhlého trojúhelníku po řadě a krát a b krát, dostaneme podobné trojúhelníky, z nichž lze složit podobný trojúhelník, jehož strany jsou c násobky stran původního trojúhelníku. Celý postup můžeme znázornit schématem na obr. 6, z něhož je patrná pythagorejská rovnost $a^2 + b^2 = c^2$.

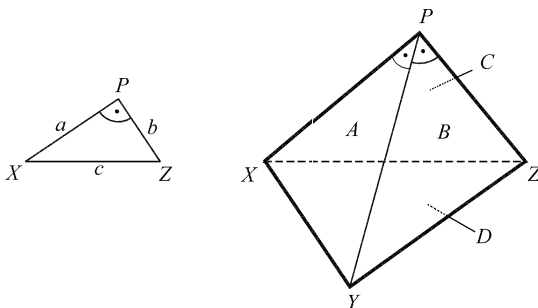


Obr. 6

Za prostorovou analogii pravoúhlého trojúhelníka můžeme považovat „pravoúhlý čtyřstěn“ podle obr. 7. Interpretujeme-li pythagorejskou rovnost $a^2 + b^2 = c^2$ jako „součet čtverců velikostí střech“ je roven čtverci „velikosti půdy“, mělo by platit pro pravoúhlý čtyřstěn analogicky

$$A^2 + B^2 + C^2 = D^2, \quad (7)$$

kde A , B , C jsou obsahy pravoúhlých trojúhelníků XPY , YZP a XZP a D je obsah ostroúhlého trojúhelníku XYZ .



Obr. 7

Toto tvrzení skutečně platí: je to Faulhaberovo zobecnění Pythagorovy věty. *Johann Faulhaber* (1580–1635) byl německý matematik. Umístíme-li pravoúhlý čtyřstěn do souřadnicového systému podle obr. 8 a označíme-li

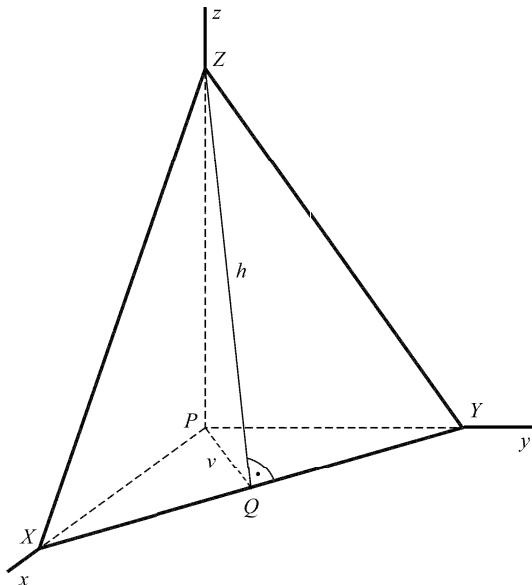
$$P[0, 0, 0], \quad X[x, 0, 0], \quad Y[0, y, 0], \quad Z[0, 0, z],$$

můžeme vypočítat

$$A = \frac{1}{2}xy, \quad B = \frac{1}{2}yz, \quad C = \frac{1}{2}xz, \quad (8)$$

Protože délky stran trojúhelníku XYZ můžeme vypočítat podle Pythagorovy věty

$$|XY| = \sqrt{x^2 + y^2}, \quad |YZ| = \sqrt{y^2 + z^2}, \quad |ZX| = \sqrt{x^2 + z^2}, \quad (9)$$



Obr. 8

nabízí se určit obsah trojúhelníku D podle Heronova vzorce a algebraicky tak dokázat platnost rovnosti (7). K důkazu nám sice stačí algebraický kalkul, ale výpočet je dosti zdoluhavý. Stereometrickou úlohu jsme tak vlastně řešili „v několika rovinách“, řešit ji „prostorově“ bude patrně jednodušší.

Dvojím vyjádřením obsahu A můžeme určit výšku v k přeponě pravoúhlého trojúhelníku PXY , Pythagorovou větou pak určíme výšku h ke straně XY v trojúhelníku XYZ a ověření platnosti tvrzení (7) je jednoduché.

K dalšímu způsobu důkazu Faulhaberovy věty můžeme využít analytickou geometrii prostoru. Podle vzorce pro vzdálenost bodu P od roviny XYZ určíme výšku čtyřstěnu sestavenou z vrcholu P a dvojím vyjádřením objemu čtyřstěnu $PXYZ$, vypočítáme obsah D trojúhelníku XYZ a ověříme platnost vztahu (7).

Patrně nejjednodušší odvození však nabízí vektorový počet. Na tento přístup mě upozornil *Svatopluk Zachariáš*.

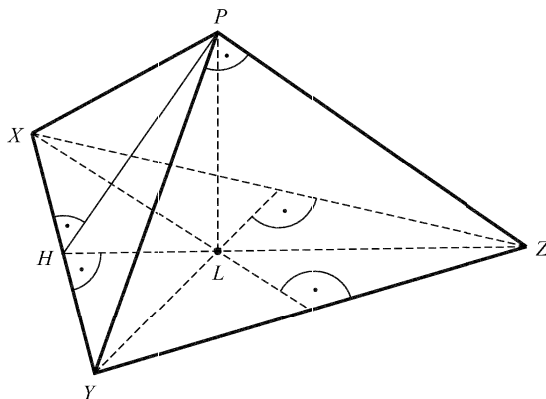
Z geometrického významu vektorového součinu plyne:

$$D = \frac{1}{2} |\vec{ZX} \times \vec{ZY}| = \frac{1}{2} |(x, 0, -z) \times (0, y, -z)| = \frac{1}{2} |(zy, xz, zy)| \quad (10)$$

Je tedy

$$D^2 = \frac{1}{4}(x^2y^2 + y^2z^2 + x^2z^2) = A^2 + B^2 + C^2. \quad (11)$$

U Thaletovy věty i u vět o těžnicích a výškách trojúhelníku byly z historie známy „nekalkulativní důkazy“. Kalkuly umožnily důkazy provést na základě výpočtů. Při hledání důkazu Faulhaberovy věty jsem nabyl přesvědčení, že její odvození bez kalkulu není možné. Z omylu mě vyvedl *Pavel Leischner*, který mi sdělil následující pěkný příběh jejího nekalkulativního odvození.



Obr. 9

Promítněme přímku PZ pravoúhle do roviny XYZ . Protože je přímka PZ kolmá k rovině PXY , je PZ kolmá k přímce XY a pravoúhlý průmět ZL je kolmý k XY (pravoúhlý průmět pravého úhlu, jehož jedno rameno je částí průmětny). Je tedy (v označení podle obr. 9) HZ výškou trojúhelníku XYZ a HP výškou trojúhelníku XPY . V pravoúhlém trojúhelníku HPZ platí podle Eukleidovy věty o odvěsně

$$|HP|^2 = |HL| \cdot |HZ| \quad (12)$$

Vynásobíme-li tuto rovnost číslem $\frac{1}{4}|XY|^2$, dostaneme

$$\frac{1}{4}|HP|^2 \cdot |XY|^2 = \left(\frac{1}{2}|HL| \cdot |XY|\right) \cdot \left(\frac{1}{2}|HZ| \cdot |XY|\right). \quad (13)$$

Označíme-li obsah trojúhelníku XYL jako A_1 , můžeme rovnost (13) interpretovat jako rovnost

$$A^2 = A_1 D. \quad (14)$$

Podobně můžeme odvodit

$$B^2 = B_1 D, \quad (15)$$

$$C^2 = C_1, \quad (16)$$

kde B_1 a C_1 jsou obsahy trojúhelníků YZL a XZL .

Sečtením rovností (14), (15) a (16) dostaneme

$$A^2 + B^2 + C^2 = D(A_1 + B_1 + C_1) = D^2.$$

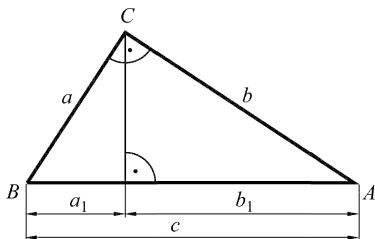
Tento důkaz je ovšem přímou analogií známého důkazu Pythagorovy věty pomocí vět Eukleidových podle obr. 10.

$$a^2 = a_1 \cdot c$$

$$b^2 = b_1 \cdot c$$

$$a^2 + b^2 = (a_1 + b_1)c = c^2.$$

Vztahy (14), (15) a (16) jsou určitými prostorovými analogiemi Eukleidových vět o odvěsnách.



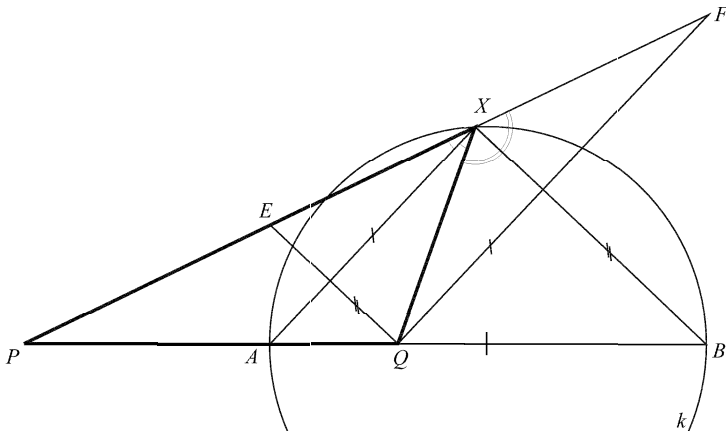
Obr. 10

5. Apollóniova kružnice

Není mi známo, jak *Apollónius z Pergy* (−260, −170) dokázal svou proslulou větou, kterou v dnešní dikci můžeme formulovat takto:

Množina všech bodů roviny, které mají od daných bodů P, Q poměr vzdáleností roven číslu m ($m \neq 1$), je kružnice s průměrem na přímce PQ .

Předpokládám však, že mohl postupovat následujícím způsobem.



Obr. 11

Je-li X jedním z bodů, který neleží na přímce PQ a splňuje podmínky věty, sestrojíme podle obr. 11 osu XA vnitřního úhlu a osu XB vnějšího úhlu trojúhelníku PXQ a body E, F přímky PX , pro něž platí

$$QE \parallel BX \quad \text{a} \quad QF \parallel AX. \quad (17)$$

Protože přímky AX, BX jsou navzájem kolmé, je

$$|EX| = |QX| = |FX|, \quad (18)$$

a platí

$$\frac{|PX|}{|QX|} = \frac{|PX|}{|FX|} = \frac{|PA|}{|QA|} = m, \quad (19)$$

$$\frac{|PX|}{|QX|} = \frac{|PX|}{|EX|} = \frac{|PB|}{|QB|} = m. \quad (20)$$

Bod X tedy leží na Thaletově kružnici k s průměrem AB .

Ukažme dále, že libovolný bod X kružnice k má poměr vzdáleností od bodů P, Q rovný číslu m .

K bodům A, B , pro něž platí

$$\frac{|PA|}{|QA|} = \frac{|PB|}{|QB|} = m, \quad (21)$$

sestrojme na přímce PX body E, F tak, že platí

$$\frac{|PA|}{|QA|} = \frac{|PX|}{|FX|} = m, \quad \frac{|PB|}{|QB|} = \frac{|PX|}{|EX|} = m. \quad (22)$$

Je tedy $|EX| = |FX|$ a protože je $AX \perp BX$, prochází kružnice s průměrem EF bodem Q . Platí tedy $|FX| = |QX|$ a bod X má požadovanou vlastnost.

Řešení úlohy vyžadovalo jen znalost podobnosti trojúhelníků, bylo však založeno na nápadu konstruovat osu vnitřního a vnějšího úhlu u vrcholu X trojúhelníku PXQ .

Máme-li k dispozici kalkul analytické geometrie, můžeme úlohu vyřešit pouhým „převodem textu do rovnice“ a její úpravou. V kartézské soustavě souřadnic volme $P[0, 0]$, $Q[q, 0]$, $q > 0$, $X[x, y]$. Pro body hledané množiny má platit

$$\frac{\sqrt{x^2 + y^2}}{\sqrt{(x - q)^2 + y^2}} = m. \quad (23)$$

Protože tuto rovnost můžeme upravit na tvar

$$\left(x - \frac{m^2 q}{m^2 - 1}\right) + y^2 = \frac{m^2 q^2}{(m^2 - 1)^2}, \quad (24)$$

je hledanou množinou kružnice se středem

$$S \left[\frac{m^2 q}{m^2 - 1}, 0 \right] \quad \text{a poloměrem} \quad \frac{mq}{|m^2 - 1|}.$$

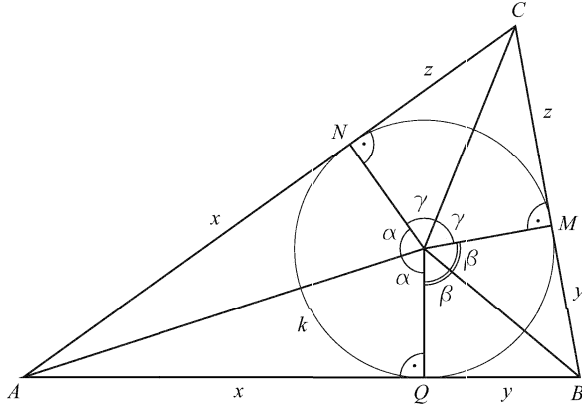
6. Heronův vzorec

Někdy kolem počátku našeho letopočtu dal *Heron z Alexandrie* dohromady příběh svého vzorce

$$S = \sqrt{s(s - a)(s - b)(s - c)} \quad (25)$$

pro obsah S trojúhelníku se stranami a, b, c , kde $s = \frac{1}{2}(a + b + c)$

S obdivem nad Heronovou intuicí a důvtipem zde jeho důkaz zprostředkovaný *Moritzem Cantorem* [9] připomenou.



Obr. 12

V trojúhelníku ABC se stranami a, b, c je $k(S; r)$ kružnice, která se dotýká jeho stran v bodech M, N, Q . V označení podle obr. 12 platí:

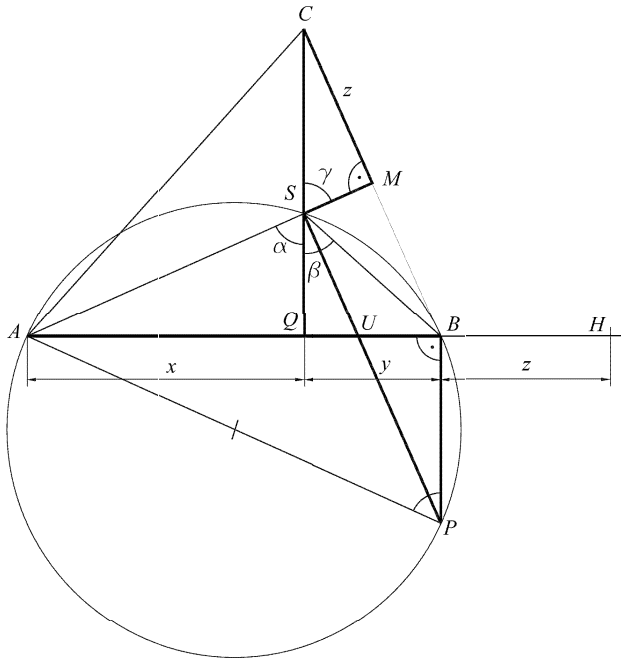
$$\begin{aligned}x + y &= c \\y + z &= a \\x + z &= b\end{aligned}\tag{26}$$

$$\alpha + \beta + \gamma = 180^\circ.\tag{27}$$

Řešíme-li soustavu (26) vzhledem k neznámým x, y, z , dostaneme

$$\begin{aligned}x &= \frac{1}{2}(b + c - a) = s - a, \\y &= \frac{1}{2}(a + c - b) = s - b, \\z &= \frac{1}{2}(a + b - c) = s - c,\end{aligned}\tag{28}$$

Sestrojíme trojúhelníky ABP a SUQ podle obr. 13 ($AB \perp BP$, $PS \perp AS$, $U \in AB \cap SP$).



Obr. 13

Podle konstrukce je čtyřúhelník $ASBP$ tětíkový a v důsledku rovnosti (27) má úhel APB velikost γ . V důsledku podobnosti trojúhelníků ABP a CMS platí

$$\frac{|BA|}{|BP|} = \frac{|CM|}{|SM|} = \frac{|BH|}{|SQ|}, \quad (29)$$

kde $|BH| = |CM| = z$ podle obr. 13.

Rovnost (29) můžeme upravit na tvar

$$\frac{|BA|}{|BH|} = \frac{|BP|}{|SQ|}. \quad (30)$$

Z podobnosti trojúhelníků UBP , UQS plyne

$$\frac{|BP|}{|SQ|} = \frac{|BU|}{|UQ|}. \quad (31)$$

Platí tedy

$$\frac{|BA|}{|BH|} = \frac{|BU|}{|UQ|}, \quad (32)$$

a tedy i

$$\frac{|BA|}{|BH|} + \frac{|BH|}{|BH|} = \frac{|BU|}{|UQ|} + \frac{|UQ|}{|UQ|}, \quad (33)$$

neboli

$$\frac{|AH|}{|BH|} = \frac{|BQ|}{|UQ|}. \quad (34)$$

Rovnost (34) můžeme upravit na tvar

$$\frac{|AH|^2}{|BH| \cdot |AH|} = \frac{|BQ| \cdot |AQ|}{|UQ| \cdot |AQ|}. \quad (35)$$

Protože podle Eukleidovy věty pro trojúhelník ASU platí

$$|UQ| \cdot |AQ| = |SQ|^2, \quad (36)$$

můžeme rovnost (35) přepsat na tvar

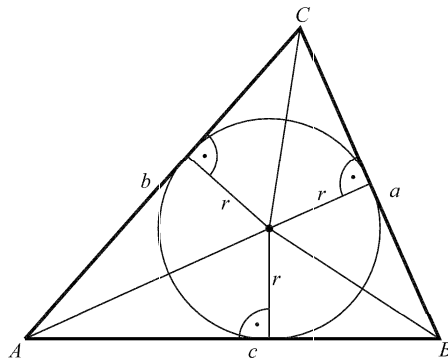
$$(|AH| \cdot |SQ|)^2 = |AH| \cdot |AQ| \cdot |BQ| \cdot |BH| \quad (37)$$

neboli

$$S = \sqrt{s(s-a)(s-b)(s-c)}, \quad (25)$$

neboť $|AH| = x + y + z = s$ a pro obsah S trojúhelníku se stranami a, b, c a poloměrem r kružnice vepsané platí podle obr. 14

$$S = \frac{1}{2}r(a + b + c) = sr. \quad (38)$$



Obr. 14

Dnešní středoškolák může odvodit Heronův vzorec téměř samostatně, má-li k dispozici trigonometrii a umí upravovat algebraické výrazy. Může postupovat např. takto:

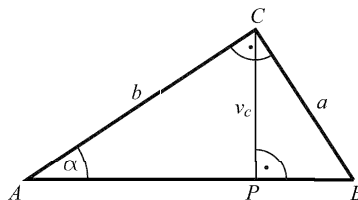
Vyjde-li ze vzorce

$$S = \frac{1}{2} c \cdot v_c \quad (39)$$

potřebuje vyjádřit výšku v_c pomocí délek stran. To mu umožní např. aplikace kosinové věty. V označení podle obr. 15 platí:

$$|AP| = b \cos \alpha, \quad (40)$$

$$v_c^2 = b^2 - b^2 \cos^2 \alpha. \quad (41)$$



Obr. 15

Z kosinové věty pro trojúhelník ABC můžeme vypočítat

$$\cos \alpha = \frac{b^2 + c^2 - a^2}{2bc} \quad (42)$$

a je tedy

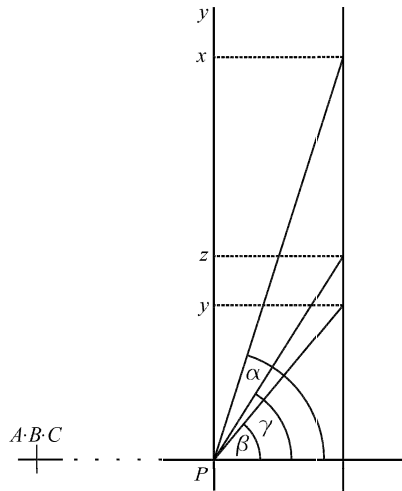
$$v_c = b \cdot \sqrt{1 - \left(\frac{b^2 + c^2 - a^2}{2bc} \right)^2}. \quad (43)$$

Pouhou algebraickou úpravou dostaneme odtud s použitím vztahů (28) vyjádření

$$v_c = \frac{2}{c} \cdot \sqrt{s(s-a)(s-b)(s-c)}, \quad (44)$$

z něhož plyne po dosazení do vzorce (39) vzorec Heronův.

Elegantnější přístup založený na počítání s komplexními čísly zveřejnil nedávno *Miles Dillon Edwards* [10]. Uvedme jeho postup.



Obr. 16

Přemístíme trojúhelníky SNA , SQB , SMC z obr. 12 do Gaussovy roviny podle obr. 16. Součin $A \cdot B \cdot C$ komplexních čísel

$$A = r + xi, \quad B = r + yi, \quad C = r + zi \quad (45)$$

je vzhledem k rovnosti (27) a geometrickému významu násobení komplexních čísel číslem reálným. Jeho imaginární složka je tedy nulová.

Platí tedy

$$r^2(x + y + z) - xyz = 0 \quad (46)$$

neboli

$$r = \sqrt{\frac{xyz}{x+y+z}}. \quad (47)$$

To ovšem vzhledem ke vzorci (38), vztahům (28) a rovnosti $x + y + z = s$ znamená, že platí (25).

7. Závěr

Základní otázkou matematického vzdělávání, ale možná každé lidské činnosti, je otázka smyslu. Proč se mají děti učit malou násobilku, proč máme trápit studenty úpravou algebraických výrazů, ... ? To jsou vážné didaktické otázky, kterými se zde nemůžeme zabývat, v závěru článku se ovšem chci vyjádřit k problematice důkazů ve vyučování.

Michal Krížek se v nedávno vydané knize [11] vyznává: *Matematické věty a jejich důkazy jsou pro nás jako valouny zlata pro zlatokopy. Gustav Choquet, jedna z nejvýznamnějších postav světové matematiky druhé poloviny dvacátého století ovšem napsal: Chování vědce, ať již v matematice či v experimentálních vědách, připomíná chování průzkumníka v lese, který hledá pramen nebo vzácný druh hmyzu. Kráčí stezičkou s napnutými smysly připravenými vnímat podněty. Bez umlčení využívá postranní pěšinky. A někdy se stane zázrak. Vydal se za motýlem a objevuje potůček, v němž se povalují valouny zlata* ([12], s. 90).

Matematické vzdělávání se jistě liší podstatně od vědecké práce, navzdory optimistickým představám *Jerome S. Brunera* ze šedesátých let minulého století, že *intelektuální činnost je vždy táž, ať jde o nejvyšší vědu, či o třetí třídu ve škole. Činnost vědce za jeho psacím stolem nebo v laboratoři, činnost literárního kritika při čtení básně jsou činnosti téhož řádu jako činnost kteréhokoliv člověka zabývajícího se podobnými věcmi – snaží-li se, aby jim porozuměl. Rozdíl je zde ve stupni, nikoliv v druhu* ([13], s. 26).

Jak máme chápat důkazy a dokazování ve školní matematice?

Ruský matematik *J. A. Šichanovič* napsal: *Důkaz je úvaha, která přesvědčuje* [14]. Naproti tomu rakouský logik *Friedrich Waismann* zdůrazňuje: „... mnohý si jistě myslí, že je zcela zbytečné zeshiřovat dokazovat to, o čem stejně nikdo nepochybuje. Úlohou důkazů však není vyvolat v nás pocit přesvědčení, nýbrž dát nám nahlédnout do vzájemných souvislostí vět. Požadavek dokázat vše, co jen dokázat lze, není výplodem pochybovačné

mysli, nýbrž je to vyjádření touhy vidět strukturu větné stavby ve vši jasnosti, vidět spojení, existující mezi jednotlivými pravdami“ (citováno podle [15], s. 127). Pro oba zde citované názory můžeme najít ve školní matematice přesvědčivé argumenty. Vždy však musí žák či student pocítit smysl dokazování. Polská didaktička *Anna Zofia Krygowska* uvádí v této souvislosti příhodu s téměř anekdotickým vyústěním, kdy si žákyně sedmé třídy povzdychla: *Všem nám to bylo jasné, jen paní učitelka ještě dokazovala, že shodné trojúhelníky jsou shodné.*

Podle mého názoru nepřispívají k pochopení role důkazů ve školské matematice příliš formální postupy. *Hans Selye*, kanadský lékař a vědec, dokonce napsal: *Z překážek, které stojí v cestě pokroku vědy, je třeba na prvním místě uvést analýzu vědeckých postupů, které jsou plodem logiky ... Nesnažila se popsat metody, jimiž věda v praxi postupuje, a nepokusila se odvodit pravidla, která by se dala použít k řízení pokroku vědy ... Řád objevů nahradila řádem důkazů* ([16], s. 343). Britský matematik *Ian Stewart* formuluje stanovisko k důkazům, které se i mně, po mnohaleté pedagogické praxi, jeví jako správné: *Učebnice matematické logiky říkají, že důkaz je posloupnost tvrzení, z nichž každé plyne buďto z nějakého tvrzení předcházejícího nebo z dohodnutých axiomů – nedokázaných, ale explicitně formulovaných předpokladů, které vymezují studovanou oblast matematiky. Takto řečeno ze to asi tak informativní, jako když řekneme, že román je posloupnost vět, z nichž každá buďto ustavuje dohodnutý kontext nebo plyne věrohodně z předcházejících vět. Obě definice mýjejí něco podstatného: to, že jak důkazy, tak román musí vyprávět zajímavý příběh* ([17], s. 49).

Důkaz vyprávěný jako příběh navozuje přirozenějším způsobem souvislosti než posloupnost implikací.

V tomto článku jsem se snažil ukázat, že do příběhu, který je jádrem důkazu, lze mnohdy účinně zapojit výpočet, kalkul. Je to pochopitelné, neboť kalkuly jsou do jistého řádu zhuštěné souvislosti a jejich použití může někdy nahradit jednorázové proniknutí do problému formou chytrého nápadu.

Formálně logickým zdůrazňováním charakteru důkazu jako posloupnosti implikací lze stěží přesvědčit studenty, když navíc vědí, že implikace nevyjadřuje žádnou věcnou souvislost předpokladu a tvrzení. Hledání důkazů je věcí intuice, nikoliv věcí logiky.

Literatura

- [1] *Kuřina, F.*: Matematika a kalkuly. Matematika, fyziky, informatika, č. 1, 2008.

- [2] *Kuřina, F.*: Umění vidět v matematice. SPN, Praha 1989.
- [3] *Kuřina, F. – Půlpán, Z.*: Podivuhodný svět elementární matematiky. Academia, Praha 2006.
- [4] *Čech, E.*: Geometrie pro IV. ročník měšťanských a středních škol. JČMF, Praha 1946.
- [5] *Baltzer, R.*: Die Elemente der Mathematik, Hirzel, Leipzig 1883.
- [6] *Kočandrlé, M. – Boček, L.*: Matematika pro gymnázia. Analytická geometrie. Prometheus, Praha 1995.
- [7] *Nelsen, R. B.*: Proofs without Words II. MAA, Washington 2000.
- [8] *Maor, E.*: The Pythagorean Theorem. Princeton University Press, Princeton 2007.
- [9] *Cantor, M.*: Vorlesungen über die Geschichte der Mathematik, I., Teubner, Leipzig 1894.
- [10] *Edwards, M. D.*: A Proof of Heron's Formula. Mathematical Monthly, XII, 2007.
- [11] *Křížek, M. – Somer, L. – Šolcová, A.*: Kouzlo čísel. Academia, Praha 2009.
- [12] *Choquet, G.*: Vznik teorie kapacit: zamyšlení nad vlastní zkušeností. In: Profesor *Gustave Choquet*. Matfyzpress, Praha 2002.
- [13] *Bruner, J. S.*: Vzdělávací proces. SPN, Praha 1965.
- [14] *Šichanovič, J. A.*: Vvedeniye v sovremennuyu matematiku. Nauka, Moskva 1965.
- [15] *Thiele, R.*: Matematické důkazy. SNTL, Praha 1985.
- [16] *Selye, H.*: K záhadám vědy. Orbis, Praha 1975.
- [17] *Stewart, I.*: Čísla přírody. Archa, Bratislava 1996.

Příspěvek byl vypracován v rámci grantu GAČR 406-08-0710.

Použití jisté algebraické metody při šifrování

IVAN CHAJDA

Přírodovědecká fakulta UP, Olomouc

Už v době antické požívaly římské legie při přenosu zpráv šifrování. Chránily tak obsah zprávy před zneužitím nepovolanou osobou. V průběhu věků došlo k značnému rozvoji šifrovacích metod, které našly uplatnění zejména ve vojenství. Mezi laiky se zájem o šifrování nyní značně zvýšil po uvedení britsko amerického filmu Enigma, popisujícího průběh prolomení šifry německých armád za druhé světové války. Čtenář asi snadno pochopí,

že nejúčelnější je taková šifrovací metoda, která nepůsobí velké obtíže odesílateli při zašifrování a příjemci při rozšifrování, která však působí značné potíže a zabere mnoho času neautorizované osobě, která by chtěla šifru prolomit. Šifrování totiž vychází z poznatku, že prolomit lze v zásadě každou šifru, ale u některých důmyslných to může trvat tak dlouho, že přenášená zpráva již není v té době aktuální.

Hned v úvodu je třeba dodat, že takové šifry jsou založené na důmyslných algebraických metodách a používají hluboké znalosti teorie čísel. My se zde ovšem hodláme seznámit metodou jednodušší, která bude čtenáři snadno přístupná.

Nejprve se zmíníme o kódování. Předpokládejme, že je dána nějaká konečná neprázdná množina znaků. Tuto množinu nazýváme *abeceda*. Pro účely naší komunikace většinou používáme takovou abecedu, jejíž znaky nazýváme písmena, číslice a interpunkční znaky. V technických systémech a zařízeních, zejména v počítačích a přenosových sítích, se většinou používá tzv. *binární abeceda*, která má právě dva znaky. Zpravidla je označujeme jako 0 a 1. Je to tak z důvodu snadné technické realizovatelnosti dvou odlišných stavů systému, kterými tyto znaky realizujeme. *Kódováním* pak rozumíme jednoznačný převod znaků jedné abecedy na konečné posloupnosti znaků abecedy druhé. Čtenář jistě ví, že každý znak, ať už písmeno, číslice nebo interpunkce v naší (tzv. *latinské*) abecedě je např. v počítači zakódován pomocí konečné posloupnosti (n -tice) nul a jedniček. Binární kódy ovšem vznikly dávno před vynálezem počítače, jako příklad lze uvést *Morseovu abecedu*, kde každé písmeno a číslice je zakódována pomocí konečné posloupnosti dvou znaků, což jsou čárka a tečka. O významu Morseovy abecedy v minulosti se není třeba rozšiřovat, takto zakódované zprávy byly přenášeny např. telegrafem a zachránily tisíce lidských životů. Ve druhé polovině 20. století byly postupně telegrafy nahrazeny dálkopisy. Ty ke kódování naší abecedy používaly opět binární kód označený jako CCITT, kde každý znak byl zakódován pomocí uspořádané pětice, obsahující znaky 0 a 1. Pro představu čtenáře zde uvádíme kódy písmen anglické abecedy (o 26 písmenech):

A = 11000,	B = 10011,	C = 01110,	D = 10010,	E = 10000,
F = 10110,	G = 01011,	H = 00101,	I = 01100,	J = 11010,
K = 11110,	L = 01001,	M = 00111,	N = 00110,	O = 00011,
P = 01101,	Q = 11101,	R = 01010,	S = 10100,	T = 00001,
U = 11100,	V = 01111,	W = 11001,	X = 10111,	Y = 10101,
Z = 10001.				

Jelikož počet všech uspořádaných pětic sestavených z binárních číslic 0 a 1 odpovídá celkově $2^5 = 32$ znakům, byl tento binární kód vhodný pro přenos textových zpráv.

V dnešní době se používají poněkud důmyslnější kódy, které nazýváme *samoopravné*. Při drobné chybě při přenosu zprávy, jakou je zkomolení jednoho či dvou znaků binární abecedy, je takový kód schopen nejen chybu detekovat, ale i opravit. Samozřejmě, že pak musí být každý znak naší výchozí abecedy kódován pomocí poněkud delší posloupnosti nul a jedniček (např. desetičlenné). Popis takových kódů by ale vyžadoval poněkud pokročilejší algebraický aparát, který zde nebudeme zavádět.

Je-li tedy naše zpráva zakódována např. v binárním kódu, můžeme ji zašifrovat tak, aby ji bez problému mohl rozšifrovat pouze námi určený příjemce. K tomu slouží tzv. *šifrovací klíče*. Označme naši zprávu symbolem X . Jestliže nyní zvolíme šifrovací klíč b , pak použijeme *šifrovací proceduru* Φ_b , a tedy odesíláme již zašifrovanou zprávu $\Phi_b(X)$. Příjemce ovšem klíč b zná, a zná i *dešifrovací proceduru* Ψ_b , na tomto klíči založenou. Tuto pak použije na zprávu $\Phi_b(X)$ a obdrží původní zprávu X , neboli $X = \Psi_b(\Phi_b(X))$, kde tento symbol vyjadřuje provedení procedury Ψ_b na zašifrovanou zprávu $\Phi_b(X)$.

Jak již bylo v úvodu řečeno, cílem je najít takovou šifrovací a dešifrovací proceduru, aby šifrování bylo co nejjednodušší a nejrychlejší, ale zároveň aby činilo potíže tomu, kdo by chtěl šifru prolomit, ale klíč nezná. K tomu můžeme s výhodou použít i poměrně jednoduchý algebraický aparát. Na dvouprvkové množině $\{0,1\}$ lze zavést binární operaci, tzv. sčítání podle modulu 2, takto:

$$0 + 0 = 0, \quad 0 + 1 = 1, \quad 1 + 0 = 1, \quad 1 + 1 = 0.$$

Čtenář znalý např. Booleovy algebry snadno rozpozná, že se jedná o tzv. operaci symetrické difference na dvouprvkové Booleově algebře. Ten, kdo zná počítání v okruzích zbytkových tříd ví, že se jedná o aditivní operaci v okruhu zbytkových tříd mod 2. A konečně, odborník na konstrukce elektrických obvodů rozpozná, že se jedná o tzv. „*binární sčítání bez přenosu*“. Neznalému čtenáři lze tento pojem objasnit následovně. Sčítáme-li v dvojkové soustavě, pak samozřejmě $0 + 0 = 0$, $0 + 1 = 1$, $1 + 0 = 0$, avšak $1 + 1 = 10$, neboť číslo 2 je ve dvojkové soustavě vyjádřeno ve tvaru 10. Při sčítání $1 + 1$ je tedy výsledek v posledním řádu roven 0, a číslice 1 se přenáší do vyššího řádu. Jestliže na tento přenos „zapomeneme“, dostaneme výše uvedenou operaci. Máme-li nyní dvě uspořádané n -tice nul

a jedniček, např. $(a_1, \dots, a_n), (b_1, \dots, b_n)$, pak pro ně zavádíme operaci „+“ (často) nazývanou *symetrická diference*, a to následujícím způsobem:

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n),$$

kde na pravé straně (uvnitř závorky) používáme výše uvedené sčítání „+“ modulo 2 (operace „+“ se při počítání s n -ticemi aplikuje po složkách).

Příklad 1

$$(10101) + (11001) = (01100).$$

Lze snadno ověřit také základní algebraické vlastnosti této operace. Jsou to:

- *asociativita*, tj. $a + (b + c) = (a + b) + c$,
- *komutativita*, tj. $a + b = b + a$,
- existence neutrálního prvku, což je $o = (0, \dots, 0)$,
- *involutornost*, tj. $a + a = o$.

Již tento jednoduchý algebraický aparát nám umožní efektivní šifrování a dešifrování. Za pomoci asociativity, existence neutrálního prvku a involutornosti snadno nahlédneme, že pro každé x a každé b platí

$$(x + b) + b = x.$$

Nyní lze tedy každý znak naší abecedy, zakódovaný v binárním kódu jako x , zašifrovat klíčem b , což je libovolný ale pevně zvolený znak našeho binárního kódu, a to takto:

$$\Phi_b(x) = x + b.$$

Jestliže nyní tento znak odešleme příjemci, který klíč b zná, pak může naprosto stejným postupem znak rozšifrovat, neboť volbou $\Psi_b = \Phi_b$ dostaneme

$$\Psi_b(\Phi_b(x)) = (x + b) + b = x.$$

Metoda je velice jednoduchá, čtenář si ji může snadno ověřit na následujícím příkladu.

Příklad 2

Nechť odesílatel hodlá odeslat příjemci slovo KNIHA. Použitím kódu CCITT je toto slovo zakódováno takto:

$$K = 11110, \quad N = 00110, \quad I = 01100, \quad H = 00101, \quad A = 11000.$$

Předpokládejme nyní, že se odesílatel s příjemcem předem domluvili, že klíčem bude znak $b = 11011$. Pak zakódování slova je

$$\Phi_b(K) = 11110 + 11011 = 00101 = H,$$

$$\Phi_b(N) = 00110 + 11011 = 11101 = Q,$$

$$\Phi_b(I) = 01100 + 11011 = 10111 = X,$$

$$\Phi_b(H) = 00101 + 11011 = 11110 = K,$$

$$\Phi_b(A) = 11000 + 11011 = 00011 = O.$$

Jestliže neautorizovaná osoba klíč b nezná, nemůže sled písmen HQXKO rozluštit jinak, než že bude postupně zkoušet všech 32 kombinací pětic znaků 0 a 1, což je relativně pracný úkol (zejména bez použití počítače). Zatímco příjemce, znalý klíče b , opět pouze pomocí operace $+$ binárně „přičte“ $b = 11011$ ke každému znaku a ihned obdrží slovo KNIHA (ovšem v binárním kódu).

Čtenář si domyslí, jak snadno lze uvedenou metodu šifrování zdokonalit. Například tím, že by se pro zakódování písmen výchozí abecedy použily ne pěticí ale např. desetičlenné posloupnosti číslic 0 a 1. Pak by neznalá osoba musela k prolomení použít nikoliv 32, ale 1 024 možností. Samozřejmě, že by bylo možno využít daleko důmyslnější modifikace, např. kdybychom místo posloupnosti 0 a 1 používali prvky některého, např. tzv. *ortomodulárního svazu*. To však vyžaduje podstatně hlubší znalosti současné algebry.

60. ročník matematické olympiády

Úlohy I. kola

KATEGORIE Z6

Z6–I–1

Když Bořek natíral vrata garáže, přetřel omylem i stupnici nástěnného venkovního teploměru. Trubička se rtutí však zůstala nepoškozená, a tak Bořek původní stupnici přelepil páskem vlastní výroby. Na něj pečlivě vyrýsoval dílky, všechny byly stejně velké a označené čísly. Jeho dílek měl však jinou velikost než původní dílek, který představoval jeden stupeň Celsia, a i nulu Bořek umístil jinam, než kde bylo 0°C . Takto začal Bořek měřit teplotu ve vlastních jednotkách: bořcích. Když by měl teploměr ukazovat teplotu 11°C , ukazoval 2 bořky. Když by měl ukazovat -4°C , ukazoval -8 bořků. Jaká je teplota ve $^{\circ}\text{C}$, vidí-li Bořek na svém teploměru teplotu -2 bořky?

L. Šimůnek

Z6–I–2

Začínající písničkář prodával vždy po vystoupení CD se svou hudbou. Ve čtvrtek prodal osm stejných CD. Den nato už nabízel i své nové CD a lidé si tak mohli koupit to samé jako ve čtvrtek nebo nové. V sobotu chtěli všichni posluchači nové CD a písničkář jich prodal ten den šest. V jednotlivých dnech utržil 590 Kč, 720 Kč a 840 Kč, neprozradíme však, která částka patří ke kterému dni.

- Kolik stálo starší CD?
- Kolik nových CD prodal v pátek?

L. Šimůnek

Z6–I–3

Vojta napsal číslo 2010 stokrát bez mezer za sebou. Kolik čtyřmístných a kolik pětímístných souměrných čísel bylo ukryto v tomto zápise? (Souměrné číslo je takové číslo, které je stejné, je-li čteno zepředu i zezadu, např. 39193.)

L. Hozová

Z6–I–4

Součin věků dědy Vendelína a jeho vnoučat je 2010. Součet věků všech vnoučat je 12 a žádná dvě vnoučata nemají stejný počet let. Kolik vnoučat má děda Vendelín?

L. Hozová

Z6–I–5

Na táboře se dva vedoucí se dvěma táborníky a psem potřebovali dostat přes řeku a k dispozici měli jen jednu loďku o nosnosti 65 kg. Naštěstí všichni (kromě psa) dokázali loďku přes řeku převézt. Každý vedoucí vážil přibližně 60 kg, každý táborník 30 kg a pes 12 kg. Jak si měli počínat? Kolikrát nejméně musela loďka překonat řeku?

M. Volfová

Z6–I–6

Karel obestavěl krabici s obdélníkovým dnem obrubou z krychliček. Použil právě 22 krychliček o hraně 1 dm, které stavěl těsně vedle sebe v jedné vrstvě. Mezi obrubou a stěnami krabice nebyla mezera a celá tato stavba měla obdélníkový půdorys. Jaké rozměry mohlo mít dno krabice?

M. Krejčová

KATEGORIE Z5**Z5–I–1**

Vítek má napsána dvě čísla, 541 a 293. Ze šesti použitých číslic má nejprve vyškrtnout dvě tak, aby součet dvou takto získaných čísel byl největší možný. Poté má z původních šesti číslic vyškrtnout dvě tak, aby rozdíl dvou takto získaných čísel byl nejmenší možný (odečítá menší číslo od většího). Které číslice má vyškrtnout?

M. Petrová

Z5–I–2

V Trpasličím království měří vzdálenosti v pohádkových mílech (pm), v pohádkových sázích (ps) a v pohádkových loktech (pl). Na vstupní bráně do Trpasličího království je následující tabulka pro převody mezi jejich jednotkami a našimi:

- $1 \text{ pm} = 3,85 \text{ m}$,
- $1 \text{ ps} = 105 \text{ cm}$,
- $1 \text{ pl} = 250 \text{ mm}$.

Král Trpaslík I. nechal přeměřit vzdálenost od zámecké brány k pohádkovému jezírku. Tři pozvaní zeměměřiči dospěli k těmto výsledkům: první uváděl 4 pm 4 ps 18 pl, druhý 3 pm 2 ps 43 pl a třetí 6 pm 1 ps 1 pl. Jeden z nich se však zmýlil. Jaká je vzdálenost v metrech od zámecké brány k pohádkovému jezírku? O kolik centimetrů se spletl nepřesný zeměměřič?

M. Petrová

Z5–I–3

Čtyři kamarádi Adam, Mojmír a dvojčata Petr a Pavel získali v hodinách matematiky celkem 52 smajlíků, každý alespoň 1. Přitom dvojčata dohromady mají 33, ale nejúspěšnější byl Mojmír. Kolik jich získal Adam?

M. Volfová

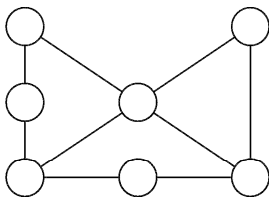
Z5–I–4

Pan Tik a pan Tak prodávali budíky v prodejnách Před Rohem a Za Rohem. Pan Tik tvrdil, že Před Rohem prodali o 30 budíků více než Za Rohem, zatímco pan Tak tvrdil, že Před Rohem prodali třikrát více budíků než Za Rohem. Nakonec se ukázalo, že Tik i Tak měli pravdu. Kolik budíků prodali v obou prodejnách celkem?

L. Hozová

Z5–I–5

Do kroužků na obrázku doplňte čísla 1, 2, 3, 4, 5, 6 a 7 tak, aby součet čísel na každé vyznačené linii byl stejný. Žádné číslo přitom nesmí být použito víckrát.



M. Smítková

Z5–I–6

Paní Široká čekala večer hosty. Nejprve pro ně připravila 25 chlebičků. Pak spočítala, že by si každý host mohl vzít dva, tři by se však na všechny nedostaly. Řekla si, že kdyby vyrobila ještě 10 chlebičků, mohl by si každý host vzít tři, ale čtyři ne každý. To jí přišlo stále málo. Nakonec uchystala dohromady 52 chlebičků. Každý host by si tedy mohl vzít čtyři chlebičky,

ale pět by se na všechny nedostalo. Kolik hostů paní Široká očekávala? Ona sama drží dietu a večer nikdy nejí.

L. Šimůnek

Zajímavé matematické úlohy

Otevíráme již 18. ročník naší pravidelné řešitelské rubriky „Zajímavé matematické úlohy“. V každém ročníku bylo dosud publikováno vždy deset úloh. V předchozích číslech našeho časopisu tak najdete již 170 zajímavých úloh. Upozorňujeme současně naše čtenáře, že kompletní soubor prvních 130 úloh této rubriky (včetně jejich úplných řešení) je možno nalézt v publikaci nakladatelství Prometheus „Sbírka netradičních matematických úloh“ autorů J. Švrčka a P. Calábka.

Řešení první dvojice úloh nového ročníku můžete zaslat nejpozději do 20. 10. 2010 na adresu: Redakce časopisu MFI, tř. 17. listopadu 12, 771 46 Olomouc. Jejich řešení lze zaslat také elektronickou cestou (pouze však v $\text{\TeX}$ ovských verzích, příp. v MS Wordu) na emailovou adresu: *mfi@upol.cz*. Zajímavá a originální řešení úloh rádi uveřejníme.

Úloha 171

Nechť a, b, c, d jsou kladná reálná čísla vyhovující podmínkám $abcd = 1$,

$$\frac{a}{b} + \frac{b}{c} + \frac{c}{d} + \frac{d}{a} < a + b + c + d.$$

- a) Ukažte, že taková čísla a, b, c, d existují.
- b) Dokažte, že pro ně platí nerovnost

$$\frac{b}{a} + \frac{c}{b} + \frac{d}{c} + \frac{a}{d} > a + b + c + d.$$

Pavel Novotný (Žilina)

Úloha 172

Je dán trojúhelník ABC , v němž $|AC| \neq |BC|$, a čtverce $ACDE$, $BCGF$ vně sestrojené nad jeho stranami. Dokažte, že kružnice s průměry DG a AB se protínají na přímce EF .

Pavel Leischner