

LETNÍ ŠKOLA
MATEMATIKY A FYZIKY 2021
SBORNÍK PŘÍSPĚVKŮ

Jazyková korektura nebyla provedena,
za jazykovou správnost odpovídají autoři příspěvků.

Rozmnožování a šíření jen se svolením Vydavatelského servisu.

1. vydání

© Magdalena Krátká, Jiří Příbyl, Jana Kasperová, 2022

ISBN 978-80-86843-74-2 (on-line)

ISBN 978-80-86843-75-9 (CD-ROM)

OBSAH

Jiří Cihlář	
Didaktická kreativita	5
Šárka Gergelitsová	
Několik pohledů na GeoGebu	29
Barbora Mikulecká, Vojtěch Hanák	
Barvy kolem nás	45
Luboš Pick	
O využití iracionality při hledání sedmého nebe	67
Zdeněk Polák	
Laboratorní a frontální práce s polovodiči	77
Jana Šestáková	
Pokusy z projektu Žiju fyzikou	89
Tomáš Urban	
Šifrování RSA	95
Tomáš Vlasák	
Geometrická konstrukce lomeného paprsku	121
Zuzana Vlasáková	
Zákony ideálního plynu	125

DIDAKTICKÁ KREATIVITA

Jiří Cihlář

ABSTRAKT

Převažující náplní hodin matematiky je řešení úloh. Kreativní přístup učitele k úlohám a jejich řešení je důležitou složkou jeho působení. Na několika vhodných úlohách různých typů jsou ukázány variantní způsoby řešení úloh i zobecňování a zjednodušování úloh.

KLÍČOVÁ SLOVA: řešení úloh, kreativita.

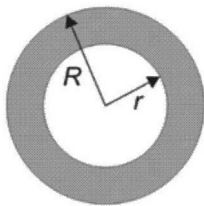
ÚVOD

Správný výběr úloh a problémů, které učitelé v rámci výuky matematiky žákům předkládají, je velmi důležitý pro celkovou úspěšnost výuky. Výběr úloh by měl být pestrý, měl by obsahovat kromě standardních procvičovacích úloh i zajímavé a inspirativní úlohy, které zvyšují motivaci žáků. U takovýchto úloh je možné porovnávat různé způsoby řešení, dále je rozvíjet jejich zobecňováním, formulovat další navazující úlohy a používat netradiční strategie řešení. Vhodné jsou i takové úlohy, při jejichž řešení se užívají různé partie matematické látky, včetně efektivního využívání výpočetní techniky, neměly by chybět ani úlohy ukazující důležitost matematiky pro praxi.

PŘEHLED ÚLOH

Úloha 1. Jednostranná lepicí páska délky $d = 50$ m je navinuta na papírový váleček o poloměru $r = 4,1$ cm tak, že vzdálenost jejího posledního „závitu“ od osy válečku je $R = 6,9$ cm.

Vypočítejte tloušťku t této pásky.



Obr. 1: Lepicí páska

Řešení. Tuto zcela reálnou úlohu (taková páska se opravdu prodává) je možné řešit dvěma podstatně odlišnými způsoby, řekněme jim třeba aritmetický, resp. geometrický.

Při prvním aritmetickém způsobu řešení budeme předpokládat, že délka pásky je rovna součtu délek soustředných kružnic s poloměry, které se zvětšují od hodnoty r , až k hodnotě R . Poloměry přitom tvoří aritmetickou posloupnost, kde je diferencí tloušťka pásky t . Podle vzorce pro součet několika prvních členů aritmetické posloupnosti získáme

$$d = \frac{n}{2} \cdot (2\pi r + 2\pi R),$$

odkud můžeme vypočítat počet závitů pásky

$$n = \frac{d}{\pi \cdot (r + R)}.$$

Tloušťka pásky je pak dána vzorcem $t = \frac{R - r}{n} = \frac{\pi}{d} \cdot (R^2 - r^2)$.

Při druhém geometrickém způsobu řešení využijeme pouze změnu tvaru tělesa, při které se nemění jeho objem. Označíme si ještě neznámou šířku pásky písmenem s .

Původně rozvinutá páska má tvar nízkého hranolu s výškou t , a s podstavou délky d a šířkou s . Jeho objem je tedy $V = d \cdot s \cdot t$.

Navinutá páska tvoří těleso, jehož objem můžeme vypočítat jako rozdíl objemů dvou válců se společnou osou a se společnou výškou s . Od objemu válce s poloměrem podstavy R odečteme objem válce s poloměrem r , tedy $V = \pi R^2 s - \pi r^2 s$.

Objem je v obou případech stejný, tedy

$$\begin{aligned} d \cdot s \cdot t &= \pi R^2 s - \pi r^2 s, \\ d \cdot t &= \pi (R^2 - r^2), \end{aligned}$$

a závěrem pak stejně jako v prvním případě

$$t = \frac{\pi}{d} \cdot (R^2 - r^2).$$

Dosazením zadaných hodnot vypočítáme skutečnou tloušťku pásky (počítáme v milimetrech):

$$t = \frac{\pi}{50\,000} \cdot (69^2 - 41^2) \approx 0,193\,522\,11$$

Tloušťka pásky je asi 0,19 mm.

Úloha 2. Zjistěte co nejvíce informací o prvočíslech, která mohou být zapsána pomocí několika navzájem shodných číslic, resp. pomocí n navzájem různých číslic $1, 2, \dots, n$?

Řešení. Uvažujme nejprve o prvočíslech, která se dají zapsat pomocí několika navzájem shodných číslic. Představíme-li si nějaká taková čísla, například 77 777, resp. 555, je ihned patrné, že pokud bude opakuji se číslice různá od jedničky, žádné takové číslo nebude prvočíslem. V našich příkladech je zřejmé, že první číslo je dělitelné číslem 7, a druhé číslo je dělitelné číslem 5. Zbývají tedy jen čísla, která jsou zapsaná pouze pomocí jedniček.

Mezi těmito čísly již prvočísla nalezneme – například prvočíslo 11.

Další číslo 111 ale není prvočíslem, protože má ciferný součet 3, a je tedy i samo dělitelné třemi.

Další číslo 1 111 také není prvočíslem, protože můžeme psát

$$1\,111 = 1\,100 + 11 = 11 \cdot 100 + 11 = 11 \cdot 101.$$

Číslo 11 111 zapsané pěti jedničkami také není prvočíslem, protože platí, že $11\,111 = 47 \cdot 271$.

U čísla 111 111 můžeme postupovat podobně, jako u čísla zapsaného čtyřmi jedničkami:

$$111\,111 = 111\,000 + 111 = 111 \cdot (1\,000 + 1) = 111 \cdot 1\,001,$$

ani toto číslo tedy není prvočíslem. Takoveto úvahy se dají ale zobecnit.

Budeme-li mít číslo, které je zapsáno n jedničkami, přičemž číslo n bude složené (bude tedy třeba $n = x \cdot y$), můžeme n jedniček rozdělit do x skupin po y jedničkách, a dané číslo bude tedy dělitelné číslem zapsaným y jedničkami.

Teď již tedy víme, že kandidáty na prvočíselnost jsou jen čísla zapsaná prvočíselným počtem jedniček (ale pozor – neplatí, že když je počet jedniček prvočíslem, pak je dané číslo také prvočíslem – viz složená čísla 111, resp. 11 111).

Tabulka 1: Rozklady čísel zapsaných prvočíselným počtem jedniček na prvočísla

Počet jedniček	Číslo	Rozklad na prvočísla
2	11	je to prvočíslo
3	111	$3 \cdot 37$
5	11 111	$47 \cdot 271$
7	1 111 111	$239 \cdot 4\,649$
11	11 111 111 111	$21\,649 \cdot 513\,239$
13	1 111 111 111 111	$53 \cdot 79 \cdot 265\,371\,653$
17	11 111 111 111 111 111	$2\,071\,723 \cdot 5\,363\,222\,357$
19	1 111 111 111 111 111 111	je to prvočíslo
23	11 111 111 111 111 111 111 111	je to prvočíslo

Prvočísla jsou mezi těmito čísly zastoupena poměrně zřídka – viz tabulka 1. Výsledky můžeme získat třeba pomocí programu Geogebra.

Uvažujme dále o prvočíslech, která jsou zapsána pomocí číslic $1, 2, \dots, n$, přičemž každá číslice se v zápise vyskytuje právě jednou.

Když máme k dispozici pouze číslici jedna, nebudeme úspěšní, protože 1 není prvočíslo.

Když máme k dispozici jen dvě nejmenší číslice 1 a 2, také z nich nesestavíme prvočíslo, protože jak číslo 12, tak i číslo 21, jsou složená čísla.

Pomocí tří číslic 1, 2 a 3 můžeme zapsat $3! = 3 \cdot 2 \cdot 1 = 6$ čísel, ale žádné z nich nebude prvočíslem, protože všechna mají ciferný součet 6, a všechna jsou tedy dělitelná třemi.

Tuto úvahu můžeme aplikovat i na čísla sestavená z číslic 1, 2, 3, 4 a 5, protože ta mají všechna ciferný součet 15, a všechna jsou tedy dělitelná třemi.

Podobně platí, že čísla sestavená z číslic 1, 2, 3, 4, 5 a 6 mají všechna ciferný součet 21, čísla sestavená z číslic 1, 2, 3, 4, 5, 6, 7 a 8 mají všechna ciferný součet 36, a konečně čísla sestavená ze všech 9 číslic mají ciferný součet 45. Žádné z těchto čísel tedy nemůže být prvočíslem.

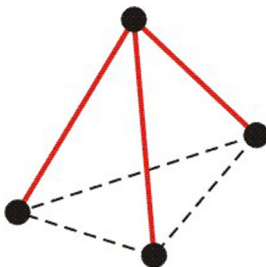
Zbývá nám tedy prozkoumat pouze dalších $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$ čísel zapsaných číslicemi 1, 2, 3 a 4, resp. $7! = 5\,040$ čísel, zapsaných sedmi nejmenšími číslicemi 1, 2, až 7.

V prvním případě, kdy máme k dispozici pouze číslice 1, 2, 3 a 4, můžeme naše vyšetřování ještě omezit pouze na lichá čísla, kterých je 12. Mezi těmito čísly můžeme pak nalézt právě čtyři prvočísla, a to: 1 423, 2 143, 2 341 a 4 231.

Také mezi 5 043 čísly zapsaných sedmi nejmenšími číslicemi nalezneme prvočísla, například číslo 1 532 647.

Úloha 3. V rovině je dána množina M šesti bodů. Žádné tři body z množiny M neleží na jedné přímce. Každé dva body množiny M jsou spojeny úsečkou, která je buď červená, anebo modrá. Dokažte, že platí: Z množiny M lze vybrat tři body, které určují jednobarevný trojúhelník (všechny strany trojúhelníka jsou červené nebo všechny strany jsou modré).

Řešení. Nejprve dokážeme, že když z jednoho bodu vycházejí tři úsečky stejné barvy, pak existuje jednobarevný trojúhelník. Necht' jsou tyto tři úsečky třeba červené (viz obrázek 2).



Obr. 2: Barvení grafu

Soustředíme se na tři čárkované úsečky v obrázku.

Je-li alespoň jedna z nich červená, pak existuje jednobarevný červený trojúhelník.

Není-li žádná z nich červená, pak jsou všechny čárkované úsečky modré, a pak také existuje jednobarevný, tentokrát modrý trojúhelník.

Kdyby byly tři úsečky vycházející z jednoho bodu modré, důkaz by byl obdobný.

Vyberme si nyní libovolný bod z množiny M , z něj pochopitelně vychází pět úseček. Uvažme všechny možnosti pro počty jejich barev (viz tabulka 2).

Tabulka 2: Možné počty úseček dané barvy vycházejících z libovolného bodu

červená	5	4	3	2	1	0
modrá	0	1	2	3	4	5

Je patrné, že ve všech případech vychází z tohoto bodu alespoň tři úsečky stejné barvy.

Tím je důkaz proveden.

Úloha 4. Plášť určitého kužele lze rozvinout do tvaru půlkruhu o poloměru $l = 3$ cm. Vypočítejte objem tohoto kužele.

Řešení. Abychom mohli vypočítat objem tohoto kužele, potřebujeme znát poloměr r jeho podstavy a jeho výšku v . Objem pak vypočítáme podle vzorce $V = \frac{1}{3} \cdot \pi r^2 v$.

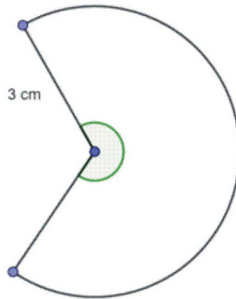
Poloměr podstavy zjistíme snadno, protože délka podstavné kružnice $2\pi r$ je vzhledem k rozvinutí rovna délce půlkružnice s poloměrem l . Platí tedy, že $2\pi r = \pi l$, odkud plyne, že $r = \frac{l}{2}$.

Neznámou výšku kužele pak zjistíme pomocí Pythagorovy věty: $v = \sqrt{l^2 - r^2}$. Závěrem pak získáme, že

$$V = \frac{1}{3} \cdot \pi r^2 v = \frac{1}{3} \cdot \pi \cdot \frac{l^2}{4} \cdot \sqrt{l^2 - \frac{l^2}{4}} = \frac{1}{3} \cdot \pi \cdot \frac{l^2}{4} \cdot \sqrt{\frac{3}{4}l^2} = \frac{\sqrt{3}}{24} \cdot \pi \cdot l^3.$$

Numericky: dosazením za l nám vyjde $V = \frac{\sqrt{3}}{24} \cdot \pi \cdot 3^3 = \frac{9 \cdot \sqrt{3}}{8} \cdot \pi \approx 6,1216 \text{ cm}^3$.

Tato úloha přímo volá po zobecnění, zformulujme tedy tuto úlohu (viz obrázek 3).



Obr. 3: Plášť kužele

Pláštěm kužele je kruhová výseč z kružnice o poloměru 3 cm se středovým úhlem $\alpha \in (0, 2\pi)$.

Vypočítejte objem kužele jako funkci proměnné α .

Čím se řešení zobecněné úlohy bude lišit od řešení původní úlohy? K výpočtu objemu se bude používat stejný vzorec, výška kužele se bude opět počítat pomocí Pythagorovy věty, jediný rozdíl bude v tom, že délka podstavné kružnice $2\pi r$ nebude délkou půlkružnice, ale délkou oblouku, který přísluší kruhové výseči se středovým úhlem α .

Délka oblouku výšece je přímo úměrná velikosti středového úhlu v obloukové míře, a proto platí: $\frac{2\pi l}{2\pi} = \frac{2\pi r}{\alpha}$, odkud vypočítáme, že $r = l \cdot \frac{\alpha}{2\pi}$. Pro přehlednost dalších výpočtů si ještě zavedme substituci $x = \frac{\alpha}{2\pi}$, nová proměnná $x \in (0, 1)$ tedy vyjadřuje poměr úhlu výšece k plnému úhlu.

Při tomto označení tedy platí, že $r = l \cdot x$.

Další výpočet probíhá již obdobně, jako u původní úlohy:

Výšku kužele zjistíme pomocí Pythagorovy věty: $v = \sqrt{l^2 - r^2}$, a závěrem (i po dosazení) máme

$$V = \frac{1}{3} \cdot \pi r^2 v = \frac{1}{3} \cdot \pi \cdot l^2 x^2 \cdot \sqrt{l^2 - l^2 x^2} = \frac{1}{3} \cdot \pi \cdot l^3 \cdot x^2 \sqrt{1 - x^2} = 9\pi \cdot x^2 \sqrt{1 - x^2}.$$

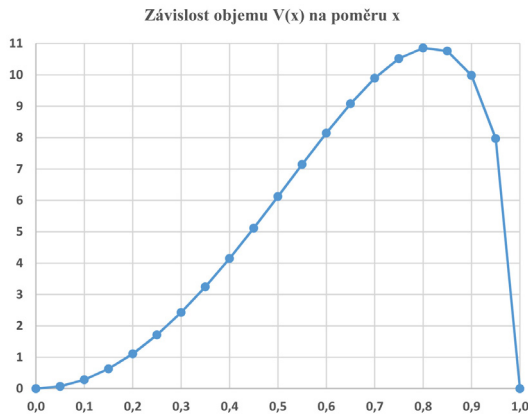
Průběh této funkce ukazují hodnoty z tabulky 3 a graf na obrázku 4.

Tabulka 3: Objem kužele

x	$V(x)$
0,00	0,000 0
0,05	0,070 6
0,10	0,281 3
0,15	0,629 0
0,20	1,108 1
0,25	1,711 0
0,30	2,427 5

x	$V(x)$
0,35	3,244 5
0,40	4,146 2
0,45	5,113 1
0,50	6,121 6
0,55	7,143 2
0,60	8,143 0
0,65	9,078 1

x	$V(x)$
0,70	9,894 0
0,75	10,519 7
0,80	10,857 3
0,85	10,761 2
0,90	9,982 8
0,95	7,967 9
1,00	0,000 0



Obr. 4: Objem kužele

Pohledem do tabulky zjistíme, že pro hodnotu $x = \frac{\alpha}{2\pi} = 0,5$ je velikost objemu $V = 6,1216 \text{ cm}^3$, což je ve shodě s řešením původní úlohy.

Také je dobře vidět, že pro velmi malé hodnoty α vzniká velmi úzký a relativně vysoký kužel s takřka nulovým objemem, a podobně pro velké hodnoty α , blízké hodnotě 2π , vzniká velmi široký a relativně nízký kužel, který má taktéž skoro nulový objem.

Přírozně vzniká otázka, pro jakou hodnotu úhlu α je objem kužele maximální.

Pro studenty, kteří znají základy diferenciálního počtu, je cesta snadná – stačí vyhledat vhodný nulový bod první derivace funkce $x^2\sqrt{1-x^2}$, která se ve vzorci pro objem vyskytuje. Pro žáky by bylo ale užitečné, aby se seznámili s i metodou postupných aproximací, která je pomocí programu v Excelu přístupná nejenom středoškolákům, ale i žákům 2. stupně základních škol.

Nejprve tedy využijme derivace:

$$\left(x^2 \cdot \sqrt{1-x^2}\right)' = 2x\sqrt{1-x^2} + x^2 \cdot \frac{1}{2}(1-x^2)^{-\frac{1}{2}} \cdot (-2x).$$

Po úpravách pravé strany obdržíme, že

$$\left(x^2 \cdot \sqrt{1-x^2}\right)' = \frac{x}{\sqrt{1-x^2}} \cdot (2-3x^2).$$

Když pak řešíme rovnici $2-3x^2 = 0$, získáme, že $x^2 = \frac{2}{3}$, resp.
 $x = \sqrt{\frac{2}{3}} \approx 0,8165$.

Dosazením za x^2 do vzorce pro objem dostaneme jeho maximální hodnotu:

$$V_{\max} = 9\pi \cdot \frac{2}{3} \cdot \sqrt{\frac{1}{3}} = 2\pi\sqrt{3} \approx 10,8828 \text{ cm}^3.$$

Příslušný středový úhel α výšece získáme z podmínky $x = \sqrt{\frac{2}{3}} = \frac{\alpha}{2\pi}$, její úpravou máme

$$\alpha = 2\pi \cdot \sqrt{\frac{2}{3}} \approx 5,1302 \text{ rad} \approx 293,94^\circ.$$

A nyní hledejme maximální hodnotu objemu v Excelu pomocí metody postupných aproximací.

V tabulce 3 si můžeme povšimnout, že maximum nabývá objem pro hodnotu x někde mezi hodnotami 0,75 a 0,85. Výpočet objemu ponecháme stejný,

ale budeme jej počítat jen pro zjemnělé hodnoty 0,75, 0,76, 0,77, až 0,85. V této podrobnější tabulce pak nalezneme ještě užší obor hodnot pro x , atd. Technický postup výpočtu je jednoduchý, pouze kopírujeme první řádky tabulky, nastavujeme počáteční hodnoty, a roztahujeme bloky buněk dolů. Postup je vidět v tabulce 4.

Tabulka 4: Postupné aproximace maximálního objemu

x	$V(x)$	x	$V(x)$	x	$V(x)$
0,75	10,519 7	0,812	10,880 8	0,815 2	10,882 63
0,76	10,614 1	0,814	10,882 2	0,815 4	10,882 68
0,77	10,696 1	0,816	10,882 8	0,815 6	10,882 72
0,78	10,764 7	0,818	10,882 6	0,815 8	10,882 75
0,79	10,818 9	0,820	10,881 6	0,816 0	10,882 77
0,80	10,857 3	0,822	10,879 8	0,816 2	10,882 79
0,81	10,878 7	0,824	10,877 2	0,816 4	10,882 80
0,82	10,881 6	0,826	10,873 7	0,816 6	10,882 80
0,83	10,864 2	0,828	10,869 4	0,816 8	10,882 79
0,84	10,824 8	0,830	10,864 2	0,817 0	10,882 77
0,85	10,761 2	0,832	10,858 2	0,817 2	10,882 75

Z pravé části tabulky je vidět, že můžeme i touto metodou rychle získat uspokojivě přesné hodnoty.

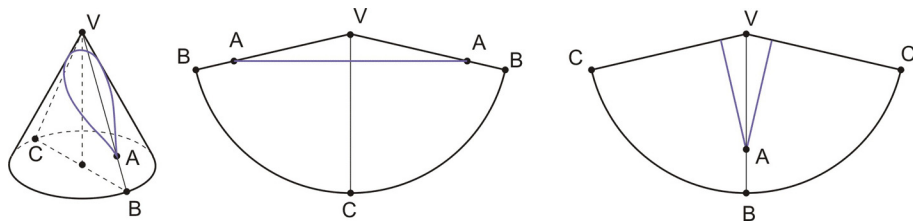
Na úlohu o rozvinutém plášti kužele může navázat i hezká úloha o chytré a přitom líné mouše, která má toto znění:

Pláštěm kužele je kruhová výseč z kružnice o poloměru 3 cm se středovým úhlem $\alpha \in (0, \pi)$. Na kuželi je v bodu A moucha, její vzdálenost od vrcholu je d , $0 < d < 3$. Nalezněte délku nejkratší dráhy, po které se moucha musí pohybovat, aby oblezla celý kužel kolem dokola, a vrátila se do zpět do výchozího bodu A .

Tvar i konstrukce nejkratší dráhy je na obrázku 5. O správnosti konstrukce podle prostředního obrázku nepochybujeme – úsečka je jistě nejkratší spojnicí dvou bodů. Konstrukce na obrázku vpravo využívá toho, že dráha mouchy je na protější úsečce AC kolmá. Obě konstrukce vedou ke stejné délce dráhy, což plyne ze shodnosti trojúhelníků s přeponou d v obou obrázcích.

A jaká je tedy délka l této nejkratší dráhy? Z obrázku vpravo plyne, že $\frac{l}{2} = d \cdot \sin \frac{\alpha}{2}$, a tedy

$$l = 2d \cdot \sin \frac{\alpha}{2}.$$



Obr. 5: Nejkratší dráha mouchy a její konstrukce

Je zajímavé, že jsme schopni vypočítat délku této křivky, i když to je prostorová křivka. Že křivka neleží v rovině plyne z toho, že všechny křivky, které jsou průnikem kuželové plochy s rovinou, jsou kuželosečky. V našem případě by se tedy muselo jednat o elipsu, ale elipsa nemá žádný hrot, jako naše křivka v bodě A.

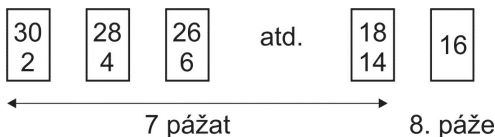
Úloha 5. Jednou si král zavolal všechna svá pážata a postavil je do řady. Prvnímu pážeti dal určitý počet dukátů, druhému dal o dva dukáty méně, třetímu opět o dva dukáty méně, a tak dále. Když došel k poslednímu pážeti, dal mu příslušný počet dukátů, otočil se a obdobným způsobem postupoval na začátek řady (tj. předposlednímu pážeti dal o dva dukáty méně než před chvílí poslednímu, atd.) Na první páže v tomto kole vyšly dva dukáty. Poté jedno z pážat zjistilo, že má 32 dukátů.

Kolik mohl mít král pážat a kolik celkem jim mohl rozdat dukátů?

Řešení. Aby mělo zadání úlohy smysl, budeme požadovat, aby počet pážat byl alespoň 2. Žáci by si nejprve měli povšimnout toho, že všechna pážata kromě posledního v řadě dostanou stejný počet dukátů, a že tento počet dukátů je dvakrát větší, než počet dukátů, který dostalo poslední páže. To je zřejmé z této úvahy: dostalo-li poslední páže například x dukátů, pak předposlední páže dostalo celkem $(x + 2) + (x - 2)$ dukátů, páže před předposledním dostalo $(x + 4) + (x - 4)$ dukátů, atd.

Pak již můžeme zpětným postupem nalézt pomocí schematických nákresů dvě řešení úlohy:

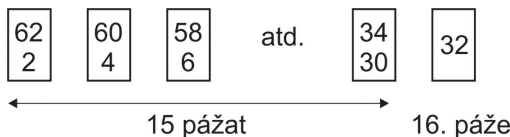
- 32 dukátů má první páže (a tedy i všechna další pážata kromě posledního)



Obr. 6: První řešení úlohy 5

Král má 8 pážat a rozdal celkem $7 \cdot 32 + 16 = 240$ dukátů.

- 32 dukátů má poslední páže



Obr. 7: Druhé řešení úlohy 5

Král má 16 pážat a rozdál celkem $15 \cdot 64 + 32 = 992$ dukátů.

Jak můžeme tuto úlohu zobecnit? Pomůže univerzální metoda: nahrazení konstant proměnnými. Pak se ale úloha stane úlohou s parametry, a bude tedy třeba provést její diskusi.

Neznámý počet pážat označme p , neznámý celkový počet dukátů, které král rozdál, označme d , a další dvě konstanty úlohy označme takto (jsou to opět přirozená čísla):

- symbolem r označme rozdíl mezi počty darovaných dukátů u dvou sousedních pážat (a zároveň počet dukátů, které dostalo první páže v druhém kole),
- a symbolem n označme počet dukátů, který dostalo některé z pážat.

Máme nalézt neznámá čísla p a d , a samozřejmě provést diskusi pro parametry r a n , tj. stanovit takové podmínky, kdy zobecněná úloha má opět dvě řešení, resp. kdy má jen jedno řešení, resp. nemá žádné řešení. Opět budeme předpokládat, že král má alespoň dvě pážata.

Stejně jako v původní úloze zjistíme, že poslední páže dostalo $p \cdot r$ dukátů, a první páže (stejně tak jako všechna další pážata až k předposlednímu) dostalo $2 \cdot p \cdot r$ dukátů. Z toho plyne, že celkový počet dukátů je: $d = (p - 1) \cdot 2pr + pr = pr \cdot (2p - 1)$.

Podle podmínek úlohy má n dukátů buď první páže, a platí $n = 2 \cdot p \cdot r$, anebo má n dukátů poslední páže, a platí $n = p \cdot r$.

V prvním případě platí $p = \frac{n}{2r} \geq 2$, tedy $2r$ musí být dělitelem čísla n , a přitom $n \geq 4r$.

Počet dukátů je pak $d = \frac{n}{2r} \cdot r \cdot \left(2 \frac{n}{2r} - 1\right) = \frac{n}{2} \cdot \left(\frac{n}{r} - 1\right)$.

V druhém případě platí $p = \frac{n}{r} \geq 2$, tedy r musí být dělitelem čísla n , a přitom $n \geq 2r$.

Počet dukátů je pak $d = \frac{n}{r} \cdot r \cdot \left(2 \frac{n}{r} - 1\right) = n \cdot \left(2 \frac{n}{r} - 1\right)$.

Můžeme si povšimnout, že platí-li podmínky z prvního případu, pak platí i podmínky z druhého případu, a úloha má dvě řešení (například pro hodnoty

$r = 2$ a $n = 32$ z původní úlohy). Když platí pouze podmínky z druhého případu, pak má úloha jedno řešení (třeba pro hodnoty $r = 2$ a $n = 30$). Když neplatí žádná z uvedených dvou podmínek, pak úloha nemá řešení.

Úloha 6. Dominové kameny mají na každém ze svých dvou polí nejvýše šest teček. Žádné dva kameny nejsou stejné, každé neuspořádané dvojici z čísel 0 až 6 odpovídá jeden kámen.

- a) Kolik je dominových kamenů celkem?
- b) Kolik teček je na všech kamenech dohromady?

Řešení. Tato úloha je uváděna zejména proto, že je ji možno řešit mnoha různými způsoby.

Bez nápadu ji můžeme řešit „jen hrubou silou“, tedy systematickým výpisem všech možností, zjištěním celkového počtu teček pro každou možnost, a konečně sečtením všech teček pro všechny možnosti.

Vypíšeme tedy nejprve všechny možnosti: 00, 01, 02, ..., 06, 11, 12, ..., 16, 22, 23, ...

Pak ke každé možnosti spočítáme počet teček: 0, 1, 2, ..., 6, 2, 3, ..., 7, 4, 5, ...

A nakonec sečtením vypočítáme celkový počet teček.

I když obdržíme správné řešení, matematiku bychom ale takovýmto postupem spíše uráželi.

Pro první část úlohy o počtu všech dominových kamenů můžeme použít i kombinatorické vzorce pro k -členné kombinace z n prvků s opakováním či bez opakování:

$$K_{\text{op}}(k, n) = \binom{n+k-1}{k}, \text{ resp. } K(k, n) = \binom{n}{k}.$$

Podle prvního vzorce můžeme vypočítat počet všech kamenů: $K_{\text{op}}(2, 7) = \binom{8}{2} = 28$.

Podle druhého vzorce můžeme nejprve vypočítat počet všech kamenů, na nichž jsou v obou polích různé počty teček: $K(2, 7) = \binom{7}{2} = 21$. Následně pak můžeme přičíst 7 kamenů, na nichž jsou v obou polích stejné počty teček, a získáme tak tentýž výsledek, jako v prvním případě. Tato dílčí úloha může být vhodná, pokud chceme procvičit odlišování kombinatorických objektů s opakováním a bez opakování.

Další postupy řešení můžeme získat, pokud si všechny možnosti uspořádáme do tabulky 5.

Tabulka 5: Součty teček na dominových kamenech

	0	1	2	3	4	5	6	Součet
0	0	1	2	3	4	5	6	21
1	1	2	3	4	5	6	7	28
2	2	3	4	5	6	7	8	35
3	3	4	5	6	7	8	9	42
4	4	5	6	7	8	9	10	49
5	5	6	7	8	9	10	11	56
6	6	7	8	9	10	11	12	63

Tabulku bychom pochopitelně nemuseli vyplňovat celou, stačilo by vyplnit jen modře označená pole, ale ukáže se, že je vhodné vyplnit symetricky i bílá pole pod diagonálou.

Pak je zřejmé, že počet kamenů (počet všech modrých polí) můžeme získat jako součet

$$1 + 2 + 3 + 4 + 5 + 6 + 7 = \frac{1}{2} \cdot 7 \cdot 8 = 28.$$

Hodnotu součtu můžeme počítat podle vzorce pro součet několika prvních členů aritmetické posloupnosti. Ale i žáci, kteří ještě neprobírali látku o posloupnostech, ji mohou také snadno získat pomocí „postupu malého Gausse“: pod součet 1 až 7 si napíšou tento součet ještě jednou, ale v obráceném pořadí, tedy od 7 až do 1. Pak si povšimnou, že ve všech dvojicích čísel nad sebou je stejný součet 8, tedy dvojnásobek součtu má tedy hodnotu $8 \cdot 7$, a součet samotný je roven 28.

Pro počet teček na kamenech (součet čísel v modrých polích) můžeme volit různé postupy, ale snad nejlepší bude následující postup, kde budeme využívat celou vyplněnou tabulku.

Pro obě naše úlohy (počet kamenů, resp. počet teček) můžeme vzhledem k symetrii tabulky používat totéž ideové schéma z následující „formule“:

$$\text{modrá pole tabulky} = (\text{celá tabulka} - \text{diagonála}) : 2 + \text{diagonála}.$$

Pro počet kamenů, který byl již dříve dvakrát vypočítán, dostaneme tímto způsobem opět

$$(7 \cdot 7 - 7) : 2 + 7 = 42 : 2 + 7 = 21 + 7 = 28.$$

Pro počet teček si nejprve musíme vypočítat součty teček v celé tabulce a součet

teček na diagonále. Pro celou tabulku dostaneme

$$21 + 28 + 35 + 42 + 49 + 56 + 63 = \frac{1}{2} \cdot 7 \cdot (21 + 63) = \frac{1}{2} \cdot 7 \cdot 84 = 294.$$

Pro diagonálu dostaneme

$$0 + 2 + 4 + 6 + 8 + 10 + 12 = \frac{1}{2} \cdot 7 \cdot (0 + 12) = \frac{1}{2} \cdot 7 \cdot 12 = 42.$$

S použitím ideového schématu pak vypočítáme počet teček v modrých polích (na všech kamenech):

$$(294 - 42) : 2 + 42 = 252 : 2 + 42 = 126 + 42 = 168.$$

Úloha 7. Ze šedých a bílých čtvercových dlaždic se postupně vytvářejí obdélníkové obrazce.

První obrazec je složen ze dvou šedých dlaždic.

Druhý obrazec vznikne z prvního tak, že zleva a shora přidají bílé dlaždice.

Třetí obrazec vznikne z druhého tak, že zleva a shora přidají šedé dlaždice.

Čtvrtý obrazec vznikne z třetího tak, že zleva a shora přidají bílé dlaždice.

A tak dále (viz obrázek 8).



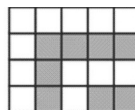
1. Obrazec



2. Obrazec



3. Obrazec



4. Obrazec

Atd.

Obr. 8: Vývoj obrazců v úloze 7

Vypočítejte, kolik šedých a kolik bílých dlaždic je v n -tém obrazci.

Řešení. Nejprve si uvědomíme, kolik dlaždic (bez ohledu na jejich barvu) je v n -tém obrazci. Protože je to obdélník, jejich počet bude $n \cdot (n + 1)$. Dále si vypočteme, kolik dlaždic musíme přidat, abychom z n -tého obrazce vytvořili následující obrazec s pořadovým číslem $(n + 1)$. Bude to rozdíl

$$(n + 1) \cdot (n + 2) - n \cdot (n + 1) = (n + 1) \cdot (n + 2 - n) = 2 \cdot (n + 1).$$

Při přechodu od 1. obrazce ke 2. obrazci tedy přibudou $2 \cdot (1 + 1) = 4$ bílé dlaždice, při přechodu od 2. obrazce ke 3. obrazci přibude $2 \cdot (2 + 1) = 6$ šedých dlaždic. Při přechodu od 3. obrazce ke 4. obrazci přibude $2 \cdot (3 + 1) = 8$ tentokrát opět bílých dlaždic, atd.

Tyto přírůstky počtů dlaždic tvoří tedy posloupnost sudých čísel čtyřkou počínaje. Pokud přecházíme od lichého čísla obrazce k následujícímu sudému číslu, přidává se příslušný počet bílých dlaždic (a počet šedých dlaždic se nemění), a naopak, pokud přecházíme od sudého k následujícímu lichému číslu, zvětšuje se počet šedých dlaždic (a počet bílých dlaždic se nemění).

Pomocí těchto faktů můžeme postupně vypočítat počty dlaždic v prvních deseti obrazcích, výsledky jsou uvedeny v tabulce 6. Přírůstky, které jsou dány vzorcem $2 \cdot (n + 1)$, jsou v tabulce označeny modrými šipkami.

Tabulka 6: Počty šedých a bílých dlaždic v prvních deseti obrazcích

Číslo obrazce n	Počet šedých dlaždic s_n	Počet bílých dlaždic b_n	Celkový počet dlaždic
1	2	0	2
2	2	4	6
3	8	4	12
4	8	12	20
5	18	12	30
6	18	24	42
7	32	24	56
8	32	40	72
9	50	40	90
10	50	60	110

Tímto rekurentním postupem bychom principiálně mohli vypočítat počty šedých i bílých dlaždic pro libovolně velká n , ale bylo by to velmi nepohodlné, protože k těmto hodnotám bychom se museli postupně propracovávat dlouhými výpočty, kdy ze znalosti předchozích hodnot bychom mohli vypočítávat jen hodnoty nejbližší následující. Přesto jsou tyto výsledky cenné, zapišme je tedy rovnicemi:

$$s_1 = 2$$

$$b_1 = 0$$

pro každé $n > 1$ sudé platí, že $s_{n+1} = s_n + 2 \cdot (n + 1)$ $b_{n+1} = b_{n-1}$

pro každé $n > 1$ liché platí, že $s_{n+1} = s_n$ $b_{n+1} = b_n + 2 \cdot (n + 1)$

A nyní se budeme snažit nalézt explicitní vyjádření pro obě posloupnosti, tedy odvodit vzorce, pomocí nichž budeme moci počítat hodnoty jejich členů přímo, pouze dosazením za n .

Pomůžou nám výpočty, které provedeme v následující tabulce 7.

První tři sloupce jsou převzaty z předcházející tabulky 6. Ve čtvrtém sloupci je aritmetický průměr Φ z počtů šedých a bílých dlaždic, hodnoty v tomto sloupci jsou pochopitelně poloviční vůči hodnotám z posledního sloupce tabulky 6. Vezmeme-li v úvahu výše odvozené vyjádření pro součet $s_n + b_n$, pak nás nepřekvapí, že hodnoty Φ jsou tzv. trojúhelníková čísla, která nalezneme také v druhé diagonále Pascalova trojúhelníku.

Zajímavé výsledky ale přinášejí hodnoty v posledních dvou sloupcích tabulky. Jsou to odchylky počtů s_n a b_n od jejich aritmetického průměru Φ . Je zřejmé, že součet obou odchylek v jednom řádku musí být roven nule – to vyplývá z definice průměru. Co nám ale při našem řešení může pomoci je to, že absolutní hodnoty odchylek jsou stejné pro $n = 1$ a $n = 2$, stejně tak jako pro následující dvojici čísel n (3 a 4), stejně tak jako pro následující dvojici 5 a 6, atd. Navíc je vidět, že tato absolutní hodnota je rovna pro větší (sudá) čísla z dvojice výrazu $\frac{n}{2}$.

Pro menší (lichá) čísla z dvojice není zlomek $\frac{n}{2}$ celým číslem, ale správnou absolutní hodnotu můžeme získat zaokrouhlením čísla $\frac{n}{2}$ na nejbližší vyšší celé číslo. Dále tedy použijeme symbol $[a]$, který označuje celé číslo, které je z intervalu $\langle a; a + 1 \rangle$, a říká se mu horní celá část čísla a . Střídání znamének pak ve vzorcích zrealizujeme pomocí výrazu $(-1)^n$, který nabývá střídavě hodnot $(+1)$ a (-1) .

Tabulka 7: Další výpočty potřebné k nalezení explicitních vzorců

n	s_n	b_n	$\Phi = \frac{1}{2} \cdot (s_n + b_n)$	$\Delta_n^s = s_n - \Phi$	$\Delta_n^b = b_n - \Phi$
1	2	0	1	+1	-1
2	2	4	3	-1	+1
3	8	4	6	+2	-2
4	8	12	10	-2	+2
5	18	12	15	+3	-3
6	18	24	21	-3	+3
7	32	24	28	+4	-4
8	32	40	36	-4	+4
9	50	40	45	+5	-5
10	50	60	55	-5	+5

Po těchto úvahách můžeme závěrem odvodit hledané vzorce:

$$\begin{aligned} s_n &= \Phi + \Delta_n^s = \frac{1}{2} \cdot (s_n + b_n) + \Delta_n^s = \frac{1}{2} \cdot n \cdot (n+1) - (-1)^n \cdot \left\lceil \frac{n}{2} \right\rceil \\ b_n &= \Phi + \Delta_n^b = \frac{1}{2} \cdot (s_n + b_n) + \Delta_n^b = \frac{1}{2} \cdot n \cdot (n+1) + (-1)^n \cdot \left\lceil \frac{n}{2} \right\rceil \end{aligned}$$

V tuto chvíli by se mohlo zdát, že řešení naší úlohy je ukončeno, ale to by nebylo korektní. Proč? Vyjádření diferencí z posledních dvou sloupců tabulky 7 jsme totiž odhadli jen intuitivně, a nemáme tedy jistotu, že platí opravdu pro všechna přirozená n . Je tedy třeba oba vzorce pro počty šedých a bílých dlaždic v n -tém obrazci dokázat matematickou indukcí. Budeme se přitom opírat o rekurentní předpisy pro obě posloupnosti, které byly dokázány korektně.

Dokažme tedy matematickou indukcí, že platí $s_n = \frac{1}{2} \cdot n(n+1) - (-1)^n \cdot \left\lceil \frac{n}{2} \right\rceil$.

V prvním kroku musíme dokázat, že tento vzorec je správný pro $n = 1$. Dosadíme tedy tuto hodnotu, a získáme: $s_n = \frac{1}{2} \cdot 1 \cdot 2 - (-1)^1 \cdot \left\lceil \frac{1}{2} \right\rceil = 1 + 1 = 2$. Pro $n = 1$ tedy tvrzení platí.

V druhém kroku musíme dokázat, že pro všechna n přirozená platí implikace: jestliže $s_n = \frac{1}{2} \cdot n \cdot (n+1) - (-1)^n \cdot \left\lceil \frac{n}{2} \right\rceil$, pak $s_{n+1} = \frac{1}{2} \cdot (n+1) \cdot (n+2) - (-1)^{n+1} \cdot \left\lceil \frac{n+1}{2} \right\rceil$.

Důkaz rozdělíme na dva případy podle parity čísla n , implikaci budeme dokazovat zvlášť pro n lichá a pro n sudá.

Nechť je tedy nejprve n liché číslo větší než 1. Pak pomocí rekurentní formule a indukčního předpokladu získáme:

$$\begin{aligned} s_{n+1} &= s_n = \frac{1}{2} \cdot n \cdot (n+1) - (-1)^n \cdot \left\lceil \frac{n}{2} \right\rceil = \\ &= \frac{1}{2} \cdot n \cdot (n+1) + (n+1) - (n+1) - (-1)^n \cdot \left\lceil \frac{n}{2} \right\rceil = \\ &= \frac{1}{2} \cdot n \cdot (n+1) + \frac{1}{2} \cdot 2 \cdot (n+1) - (n+1) + \frac{n+1}{2} = \\ &= \frac{1}{2} \cdot (n+1) \cdot (n+2) - \frac{n+1}{2} = \\ &= \frac{1}{2} \cdot (n+1) \cdot (n+2) - (-1)^{n+1} \cdot \left\lceil \frac{n+1}{2} \right\rceil \end{aligned}$$

Nechť je dále n sudé číslo větší než 1. Pak pomocí rekurentní formule a indukčního předpokladu tentokrát získáme:

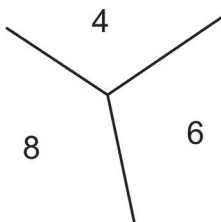
$$\begin{aligned}
 s_{n+1} &= s_n + 2 \cdot (n+1) = \frac{1}{2} \cdot n \cdot (n+1) + (n+1) + (n+1) - (-1)^n \cdot \left\lceil \frac{n}{2} \right\rceil = \\
 &= \frac{1}{2} \cdot n \cdot (n+1) + \frac{1}{2} \cdot 2 \cdot (n+1) + (n+1) - \frac{n}{2} = \\
 &= \frac{1}{2} \cdot (n+1) \cdot (n+2) + \frac{n}{2} + 1 = \\
 &= \frac{1}{2} \cdot (n+1) \cdot (n+2) + \left\lceil \frac{n+1}{2} \right\rceil = \\
 &= \frac{1}{2} \cdot (n+1) \cdot (n+2) - (-1)^{n+1} \cdot \left\lceil \frac{n+1}{2} \right\rceil
 \end{aligned}$$

Velmi podobně by probíhal i důkaz vzorce pro počet bílých dlaždic.

Naše implikace tedy platí pro všechna n , a důkaz správnosti vzorců je tím proveden.

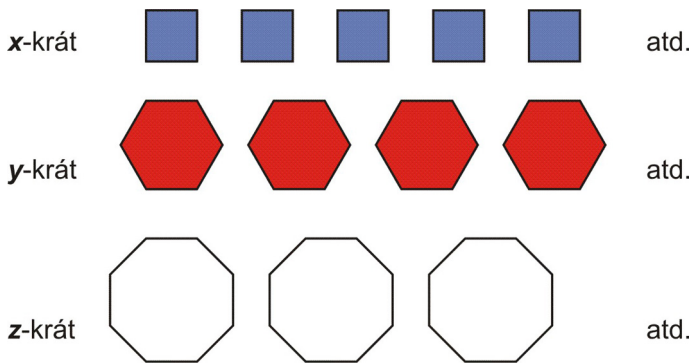
Tato úloha je ukázkou z bohaté třídy úloh, kde si žáci rozvíjejí induktivní myšlení. Patří sem úlohy o figurálních číslech či o posloupnostech pravidelně se rozvíjejících geometrických útvarů (čarách v trojúhelníkové či čtvercové síti, čtvercových dlaždic, shodných krychliček v prostoru, atd.) Nalézání zákonitostí a následné důkazy hypotéz jsou pro žáky zajímavé a motivující.

Úloha 8. Konvexní těleso má tu vlastnost, že v každém jeho vrcholu se stýkají tři stěny: jeden čtverec, jeden pravidelný šestiúhelník a jeden pravidelný osmiúhelník. Všechny mnohoúhelníky mají stejnou délku strany. Vypočítejte počet vrcholů V , počet stěn S a počet hran H tohoto tělesa. (Pro konvexní tělesa platí tzv. Eulerova věta, která říká, že $V + S = H + 2$.)



Obr. 9: Vrcholová hvězdice

Řešení. Představme si, že všechny stěny tělesa máme v počátečním stavu rozpojené. Je to x čtverců, dále pak y pravidelných šestiúhelníků, a konečně z pravidelných osmiúhelníků (viz obrázek 10).



Obr. 10: Rozpojené stěny tělesa

Každý pravidelný mnohoúhelník má n vrcholů a stejně tak má i n stran. Z toho plyne, že na všech pravidelných n -úhelnících z obrázku 10 najdeme celkem $4x + 6y + 8z$ vrcholů, a pochopitelně i stejný počet stran.

Při spojování mnohoúhelníků do povrchu tělesa se v každém vrcholu tělesa spojí tři rozpojené vrcholy a do každé hrany tělesa se spojí dvě rozpojené strany mnohoúhelníků. Z toho plyne, že počet vrcholů tělesa a počet jeho hran můžeme vyjádřit těmito výrazy:

$$V = \frac{4x + 6y + 8z}{3} \quad \text{a} \quad H = \frac{4x + 6y + 8z}{2}.$$

Počet stěn na tělese můžeme snadno vyjádřit ve tvaru $S = x + y + z$. Dosadíme-li tyto výrazy do Eulerovy věty, získáme první rovnici pro naše neznámé x , y a z :

$$\frac{4x + 6y + 8z}{3} + x + y + z = \frac{4x + 6y + 8z}{2} + 2,$$

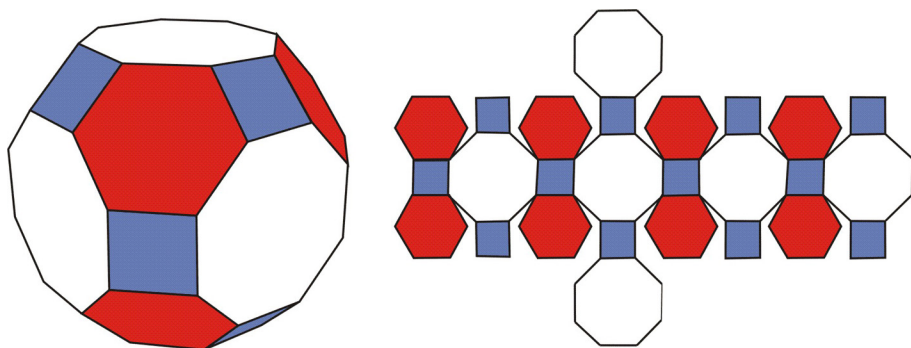
kterou můžeme upravit do tvaru $x - z = 6$.

Další dvě rovnice můžeme sestavit při pohledu na vrcholovou hvězdici. Tam se stýká jeden vrchol čtverce, jeden vrchol šestiúhelníku a jeden vrchol osmiúhelníku. Protože tato situace nastává v každém vrcholu tělesa, musí být sobě rovny počty vrcholů na rozpojených čtvercích, počty vrcholů na rozpojených šestiúhelnících i počty vrcholů na rozpojených osmiúhelnících. Odtud máme: $4x = 6y \Rightarrow 2x - 3y = 0$, a podobně $4x = 8z \Rightarrow x - 2z = 0$.

Soustavu tří rovnic již vyřešíme snadno, řešením jsou hodnoty: $x = 12$, $y = 8$ a $z = 6$.

Povrch tělesa se tedy skládá ze 12 čtverců, 8 šestiúhelníků a 6 osmiúhelníků.

Dosazením těchto hodnot do výrazů pro V , S a H pak můžeme vypočítat, že hledané těleso má 48 vrcholů, 26 stěn a 72 hran. Náznorný obrázek a síť tohoto tělesa jsou na obrázku 11.



Obr. 11: Náznorný obrázek a síť tělesa (4, 6, 8)

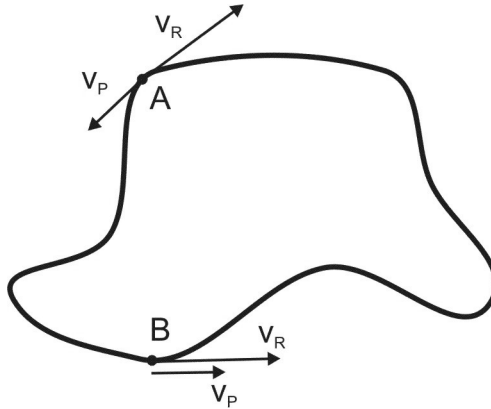
Tuto úlohu můžeme mnohonásobně variovat. Obecně jde o výpočet parametrů V , S a H pro tzv. platónská, resp. archimédovská tělesa.

U platónských těles je použit jen jeden typ mnohoúhelníků (například jen samé rovnostranné trojúhelníky, resp. jen samé čtverce), při jejich řešení vystačíme pouze s Eulerovou větou, není třeba řešit soustavu rovnic. Platónských těles je jen pět, byla známa již Euklidovi.

U archimédovských těles jsou použity dva či tři typy mnohoúhelníků, řeší se soustavy o dvou, resp. třech neznámých, které získáme z Eulerovy věty a z porovnání počtů vrcholů u jednotlivých typů mnohoúhelníků ve vrcholové hvězdici. Archimédovských těles s dvěma typy stěn je více, ale archimédovská tělesa s třemi typy stěn jsou jen tři – naše těleso a tělesa (4, 6, 10) a (3, 4, 4, 5).

Úloha 9. Po okruhu běhají dva atleti, každý jinou konstantní rychlostí. Jestliže běží opačnými směry, potkávají se každých 10 minut, jestliže běží stejným směrem, míjí rychlejší pomalejšího každých 40 minut. Za jakou dobu uběhne okruh rychlejší atlet, resp. pomalejší atlet?

Řešení. Označme si symboly v_R , resp. v_P rychlosti rychlejšího, resp. pomalejšího běžce (jednotkou bude m/min). Dále si označme symbolem d délku okruhu v metrech.



Obr. 12: Okruh se dvěma běžci

Když běžci běží opačnými směry a míjejí se třeba v bodě A , pak se zase potkají v takovém bodě, kdy součet jejich drah, které uběhnou za 10 minut, je roven délce okruhu d . Odtud plyne rovnice: $v_R \cdot 10 + v_P \cdot 10 = d$.

Když běžci běží stejným směrem a rychlejší předbíhá pomalejšího třeba v bodě B , pak k dalšímu předběhnutí dojde, až rychlejší předběhne pomalejšího o celý okruh, tedy v takovém bodě, kdy rozdíl jejich drah, které uběhnou za 40 minut, je roven délce okruhu d . Odtud plyne další rovnice: $v_R \cdot 40 - v_P \cdot 40 = d$.

Obě rovnice mají stejnou pravou stranu, musí se tedy rovnat i jejich levé strany. Po zkrácení deseti získáme:

$$\begin{aligned} v_R + v_P &= 4v_R - 4v_P \\ 5v_P &= 3v_R \\ v_P &= \frac{3}{5}v_R \end{aligned}$$

Dosazením do první rovnice obdržíme $v_R \cdot 10 + \frac{3}{5}v_R \cdot 10 = d$, a odtud můžeme vypočítat čas, za který oběhne rychlejší běžec celý okruh:

$$\frac{d}{v_R} = 10 + \frac{3}{5} \cdot 10 = 16.$$

Rychlejší běžec tedy uběhne celý okruh za 16 minut.

Pomalejší běžec uběhne celý okruh za čas

$$\frac{d}{v_P} = \frac{d}{\frac{3}{5}v_R} = \frac{5}{3} \cdot \frac{d}{v_R} = \frac{5}{3} \cdot 16 = \frac{80}{3} = 26\frac{2}{3}.$$

Pomalejší běžec tedy uběhne celý okruh za 26 minut a 40 vteřin.

Tato úloha má zajímavé zadání, které neumožňuje vypočítat hodnoty řady parametrů, které se v ní vyskytují (délka okruhu, rychlosti obou atletů), ale přesto je možné vypočítat poměry těchto parametrů, tedy například i časy, za které oběhnou atleti celý okruh.

Úloha 10. Množinu kladných celých čísel budeme nazývat čtvercovou právě tehdy, když je neprázdná a součin všech jejích prvků je druhou mocninou celého čísla.

Zjistěte, kolik podmnožin množiny $\{1, 2, 3, \dots, 20, 21\}$ je čtvercových.

Řešení. Aby si žáci uvědomili roli jednotlivých čísel při vytváření čtvercových množin, je vhodné nejdříve sestavovat příklady podmnožin, které jsou čtvercové, a příklady podmnožin, které nejsou čtvercové.

Třeba podmnožina $\{3, 7, 21\}$ je čtvercová, protože $3 \cdot 7 \cdot 21 = 3 \cdot 7 \cdot 3 \cdot 7 = (3 \cdot 7)^2$.

Nebo podmnožina $\{2, 4, 18\}$ je také čtvercová, protože $2 \cdot 4 \cdot 18 = 2 \cdot 4 \cdot 2 \cdot 9 = (4 \cdot 3)^2$.

Ale podmnožina $\{4, 9, 11\}$ není čtvercová, protože $4 \cdot 9 \cdot 11 = (2 \cdot 3)^2 \cdot 11$.

Tak si žáci postupně uvědomí, že čísla z množiny $A = \{1, 4, 9, 16\}$, která jsou druhými mocninami, je možné zařazovat zcela libovolně do čtvercových množin, bez ohledu na další čísla v podmnožině.

Také brzo poznají, že žádné číslo z množiny $B = \{11, 13, 17, 19\}$ větších prvočísel nemůže být prvkem žádné čtvercové podmnožiny.

Pak si také povšimnou, že čísla z množiny $C = \{2, 3, 5, 7\}$ menších prvočísel nemohou být prvky čtvercové podmnožiny samostatně, ale jen za přítomnosti dalšího čísla, které má dané malé prvočíslo ve svém prvočíselném rozkladu.

A nakonec zjistí, že čísla z množiny $D = \{6, 8, 10, 12, 14, 15, 18, 20, 21\}$, v jejichž prvočíselných rozkladech se vyskytují jen čísla z množiny C , také nemohou být prvky čtvercové podmnožiny samostatně, ale pouze za podmínky současného výskytu vhodných prvků z množiny C .

Závěrem si pak žáci uvědomí, že každou čtvercovou podmnožinu množiny $\{1, 2, 3, \dots, 20, 21\}$ je možné vytvořit takto:

Vezme se libovolná podmnožina množiny D . Součin jejích prvků je číslo ve tvaru $2^x \cdot 3^y \cdot 5^u \cdot 7^v$, kde čísla x, y, u, v jsou buď sudá, anebo lichá. Tato podmnožina D se sjednotí s podmnožinou množiny C , která obsahuje ta prvočísla, která mají ve vyjádření součinu prvků z D liché exponenty. Takto vytvořená podmnožina se dále sjednotí s libovolnou podmnožinou množiny A . Je třeba ale dodržet podmínku, že čtvercová množina musí být neprázdná.

Kolik tedy můžeme získat čtvercových podmnožin? Množina D má 2^9 podmnožin, množina A má 2^4 podmnožin, a neprázdných podmnožin je tedy $2^9 \cdot 2^4 - 1 = 2^{13} - 1 = 8191$.

ZÁVĚR

Úlohy z tohoto článku byly vybrány z úloh, které byly zformulovány a řešeny na jednom z odborných seminářů Katedry matematiky Přírodovědecké fakulty UJEP v Ústí nad Labem, který nese název Seminář řešení matematických více méně středoškolských úloh (SeReMaStU1). Tohoto semináře se kromě pracovníků katedry účastní i studenti fakulty, učitelé matematiky ze středních škol, jejich žáci i občasní hosté z jiných kruhů. Seminář se schází zhruba jednou měsíčně a jeho náplň přináší všem účastníkům poučení i potěšení. Více se o semináři lze dozvědět na jeho stránce

[https://kma.ujep.cz/seminare-a-kurzy/
seminar-reseni-matematickych-vice-mene-stredoskolskych-uloh](https://kma.ujep.cz/seminare-a-kurzy/seminar-reseni-matematickych-vice-mene-stredoskolskych-uloh)

Naleznete tam také kompletní seznam úloh, které jsme na něm od jeho založení řešili. U řady úloh se ale nespokojujeme s pouhým vyřešením, ale diskutujeme o různých způsobech řešení, úlohy dále pozměňujeme, zobecňujeme, vytváříme jejich různá pokračování, a tak dále.

Budu rád, pokud tento článek vzbudí zájem i o náš seminář.

NĚKOLIK POHLEDŮ NA GEOGEBRU

Šárka Gergelitsová

ABSTRAKT

Volně dostupný didaktický software GeoGebra existuje více než 20 let. Do svého původního interaktivního prostředí stále přidává nové funkce a rozšiřuje oblasti využití. Přitom díky podpoře aktuálních technologií je cenným pomocníkem nejen při prezenční výuce a domácí práci, ale i při distanční výuce. Článek připomíná základní postupy při práci s GeoGebrou, zmiňuje se o prostředí GeoGebra Classroom, seznamuje s Pravděpodobnostní kalkulačkou a ukazuje postupy, jak vytvořit soubor nebo applet, který pomůže učiteli s přípravou testů a žákům s procvičováním rutinních dovedností. Ukáže také export, přípravu a začlenění obrázku do $\text{\LaTeX}$ dokumentu.

KLÍČOVÁ SLOVA: GeoGebra, interaktivní prvky, online applet, Classroom, pravděpodobnost, $\text{\LaTeX}$ a obrázky.

GEOGEBRA JAKO INTUITIVNÍ INTERAKTIVNÍ
VÝUKOVÉ PROSTŘEDÍ I AUTORSKÝ NÁSTROJ
PRO TVORBU DIDAKTICKÝCH MATERIÁLŮ

GeoGebra je dynamický matematický software vytvořený pro didaktické účely. V principu svého návrhu spojuje do jednoho prostředí geometrii a algebru (odtud GeoGebra) a navíc zobrazení grafů funkcí, tabulkový procesor, statistiku, pravděpodobnost a analýzu a zobrazení 3D objektů.

První ocenění (European Academic Software Award) dostala GeoGebra už v roce 2002. Od té doby se komunita jejích uživatelů stále rozrůstá. Přestože GeoGebra stále vychází z původního konceptu, daří se vývojovému týmu v čele s autorem Markusem Hohenwarterem vyhovět požadavkům výuky i pro online prostředí a využívat nové technologie.

RŮZNÁ PROSTŘEDÍ A VERZE GEOGEBRY

Univerzální prostředí GeoGebry existuje ve dvou variantách: GeoGebra Klasik 5 je přizpůsobena práci na zařízení, kde uživatel používá dostatečně velký displej či tabuli a pro interakci standardní klávesnici a myš. Je nejpodobnější původní verzi. Varianta GeoGebra Klasik 6 odpovídá vzhledem a rozvržením prostředí spíše webovému prostředí a práci s dotykovým zařízením. Funkce obou variant jsou ale téměř stejné a existují a vyvíjejí se současně.

Kromě obou komplexních balíčků je možné stáhnout si z webu GeoGebry také instalační soubory pro dílčí aplikace pro řadu operačních systémů (<https://www.geogebra.org/download>).

Nainstalované aplikace se při připojení zařízení k internetu automaticky aktualizují. Existuje ale také plnohodnotná přenosná verze (tu můžeme mít třeba na flash disku), která se neinstaluje, ale přímo spouští, u níž se staráme o aktualizace sami.

ONLINE PROSTŘEDÍ

Kromě aplikací, které si uživatel nainstaluje nebo uloží do svého zařízení, je možné pracovat v GeoGebra online aplikacích, odkazy najdeme na webu GeoGebry <https://www.geogebra.org>. Jednak zde najdeme „klasickou“ variantu programu <https://www.geogebra.org/classic>, jednak další dílčí aplikace. Do výše uvedeného url <https://www.geogebra.org/> napíšeme název požadované aplikace za lomítko. K dispozici jsou: calculator, graphing, 3d, cas, scientific, geometry, notes.

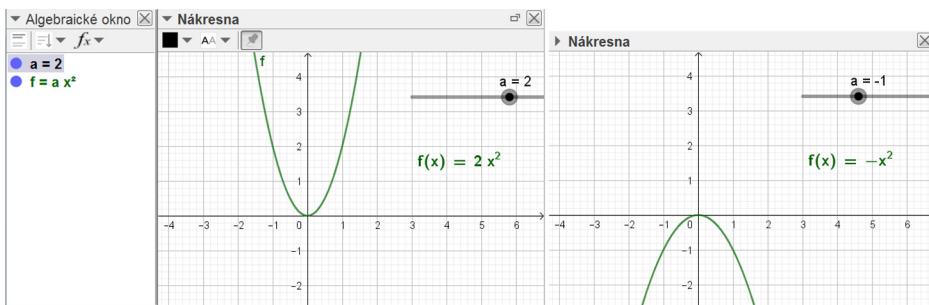
INTERAKTIVNÍ POUŽITÍ GEOGEBRY

Využíváme-li GeoGebrou pro demonstraci pojmů, postupů a řešení problémů přímo v hodině, oceníme intuitivní a rychle dostupné základní nástroje, příkazy a nastavení vlastností objektů a zejména interaktivní prvky.

Velmi rychle zobrazíme například grafy funkcí (viz obr. 1), ilustrujeme operace s vektory, význam parametrického vyjádření přímky (v rovině i v prostoru) či rovnice kuželoseček v analytické geometrii, předvedeme vlastnosti různých typů trojúhelníků a čtyřúhelníků, provedeme diskusi řešení konstrukční úlohy, rychle ověříme správnost výsledku při řešení rovnice nebo soustavy rovnic, zobrazíme komplexní čísla v Gaussově rovině. . .

Při takovém přímém použití GeoGebry oceníme přehlednost prostředí a volbu základních nástrojů (jednotlivých konstrukcí) pomocí ikon. Připomeňme si několik drobností, které interaktivní práci s GeoGebrou urychlí a usnadní:

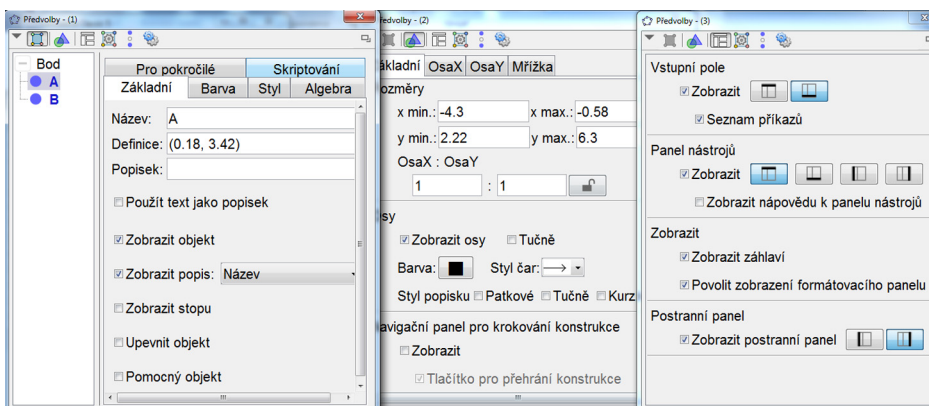
- Každé okno GeoGebry má vlastní **Panel nástrojů** s ikonami tzv. **nástrojů** pro rychlou konstrukci nových objektů a pro manipulaci s nimi. V *Nákresnách*



Obr. 1: Funkce s posuvníkem

to jsou zejména konstrukce geometrických objektů, v okně *CAS* pro symbolické výpočty pomocí ikon vybíráme operace pro úpravu výrazů, v okně *Tabulka* nástroje pro analýzu dat a tvorbu seznamů a matic.

- Pod *Panelem nástrojů* je **Formátovací panel**, který se skryje/zobrazí trojúhelníčkem vedle názvu okna. Jsou na něm ikony pro rychlý přístup k nastavení nejčastěji používaných vlastností objektu, který jsme právě vybrali (v závislosti na jeho typu). Není-li vybrán žádný objekt, jsou zde nastavení vlastností okna, v němž pracujeme (volba pohledu, zobrazení souřadnicových os, volba promítání ve 3D okně, ...), a přizpůsobení možností manipulace v něm.
- Kromě *Formátovacího panelu* slouží k nastavení vlastností objektů a prostředím dialogové okno **Vlastnosti** (viz obr. 2). V něm najdeme veškerá možná



Obr. 2: Co najdeme v okně Vlastnosti

nastavení, tedy i ta která se nevešla na *Formátovací panel*. Toto dialogové okno má několik stránek-záložek (podle toho, jaký objekt jsme vybrali a jaká okna jsou v GeoGebře aktivní) a hledáme v něm zejména pokročilejší nastavení: podmínky pro viditelnost, podmíněné (*dynamické*) barvy, fixaci objektů, dále vlastnosti *Nákresen*, nastavení souřadnicových os, rozvržení oken GeoGebry, ...

- Další **příkazy**, které nemají svou ikonu v *Panelu nástrojů*, zadáváme ze **Vstupního řádku**. Vytvářené objekty není třeba pojmenovávat, GeoGebra je pojmenuje sama, příkazem $A = (2, -1)$ ale vytvoříme bod, zatímco příkazem $a = (2, -1)$ vektor.
- Zadáváme-li funkci, pak vstup píšeme buď ve tvaru $f: x + 1$ nebo $g(x) = \sin(x)$, nikoliv $y = x^2 + 1$, takový předpis je považován za polynom a výsledný objekt není funkce, ale kuželosečka, tedy parabola. Pro každý z těchto typů objektů má GeoGebra jiné příkazy.

Pokud svěříme pojmenování funkce GeoGebře, stačí zadávat jen předpis funkce, tedy „pravou stranu“, výraz v proměnné x .

- **Vstupní řádek** má paměť, kterou rozbalíme klávesou šipka (nahoru nebo dolů) a můžeme z ní vybrat a znovu zadat dříve vložený příkaz.

Při zadávání parametrů příkazu není dobré do polí pro jednotlivé parametry v příkazu klikat, lépe je přejít na (další) parametr tabulátorem nebo šipkou a rovnou psát.

- Pro **vkládání speciálních znaků** můžeme využít *tabulku znaků* (ikonka je viditelná po zahájení editace vpravo ve vstupním poli), *virtuální klávesnici* (vyvolá se z *Hlavního menu – Zobrazit*) nebo klávesové kombinace s klávesou **Alt**: **Alt+a** (α), **Alt+o** (stupeň), **Alt+p** (ale stačí napsat π), **Alt+i** (imaginární jednotka), **Alt+e** (Eulerovo číslo).
- Chceme-li vrátit do *Vstupního řádku* **definici nějakého objektu**, klikneme na objekt a stiskneme funkční klávesu **F3**. Klávesa **F4** vloží do řádku aktuální hodnotu objektu a klávesa **F5** jeho název.
- Do **režimu výběru objektů** (pro manipulaci či nastavení vlastností) přejdeme po provedení libovolné konstrukce nástrojem *Výběr* (ikona šipka), rychleji a praktičtěji klávesou **Esc**.
- **Algebraické okno** (zobrazí se z *Hlavního menu* programu v podmenu *Zobrazit* či **Ctrl+Shift+A**) zobrazuje textový seznam sestrojených objektů, které v něm můžeme vybírat stejně jako v *Nákresně* a zejména skrývat/zobrazovat díky „kuličce“ před názvem objektu. Poklikáním na objekt v *Algebraickém okně* aktivujeme pole, v němž můžeme objekt okamžitě předefinovat.

- **Algebraické okno** je vhodné zobrazit při interaktivní práci. Máme-li materiál dopředu připravený, pak okno obvykle skryjeme. Pokud chceme před zvidavými zraky žáků opravdu skrýt definice (všech nebo některých) objektů, nastavíme těmto objektům vlastnost *Pomocný objekt* a první ikonkou na *Formátovacím panelu Algebraického okna* přepneme zobrazení pomocných objektů.
- **Posuvník** je „zviditelněné“ číslo. Můžeme ho v *Nákresně* vytvořit pomocí *nástroje* (ikony) nebo místo toho do *Vstupního řádku* zapsat například $b=5$, a následně aktivovat zobrazovací kuličku u proměnné b , čímž zobrazíme číslo b jako posuvník.
- **Zaškrťovací políčko** je podobně „zviditelněná“ logická proměnná. Můžeme ji v *Nákresně* vytvořit pomocí *nástroje* (ikony) nebo do *Vstupního řádku* zapsat například $\text{zobraz} = \text{true}$ a aktivovat kuličku u proměnné zobraz – zobrazit ji jako zaškrťovací políčko.
- **Šipky a myš** – objekty můžeme přesouvat či jejich hodnoty měnit jednak tažením myši, jednak kurzorovými klávesami (šípkami), případně při současném stisku **Ctrl**, **Shift**, **Alt**. Pro pohyb mezi hodnotami posuvníku můžeme použít i klávesy **PageUp**, **PageDown**, **Home**, **End**.
- **Zafixovat souřadnicovou síť** je volba dostupná z *Formátovacího panelu Nákresny* (ikona magnetu). Způsobí to, že při manipulaci myší budou objekty (body) doskakovat jen do mřížových bodů zvolené souřadnicové sítě. To se hodí vždy, když preferujeme celočíselné souřadnice bodů, například pro zadání úloh v analytické geometrii. Při interaktivní manipulaci s grafem (při studiu vlastností funkcí) můžeme sestrojené grafy přetahovat myší stejně jako jiné geometrické objekty. Při zafixované souřadnicové síti je budeme myší přetahovat o preferovaný krok. Zafixování sítě ovlivní pouze manipulaci myší, jinými způsoby (pohybem klávesami, přepsáním souřadnic, ...) změníme polohu objektu libovolně.
- Pokud nám nejde přesouvat objekty myší, jsou nejspíš *upevněné*. Tehdy vstoupíme do okna *Vlastnosti* (*Hlavní menu* – *Úpravy* – *Vlastnost*, nebo **Ctrl+E**, nebo vybereme položku *Vlastnosti* z kontextového menu po stisku pravého tlačítka myši) a na záložce *Základní* přepneme (deaktivujeme) volbu **Upevnit objekt**.
- **Popisek** sestavíme na kartě *Základní* v okně *Vlastnosti*. Pokud se nám nehodí popisovat objekt ani názvem ani předdefinovaným způsobem zobrazení hodnoty, můžeme do popisku vložit libovolný statický text, případně s využitím příkazů $\text{\LaTeX}$ (pokud ho uzavřeme mezi znaky $\$ \dots \$$), například $A^2\$$

zobrazí popisek A^2 . Chceme-li do popisku zahrnout jednotlivé souřadnice, použijeme zástupný odkaz ve tvaru $\%x$, $\%y$, $\%z$, případně $\%v$ (hodnota), $\%n$ (název).

Příklad: Pokud nám nevyhovuje přednastavený popisek bodu A ve tvaru $A = (4, 2)$, zapíšeme do jeho pole *Popisek* výraz $\$n[\%x; \%y]\$$ – výsledkem bude tvar popisku $A[4; 2]$.

- V popisku nemůžeme vyhodnocovat výrazy ani se odkazovat na hodnoty jiných objektů, nově ale můžeme jako popisek objektu využít jiný, dříve připravený objekt typu *text*.

Uvedme ještě pár užitečných příkazů GeoGebry (příkazy zde uvádíme pro zvolený jazyk čeština, vždy je ale možné používat anglickou variantu). Názvy příkazů neobsahují diakritiku ani mezery.

- $\text{UplnyCtverec}(x^2 + 4x - 1) \rightarrow (x + 2)^2 - 5$
- $\text{ParcialniZlomky}((2x - 5)/(x + 3)) \rightarrow 2 - 11/(x + 3)$
- $\text{PrvociselnyRozklad}(120) \rightarrow \{2, 2, 2, 3, 5\}$
- $\text{SeznamDelitelu}(120) \rightarrow \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}$
- $\text{Rozklad}(x^6 - 1) \rightarrow (x - 1)(x + 1)(x^2 - x + 1)(x^2 + x + 1)$
- $\text{Rozsirit}((x - 1)(x + 1)(x^2 - x + 1)(x^2 + x + 1)) \rightarrow x^6 - 1$
- $\text{IracionalniText}(\text{sqrt}(2)) \rightarrow \text{text}$ v *Nákresně*, který obsahuje symbol odmocniny
- $\text{Teziste}(A, B, C)$, též $(A + B + C)/3$

VYUŽITÍ GEOGEBRY PRO TVORBU VÝUKOVÝCH APLETŮ

GeoGebra je také velmi výkonný nástroj, který nám umožní připravit pro studenty kvalitní didaktické materiály. Tehdy oceníme pokročilé nástroje a volby, možnost využít dvě *Nákresny*, vkládat do nich vedle konstrukcí také kvalitní matematické texty. Oceníme možnosti tisku či exportu obrázků. S pomocí interaktivních prvků a případně tlačítek, která spustí připravené skripty, můžeme vytvořit applety sloužící k procvičování zvolených rutinních dovedností.

Pro skriptování máme dvě možnosti: můžeme použít **GeoGebra Script**, který umožní sestavit posloupnost příkazů GeoGebry, která se bude provádět v reakci na kliknutí na zvolený objekt či po jeho aktualizaci. Nejde o plnohodnotný programovací jazyk. Potřebujeme-li ve skriptu využít standardní větvení, cykly a podobně, můžeme využít také **javascript**. Javascript přistupuje k objektům appletu přes API, https://wiki.geogebra.org/en/Reference:GeoGebra_Apps_API.

ZPŘÍSTUPNĚNÍ APPLETU PROSTŘEDNICTVÍM WEBU GEOGEBRY

Pokud jsme takový applet pro studenty připravili, potřebujeme ho studentům dát k dispozici nebo nějak zveřejnit. To můžeme udělat několika způsoby:

Můžeme jim předat samostatný *.ggb soubor, s nímž budou pracovat, mají-li k dispozici GeoGebra.

Můžeme vyexportovat vytvořený applet jako html stránku, a tu studentům dát. Potom jim k práci s appletem bude stačit libovolný webový prohlížeč.

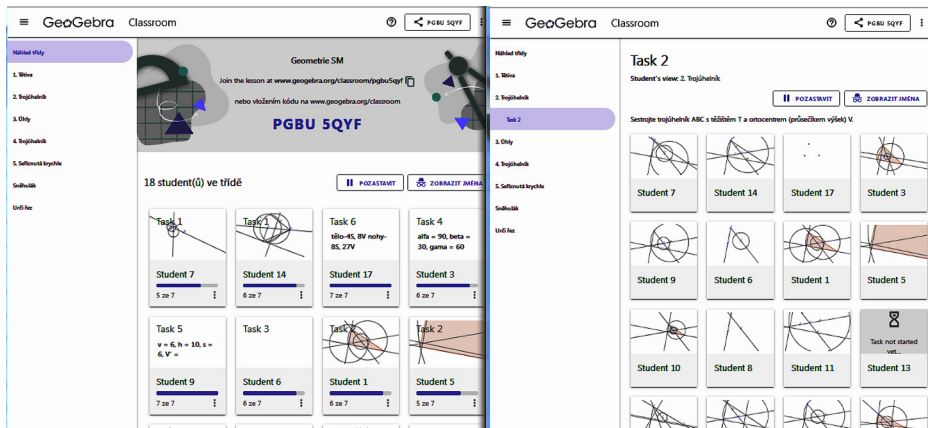
Nejčastější a zřejmě nejpohodlnější cesta ale bude uložit vytvořený applet na web GeoGebra. To můžeme udělat rovnou při ukládání vytvořeného appletu: z varianty Klasik 5 zvolíme možnost *Sdílet* (možnost *Uložit* ukládá na lokální disk), varianta Klasik 6 nabízí pod volbou *Uložit* obě možnosti. Potřebujeme jen mít na webu GeoGebra účet, který je ale bezplatný (stejně jako je bezplatné veškeré nekomerční využití GeoGebra). To, komu bude applet dostupný, poté nastavíme.

Na webu <https://www.geogebra.org/materials> ale možná zjistíme, že to, co plánujeme pro žáky připravit, už připravil a zveřejnil někdo dříve. Veřejně dostupné materiály můžeme volně zpřístupnit svým žákům. Materiálů je na webu velké množství, pro různé stupně školy i různá témata.

GEOGEBRA WEB JAKO PROSTŘEDÍ PRO ONLINE VÝUKU, CLASSROOM

Při distanční výuce můžeme využít *GeoGebra Classroom*. Pro učitele, který má GeoGebra účet, je založení *třídy* velice jednoduché a přímočaré. Z libovolného materiálu (na webu se používá název *aktivita*) založíme *třídu* na jedno kliknutí. *Aktivita* je cosi jako pracovní list. Může obsahovat několik částí, a to i různých typů: úlohy, konstrukce, texty, otázky, tabuli (whiteboard). Můžeme ji sestavit sami (rovnou v online prostředí nebo z dříve připraveného materiálu, případně i z tzv. *GeoGebra Knihy*; *Knihy* ale obvykle má větší rozsah, než potřebujeme pro *aktivitu* do *třídy*). Můžeme také použít volně dostupnou *aktivitu* jiného autora.

Na stránce s připravenou *aktivitou* pak stačí kliknout na „tlačítko“, ikonu v pravém horním rohu okna stránky nadepsanou VYTVOŘIT TŘÍDU. Vytvoří se url, odkaz, který žákům předáme (nasdílíme). Žáci se mohou do *třídy* přihlásit také přímo z webu GeoGebra, pokud z její hlavní stránky v panelu vlevo okna vyberou volbu *Classroom* a zadají osmimístný kód *třídy* (modrý nápis na obr. 3



Obr. 3: GeoGebra Classroom

vlevo), který se nám vygeneruje spolu s odkazem. Do *třídy* se žáci hlásí anonymně, pod vlastní zvolenou přezdívku. Pod touto přezdívku pak učitel vidí jejich řešení. Učitel sleduje řešení žáků v reálném čase, ale nemůže do něho zasahovat.

Na adrese <https://www.geogebra.org/m/hncrgruu> najdeme podrobný tutoriál k práci s *třídou*.

Učitel vidí přehled řešení celé *třídy*, může sledovat jednak práci jednotlivých žáků, jednak řešení jednotlivých úloh, s nimiž žáci pracují.

Vybere-li si učitel jednoho žáka, vidí aktuální stav jeho práce, tedy přesně to, co právě žák dělá a co a jak má vyřešeno (s omezeními danými rychlostí přenosu).

Pokud si zvolí přehled úloh, vidí u každé úlohy přehled řešení všech žáků. V případě, že jde o uzavřenou otázku s výběrem odpovědi, je učitelův přehled doplněn ještě živým sloupcovým grafem ukazujícím, kolik žáků volilo jednotlivé varianty odpovědi. Jména žáků je možné skrýt (chceme-li například sdílet žákům pokrok celé skupiny při řešení). Na obrázku 3 vlevo vidíme náhled celé *třídy*, vpravo pak přehled řešení úlohy 2. Jde o reálnou *třidu*, jména žáků jsou kvůli ochraně dat skryta.

Přihlásí-li se žák do Classroomu znovu, zejména pokud se hlásí z anonymního okna nebo z jiné aplikace, která si „nepamatuje“ předchozí přihlášení, založí se mu nové řešení, žák nemá (pro Classroom nepotřebuje) žádný vlastní účet. Je tedy ideální používat Classroom pro práci „v hodině“.

Existující *třidu* může učitel kdykoli **pozastavit** (v pozastavené třídě nemohou žáci pokračovat v řešení) a kdykoli opět **pokračovat**. Toto tlačítko je vidět i v obr. 3.

PRAVDĚPODOBNOSTNÍ KALKULAČKA

Pravděpodobnostní kalkulačka je velice efektivní nástroj užitečný pro pochopení pravděpodobnosti jevů a vztahů mezi nimi a pro vytvoření představy o hodnotách pravděpodobnosti jevů. Je dostupná jednak jako samostatné okno v balíku GeoGebry Klasik z *Hlavního menu – Zobrazit* (**Ctrl+Shift+P** – pozor na klávesovou zkratku **Ctrl+P**, ta vyvolá nastavení tisku a exportu obrázku), jednak jako samostatná aplikace v online verzi, jak jsme uvedli výše. Je součástí aplikace <https://www.geogebra.org/classic>, odkud ji lze z rozbalovacího menu v horní liště vybrat, přímo ji vyvoláme z url: <https://www.geogebra.org/classic#probability>.

Na adrese <https://www.geogebra.org/m/zwybyg58#chapter/318091> najdeme tutoriál k použití kalkulačky.

Ukažme si jeden konkrétní příklad použití tohoto nástroje pro řešení úlohy ze středoškolské sbírky.

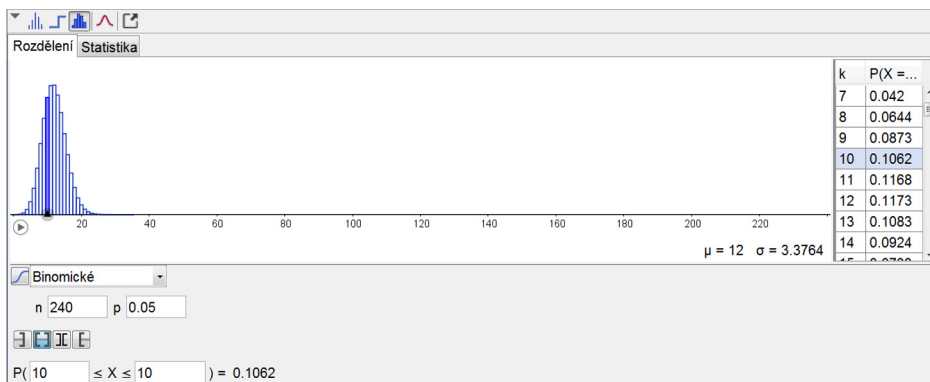
Předpokládejme, že jsme žáky seznámili s binomickým rozdělením pravděpodobnosti a pomocí odvozených vzorců a kalkulačky jsme vyřešili několik úloh. Žáci tedy vědí, jak pravděpodobnost počítat. K tomu, aby získali odhad a cit pro určení pravděpodobnosti (mimo jiné i cenou schopnost odhadnout, zda výsledek získaný na kalkulačce není vinou chyby při zadání nesprávný), je však třeba vyřešit větší počet úloh a prodiskutovat různé situace a problémy. Výpočty pomocí kalkulačky jsou však zdoluhavé a často se potýkáme s vlastními chybami při vkládání hodnot. A tady nám pomůže právě *Pravděpodobnostní kalkulačka*. Podívejme se na úlohu ze sbírky maturitních úloh:

Stroj vyrobí jednu součástku za dvě minuty. Pravděpodobnost, že součástka je vadná, je 0,05. Jaká je pravděpodobnost, že za směnu (8 hodin) vyrobí stroj *právě* 10 vadných součástek? [1]

Vyřešme úlohu a spočítáme pravděpodobnost pomocí kalkulačky. Získaná hodnota 0,1062 (při zvolené přesnosti) by nás mohla překvapit. Počet vadných výrobků může být kterákoliv hodnota mezi 0 a 240 (8×30). Proč právě počet 10 má tak vysokou pravděpodobnost?

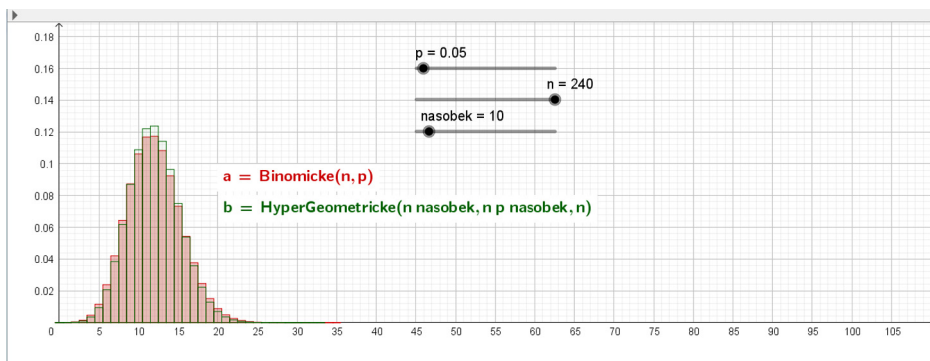
Pokud modelujeme binomické rozdělení pravděpodobnosti pro uvedenou úlohu (viz obr. 4), je důvod okamžitě vidět. Můžeme se zde také zmínit o intuitivním významu pojmu očekávaná hodnota (pro binomické rozdělení $n \times p$), byť tento pojem není do středoškolského učiva zařazen.

Přesnost hodnot ovlivňujeme volbou zaokrouhlení v celém prostředí GeoGebry. Při nastavení zaokrouhlování zobrazovaných čísel v prostředí GeoGebry na 2 desetinná místa se hodnoty pravděpodobnosti v polích *Pravděpodobnostní kalkulačky* zaokrouhlují na 4 desetinná místa.



Obr. 4: Pravděpodobnostní kalkulačka

Zajímavé může být také srovnání binomického a hypergeometrického rozdělení pravděpodobnosti (losujeme předměty z osudí bez vracení). V *Pravděpodobnostní kalkulačce* můžeme v daný moment zobrazit jen jedno rozdělení pravděpodobnosti, grafy různých rozdělení však můžeme vkládat i do *Nákresny* (viz obr. 5) pomocí příkazu *Binomické*($\langle \text{Počet pokusů} \rangle$, $\langle \text{Pravděpodobnost úspěchu} \rangle$) a příkazu *HyperGeometrické*($\langle \text{Velikost populace} \rangle$, $\langle \text{Počet úspěchů} \rangle$, $\langle \text{Velikost vzorku} \rangle$).



Obr. 5: Rozdělení pravděpodobnosti – graf v Nákresně

U většiny témat se ve škole potýkáme s nedostatkem času, obvykle nedokážeme vyřešit tolik úloh, kolik bychom chtěli. Pokud si „úlohy, které jsme nestihli“ modelujeme a jejich řešení vysvětlíme s pomocí takového interaktivního nástroje, jistě tím podpoříme pochopení zkoumaných zákonitostí.

PŘÍPRAVA ZADÁNÍ TESTU

GeoGebrou můžeme použít pro vlastní práci: přípravu a tisk či kontrolu připravených zadání a ověření správných řešení, pokud připravujeme test nebo samostatnou práci pro žáky. Pracujeme-li v základním okně GeoGebry, můžeme jako proměnné ve výrazech a příkazech pro úpravu algebraických výrazů používat pouze x , y , případně z . Jiné názvy jsou považovány za parametry (posuvníky). Budeme-li pracovat v *okně CAS*, můžeme používat proměnné libovolných názvů.

Některé algebraické příkazy GeoGebry jsme již uvedli dříve. Seznam příkazů rozbalíme ikonou osmiúhelníku s vykřičníkem, vedle vstupního řádku. V následujícím příkladu použijeme příkazy pro podíl a zbytek při dělení polynomů: *CelociselnýPodíl*(dělenec, dělitel) a *Mod*(dělenec, dělitel).

Zadání můžeme připravit do *Tabulky* (viz obr. 6). Do buněk *Tabulky* můžeme vkládat nejen čísla a vzorce, jako v obvyklých tabulkových kalkulátorech, ale jakékoliv objekty GeoGebry.

Poznámka: Pojmenujeme-li nějaký objekt (třeba bod) A1, objeví se nám jeho definice v první buňce *Tabulky*. Adresa buňky je název objektu a naopak, lze-li název objektu považovat za adresu buňky, objeví se tento objekt v příslušné buňce.

Obrázek 6 ukazuje využití *Tabulky* pro přípravu sady zadání úloh cvičících dělení polynomů. Do první řádky tabulky jsme (jen) kvůli srozumitelnosti obrázku vložili texty zadání (pro řádek 2), tedy předpisy polynomu nebo příkazy GeoGebry, v dalších řádcích jsou konstrukce jednotlivých zadání a jejich výsledné výrazy.

	A	B	C	D	E
1	$x^3 - 5x^2 + 2x - 1$	$x - 3$	$A2(x) / B2(x)$	$CelociselnýPodíl(A2, B2)$	$Mod(A2, B2)$
2	$x^3 - 5x^2 + 2x - 1$	$x - 3$	$\frac{-5x^2 + 2x - 1}{x - 3}$	$x^2 - 2x - 4$	-13
3	$x^4 + 3x^2 + 1$	$x^2 + 2$	$\frac{x^4 + 3x^2 + 1}{x^2 + 2}$	$x^2 + 1$	-1
4	$x^4 + 3x^2 + 1$	$x^2 + x + 1$	$\frac{x^4 + 3x^2 + 1}{x^2 + x + 1}$	$x^2 - x + 3$	$-2x - 2$
5	$x^5 - 1$	$x - 1$	$\frac{x^5 - 1}{x - 1}$	$x^4 + x^3 + x^2 + x + 1$	0
6					
7					

Obr. 6: Dělení polynomů v prostředí *Tabulky*

Texty v prvním řádku získáme příkazem *Text()*: text v buňce *C1* vytvoříme z výrazu (objektu) *C2* příkazem *Text(C2, false)*. Parametr *false* říká, že se do definice (podílu) nemá dosazovat, ale má se zobrazit samotná definice. V buňce *A1* na hodnotě tohoto parametru nezáleží, nemusíme ho uvádět.

Příkaz *Mod()* vrací nejen zbytek po celočíselném dělení, ale také zbytek při dělení polynomů.

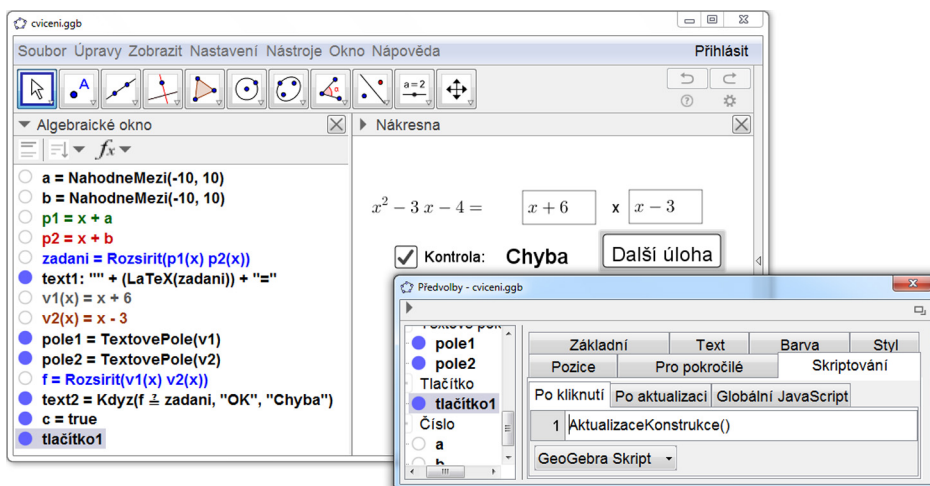
Obsah *Tabulky* je možné přímo tisknout (*Soubor – Náhled*), ale nemůžeme ho ukládat jako obrázek.

Pro postupné generování sady úloh často využijeme také parametry (*posuvníky*), které nám usnadní nalezení vhodného zadání.

PŘÍPRAVA APLETU K PROCVIČENÍ RUTINNÍCH DOVEDNOSTÍ

Připravujeme-li applet, v němž by si měli žáci cvičit nějakou rutinní, základní dovednost, můžeme s výhodou využít generátoru náhodných čísel. Ukažme si, jak připravit cvičení na rozklad kvadratického trojčlenu v součin dvou lineárních členů.

Nebudeme náhodně volit koeficienty zadávaného kvadratického trojčlenu, ale zadání vyrobíme z požadovaného výsledku. Obrázek 7 zobrazuje v *Algebraickém okně* hodnoty objektů, ale použité příkazy (toto zobrazení přepneme třetí ikonou ve *formátovacím panelu* okna).



Obr. 7: Rozklad kvadratického trojčlenu – cvičení

Lineární členy $p1$, $p2$ pro přípravu zadání definujeme pomocí náhodných čísel a , b . Součin $p1$, $p2$ s roznásobenými závorkami je zadání, které zobrazíme do *Nákresny* jako objekt (ikonou) *Text*.

Připravíme si lineární členy $v1$, $v2$, které budou obsahovat odpověď uživatele.

Vedle zadání vložíme do *Nákresny* pomocí ikony v *Panelu nástrojů* dvě tzv. *textová pole*: $pole1$, $pole2$, tj. pole, do nichž může uživatel zapisovat, vkládat hodnoty. Při vkládání těchto polí do *Nákresny* budeme dotázáni, s jakými objekty mají být propojena – s připravenými výrazy $v1$, $v2$.

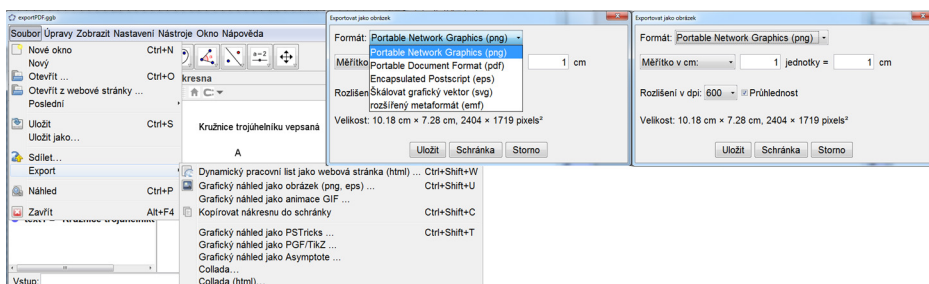
Sestrojíme objekty, pomocí nichž budeme dávat žákovi na vědomí, zda řeší správně nebo ne:

Aby GeoGebra mohla porovnat odpověď žáka se správným řešením, potřebujeme totožné výrazy. Rozšíříme proto součin polynomů $v1$, $v2$ do proměnné f a tu porovnáme se *zadáním*. Text $text2 = Kdyz(f^2 = zadani, "OK", "Chyba")$ může žák zobrazovat/skrývat zaškrtávacím políčkem c .

Nakonec vložíme do *Nákresny* tlačítko, jemuž přidáme jednoduchý skript, který se provede vždy po kliknutí na tlačítko. Příkaz *AktualizaceKonstrukce* způsobí vygenerování nových hodnot náhodných čísel a , b . GeoGebra Skript vidíme v okně *Vlastnosti* tlačítka na záložce *Skriptování*.

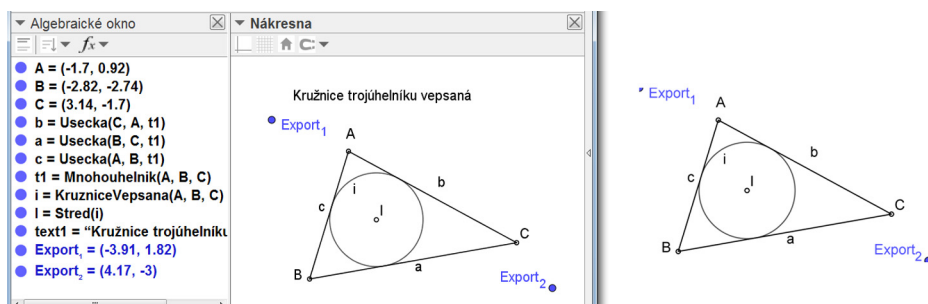
GEOGEBRA, L^AT_EX A OBRÁZKY

Hlavní menu GeoGebry nabízí pro export obrázku dialogové okno z menu: *Soubor – Export*. Můžeme zvolit vhodný formát výstupu a parametry výsledného obrázku (viz obr. 8).



Obr. 8: Generování obrázku

Pokud nám ve výsledném obrázku nevyhovuje volné místo okolo zobrazované konstrukce, můžeme do *Nákresny* vložit body se speciálními názvy *Export_1*, *Export_2*, které vymezí úhlopříčku obdélníku zobrazovaného výřezu.



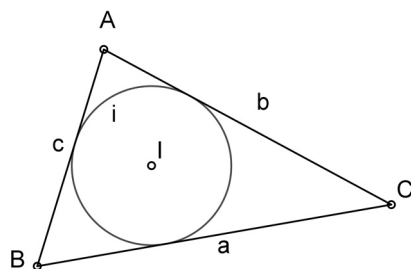
Obr. 9: Omezení zobrazované oblasti Nákrasny

Na obrázku 9 jsme tyto body záměrně nechali viditelné, při exportu skutečného obrázku je po nastavení polohy samozřejmě skryjeme. Vlevo je výstřížek obrazovky části okna GeoGebry, vpravo vygenerovaný obrázek ve formátu png.

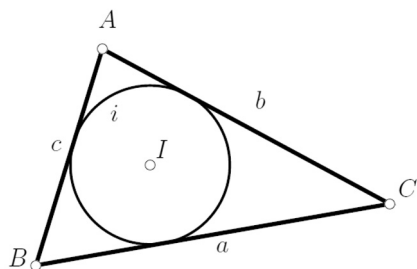
Z GeoGebry můžeme přímo exportovat i obrázek ve formátu pdf, který však obvykle nevyhovuje požadavkům na obrázky geometrických konstrukcí ve skriptech či učebnicích. Z konstrukce vytvořené v GeoGebře ale můžeme takový obrázek v $\text{T}_{\text{E}}\text{X}$ ovské kvalitě vygenerovat. Použijeme export konstrukce, kterou jsme sestavili v *Nákresně*, do kódu PSTricks. Tento export vygeneruje PSTricks kód dokumentu. Jeho obsah můžeme buď vložit přímo do $\text{L}_{\text{A}}\text{T}_{\text{E}}\text{X}$ zdrojového kódu připravovaného článku, nebo si můžeme předem připravit samotný obrázek ve formátu pdf podle našich potřeb. Do „obrázku“, tedy textu – kódu PSTricks, můžeme snadno zasáhnout (měnit typy čar a značek, polohu bodů, ...) a obrázek tím libovolně upravit.

Na obr. 10 vlevo vidíme vzhled přímo vyexportovaného obrázku pdf a vpravo pdf obrázek vygenerovaný exportem do PSTricks. Kód jsme doplnili o preambuli, která nastaví typ dokumentu a zavolá potřebné/užitečné balíčky:

Kružnice trojúhelníku vepsaná



Kružnice trojúhelníku vepsaná



Obr. 10: Vlevo obrázek uložený (vyexportovaný) GeoGebrou jako pdf, vpravo obrázek vygenerovaný pomocí $\text{L}_{\text{A}}\text{T}_{\text{E}}\text{X}$ u a PSTricks

soubor obrazek.tex:

```
%PŘEKLÁDAT LaTeX-> ps-> pdf
\documentclass[12pt]{standalone}
\usepackage{pstricks-add}
\usepackage{amssymb,amsthm}
\usepackage{xcolor}
\usepackage{graphicx}
\usepackage{fancyhdr}
\usepackage[czech]{babel}
\usepackage[cp1250]{inputenc}

\begin{document}
\psset{xunit=1.0cm,yunit=1.0cm,algebraic=true,dimen=middle,
dotstyle=o,dotsize=5pt,
linewidth=2.pt,arrowsize=3pt 2,arrowinset=0.25}
\begin{pspicture*}(-5.09,-3.64)(5.09,3.64)
\pspolygon[linewidth=2.pt](-1.7,0.92)(-2.82,-2.74)(3.14,-1.7)
\psline[linewidth=1.2pt](-1.7,0.92)(-2.82,-2.74)
\psline[linewidth=1.2pt](-2.82,-2.74)(3.14,-1.7)
\psline[linewidth=1.2pt](3.14,-1.7)(-1.7,0.92)
\pscircle[linewidth=1.2pt](-0.8963460095689835,-1.041575778514708)
{1.3424678589992625}
\rput[tl](-3.31,2.62){Kružnice trojúhelníku vepsaná}
\psdots(-1.7,0.92)
%\begin{scriptsize}
\rput[bl](-1.77,1.28){$A$}
\psdots(-2.82,-2.74)
\rput[bl](-3.29,-2.76){$B$}
\psdots(3.14,-1.7)
\rput[bl](3.28,-1.58){$C$}
\rput[bl](-2.57,-0.8){$c$}
\rput[bl](0.21,-2.52){$a$}
\rput[bl](0.87,-0.1){$b$}
\rput[bl](-1.57,-0.3){$i$}
\psdots(-0.8963460095689835,-1.041575778514708)
\rput[bl](-0.81,-0.92){$I$}
%\end{scriptsize}
\end{pspicture*}
\end{document}
```

ZÁVĚR

Možnosti GeoGebry jsou opravdu široké a pokud hledáme návody, jak ji využít, položka *Návody* v *Hlavním menu* nás odkáže na stránky s českými tutoriály: <https://www.geogebra.org/m/zwbyag58> . Spoustu dalších (cizojazyčných) návodů najdeme zde: <https://www.geogebra.org/search/Tutorials>.

Ale i bez studia tutoriálů, při intuitivním využití, nám GeoGebra ve výuce výborně poslouží.

LITERATURA

- [1] Petáková, J. (2003). *Matematika – příprava k maturitě a k přijímacím zkouškám na vysoké školy*. Praha: Prometheus.

BARVY KOLEM NÁS

Barbora Mikulecká, Vojtěch Hanák

ABSTRAKT

Svět bez barev by byl jako jídlo bez chuti. Barvy budeme skládat a rozkládat a podíváme se, jak důmyslně je umí tvořit příroda a jak si s tím naopak poradil člověk v moderním světě. Pojďme více porozumět barvám kolem nás. Protože svět je krásnější, když víte, jak funguje.

KLÍČOVÁ SLOVA: barvy, spektra, oko, afterimage, RGB, CMYK, jednobarevné vidění, spektroskop, difrakce, rozptyl.

MIKROSKOPOVÁNÍ TELEFONU

Seminář byl uveden mikroskopováním telefonu. Jednoduchý a levný USB mikroskop snadno připojíte k počítači a můžete rovnou snímat jakýmkoli softwarem pro USB kamery. Jistě ho oceníte při zkoumání světa i v dalších oblastech fyziky.

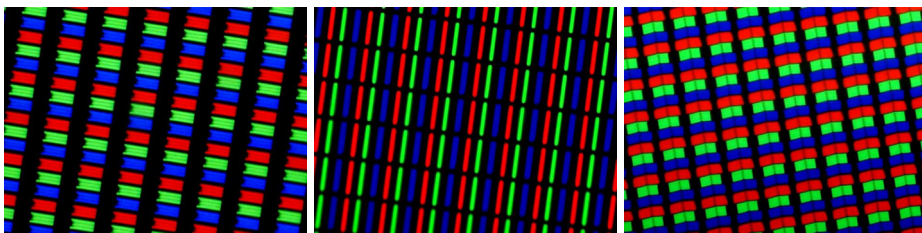


Obr. 1: USB mikroskop

Aby byly pixely dobře vidět, musí mít telefon nastaven maximální jas obrazovky. Ač výrobci deklarují tisíce a někdy dokonce více než 16 milionů barev,

Úžasné divadlo fyziky ÚDiF, bara.mikulecka@udif.cz, vojta.hanak@udif.cz

zjistíte s dětmi, že ve skutečnosti mají pixely barvy pouze tři. Je to červená, modrá a zelená, a dokonce jsou na všech typech telefonů všechny ve stejném konkrétním odstínu.



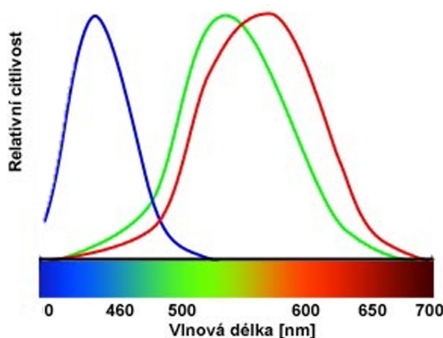
Obr. 2: Barevné pixely různých telefonů vyfocené USB mikroskopem

Je jasné, že tato světla se nějak míchají a vytváří vjem dalších barev. Barevná škála telefonu je pak jen daná krokem, kterým telefon umí jednotlivé subpixely pohasínat nebo zjasňovat. Jak to ale v našem oku funguje a jak to interpretuje mozek? A proč se místo takzvaných RGB barev nepoužívají barvy jiné? To už vyžaduje složitější odpověď.

JAK VNÍMÁ ČLOVĚK BARVY

CO VIDÍ OČI

Lidské oko vnímá světlo pomocí dvou druhů buněk na své sítnici – tyčinek a čípků. Tyčinky jsou buňky, které vnímají jenom intenzitu světla, na všechny barvy jsou citlivé stejně a vidí tedy jen černobíle. Naopak čípky existují trojího druhu podle citlivosti na konkrétní barvy. Jeden druh je nejcitlivější na červenou oblast barev, druhý je citlivý v zelené části spektra a třetí v modré části spektra. Citlivost jednotlivých čípků ukazuje následující obrázek.



Obr. 3: Barevná citlivost lidského oka

Pokud do našich očí dopadá červené světlo, podráždí červené čípky a ty pošlou mozku signál, že vidí. To samé se stane s modrou a zelenou barvou.

Žluté světlo leží v duze mezi červenou a zelenou. Spadá do citlivosti červených i zelených čípků, ale nikoliv modrých. Dopadne-li do našich očí žluté světlo, vybudí signál v červených a zelených čípcích, ale modré ho neuvidí.

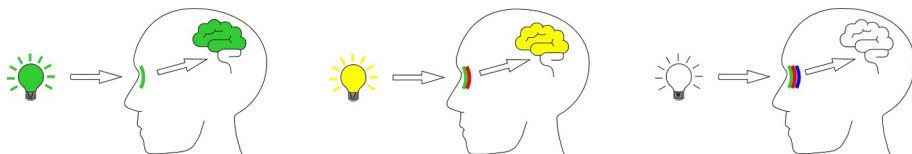
Podobné to dopadne s tyrkysovým světlem. To je v duze mezi modrou a zelenou a mohou ho tedy detekovat modré a zelené čípky.

Bílé světlo obsahuje všechny barvy duhy. Musí být proto schopné podráždit všechny tři typy čípků v našich očích. Pokud tedy vidí červené, modré i zelené čípky, vnímáme ho jako bílé světlo.

CO VIDÍ MOZEK

Nemůžeme to chápat tak, že bychom viděli jen červenou, zelenou a modrou barvu. Mozek si signály z jednotlivých čípků skládá a výsledek nějak interpretuje. Jediné, co mozek ví, je, kolik světla vidí modré, zelené a červené čípky.

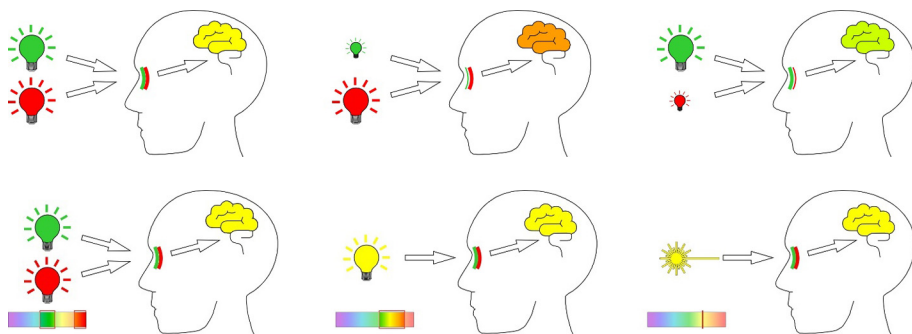
Vidí-li světlo zároveň červené, zelené i modré čípky, pak nám musí do očí dopadat světlo obsahující všechny barvy, tedy světlo bílé barvy. Pokud ale mozek ví, že pouze červené čípky jsou ty jediné, které vidí světlo, je jasné, že se díváme na červené světlo. Stejně je to se zelenou a modrou barvou.



Obr. 4: Obrázek světla a sítnice a mozku

Pokud ale mozek ví, že světlo vidí červené i zelené čípky, interpretuje to jako žlutou barvu. Jakým způsobem ale byly červené a zelené čípky nabuzeny, to mozek neví a mohlo se stát hned několik možností. Do našich očí může dopadat červené a zelené světlo, ale žádné žluté světlo. Může do nich dopadat jen úzký proužek žluté části duhy, ale žádné červené ani zelené světlo. Může do něj dopadat všechno světlo od červené do zelené včetně žluté. Která možnost nastala, mozek neví. Ve všech případech ale díky interpretaci mozku vidíme žlutou.

Podle této logiky mozek rozlišuje i odstíny. Pokud vidí zelené čípky více světla než ty červené, dopadá nám nejspíš do očí světlo, které je v duze posunuté od žluté směrem k zelené. Pokud ale vidí červené čípky více světla, bude ono světlo posunuté spíš k červené a tedy od žluté do oranžové.



Obr. 5: Různá množství červeného a zeleného světla (nahore) a různé spektrální zdroje vytvářející stejný vjem žluté

S modrou a zelenou je to podobné. Pokud vidí zelené a modré čípky, mozek nám nabídne barvu, která je v duze mezi modrou a zelenou, tedy tyrkysovou. Složitější situace nastane, pokud vidí pouze červené a modré čípky, ale zároveň zelené čípky světlo nevidí. Pokud bychom pokračovali podle stejné logiky, mozek by opět měl vidět barvu, která je v duze mezi červenou a modrou. Tou barvou je zelená. Jenže zelené čípky žádné světlo nevidí, takže zelená barva nám do očí určitě nesvítí. Mozek to vyřeší tak, že si vymyslí barvu, která v duze není. Této barvě se říká purpurová nebo magenta.

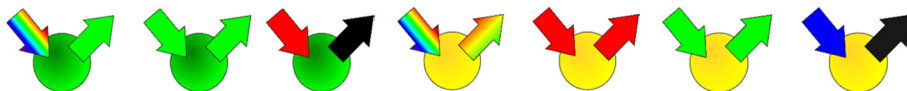
ODRAZ SVĚTLA OD BAREVNÝCH PŘEDMĚTŮ

Jak se stane, že vidíme červené rajče a zelenou okurku? Na okurku dopadá světlo všech barev. Abychom před sebou viděli zelenou, musí do našich očí dopadat jen zelené světlo. Povrch okurky tedy ze všeho dopadajícího světla odráží jen zelenou. Ostatní barvy, červenou a modrou, pohlcuje a neodráží je.

Červené rajče odráží červenou a pohlcuje zelenou a modrou. Žlutá pampeliška se nám zdá žlutá. Proto musí do našich očí odrážet ty barvy, které nám v mozku vytváří žlutou. Těmi jsou červená spolu se zelenou.

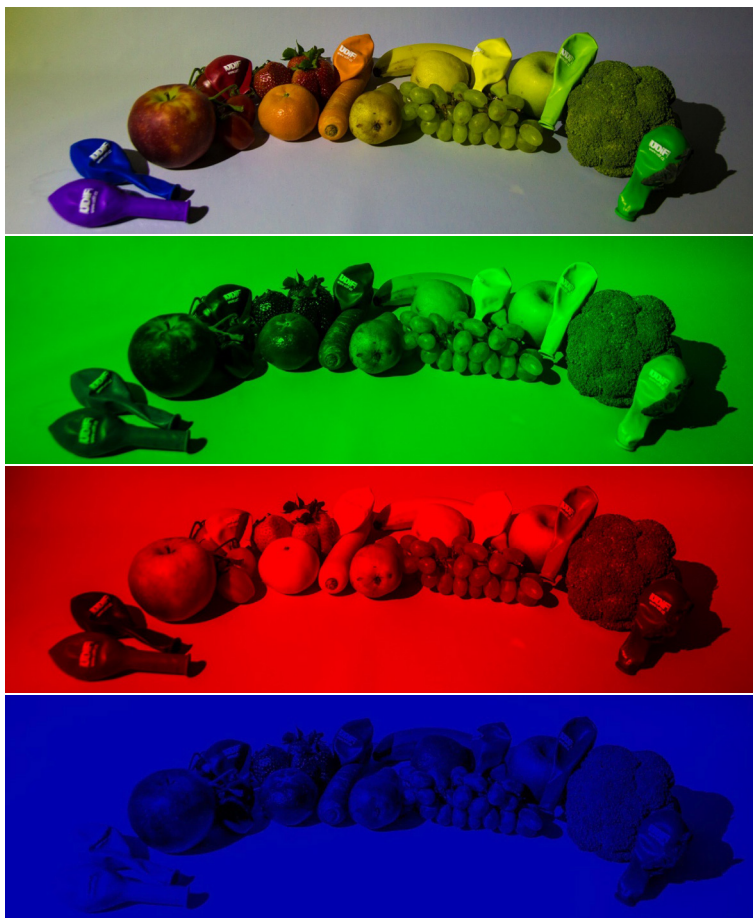
Bílé předměty musí odrážet světlo jakékoliv barvy. Čím více světla předmět odráží, tím světlejší se nám zdá. Funguje to i naopak. Černé předměty všechno světlo pohlcují a žádné neodráží.

Tato jednoduchá pravidla si můžeme vychutnat, když ve tmavé místnosti začneme svítit barevnými světly na barevné předměty. Pokud předmět barvu našeho světla odráží, bude se nám zdát světlý, jasný. Pokud ale tuto barvu pohlcuje a neodráží, uvidíme ho tmavý až černý.



Obr. 6: Odraz různých světél od zeleného a žlutého míčku

Červená paprika bude pod červeným světlem zářivě jasná, ale pod modrým a zeleným světlem ztmavne. Žlutý banán bude světlý pod zeleným a červeným světlem. V modrém světle bude ale tmavý. Samostatnou kapitolou je nechat děti třídit lentilky podle barev pod barevným osvětlením.

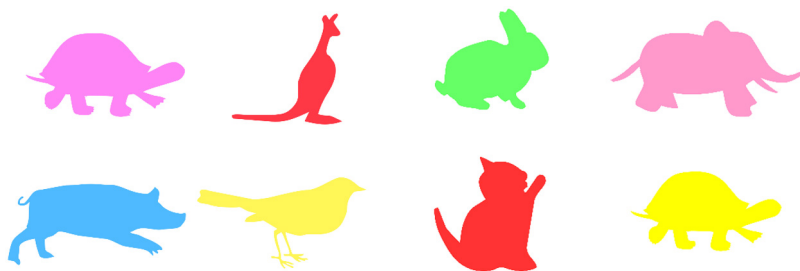


Obr. 7: Pohled na svět pod zeleným, červeným a modrým světlem

Pokud nemáte možnost zatemnění, můžete se zkusit na barevné předměty podívat přes barevné filtry nebo folie. Přes červenou folii projde jen červené světlo a přes modrou jen modré. Červené jablko odráží jen červené světlo. Při pohledu přes červenou folii se tedy bude jevit světlé, ale za modrou folií bude tmavé.

V semináři svítíme jasným barevným světlem na nápis Y/A na bílém papíře. Bílý papír musí odrážet každé světlo, kterým na něj posvítíme. Červené písmeno ale odráží jen červenou a modré jen modrou. Pokud papír nasvítíme červeným světlem, papír ho odrazí a bude se nám zdát červený. Červené písmeno na červeném papíře zmizí. Modré písmeno ale červenou pohlcuje. Bude se nám zdát černé a na červeném papíře bude dobře vidět. Když vyměníme červené světlo za modré, písmena se vystřídají.

Barevnými světly můžete také svítit na barevně tisknutá zvířátka na bílém papíře. Je potřeba vyladit barvu tisku, aby odpovídala barvě vašeho světla (každá barevná tiskárna to bude mít trochu jinak), ale pokud se vám podaří světlo a tisk sladit, získáte hezký efekt. Děti mohou zkoumat, pod kterou barvou světla jim mizí různě barevná zvířata. Zdrojům barevného světla věnujeme samostatnou část.



Obr. 8: Barevná zvířátka

JAK VNÍMAJÍ BARVY ZVÍŘATA

Oko každého druhu živočichů se vyvinulo jiným způsobem. Například pes nebo kočka mají pouze dva druhy čípků, v zelené a modré oblasti. Svět je pro ně tedy spíše modrozelený a pokud se dívají na červený míček, vidí ho jako černý. Dávejte si proto pozor, jakou barvu míčku házíte svému miláčkovi do zelené trávy.

Jsou druhy, kterým se barevné vnímání vytvořilo ještě širší, než má člověk. Některý hmyz nebo ptáci, kupříkladu včela a kolibřík, vidí až do blízké ultrafialové oblasti, které člověk přiřadit barvy neumí. Obrázek 10 ukazuje, jak bychom si jejich svět mohli představit.



Obr. 9: Fotografie louky, jak ji vidí člověk (vlevo) a pes (vpravo)



Obr. 10: Květina, jak ji vnímá člověk (vlevo) a kolibřík (vpravo)

Druh, který vidí svět nejbarevněji, nenajdete v říši savců. Jedná se o langustu (strašek kudlankový) žijící na korálových útesech. Její oči mají až 16 světlocitlivých druhů buněk.

MÍCHÁNÍ SVĚTEL RGB

Míchání barev máme ze zkušenosti spojené s mícháním barviv a pigmentů. Naše zkušenost velí, že pokud smícháme dvě barvy dohromady, výsledkem je tmavší barva. Proto také malíři používají k míchání světlé barvy a hlavně spoustu bílohy.

Míchání světél je ale pravým opakem této zkušenosti. Pokud přes sebe přeložíme dva světelné kužely, výsledkem musí být více světla a tedy světlejší barva. Opět to budeme popisovat tak, jak to vidí naše oči a interpretuje náš mozek. K míchání světél budeme používat barvy, které většina z nás zná jako základní – červenou, modrou a zelenou. V angličtině Red, Green a Blue, tedy RGB.

Pokud do jednoho místa svítí modré a červené světlo a odráží se do našich očí, musí nám v očích podráždit modré a červené čípky a my uvidíme purpurovou barvu neboli magentu.

Pokud takto přeložíme přes sebe červené a zelené světlo, v oku dojde k podráždění červených a zelených čípků a my uvidíme žlutou. Modré a zelené světlo vytvoří na zdi modrozelenou barvu.



Obr. 11: Míchání světél RGB – červená, zelená a modrá

Tam, kde se překrývají všechna tři světla, vznikne oblast, ze které do našich očí dopadá červené, zelené i modré světlo. Naše oči tuto plochu uvidí jako bílou. Opět připomínáme, že takto funguje míchání světél, nikoliv míchání barviv. Pokud bychom smíchali červenou, zelenou a modrou temperu, získáme hodně tmavou až černou barvu.

Tímto způsobem míchají barvy téměř všechny barevné displeje, ať už v televizi, na monitoru u počítače nebo ve vašem mobilním telefonu. Každý pixel sestává ze tří svítících plošek – červené, zelené a modré. Jas těchto plošek se mění podle toho, jakou výslednou barvou má pixel svítit.

To, že se v barevných displejích používá právě červená, zelená a modrá, má samosebou příčinu právě v tom, jak vidí naše oko. Pokud si naše oči skládají barvy z těchto tří základních barev, nedává žádný smysl používat v displejích jakékoliv jiné barvy. Volba červené, zelené a modré je dána tím, že se na displej dívají lidé. Jiní živočichové ale nemusí mít stejný barvocit. Například pes nebo kočka vidí pouze ve dvou barevných kanálech (modrá a žlutá), červené pixely by jim tak byly k ničemu.

ZDROJE BAREVNÉHO SVĚTLA

V této části představíme několik možností, jak získat pro výuku zdroje barevného světla.

Barevné filtry představují nejprostší cestu, jak z bílého světla odříznout jen ty barvy, které chceme. My používáme osvětlovačské filtry firmy LEE Filters.

Jsou dostupné v mnoha barvách a velikostech. Důležité je ale hlavně to, že jejich katalog obsahuje také spektrum filtru. Můžeme si tedy přesně vybrat, které barvy má filtr propouštět a které ne. V Česku je dodává například firma Prodance, jejíž eshop zobrazuje u filtrů také jejich spektra. Pro naše účely jsou vhodná tato katalogová čísla a jména filtrů:

Červená: č. 029, název „Plasa red“

Zelená: č. 139, název „Primary green (světlejší)“

Modrá: č. 716, název „Mikkel blue“

Žlutá: č. 101, název „Yellow“

Tyrkysová: č. 116, název „Medium blue-green“

Magenta: č. 797, název „Deep purple“

Tyto filtry můžeme nalepit například na kapesní svítilnu, přes ledku telefonu nebo na lampičku. Získáme tak zdroj světla konkrétní barvy. Nevýhodou ovšem je fakt, že pro různé barvy musíme měnit filtry nebo používat více zdrojů světla.

RGB LED neboli barevné ledky jsou druhou možností. Za nevelké peníze můžete pořídit RGB barevný ledkový pás i s dálkovým ovládáním, pomocí kterého můžete nastavovat barvu, kterou ledky svítí. Existují i kompaktní provedení RGB ledek, která lze zašroubovat do stolní lampičky a barvu také ovládat dálkovým ovladačem.

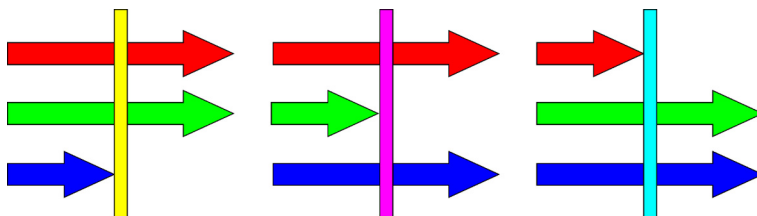
Osvětlovací technika je profesionální varianta v řádu vyšších stokorun. Jedná se o efektová barevná světla pro osvětlování divadel a koncertů. Tato cesta je komplikovanější na řízení barev, které je možné pomocí přepínačů přímo na světle nebo dálkovým řízením z osvětlovacího pultu. Pokud chcete se světlem a barvami provádět složitější věci, tato cesta se vyplatí. Pokud chcete pouze smíchat barevná světla a posvítit si barevným světlem na ovoce, doporučujeme kterékoliv jednodušší řešení.

BAREVNÉ TISKÁRNY A CMYK

Barevná tiskárna nepoužívá k tisku červenou, zelenou a modrou. Tisk na nás totiž nesvítí, ale naopak odebírá světlo, které se odráží od bílého papíru. Když jsme míchali světla, vznikala nám vždy světlejší barva. Tiskárna ale vrství pigmenty (barviva), takže nám musí vznikat tmavší barva. Proto v tiskárně musíme používat světlejší barvy. Tedy filtry, které propouští více barev.

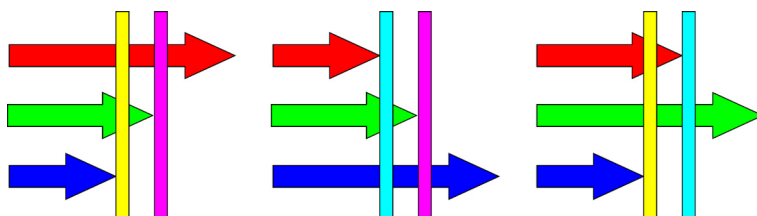
Tiskárny používají žlutou, tyrkysovou a magentu (v angličtině Cian, Magenta a Yellow, tedy CMY). To jsou právě ty, které získáme mícháním červeného, modrého a zeleného světla. Pokud se v tomto textu už orientujete, mělo by být jasné, jak se z nich získají ostatní barvy. Ukážeme si to opět na barevných osvětlovacích filtrech.

Přes žlutý filtr projde červené a zelené světlo, modré světlo se pohltí. Přes magentový filtr projde modré a červené světlo, ale zelené se pohltí. Přes tyrkysový filtr projde jen zelené a modré světlo.

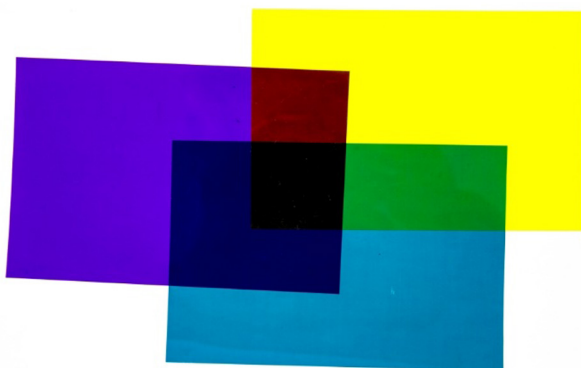


Obr. 12: Průchod světla přes barevné CMY filtry

Položme nyní dva filtry přes sebe. Vyberme například filtr žlutý a magentový. Přes žlutý filtr projde červená a zelená. Přes magentový filtr projde červená a modrá. Přes oba filtry tedy může projít jen červené světlo. Když tyto filtry položíme přes sebe, uvidíme červenou. Ostatní barvy si určitě zvládnete takto rozebrat sami.



Obr. 13: Průchod světla přes dva barevné CMY filtry



Obr. 14: Pohled přes osvětlovačské CMY filtry: tyrkysový, žlutý a magentový

AFTERIMAGE

Anglické slovo *afterimage* (česky bychom přeložili jako následný obraz) je efekt, který pozorujeme, pokud se podíváme do příliš jasného zdroje světla. Například do žárovky nebo do slunce. Jde o ony barevné mžítiky před očima, které nám chvíli zůstávají v zorném poli. Jejich původ je daný tím, jak oko detekuje světlo na molekulární úrovni.

Jak vlastně čípky v naší sítnici reagují na světlo? V čípku jsou molekuly rodopsinu (opět jsou tři druhy rodopsinů). Pokud tato molekula pohltí světlo, překloupí se její tvar mezi stavy, které chemici popisují jako *cis* a *trans*. Jednoduše si to můžeme představit jako plíšek, ve kterém to lupne a přeskočí. V *trans* stavu molekula setrvá po krátkou dobu a během této doby nemůže pohltit další světlo. Po uplynutí této relaxační doby se překloupí nazpět do stavu *cis* a může opět vidět. Tyto vlastnosti nyní začneme využívat a zneužívat.

Představme si, že se upřeným zrakem díváme na modře svítící displej. V našich očích se spotřebovává modrý rodopsin. Když se pak podíváme na bílou zeď, měli bychom vnímat, červené, zelené a modré odražené světlo stejně jasně. Modré světlo teď ale nemáme jak a čím vnímat. Proto před sebou na zdi uvidíme *afterimage* – obdélník červeného a zeleného světla, tedy žlutý obdélník.

Pokud tento efekt chcete dotáhnout k dokonalosti, je dobré se naučit základní manipulaci s obrázkem v počítači. Nejprve potřebujete hodně barevný přehledný obrázek. Výborné jsou vlajky, my používáme obrázek babočky pavího oka nebo letícího papouška. Z tohoto obrázku vytvoříme dvě verze. První bude ta, na kterou se budeme upřeně dívat. Ta má spotřebovat rodopsin těch barev, které pak v *afterimage* nechceme vidět. Potřebujeme tedy z našeho původního obrázku vytvořit negativ (některé editory to nazývají inverze barev). V tomto negativu také potřebujeme mít něco, na co se naše oči zafixují, aby netékaly (náhodné pohyby očí by *afterimage* rozmazaly). Stačí malý puntík kontrastní barvy uprostřed obrázku.

Už takto by *afterimage* fungoval při pohledu na bílou zeď. Efekt ale ještě vylepšíme zvýšením kontrastu. Druhý obrázek, který k tomu použijeme, bude černobílá verze původního obrázku (některé editory tomu říkají *desaturace*). Černobílý obrázek nám dodá kontrast a kontury a *afterimage* v naší sítnici vytvoří dojem barev, které ale v obrázku, na který se díváme, vůbec nejsou.

Při provedení se studenty doporučujeme nechat je hledět na negativ alespoň deset sekund (čím déle, tím lépe). Efekt je také lepší když se dívají z tmavé místnosti na jasný obraz. Hezky funguje i opakované provedení pokusu, kdy požádáme část žáků, aby při promítání negativu zavřeli oči a otevřeli je až na černobílou verzi. Tito žáci ověří, že nepodvádíme a opravdu promítáme černobílý obrázek a nikoliv animaci. Hezké je, že v tu chvíli máte část studentů, která je nadšená právě proto, že pro ně efekt nefunguje.



Obr. 15: Původní obrázek motýla



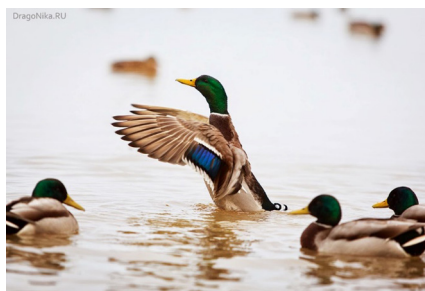
Obr. 16: Černobílý obrázek motýla



Obr. 17: Negativ obrázku motýla s invertovanými barvami

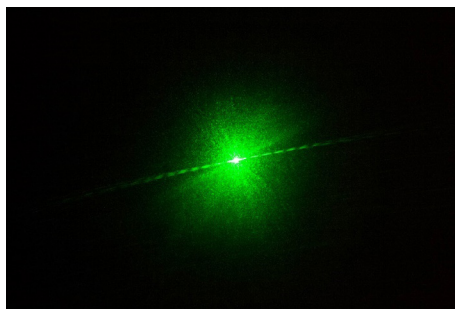
BARVY VZNIKLÉ OHYBEM SVĚTLA

Světlo se na jemné struktuře chová zvláště a jeho chování popisuje vlnová optika. Na drobných strukturách se světlo může ohýbat (difrakce) a skládat (interference). Tak nám příroda vytváří duhu, a dokonce toho využívají i zvířata. Například kachní peří nebo křídla motýlů, ba dokonce i měnivé barvy chameleona jsou toho krásným příkladem.



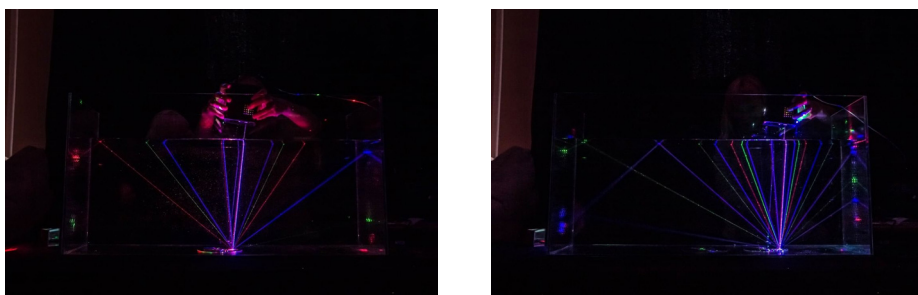
Obr. 18: Difrakce v říši zvířat

O vzniku difrakce a interference zde mluvit obsáhle nebudeme, ale zaměříme se na běžně pozorovatelné jevy. Nejsnáze dostupné budou pro většinu čtenářů vlasy nebo chlupy na rukou na které sviťte laserem. Jsou dost tenké na to, abyste na nich difrakci laseru nebo vzdáleného bodového zdroje světla viděli. Očekávejte tenké dlouhé pruhy světla. Na menší, tenčí překážce je difrakce výraznější a čáry budou vzdálené od sebe dál. Můžete tak zjistit, zda je silnější vlas nebo chlup. Hezkou difrakci nabídne také velké množství různých tkanin. Například gáza, organza, hedvábí, silonky a podobně. Na to opět můžete svítit laserem nebo se skrz ně můžete dívat na vzdálené bodové zdroje, třeba pouliční lampy.



Obr. 19: Difrakce laserového paprsku na vlasech

Podrobněji se zastavíme u CD, DVD a BlueRay. Nechejte laserový paprsek odrazit od datového povrchu disku a na zdi pozorujte odražená interferenční maxima. Můžete si všimnout, že maxima jsou u CD blíže a u DVD dále. Na DVD se vejde násobně více dat, struktura datového zápisu je tak mnohem jemnější a jemnější struktura poskytuje výraznější difrakci. Efektní je ukázat difrakci laserového světla na CD a DVD v mírně zakaleném akváriu.



Obr. 20: Difrakce RGB laseru na DVD (vlevo) a CD (vpravo)

Malou štěrbinu si můžete vyrobit i pomocí tří svých prstů. Tady už nepracujeme s laserem, ale můžeme se dívat na libovolné bodové zdroje světla, například vzdálené pouliční lampy, LED a podobně. Dáte-li palec, ukazováček a prostředník k sobě, vznikne vám mezi nimi malý trojúhelníkový otvor. Sevřením prstů můžete otvor zmenšovat a pozorovat difrakci na něm. Difrakce si ostatně můžete všimnout už jen, když přivřete oči.

Profesionálněji se můžete na difrakci podívat skrze difrakční folii. Můžete ji pořídit ve specializovaných obchodech, spíše však ve větším množství. My ji kupujeme v Edmund Optics ve variantě lineárních vrypů v počtu 500 vrypů na milimetr nebo 1 000 vrypů na mm. Můžete ji tedy získat v předprodeji v malém množství u nás. Případně se s ní můžete potkat na hvězdárnách, kde je součástí difrakčních brýlí. Tam bývá většinou čtvercová mřížka, která není tak moc vhodná na výrobu spektroskopu, ale dělá větší efekty.

BARVY VZNIKLÉ ROZPTYLEM

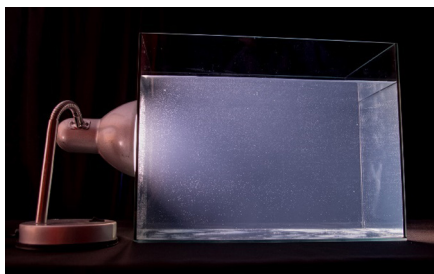
Existuje ještě jeden způsob, jak si příroda tvoří barvy. Rozptyl. Právě ten je totiž zodpovědný za to, že se naši planetě říká „modrá“ planeta. Rozptyl barví mraky na bílo, oblohu na modro a některým zvířatům barví na modro i srst.



Obr. 21: Rozptylová modrá v říši zvířat

Rozptyl vzniká, když světlo dopadne na malé částice. Pokud jsou částice vhodné velikosti, vznikne tzv. Rayleighův rozptyl. Intenzita světla je silně závislá na vlnové délce světla, a to se čtvrtou mocninou ve jmenovateli. Mnohem více se při něm proto rozptylují krátké vlnové délky.

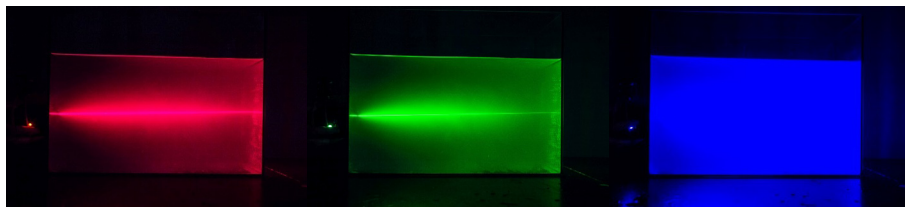
Ve vzduchu vzniká Rayleighův rozptyl na náhodných shlucích molekul, které mají pro něj tu správnou velikost. Na kapičkách vody v mracích se již mluví o Mieově rozptylu, protože na Rayleighův rozptyl jsou příliš velké. Všechny vlnové délky se při něm rozptylují stejně a my vidíme oblaka bílá.



Obr. 22: Namodralá barva světla v mléčné vodě

Dětem můžete Rayleighův rozptyl ukázat jednoduše v akváriu. Do vody přidejte pár malých kapiček mléka, raději ale méně, než více. Do akvária posvítte skrz celou délku lampičkou a pozorujte, že voda se zbarvila u lampičky více do modra a dál od lampičky odmodrává a je tedy více červená. To je právě případ červánků, kde je slunce nízko u obzoru a prochází tlustou vrstvou atmosféry.

Do akvária můžete přidat více mléka a sledovat případné změny. Hezké je také ukázat rozptyl pomocí červeného, zeleného a modrého laseru. Modrý laser se rychle rozptýlí a nedojde v akváriu nijak daleko. Červený laser naproti tomu projde bez výrazného rozptylu až na konec.

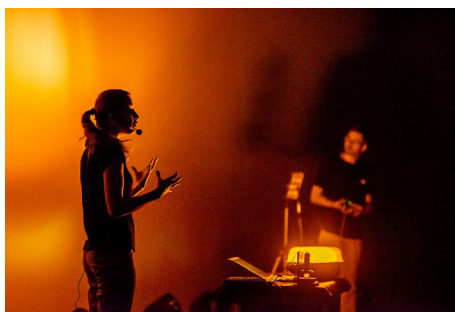


Obr. 23: Rozptyl laseru v akváriu.

Více o rozptylu se můžete dozvědět včetně popsanych experimentů ve videu z cyklu Badatelna: <https://youtu.be/theWxcqn3jg>.

JEDNOBAREVNÉ VIDĚNÍ

Velmi speciálním zdrojem světla je méně využívané pouliční světlo nízkotlaké sodíkové výbojky. V Čechách je vidět zřídka na některých úsecích dálnic. Její bezkonkurenční výhodou je největší účinnost ze všech světelných zdrojů. Mnohem zajímavější je ale její spektrum tvořené pouze dvěma velmi blízkými čarami, tzv. sodíkový dublet. Jedná se proto o jednobarevné světlo a pokud se podíváme na svět v této sodíkové barvě, úplně ztratíme vjem barev kolem nás.



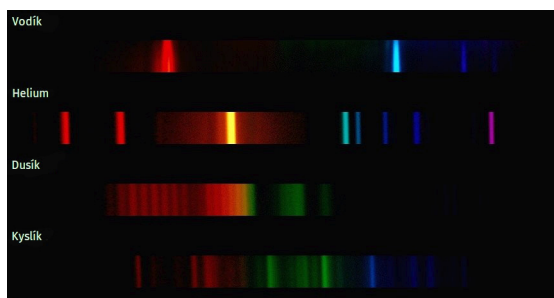
Obr. 24: Světlo sodíkové výbojky

SPEKTRA

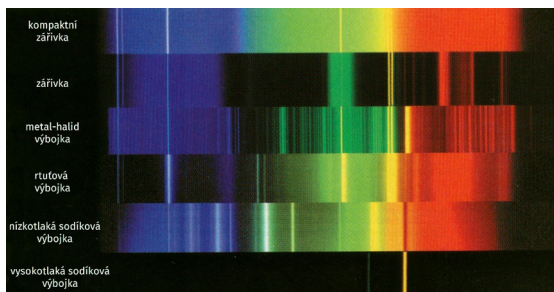
Pomocí CD nebo difrakční folie si můžeme s žáky postavit vlastní jednoduchý spektroskop a pozorovat spektra různých zdrojů světla. Pro představu také přikládáme fotografie spekter různých světelných zdrojů a několika výbojů v plynech.

Spektrum žárovky je nejvíce podobné spektru slunečnímu a bude vypadat jako plná duha. Tak vypadají všechny zdroje světla, které svítí, protože jsou horké. Zářivkám i bílým LED některé části duhy chybí v závislosti na tom, jaký mají na sobě luminofor. LED konkrétních barev v sobě obsahují jen užší pásy těchto barev a kdybyste se dívali na odraz laseru, uvidíte jen jednu vlnovou délku, jednu jedinou čáru.

Spektra nám také hodně vypovídají o tom, jaké atomy svítí. Každý atom vyzařuje konkrétní energie a ve světle to vidíme jako spektrální čáry. Je to jedinečný znak atomů a můžeme je podle toho snadno poznat i ve vzdálených hvězdách.



Obr. 25: Spektra výbojů v plynech

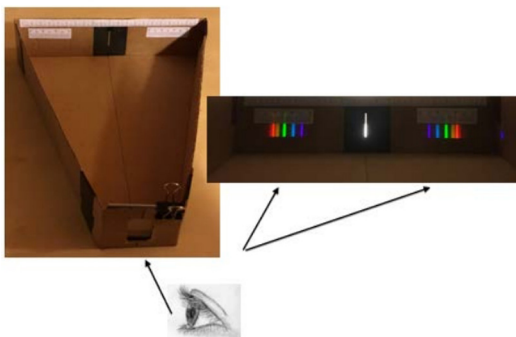


Obr. 26: Spektra světelných zdrojů pouličního osvětlení

S mladšími dětmi si můžete vyrobit velmi jednoduše difrakční brýle. Skrz ně mohou žáci pozorovat různé zdroje světla zábavně, ale zároveň mohou pozorovat, jak spektra zdrojů vypadají, a mohou přes ně udělat velmi pěkné fotografie. Doporučujeme na to dobu Vánoc, kdy o různá světýlka není nouze. Můžete se inspirovat naší verzí brýlí, která je tvořená jednoduchými obroučkami a uchycené jsou pouze pružným provázkem.

Sofistikovanější a vědecktější je s dětmi vyrobit spektroskop. Nejjednodušší a asi i nejdostupnější je verze z CD a papírové krabičky se štěrbinou. Návod na papírovou krabičku kolující doslova všemi internety, také přikládáme. Krabičku je dobré vytisknout na černý papír nebo počernit. Veškeré parazitní světlo mimo štěrbinu výsledek kazí.

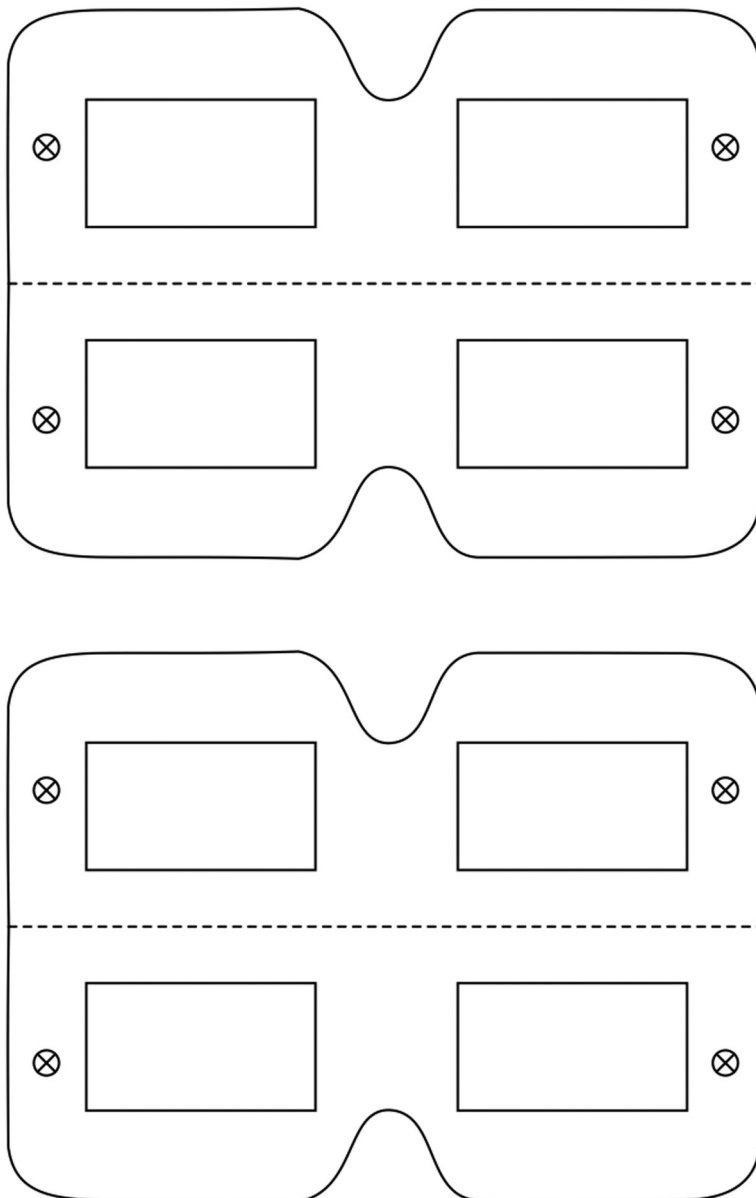
Verze spektroskopu, která zaujala nás, je od pana Václava Pazdery, který jej sdílel na dílnách konference Heuréky. Šablona se vystřihne z tvrdého papíru, ještě ideálnější je výroba z kartonu. Dále se složí do jakési otevřené krabice, ve které se z jedné strany před slepením krabice udělá tenká štěrбина. Z druhé strany se do vystřiženého okénka vlepi difrakční folie 500 vrypů na mm. Výhodou této konstrukce je, že ji můžete zkalibrovat podle známé vlnové délky laserového ukazovátka, které můžete folií prosvítit a na druhé straně si vyznačit stupnici. Ze spektrografu pak máte rázem spektrometr. A to už stojí za trochu námahy se sháněním difrakční folie.



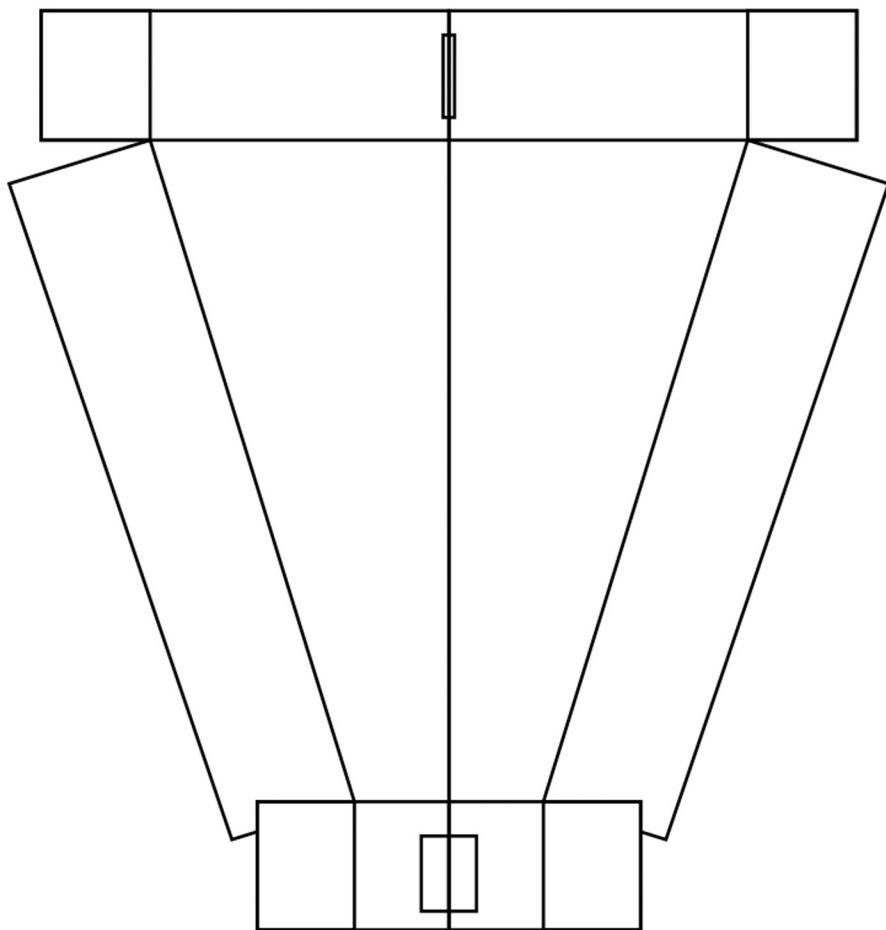
Obr. 27: Fotografie spektrometru Václava Pazdery. Zdroj sborník Heuréky 2016

PODĚKOVÁNÍ

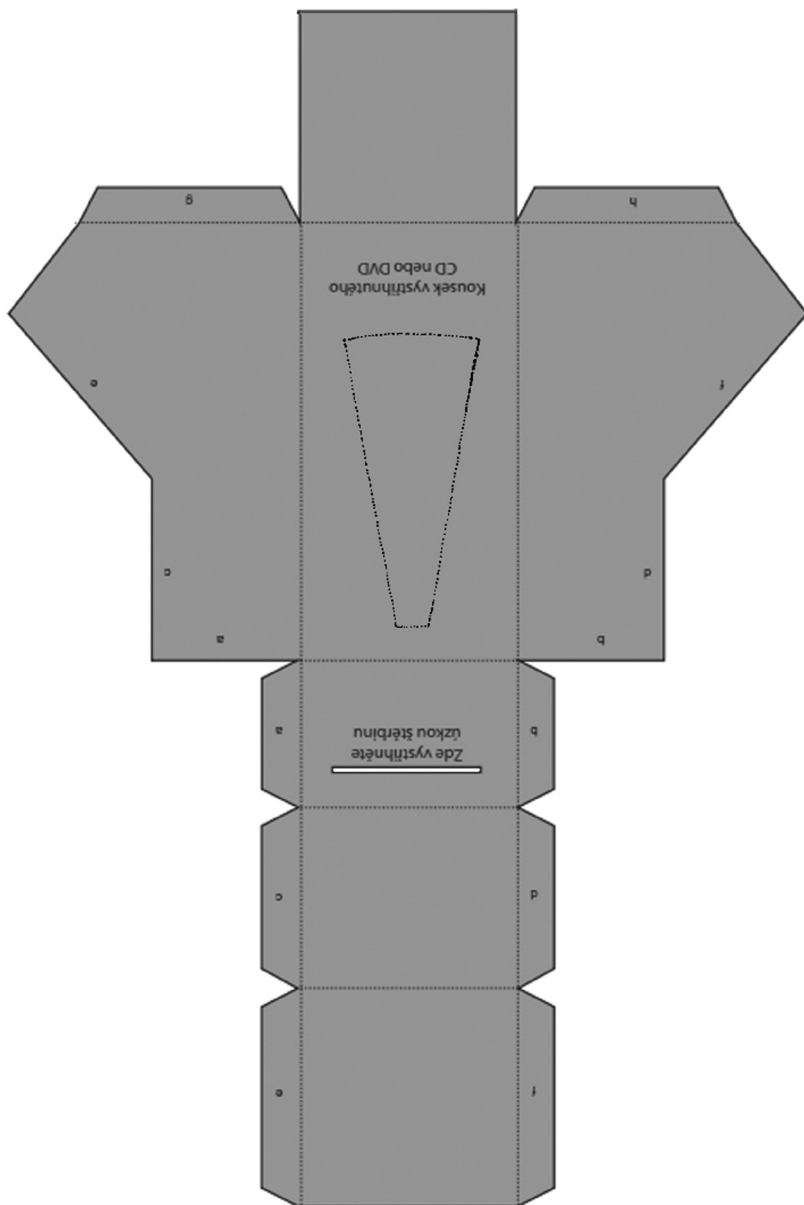
Tento materiál vznikl jako součást akreditovaných seminářů Divadla fyziky ÚDiF. Více o ÚDiFu se můžete dozvědět zde: <http://www.udif.cz>.



Obr. 28: Šablona difrakčních brýlí



Obr. 29: Šablona pro výrobu spektroskopu z difrakční folie



Obr. 30: Šablona pro výrobu spektroskopu z kousku CD nebo DVD

O VYUŽITÍ IRACIONALITY PŘI HLEDÁNÍ SEDMÉHO NEBE

Luboš Pick

ABSTRAKT

Věnujeme se problému V.I. Arnol'da, zda nějaká mocnina dvojky začíná číslicí sedm. Uvedeme dvě různá řešení problému a zmíníme se o některých souvisejících otázkách a možnostech zobecnění.

KLÍČOVÁ SLOVA: Arnol'dův problém, sedmé nebe, dekadický zápis čísla, mocnina dvojky, logaritmus, iracionální číslo, celá část reálného čísla.

FORMULACE PROBLÉMU

V tomto článku budeme symboly $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ a $\mathbb{R}$ označovat po řadě množinu přirozených, celých, racionálních a reálných čísel. Funkce $\log$ bude označovat *dekadický* logaritmus, tedy funkci $\log_{10}$.

Vyjdeme z jednoho zajímavého problému, který ve své knize [1] uvádí velký ruský matematik Vladimir Igorevič Arnol'd. Problém se v různých modifikacích vyskytuje porůznu v matematické literatuře. Mně jsou známy například ještě zdroje [2] a [3], výčet však jistě zdaleka není úplný. Pravděpodobně první podrobné řešení uvádí Paweł Strzelecki v článku [3]. Téma později moc pěkně zpracoval Jirka Bouchala v přednášce na semináři OSMA [4].

Problém. *Posuďte posloupnost mocnin dvojky*

$$\{2^0, 2^1, 2^2, 2^3, \dots, 2^n, \dots\},$$

tedy přesněji

$$\{1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, \dots\},$$

a všimějme si jen prvních číslic. Dostaneme pozoruhodnou posloupnost

1, 2, 4, 8, 1, 3, 6, 1, 2, 5,
1, 2, 4, 8, 1, 3, 6, 1, 2, 5,
1, 2, 4, 8, 1, 3, 6, 1, 2, 5,
1, 2, 4, 8, 1, 3, 6, 1, 2, 5, ...

Označme tuto posloupnost symbolem $\{c_n\}_{n=0}^\infty$. Otázka zní: objeví se v této posloupnosti sedmička?

Na první pohled se zdá (a naše grafické uspořádání tomuto pohledu na věc vydatně napomáhá), že posloupnost je periodická se základní periodou 10. Kdyby tomu tak opravdu bylo, odpověď na otázku by byla triviálně záporná a problém by byl vyřešen. My zatím ale nevíme s jistotou, zda tomu tak opravdu je. Mnohý příklad známe, kdy několik prvních členů určité posloupnosti vede ke klamnému závěru. Jen v článku [5] najdeme takových příkladů pětatřicet.

Ve skutečnosti bychom mohli zformulovat hned několik otázek. Například:

- (a) Je posloupnost opravdu periodická s periodou 10?
- (b) Obsahuje sedmičku?
- (c) Pokud ano, kolikrát?

Abychom celé věci dopřáli smysluplný matematický rámec, zavedeme nový pojem.

Definice. Množinu

$$\mathbb{N}_7 = \{m \in \mathbb{N} \cup \{0\} : \text{první cifra čísla } 2^m \text{ je rovna } 7\}$$

nazveme *sedmým nebem*.

HRUBÁ SÍLA

Jeden z možných postupů, jak se rychle a bez skrupulí dobrat odpovědi na naše otázky, uvádí na diskusním fóru Mathematics Stack Exchange ve svém příspěvku [6] osoba skrývající se pod identifikátorem P. Vanchinathan. Na stránce dále nalezneme rozsáhlou diskusi k problému, k jeho původu, aplikacím i řešení. Řešení uvedeme ve třech krocích.

První krok: Násobme či mocněme dostatečně dlouho a doufejme, že se vytoužená sedmička v dohledné době objeví. Kupodivu nám tato na první pohled

poněkud pošetilá taktika vyjde a ani to nebude trvat tak dlouho. Naše vytrvalost totiž bude odměněna již ve čtyřicátém šestém kroku, a to číslem

$$a = 2^{46} = 70\,368\,744\,177\,664.$$

Odtud hned plyne, že množina $\mathbb{N}_7$ je neprázdná. To znamená, že odpověď na otázku (b) je kladná a odpověď na otázku (a) musí být záporná. Navíc je teď dobře vidět, proč jsme si ve výše uvedené tabulce nemohli dovolit uvést pátý řádek. Zbývá ale ještě otázka (c).

Druhý krok: Nalezneme dvě další velmi užitečné mocniny dvojky, a to

$$b = 2^{10} = 1\,024 \quad a \quad c = 2^{53} = 9\,007\,199\,254\,740\,992.$$

K čemu nám budou tato čísla dobrá, uvidíme záhy.

Třetí krok: Poslední etapa je založena na pozoruhodné alternativě. Než přikročíme k její formulaci, bude užitečné si připomenout, že je-li $m \in \mathbb{N}_7$, potom má číslo 2^m alespoň dvě cifry. (Má jich ve skutečnosti alespoň čtrnáct, ale nám budou stačit dvě).

Větička. *Předpokládejme, že $m \in \mathbb{N}_7$. Jestliže je druhá cifra čísla 2^m prvkem množiny $\{0, 1, 2, 3, 4, 5, 6, 7\}$, pak $m + 10 \in \mathbb{N}_7$. Je-li druhá cifra čísla 2^m rovna 8, nebo 9, pak $m + 53 \in \mathbb{N}_7$.*

Důkaz.

Jestliže $m \in \mathbb{N}_7$ a druhá cifra čísla 2^m je prvkem množiny $\{0, 1, 2, 3, 4, 5, 6, 7\}$, potom existuje $j \in \mathbb{N}$, $j \geq 2$, takové, že

$$7 \times 10^j \leq 2^m \leq 7 \times 10^j + 8 \times 10^{j-1}.$$

Odtud vyplývá, že

$$7 \times b \times 10^j \leq 2^m \times b \leq 7 \times b \times 10^j + 8 \times b \times 10^{j-1},$$

to jest

$$7\,168 \times 10^j \leq 2^{m+10} \leq 7\,168 \times 10^j + 8\,192 \times 10^{j-1}.$$

Protože

$$1\,680 + 8\,192 < 10^4,$$

mají obě čísla stojící na mantinelech stejný počet číslic (přesněji $j + 3$) a na prvním místě jejich desetinného zápisu stojí sedmička. Členu uprostřed tudíž nezbyvá, než aby na tom byl stejně. Jinými slovy, $m + 10 \in \mathbb{N}_7$. Důkaz toho, že $m + 53 \in \mathbb{N}_7$ za předpokladu, že druhá cifra čísla 2^m je rovna 8, nebo 9, lze provést obdobně. $\square$

A nyní jednoduchou aplikací principu matematické indukce ukážeme, že sedmé nebe je nejen neprázdné, ale dokonce má nekonečně mnoho prvků.

Důsledek. *Sedmé nebe je bez konce.*

Důkaz.

Začneme u čísla $m_1 = 46$. Máme-li již zafixována všechna čísla

$$m_1, \dots, m_n \quad \text{pro nějaké } n \in \mathbb{N},$$

potom podle chování druhé cifry čísla 2^{m_n} položíme buď $m_{n+1} = m_n + 10$ (to když je druhá cifra menší nebo rovna sedmičce), nebo $m_{n+1} = m_n + 53$ (když je druhá cifra rovna osmičce nebo devítce). Tak získáme nekonečnou posloupnost prvků sedmého nebe. $\square$

Uvedeným postupem například zjistíme, že čísla 46, 56, 66, 76, 86 a 96 jsou prvky sedmého nebe (zase ta periodičita s desítkou?), výpočtem však lze ověřit, že 106 již jeho prvkem není. Zápis čísla 2^{96} ovšem začíná 79..., na druhém místě tedy stojí devítka, takže použijeme druhou možnost a dostaneme, že $96 + 53 = 149 \in \mathbb{N}_7$. Nejspíš takto nedostaneme všechny prvky sedmého nebe, ale na to se nikdo neptal. Každopádně je nyní zodpovězena otázka (c): sedmička se v posloupnosti vyskytuje nekonečněkrát.

ZHODNOCENÍ PRVNÍHO ŘEŠENÍ

Uvedený postup, jakkoli je nápaditý a elegantně jednoduchý, má několik nevýhod. Za prvé nám nic neříká o podstatě problému a za druhé jej nelze zobecnit. Mohly by nás totiž zajímat všelijaké modifikace naší základní otázky. Například bychom se mohli ptát, zda existují mocniny dvojky, jejichž dekadický zápis začíná nějakou předem stanovenou konečnou posloupností číslic. Z prvních čtyřiceti členů posloupnosti například není jasné, jestli se v ní někdy objeví devítka, konečnosc sedmé nebe se v angličtině označuje výrazem *cloud nine*. Tuhle otázku jsme zrovna náhodou vyřešili (pohledme znovu na 2^{53}), ale mohlo by nás kupříkladu zajímat, jestli zápis některých mocnin dvojky začíná výrazem 77, nebo třeba nějakým naším oblíbeným letopočtem. A také na světě není jen dvojka, můžeme vesele mocnit i jiná přirozená čísla, řekněme větší než 1.

Ukazuje se, že i na takové otázky umíme nalézt odpověď, ale musíme na to jít jinak.

HLEDÁNÍ NOVÝCH CEST

Položme si otázku, co to vůbec znamená, že nějaké číslo padne do sedmého nebe. Není těžké si uvědomit, že $m \in \mathbb{N}_7$ právě tehdy, když existuje $k \in \mathbb{N}$ takové, že

$$7 \times 10^k \leq 2^m < 8 \times 10^k.$$

Tuto dvojici nerovností (takzvaný sendvič) nyní zlogaritmuje. To znamená, že na všechny strany vypustíme funkci $\log$ (která je rostoucí, a tedy se nerovnosti nezmění), a dostaneme tak

$$\log 7 + k \leq m \log 2 < \log 8 + k,$$

to jest

$$\log 7 \leq m \log 2 - k < \log 8.$$

Nyní přicházíme ke klíčovému pozorování. Protože $0 < \log 7 < \log 8 < 1$, plyne odtud, že

$$m \log 2 - k \in (0, 1).$$

To je ale možné jedině tehdy, když je k takzvanou *celou částí* čísla $m \log 2$, což obvykle zapisujeme ve tvaru

$$k = [m \log 2].$$

Připomeňme, že celá část reálného čísla x je definována jako (jediné) celé číslo j splňující $j \leq x < j + 1$. Pak tedy píšeme $j = [x]$.

MAGICKÁ POSLOUPNOST

Jsouce vyzbrojeni operací celé části reálného čísla, podívejme se teď na chování jedné zajímavé posloupnosti. Mějme nějaké pevně stanovené reálné číslo x a definujme posloupnost reálných čísel $\{a_n\}$ předpisem

$$a_n = nx - [nx] \quad \text{pro } n \in \mathbb{N}.$$

Následující pozorování není těžké.

Větička. (a) Je-li $x \in \mathbb{Z}$, pak $\{a_n\} = \{0, 0, 0, \dots\}$.

(b) Je-li $x \in \mathbb{Q}$, pak $\{a_n\}$ je periodická posloupnost. Je-li navíc $x = \frac{p}{q}$, kde $p \in \mathbb{Z}$ a $q \in \mathbb{N}$, pak q je periodou posloupnosti $\{a_n\}$.

Důkaz.

Tvrzení (a) je triviální. Pro důkaz tvrzení (b) předpokládejme, že $x = \frac{p}{q}$, kde $p \in \mathbb{Z}$ a $q \in \mathbb{N}$. Potom pro každé $n \in \mathbb{N}$ platí

$$\begin{aligned} a_{n+q} &= (n+q) \frac{p}{q} - \left[(n+q) \frac{p}{q} \right] = n \frac{p}{q} + p - \left[n \frac{p}{q} + p \right] \\ &= n \frac{p}{q} + p - \left[n \frac{p}{q} \right] - p = n \frac{p}{q} - \left[n \frac{p}{q} \right] = a_n, \end{aligned}$$

a tedy $\{a_n\}$ je periodická s periodou q . □

Větička nám ovšem neřekla to nejzajímavější.

Otázka. Jak se chová posloupnost $\{a_n\}$ pro *iracionální* x ?

Odpověď na tuto otázku je jádrem tohoto článku. Následující věta bývá připisována Wacławu Sierpinskému, Hermannu Weylovi či Piersu Bohlovi a jako letopočet, ve kterém ji uvedení pánové dokázali nezávisle na sobě, bývá uváděn rok 1910. Obecnější formu věty nalézáme též v pozdější práci Georga Davida Birkhoffa z roku 1931.

Věta. *Nechť $x \notin \mathbb{Q}$. Potom $\{a_n\}$ je prostá a navíc pro každá $\alpha, \beta \in [0, 1]$ splňující $\alpha < \beta$ je množina $\{a_n\} \cap (\alpha, \beta)$ nekonečná.*

Důkaz.

Dokážeme nejprve, že posloupnost $\{a_n\}$ je prostá. Předpokládejme, že pro nějaká $m, n \in \mathbb{N}$ platí $a_n = a_m$. Potom

$$nx - [nx] = mx - [mx],$$

tedy

$$(n - m)x = [nx] - [mx].$$

Zřejmě platí $[nx] - [mx] \in \mathbb{Z}$, a tudíž také $(n - m)x \in \mathbb{Z}$. To je ale díky iracionalitě čísla x možné jedině tehdy, když $n - m = 0$. Jinými slovy, pro m a n různá platí $a_m \neq a_n$, takže posloupnost $\{a_n\}$ je prostá.

Nyní obraťme pozornost ke druhé části tvrzení. Víme, že $\beta - \alpha > 0$, a tedy můžeme nalézt $n \in \mathbb{N}$ dost velké k tomu, aby

$$\frac{1}{n} < \beta - \alpha.$$

Uvažujme čísla $a_1, \dots, a_{n+1}$. Všechna tato čísla jsou prvky intervalu $[0, 1]$. Podle Dirichletova principu se tudíž mezi nimi najdou alespoň dvě, jejichž vzdálenost

nepřesáhne hodnotu $\frac{1}{n}$. Matematicky zapsáno to znamená, že existují $i, s \in \mathbb{N}$ taková, že $i, i + s \in \{1, \dots, n + 1\}$ a navíc

$$|a_i - a_{i+s}| \leq \frac{1}{n} < \beta - \alpha.$$

Označme $\varepsilon = |a_i - a_{i+s}|$. Potom tedy

$$0 < \varepsilon < \beta - \alpha.$$

Nyní si představme, že na kružnici K se středem v počátku a mající *délku obvodu* rovnou 1 (nejde tedy o klasickou jednotkovou kružnici, nýbrž o kružnici o poloměru $\frac{1}{2\pi}$) navineme reálnou přímkou jako na cívku, přičemž kladný směr uvažujeme proti směru hodinových ručiček. Navíc v některém bodě na kružnici vyznačíme bod 0. Ten pak tedy díky periodicitě zároveň reprezentuje body $1, 2, \dots$ a také $-1, -2, \dots$, neboli všechna celá čísla. Body α a β nanese tak, aby délka oblouku mezi nimi a bodem nula byla po řadě rovna jejich hodnotám.

Uvažujme zobrazení $f: K \rightarrow K$ definované jako otočení (v kladném směru) o úhel $2\pi x$ radiánů. Na kružnici definujeme dále posloupnost bodů $\{b_n\}_{n=1}^{\infty}$ rekursivním předpisem $b_n = f(b_{n-1})$, tedy

$$\begin{aligned} b_0 &= 0, \quad b_1 = f(0), \quad b_2 = f(b_1) = (f \circ f)(0), \dots, \\ b_n &= (f \circ \dots \circ f)(0) \quad (n\text{-krát složené zobrazení}) \text{ pro } n \in \mathbb{N}. \end{aligned}$$

Potom je délka oblouku mezi body b_n a 0 rovna hodnotě a_n . Speciálně mezi body b_i a b_{i+s} je rovna $\varepsilon < \beta - \alpha$. Odtud vyplývá, že zobrazení

$$f^s = f \circ \dots \circ f \quad (s\text{-krát složené zobrazení})$$

je otočení o $2\pi\varepsilon$ radiánů (v kladném, nebo v záporném směru). Každopádně při průchodu zobrazením f^s naší kružnici se oblouku mezi α a β nelze vyhnout, toto zobrazení jej nemůže přeskočit. Tedy po nějakém násobku s otoček se objeví bod b_n na oblouku mezi α a β . Všechny tyto body jsou různé, neboť posloupnost $\{a_n\}$ je prostá, jak jsme již dokázali. To znamená, že v (kladné části) oblouku mezi α a β se nachází nekonečně mnoho různých prvků množiny $\{b_s, b_{2s}, b_{3s}, \dots\}$. Z korespondence mezi posloupnostmi $\{a_n\}$ a $\{b_n\}$ tedy dostáváme, že v intervalu (α, β) se nachází nekonečně mnoho prvků množiny $\{a_s, a_{2s}, a_{3s}, \dots\}$, a tedy nekonečně mnoho členů posloupnosti $\{a_n\}$. Tím je důkaz hotov. $\square$

APLIKACE

Z věty uvedené v předcházejícím oddílu můžeme vyvodit řešení našeho problému. Jeho formulace nám sice cosi připomene (už to tu jednou bylo), ale tentokrát můžeme získané řešení rozličnými způsoby zobecňovat.

Důsledek. *Sedmé nebe je bez konce.*

Důkaz.

Položme

$$\alpha = \log 7, \quad \beta = \log 8 \quad \text{a} \quad x = \log 2.$$

Protože

$$1 < 7 < 8 < 10,$$

platí po aplikaci funkce $\log$

$$0 < \alpha < \beta < 1.$$

Připomeňme si důležitou okolnost, že číslo x je iracionální. Tento fakt pro jistotu ověříme. Předpokládejme pro spor, že $x = \frac{p}{q}$, kde $p \in \mathbb{Z}$ a $q \in \mathbb{N}$. Potom

$$2 = 10^{\frac{p}{q}},$$

to jest

$$2^q = 10^p$$

Pak ale díky jednoznačnosti prvočíselného rozvoje dělí číslo 5 pravou stranu poslední rovnosti, ale nikoli levou, a tedy dostáváme spor. Odtud plyne, že $x \notin \mathbb{Q}$. Aplikací věty z předchozího oddílu potom dostáváme tvrzení důsledku. $\square$

Poznámka. Na uvedeném postupu je zajímavé a elegantní to, že sedmička zde nehraje žádnou zvláštní roli. Zcela obdobně můžeme dokázat, že množina mocnin dvojky, jejichž dekadický zápis začíná posloupností 2 022, je nekonečná. A místo 2 022 lze dosadit téměř libovolný jiný shluk číslic.

Je načase uvést obecnou formulaci výsledku. Důkaz lze provést zcela obdobně výše uvedenému postupu.

Věta. *Nechť $p > 1$ je přirozené číslo, které není celočíselnou mocninou čísla 10, a X je nějaká konečná posloupnost číslic. Potom existuje přirozené číslo n takové, že desítkový zápis čísla p^n začíná posloupností X .*

ZÁVĚR

Položme si na závěr otázku, která je možná více filosofické, než matematické povahy.

Otázka. Proč se posloupnost tak dlouho jeví jako by byla periodická s periodou 10?

Odpověď je překvapivě jednoduchá. Tento jev je prostě způsoben tím, že číslo x , tedy

$$\log 2 = 0,301\,029\,995\,663\,981\,195\,213\,738\,894\,724\,49\dots,$$

je sice iracionální, avšak má velmi dobrou aproximaci v podobě zlomku $\frac{3}{10}$. Pak už si jen stačí připomenout druhou z našich větíček.

Poznámka. Z výše uvedeného se dá odvodit spousta dalších zajímavých informací. Označme kupříkladu pro $\alpha, \beta \in [0, 1]$, $\alpha < \beta$, a pro $n \in \mathbb{N}$

$$k(n, \alpha, \beta) = \#\{1 \leq i \leq n: a_i \in (\alpha, \beta)\},$$

kde symbol $\#$ označuje *počet prvků* za ním stojící množiny. Potom

$$\lim_{n \rightarrow \infty} \frac{k(n, \alpha, \beta)}{n} = \beta - \alpha.$$

Tedy: budeme-li se pravidelným krokem iracionální délky dostatečně dlouho procházet po obvodu kružnice, pak do každé jámy spadneme s frekvencí přímo úměrnou její velikosti. To zní skoro jako nějaké přísloví nebo pranostika. Lze odtud ale vyvodit zajímavý fakt. Pro $n \in \mathbb{N}$ označme

$$a(7, n) = \text{počet sedmiček v množině } \{c_1, \dots, c_n\}$$

a

$$a(8, n) = \text{počet osmiček v množině } \{c_1, \dots, c_n\}.$$

Potom

$$\lim_{n \rightarrow \infty} \frac{a(7, n)}{n} = \log 8 - \log 7 \quad \text{a} \quad \lim_{n \rightarrow \infty} \frac{a(8, n)}{n} = \log 9 - \log 8,$$

takže

$$\lim_{n \rightarrow \infty} \frac{a(7, n)}{a(8, n)} = \frac{\log 8 - \log 7}{\log 9 - \log 8} = 1,133\,7\dots > 1.$$

Ano, vidíte správně, mocniny dvojky dodržují Benfordův zákon. Tedy, mimo jiné, dost velké fragmenty posloupnosti $\{c_n\}$ budou obsahovat *více* sedmiček než osmiček, ač tomu prvních čtyřicet členů moc nenapovídá.

Poznámka do šatny. Jak už bylo řečeno, za číslo X si můžete pro radost dosadit například datum svého narození. Jak Paweł Strzelecki [3], tak i Jirka Bouchala [4] uvádějí tabulky takových příkladů. Zatímco v [3] nalézáme výběr dat významných historických událostí jako například založení polského státu, vítězství Jana III. nad Turky či bitvu u Waterloo, [4] obsahuje rozsáhlý seznam všech letopočtů od 1931 po 2005 včetně. Díky Jirkovi tedy vím, že desetinný zápis čísla 2^{187} začíná významnou posloupností 1961. Ovšem pozor, věc má svá úskalí. Je-li Vaším oblíbeným historickým mezníkem korunovace Štěpána I. uherským králem, pak Vám naše metoda nepomůže.

PODĚKOVÁNÍ

Tento příspěvek byl podpořen Jednotou českých matematiků a fyziků v rámci projektu Vědcem nanečisto V – Podpora talentovaných žáků v matematice a fyzice v severočeském regionu – 0033/7/NAD/2021.

LITERATURA

- [1] Arnol'd, V. I. (1978). *Mathematical methods of classical mechanics*. Graduate Texts in Mathematics, 60. Springer-Verlag, New York-Heidelberg.
- [2] Marciniak, Z. (1991). Spacerující matematyk. *Delta, lipiec 1991*.
- [3] Strzelecki, P. (2004). On powers of 2. *EMS Newsletter*, 52, s. 7–8.
- [4] Bouchala, J. (2012). *O jednom racionálním využití iracionality*. Dostupné z <http://am-nas.vsb.cz/vod03/osma/>
- [5] Guy, R. K. (1988). The strong law of small numbers. *The American Mathematical Monthly*, 95(8), s. 697–712.
- [6] Vanchinathan, P. (2017). [Answer to:] *Show that there are infinitely many powers of two starting with the digit 7*. Dostupné z <https://math.stackexchange.com/questions/2230226/>

LABORATORNÍ A FRONTÁLNÍ PRÁCE S POLOVODIČI

Zdeněk Polák

ABSTRAKT

Príspevok se zabýva frontálnymi a laboratornými prácami zaměřenými na výuku o polovodičích na střední škole. Jde o soubor kvalitativních i kvantitativních experimentů prováděných žáky podle pracovních listů. Využíváme námi vytvořeného stavebnicového systému elektrických součástek dlouhodobě používaného na naší škole. Používáme jej při zapojování elektrických obvodů a měření vlastností součástek.

KLÍČOVÁ SLOVA: laboratorní práce, frontální práce, polovodiče, dioda, tranzistor, zapojování elektrických obvodů, měření digitálními měřicími přístroji.

ÚVOD

V letech 2002–2003 učitelé fyziky na našem gymnáziu, Zdeněk Polák a Jaroslav Klemenc, za pomoci studentů vytvořili rozsáhlý stavebnicový systém pro sestavování, zapojování a následné měření elektrických obvodů. Základní myšlenka byla, aby každý žák pracoval sám, popřípadě při frontálních pracích s celou třídou, ve dvojicích. Bylo nutno tedy vytvořit 16 neustále funkčních sad součástek, zdrojů, měřicích přístrojů a vodičů. Aby fungovalo 16 sad, bylo vytvářeno vždy sad 20 a poškozené součástky, vodiče či měřicí přístroje průběžně opravovány. Celý v podstatě dotvořený systém byl předveden na Dílnách Heuréky v Náchodě r. 2009 a podrobně popsán ve sborníku [1]. Systém neustále obměňujeme a pracujeme s ním dodnes. Všechny laboratorní a frontální práce jsou popsány na našem webu [2]. Zde jsou zcela volně ke stažení ve formátu doc tak, aby si je mohl kdokoli samostatně upravit podle svých potřeb.

EXPERIMENTÁLNÍ ČINNOSTI PŘI POZNÁVÁNÍ VLASTNOSTÍ POLOVODIČOVÝCH SOUČÁSTEK

Když mají žáci cokoli poznat, je nutno, aby si na věci sáhli, aby je pozorovali a sledovali. Aby prováděli a zapisovali a zhodnocovali výsledky měření. Co lze tedy dělat? Uvedu některé možnosti a činnosti, které se nám osvědčily.

1. **Ukázat, jak věci vypadají.** Přinášíme a ukazujeme křemík, jednotlivé součástky, jako jsou termistory, fotorezistory, diody různých druhů a použití, tranzistory, tyristory, integrované obvody, rozřezané součástky, aby bylo vidět dovnitř; volné čipy i dohotovené integrované obvody, ...
2. **Ukázat z dálky, jak věci fungují.** Demonstračně ukazujeme, jak se mění odpor termistoru při zahřátí a odpor fotorezistoru při změně osvětlení, na panelu máme diodu a ukazujeme propustný a závěrný proud tím, že žárovka svítí či nesvítí podle polarizace diody a zdroje. Ukazujeme, jak funguje fotočlánek i polovodičový Peltierův článek. Máme tranzistor na panelu a ukazujeme, že malým proudem ve vstupním obvodu můžeme ovládat velký proud v obvodu výstupním. Uvádím jen příklady toho, co demonstračně ukazujeme žákům.
3. **Ukázat z blízka, jak se věci chovají.** Necháváme po třídě kolovat malé experimenty. termistor a fotorezistor připojený k ohmmetru, fotočlánek připojený k ampérmetru a různé materiály k jeho zakrytí, aby se ukázalo na jaké vlnové délky je fotočlánek nejcitlivější.
4. **Demonstrační měření a úlohy zadané experimentem.** Demonstračně měříme závislost odporu vodiče a polovodiče na teplotě. Do varné konvice plné vody vložíme měděnou cívku a termistor připojené k ohmmetru a obyčejný teploměr. Při pomalém ohřevu (cca 50 °C za 10 minut). Ke zpomalení ohřevu mám dvě možnosti – připojení konvice přes regulační transformátor anebo jednodušeji, zapojit dvě konvice za sebe – do série. Výkon každé z nich je pak čtvrtinový a voda se ohřívá čtyřikrát pomaleji.
5. **Frontální práce s celou třídou v běžné učebně.** V oblasti polovodičů děláme dvě. Jednu zaměřenou na diodu a druhou na tranzistor. Pro obě máme pro studenty vypracovány pracovní listy. Podrobně rozebereme dále.
6. **Laboratorní práce s polovinou třídy (cca 16 žáků) v laboratoři.** Zaměřené na polovodiče jsou:
 - (a) voltampérová charakteristika diody,
 - (b) voltampérové charakteristiky barevných LED,
 - (c) aplikace tranzistoru v zapojení – konstrukce zesilovače.

FRONTÁLNÍ PRÁCE S CELOU TŘÍDOU

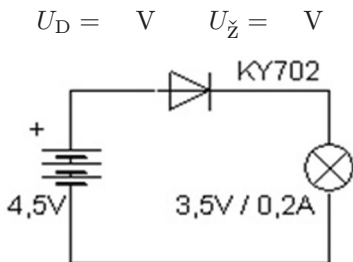
I) DIODA A JEJÍ VLASTNOSTI

V následujících odstavcích je popsána frontální práce na vlastnosti diod, číslování obrázků odpovídá pracovnímu listu a je lokální pro tento oddíl textu. Poznámky k činnosti jsou psány kurzívou.

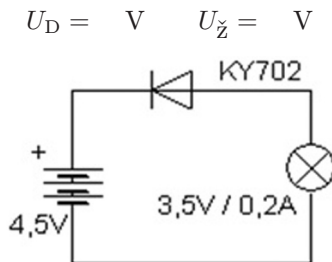
Pomůcky: Plochá baterie, křemíková dioda, žárovka 3,5 V/0,2 A, rezistor 200 Ω , digitální měřicí přístroj VA Ω , sada LED červená, zelená, modrá, bílá, fotočlánek, sada vodičů s krokosvorkami a banánky.

1) DIODA VEDE PROUD JEDNÍM SMĚREM

Zapojte obvod podle obr. 1, a pak podle obr. 2. V obou případech změřte napětí na diodě U_D i na žárovce U_Z a запиšte. V jakém směru je zapojena dioda v jednotlivých případech?



Obr. 1



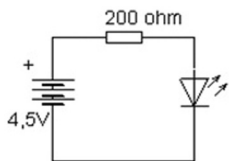
Obr. 2

V bodě 1) zdůrazníme, že v propustném směru je na křemíkové diodě asi 0,7 V, závěrném směru je na diodě plné napětí a na žárovce nulové. Proud prakticky neprochází.

2) LED DIODA (SVÍTIVÁ DIODA)

Změřte odpor rezistoru s uvedenou hodnotou 200 Ω a запиšte jeho skutečnou hodnotu. $R = \quad \Omega$.

Zapojte podle obr. 3 LED diodu v sérii s rezistorem, a připojte k baterii tak, aby LED svítila. Změřte napětí voltmetrem na rezistoru U_R i na diodě U_D . Opakujte pro diody všech barev. Hodnoty запиšte. Dopačtete proud I procházející obvodem při každém měření podle vztahu $I = U_R/R$.



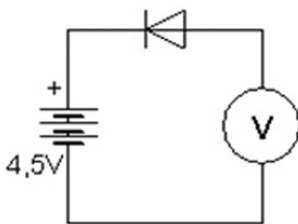
Obr. 3

Dioda	U_R (V)	U_D (V)	I (mA)
Červená (R)			
Zelená (G)			
Modrá (B)			
Bílá (W)			

V bodě 2) Zdůrazníme, že LED nejsou z křemíku, jde o polovodičový materiál na bázi sloučenin galia a arzenu, napětí v propustném směru je závislé na vlnové délce produkovaného světla a že bílá dioda má v propustném směru stejné napětí jako modrá dioda – jde o modrou diodu vybavenou lumínoforem k získání dlouhovlnné části viditelného spektra.

3) DIODA V ZÁVĚRNÉM SMĚRU

Změřte a zapište napětí baterie. Zapojte obvod podle obr. 4. Jako diodu použijte křemíkovou diodu. Zapište napětí na voltmetru. Vypočtete proud procházející obvodem, jestliže víme, že odpor voltmetru je $10\text{ M}\Omega$. Na několik sekund zahřejte jeden vývod diody zapálenou sirkou tak, aby se dioda trochu zahřála. Jak se změní závěrný proud diody?



Obr. 4

V bodě 3) poukážeme na dvě věci. Voltmetr o vnitřním odporu $10\text{ M}\Omega$ na rozsahu 200 mV funguje jako ampérmetr o rozsahu 20 nA . Používáme ho jako nanoampérmetr a zapojujeme do série se spotřebičem. Dále to, že při zahřátí diody se prudce zvyšuje závěrný proud, generuje se velké množství párů díra–elektron. Zahřívejte skutečně jen vývod, ne diodu samotnou, a jen po několik sekund.

4) LED DIODA JAKO ZDROJ NAPĚTÍ

Připojte voltmetr přímo k LED diodě a nechte na ni dopadat světlo. Jak se mění napětí při osvětlení a zatemnění diody? Na diodu můžete posvítit žárovkou

připojenou k baterii.

Jaké naměříte napětí na různých diodách (R,G,B)?

$$U_R = \quad , \quad U_G = \quad , \quad U_B =$$

Pak připojte k diodě měřicí přístroj jako ampérmetr a zkuste naměřit, jaký proud LED dodá jako zdroj napětí.

V bodě 4) poukážeme na to, že dioda sice dává napětí, ale proud je nejvýše jednotky mikroampér. Generovaný proud závisí na intenzitě osvětlení a na ploše PN přechodu, na kterou světlo dopadá. Pokus není vhodný pro bílou diodu, která má PN přechod zakrytý luminoforem.

5) FOTOČLÁNEK

Osvětlete fotočlánek žárovkou a při neměnné poloze žárovky změřte napětí na fotočlátku bez zatížení, $U_1 =$ V. Napětí po připojení rezistoru $200 \, \Omega$, $U_2 =$ V a zkratový proud fotočlátku $I_k =$ mA.

V bodě 5) zdůrazníme, že proud fotočlátku závisí na ploše přechodu a zátěži. Pokud zbývá čas, je možno fotočlánek překrýt černým filtrem, který propouští NIR a zachytí světlo. Ukážeme, že napětí a proud fotočlátku poklesnou jen málo, zatímco překryjeme-li fotočlánek průhledným filtrem zachycujícím NIR, fotočlánek prakticky přestane pracovat.

(NIR = světlu blízká oblast spektra infračerveného záření)

II) TRANZISTOR A JEHO VLASTNOSTI

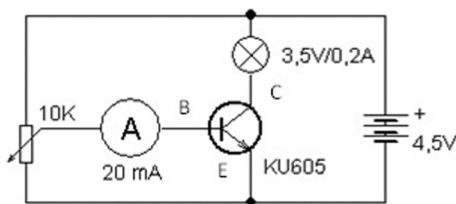
V následujících odstavcích je popsána frontální práce na vlastnosti tranzistorů, číslování obrázků odpovídá pracovnímu listu a je lokální pro tento oddíl textu. Poznámky k činnosti jsou psány kurzívou. Předpokládá se, že převodní charakteristika tranzistoru byla již naměřena jako demonstrační pokus. Naopak zapojování tranzistoru v obvodech budou studenti procvičovat v následné laboratorní práci.

Pomůcky: výkonový tranzistor, tranzistorový kaskádový zesilovač, vodiče, plochá baterie, potenciometr $10 \, k\Omega$, žárovka $3,5 \, V/0,2 \, A$, fotorezistor, LED diody, $2 \times$ DMM

Sestavte následující obvody, vyzkoušejte u všech činností obvodů.

1) ZESÍLENÍ TRANZISTORU

Sestavte obvod na obr. 5). Měňte polohu jezdcu potenciometru, měřte proud na rozsahu $20 \, mA$. Tento rozsah neměňte. Jaký nejmenší proud do báze tranzistoru stačí k plnému rozsvícení žárovky? Odhadněte zesilovací činitel, jestliže předpokládáme plný proud žárovkou $200 \, mA$



$$I_B = \quad \text{mA}$$

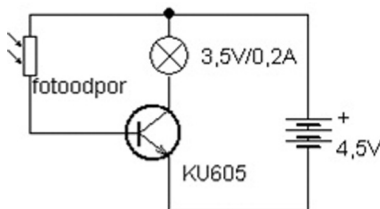
$$\beta =$$

Obr. 5: Schéma obvodu s potenciometrem

V bodě 1) zdůrazníme, aby do báze tranzistoru žáci nepouštěli proud větší než je rozsah přístroje. Robustní konstrukce tranzistoru sice zajišťuje jeho ochranu před zničením, ale mohla by se spálit pojistka měřicího přístroje. Jezdec potenciometru na začátku je dobré mít někde uprostřed.

2) TRANZISTOR OVLÁDANÝ FOTOŘEZISTOREM

Sestavte obvod s fotorezistorem podle schématu na obr. 6. Popište chování žárovky při zakrytí a odkrytí fotorezistoru.



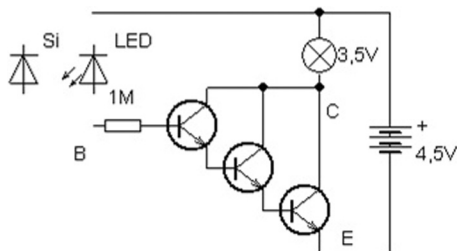
Obr. 6: Schéma obvodu s fotorezistorem

V bodě 2) je třeba mít odzkoušeno, že při osvětlení fotorezistoru poklesne jeho odpor natolik, že proud do báze otevře tranzistor tak, aby se žárovka rozsvítila. Situaci je možné zachránit tak, že žáci na fotorezistor posvítí žárovkou připojenou k baterii, nebo mobilem.

3) ZESÍLENÍ KASKÁDY TRANZISTORŮ, MĚŘENÍ NEPATRNÝCH PROUDŮ

- Sestavte obvod podle obr. 7. Skládá se pouze z baterie, žárovky, kaskády tranzistorů a vodičů. Jednou rukou uchopíte kladný pól baterie a druhou se dotýkáte báze B.

Utvořte obvod z několika spolužáků a spojte +baterie s bází B. Pak uchopte pouze vývod báze a vstaňte ze židle, popřípadě smýkněte nohou v obuvi po podlaze a zvedněte ji. Proč se žárovka rozsvěcí?



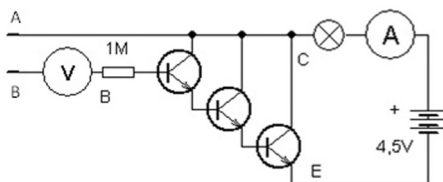
Obr. 7: Zesilovač s tranzistorovou kaskádou

- b) Pak mezi kladný pól baterie a vývod B připojte křemíkovou diodu v závěrném směru. Zahřejte jeden její vývod opatrně plaménkem sirky na několik sekund. Popište děj, který nastane.
- c) Pak nahraďte Si diodu diodou LED v závěrném směru. Zakryjte ji, odkryjte, namířte na zdroj světla, změňte typ diody. Proč se nyní žárovka rozsvítí?
- d) Ukážeme, že plamen svíčky vede proud. Spolupracují dva žáci. Jeden má špendlík připojený vodičem ke kladnému pólu baterie, druhý k bázi kaskády. Každý drží v krokosvorce jeden špendlík – jsou dobře vodivě odděleny. Pak hroty špendlíků vnoříte do plamene a procházející proud otevře kaskádu – žárovka se rozsvítí. Zkuste různé polohy hrotů špendlíků, aby žárovka ještě svítila.

V bodě 3) vysvětlíme princip kaskády tranzistorů. Můžeme ukázat rozsvícení žárovky přibližováním a oddalováním nabitě tyče k vodiči připojenému do báze kaskády B. Můžeme také připojit bázi ke kladnému pólu zdroje přes malý kondenzátor (cca 10 nF) a pozorovat jeho nabíjení – pokles svitu žárovky. Ukazujeme, že proud suchou špejlí neprochází, ale navlhčenou ano.

4) ZESÍLENÍ KASKÁDY TRANZISTORŮ, MĚŘENÍ NEPATRNÝCH PROUDŮ

Obvod zapojíme podle schématu na obr. 8. Vývody A a B propojíme přes lidské tělo a izolaci vodiče tak, aby žárovka slabě svítila.



Obr. 8: Zapojení tranzistorové kaskády pro měření celkového zesílení

Měříme proud procházející lidským tělem a proud procházející žárovkou a spočteme zesílení.

Rozsah DMM 200 mV – zapojení jako voltmetr, odpovídá při odporu voltmetru 10 MΩ proudu 20 nA. Tedy údaj v milivoltech vydělte deseti a dostanete číselnou hodnotu proudu v nA.

$$I_Z = \quad \text{mA} \quad I_{\zeta} = \quad \text{nA} \quad \text{zesílení} =$$

Proč necítíme průchod proudu přes tělo?

Bod 3) zařadíme tehdy, když máme dost času. Při měření zesílení je zapotřebí, aby žárovka nesvítla naplno, tedy aby poslední tranzistor nebyl zcela otevřen.

LABORATORNÍ PRÁCE

Laboratorní práce ve třetím ročníku na naší škole jsou dotovány jednou hodinou za dva týdny. Jak už bylo uvedeno, polovodičům jsou věnovány nejvýše 3 z celkem asi 12 prací za rok. Jsou to voltampérová charakteristika diody, voltampérové charakteristiky barevných LED a aplikace tranzistoru v zapojení – konstrukce zesilovače. První dvě jsou zcela klasické laborky. Jejich zadání lze nalézt na odkazu [2]. Zmíním tu třetí.

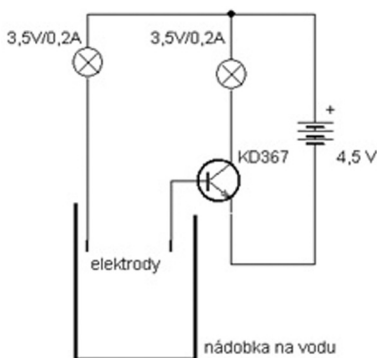
VYUŽITÍ TRANZISTORU V APLIKACÍCH

Ve všech aplikačních zapojeních používáme výkonový tranzistor KD367. Jde o Darlington, tedy o kaskádu dvou tranzistorů. Výhoda je velké zesílení, řádově 1 000, nevýhodou je minimální napětí mezi bází a emitorem cca 1,5 V a nelineární charakteristika. Použít lze jakýkoli jiný robustní tranzistor podobného typu. Obrázky jsou opět číslovány od začátku pro následující oddíl, tak jak to odpovídá číslování v pracovním listu pro žáky.

Pomůcky: Tranzistor KD637, 2× žárovka 3,5 V/0,2 A, plochá baterie, sada vodičů s krokosvorkami a banánky na propojení, kondenzátor 10 μF, potenciometr 10 kΩ, termistor, fotorezistor, fotočlánek 2 V/50 mA, nádobku se dvěma plíškami – elektrodami, obyčejnou vodu z vodovodu, destilovanou vodu, krystalek NaCl.

1) TRANZISTOR JAKO HLÍDAČ HLADINY

Zapojíme obvod podle schématu na obrázku 9. Na začátku je nádobka prázdná. Elektrody sahají do nádobky a končí kousek nade dnem. Postupně naléváme vodu, až se elektrody částečně zaplaví. Obvykle (podle vodivosti vody) stačí několik milimetrů a žárovka v kolektoru se rozsvítí. Žárovka v bázi nikoliv. Vysvětlíte.



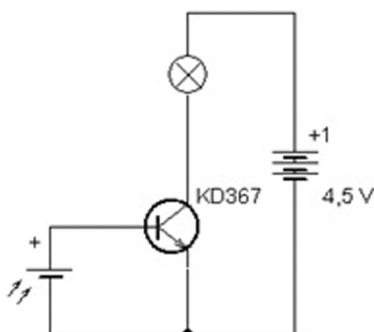
Obr. 9: Zapojení tranzistoru jako hlídače hladiny

Pak vodu vylijeme a nahradíme destilovanou vodou. Zalijeme elektrody do výše 2–3 cm a ani jedna žárovka se přesto nerozsvítí. Přidejte do vody jeden malý krystalek NaCl, zamíchejte a pozorujte, co se změní. Vysvětlete.

2) TRANZISTOR OTVÍRANÝ FOTOČLÁNKEM

Zapojíme obvod podle schématu na obr. 10.

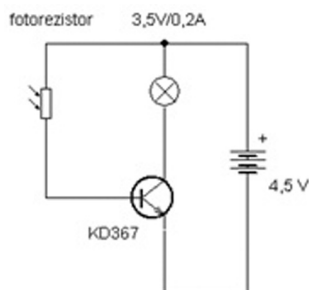
Pozorujte svít žárovky při změnách osvětlení fotočlánku. Co se stane, zaměníme-li polaritu fotočlánku?



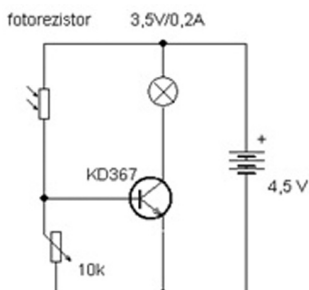
Obr. 10: Tranzistor otvíraný fotočlánkem

3) TRANZISTOR OVLÁDANÝ FOTOREZISTOREM

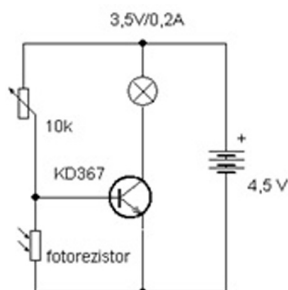
Na obrázcích 11, 12, 13 jsou celkem tři zapojení. První jen ovládá tranzistor bez možnosti regulace citlivosti na světlo, druhý umožňuje nastavit, při jakém osvětlení fotorezistoru se žárovka rozsvítí. A funkci třetího si vyzkoušejte sami.



Obr. 11



Obr. 12

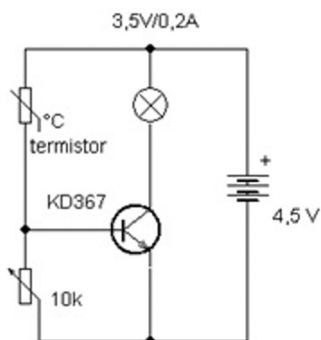


Obr. 13

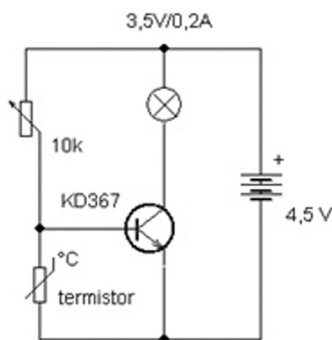
4) TRANZISTOR OVLÁDANÝ TERMISTOREM

Na obrázcích 14 a 15 jsou schémata, podle nichž zapojíte obvody pro ovládání žárovčky změnou teploty. Zapojte obvod a nastavte potenciometr tak, aby žárovka slabě svítila. Co se stane, když termistor uchopíte do prstů (termistor trochu ohřejete).

Vysvětlete.



Obr. 14



Obr. 15

ZÁVĚR

Uvedené experimenty mohou být po vynechání kvantitativních měření námětem pro experimentální činnost žáků nižšího gymnázia a odpovídajících ročníků základních škol.

LITERATURA

- [1] Polák, Z. (2011). Zapojování elektrických obvodů. In L. Dvořák, I. Dvořáková & V. Koudelková (Eds.), *Dílny Heuréky 2009–2010. Sborník konferencí projektu Heuréka*. Praha: Prometheus.
- [2] <http://fyzika.gymnachod.cz> pod odkazem „laboratorní práce“.

POKUSY Z PROJEKTU ŽIJU FYZIKOU

Jana Šestáková

ABSTRAKT

Nabízím připomenutí pokusů pro domácí bádání i do hodin fyziky. „Na vlastní kůži“ si můžete znovu zkusit střelení raketou, výrobu vznášedla, lepení brček na zeď bez lepidla a stlačení plechovky vzduchem.

Taky pro vás sdílím ukázky dvou kreslených videí, prostřednictvím kterých se děti (i dospělí) v projektu Žiju fyzikou učí fyziku.

KLÍČOVÁ SLOVA: projekt, experiment, výukové video, metoda peer instruction.

BRČKOVÁ VÝZVA

Úkol: Bez pomoci lepidla „přilepte“ brčko na zeď. Až ovládnete „lepící kouzlo“, sestavte z brček na zdi domeček.

Pomůcky: brčka, nůžky (na stříhání brček na stavbu oken a dveří), zeď, tričko nebo papírové kapesníky



Obr. 1: Brčka na zdi

Vysvětlení, proč a jak pokus funguje:

Brčka drží na zdi díky elektrostatičce. Plastové brčko pěkně reaguje na tření papírovým kapesníkem, při kterém se elektrony přesouvají z kapesníčku na brčko. Když pak elektricky nabitě brčko přiblížíte ke zdi, elektrony ve zdi se „trochu pohnou“ (tak málo, jak jim to zeď dovolí), aby před nabitým brčkem „utekly“ (protože náboje stejného znaménka se odpuzují). Ve zdi blíž u brčka tak zůstanou „kladné zbytky zdi“, které brčko na zdi udrží. Dvě takto nabitá brčka se budou od sebe navzájem (lehce, ale pozorovatelně) odpuzovat.

Tip: Při tření je potřeba brčko zmáčknout (až rozplácnout). Když kapesníčkem brčko jen „pohladím“, asi se dostatečně nenabije a často na zdi nedrží.

Záznam živého vysílání pro Facebook stránku Žiju fyzikou na téma Brčková výzva:

<https://www.youtube.com/watch?v=5Lcnyba8pDM>

DOMÁCÍ VZNÁŠEDLO

Pomůcky: CD, víčko od lahve s dírkou, nafukovací balonek, tavná pistole, velká hladká plocha (stůl, podlaha)

Jak vyrobit vznášedlo a proč a jak funguje:

Doprostřed CD nad díru nalepte víčko od lahve s vyvrtanou dírkou. Na víčko navlékněte nafouknutý balonek. Takto vyrobené vznášedlo položte na hladkou plochu a do CD lehce šfouchněte. Vzduch, který skrz díрку ve víčku a v CD proudí na podložku, vznášedlo nadzvedává a vznášedlo se tak pohybuje na vzduchovém polštáři.

CD na vzduchovém polštáři dokáže dojet výrazně dál než CD, které je přímo v kontaktu s podložkou a musí tak překonávat tření.

Tip: Je možné vyrobit „vyšší verzi vznášedla“ se startovacím víčkem. Víčko má uzávěr jako na cyklistické lahvi, které jde otevřít vytažením části špuntíku. Na takové vznášedlo se snadněji navléká nafouknutý balonek, protože uzávěr může být při navlékání balonku zavřený. Když pak chcete vznášedlo odstartovat, stačí špuntík nadzvednout. Dříve se s tímto víčkem prodával nápoj Jupí, teď je k dostání na nápoji Figo.

Tip 2: Abyste nemuseli vrtat díрку do obyčejného víčka, použijte víčko z lahve od Rajce nebo od Jupí, ze kterého lze odtrhnout zavírání a vymáčknout střed s blánou, která brání protékání pití z otevřené lahve.

Ukázka jízdy vznášedla: <https://youtu.be/QAueY-ZS9rU>



Obr. 2: Tři druhy víček na vznášedle: se „startovacím víčkem“, s rozebíratelným víčkem a s víčkem s dírkou proraženou hřebíkem

DRCENÍ PLECHOVKY

Pomůcky: vaříč, rychlovarná konvice na předvaření vody, trocha vody, plechovka od pití (my používali od 250ml nápojů, ale lze použít i velké plechové sudy), modelína, chňapky, (talířek, hrnek se studenou vodou na chlazení)

Postup: Vodu uvařte v rychlovarné konvici a nalijte do plechovky (stačí malinko, třeba centimetrový sloupec vody). Plechovku postavte na vaříč, aby se voda vařila i přímo v plechovce. Potřebujeme nechat vodu vařit v plechovce tak dlouho, až začne být vidět mlha nad otvorem v plechovce, která uniká ven. V tu chvíli je plechovka připravena k rozdrčení. Ucpěte díрку v plechovce modelínou a odstavte plechovku z vaříče.

Plechovku něco rozdrťte přímo před vašima očima!

Ve videu je pokus přerušeny před jeho vysvětlením a je do videa vložena otázka „Co plechovku rozdrtilo?“ s nabídnutými možnostmi. Pak následuje ukázka použití metody Peer Instruction, kdy děti volí jednu z nabízených možností odpovědi, ve skupině odpověď diskutují a poté podruhé odpovídají na tu stejnou otázku. Na závěr je ve videu vysvětlené správné řešení.

Proč a jak se to stalo?

Voda se při varu v plechovce vypařuje a pára plní plechovku. To poznáme tak, že pára začne unikat z plechovky, srážet se zpět na kapičky a vytvářet mlhu,

která je nad dírkou v plechovce vidět. Pára naplnila plechovku a přitom vytlačila z plechovky ven vzduch.

V tu chvíli jsme ucpali plechovku a odstavili ji od zdroje tepla. Pára uvnitř plechovky začala zpět zkapalňovat a uvnitř plechovky se tak nad hladinou začalo dělat místo, do kterého by se mohl vrátit vzduch. Ale protože je ucpaná díрка v plechovce, tak vzduch nemůže zpět. Uvnitř plechovky je tak nižší tlak než okolo plechovky. Okolní vzduch, tedy ten, který my běžně dýcháme, je v tu chvíli oproti tlaku uvnitř plechovky tak velký, že plechovku z venku zvládne rozdrtit.



Obr. 3: Drcení plechovky

Záznam živého vysílání pro Facebook stránku Žiju fyzikou o drcení plechovky najdete taky: <https://youtu.be/bBe9wyk1-Gs>

STŘÍLENÍ RAKETOU

Pomůcky: 40 cm vodovodní trubky, 30 cm zahradní hadice, PET láhev velká – kolem 2 litrů, A4 list papíru na raketu, kousky papíru na křídélka, stříbrná lepicí páska, izolepa, (pastelky na výzdobu rakety)

Výroba odpalovací rampy: Vodovodní trubku, zahradní hadici a hrdlo lahve podobných průměrů slepte lepicí páskou v pořadí: trubka – hadice – lahev.

Výroba rakety: List papíru A4 namotejte na vodovodní trubku – ne úplně těsně(!), je potřeba, aby se raketa mohla po trubce volně posouvat. Tím vznikne tělo rakety, které po délce slepte izolepou. Na jednom konci tělo rakety zmáčkněte a vzniklou špičku přelepte izolepou. Na druhý konec přilepte 4 malá trojúhelníková křídélka (můžete zkusit různý počet a různé velikosti a porovnat, jak budou létat). Raketa je hotová!

Odpalování: Skrz trubku a hadici nafoukněte lahev. Navlékněte raketu na trubku, položte lahev na zem a pohybem hadice zamiřte. Dupnutím nebo skokem na lahev raketu odpalte.

Co se při střílení raket mohou děti naučit? Můžete s dětmi odhalovat závislost elevačního úhlu na doletu rakety. Nebo můžete trénovat odhad vzdálenosti a následně trénovat krokování a měření doletu rakety.



Obr. 4: Odpalovací rampa a rakety

Varování! Rakety mohou létat opravdu daleko a vysoko! Dobře mířte, ať o raketu hned při prvním letu nepřijdete, rády zůstávají na stromech nebo na střechách.

Taky nemířte na lidi a při odpalování se proti raketě nedívejte.

Tip: „Vyšší verze“ odpalovací rampy. Občas se stane, že se při odpalování rakety protrhne lahev. Pro takové případy je dobré mít vyšší verzi odpalovací rampy, kdy je na hadici navlečené víčko s dírkou. Víčko se při protrhnutí lahve pouze odšroubuje a našroubuje se nové lahev, není nutné nic přelepovat.

Tip 2: Pro výrobu rakety lze použít i novinový papír, raketa ale tolik nevydrží.

Tip 3: Je dobré střílet ve dvou lidech, kdy jeden vhodným náklonem hadice míří a druhý skáče na lahev.

Záznam živého vysílání pro Facebook stránku Žiju fyzikou o odhadu vzdálenosti při střílení raketou: https://youtu.be/KWS9i_OwqAw

A na závěr sdílím ukázkou kreslených videí, jejichž součástí je ukáзка použití vyučovací metody Peer Instruction.

Bouřka: <https://youtu.be/eGobqJPW7Rk>

Fáze Měsíce: <https://youtu.be/iciyCiAkn8Y>

Zdroje (kde jsem se inspirovala a co může inspirovat vás):

Dny otevřených dveří UJEP (2010). Drcení plechovky.

Projekt Heuréka, víkendové semináře pro učitele – „školka Heuréky“ (2010–2012). Střílení raket, lepení brček na zeď a vznášedlo a spousta dalších pokusů. Nabídka akcí a možnost přihlášení pro školní rok 2022/2023 je zde:

<https://kdf.mff.cuni.cz/heureka/index.php>

ÚDiF – Úžasné divadlo fyziky (2021). Drcení sudu na společenském večeru Veletrhu nápadů učitelů fyziky v Brně 2021.

Nabídka akcí je dostupná na: <https://udif.cz/>

Žiju fyzikou (2022). Webové stránky: <http://www.ZijuFyzikou.cz>

Facebook skupina: <https://www.facebook.com/groups/263012394984052> (propojování učitelů fyziky, fanoušků fyziky, odpovídání na fyzikální dotazy, sdílení inspirace)

Facebook stránka:

<https://www.facebook.com/%C5%BDiju-fyzikou-113487007147058> (živá vysílání s fyzikální tematikou, která je možné sdílet dál a inspirovat se z nich do výuky)

Metoda Peer Instruction (2022). Stránky o vyučovací metodě.

Dostupné z <http://www.PeerInstruction.cz>

ŠIFROVÁNÍ RSA

Tomáš Urban

ABSTRAKT

Seminář šifrování RSA vznikl jako součást diplomové práce: Úlohy z modulární aritmetiky, na které autor pracuje na katedře matematiky PřF UJEP. V první části semináře byly účastníkům představeny nástroje potřebné pro šifrování RSA. Ve druhé části účastníci tyto poznatky aktivně využívali při šifrování a dešifrování zpráv pomocí počítačového programu.

Cílem semináře bylo ověřit technickou a časovou náročnost připravených úloh a problémů.

KLÍČOVÁ SLOVA: Euklidův algoritmus, kongruence, šifrování RSA.

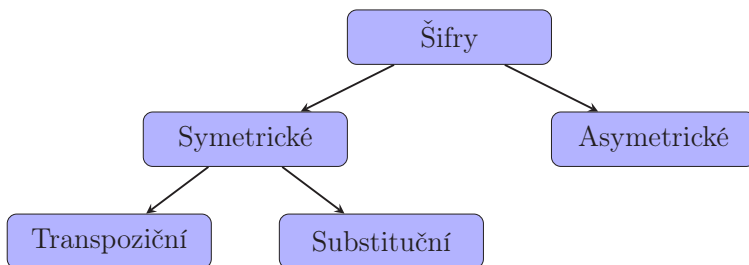
O ŠIFROVÁNÍ

V knize [1] se můžeme dočíst, že **Kryptografie**, jako věda zabývající se šifrováním a dešifrováním, zahrnuje dva obory.

- **Kryptografie** studuje teoretické aspekty navrhování šifrovacích metod.
- **Kryptoanalýza** se zaměřuje na studium metod luštění šifer.

ROZDĚLENÍ ŠIFER

Na obr. 1 je uvedeno znázornění rozdělení šifer na symetrické a asymetrické.



Obr. 1: Schéma rozdělení šifer

SYMETRICKÉ ŠIFRY

Při symetrickém šifrování používá adresát k dešifrování zprávy stejný klíč, kterým zprávu odesílatel zašifroval. Symetrické šifry můžeme dále rozdělit podle metody šifrování na šifry transpoziční a substituční.

Příkladem transpoziční šifry je nejstarší šifrovací zařízení: skytála. Jedná se o hůl s určitým obvodem, na niž se namotal proužek kůže, na kterém byla zpráva zapsána. Po sejmutí kůže z hole jsou původní znaky zprávy posunuty o určitý počet míst v závislosti na obvodu hole. Zpráva mohla být tedy opět přečtena jen na holi o stejném obvodu.

Příkladem substituční šifry je tzv. Caesarova šifra. Jedná se o šifru, ve které každé písmeno zprávy bylo nahrazeno písmenem stojícím v abecedě o 3 místa za ním. Rozdílem oproti transpoziční šifře je, že každé písmeno původní zprávy je nahrazeno jiným, které původní zpráva neobsahuje.

ASYMETRICKÉ ŠIFRY

Při asymetrickém šifrování si odesílatel nejprve vyžádá veřejný klíč, kterým zprávu zašifruje. Adresát následně doručenou zašifrovanou zprávu dešifruje svým soukromým klíčem, který je k veřejnému klíči komplementární.

Příkladem asymetrické šifry je šifrování RSA.

DĚLITELNOST

Definice 1 (Dělitelnost). Mějme celá čísla a, b , kde $b \neq 0$. Říkáme, že b dělí a (nebo také b je dělitel a , nebo také a je násobkem b) právě tehdy, když existuje celé číslo k takové, že

$$a = b \cdot k.$$

Skutečnost, že b dělí a symbolicky zapíšeme: $b \mid a$.

(časová náročnost: 5 min)

Věta 2 (Dělení se zbytkem). *Nechť jsou dána libovolná čísla $a \in \mathbb{Z}$ a $m \in \mathbb{N}$, $m \neq 0$. Potom lze najít právě jednu dvojici čísel $q \in \mathbb{Z}$ a $r \in \mathbb{N}_0$ tak, že platí vztahy:*

$$a = m \cdot q + r, \quad 0 \leq r < |m|. \quad (1)$$

(časová náročnost: 5 min)

Obecnější větu i s jejím důkazem lze nalézt v knize [2] na stranách 86–87.

Definice 3 (Celá dolní část čísla). Celou dolní částí reálného čísla r nazveme celé číslo z splňující:

$$z \leq r < z + 1.$$

Celou dolní část čísla r budeme značit $\lfloor r \rfloor$.

(časová náročnost: 5 min)

Příklad 4. Určete celou dolní část čísla:

(a) $\lfloor 8,6 \rfloor$

(b) $\lfloor 7 \rfloor$

(c) $\lfloor \pi \rfloor$

(d) $\left\lfloor \frac{18}{5} \right\rfloor$

Řešení.

(a) $8 \leq 8,6 < 9 \Rightarrow \lfloor 8,6 \rfloor = 8$

(b) $7 \leq 7 < 8 \Rightarrow \lfloor 7 \rfloor = 7$

(c) $3 \leq \pi < 4 \Rightarrow \lfloor \pi \rfloor = 3$

(d) $3 \leq \frac{18}{5} < 4 \Rightarrow \left\lfloor \frac{18}{5} \right\rfloor = 3$

□

(časová náročnost: 5 min)

MODULÁRNÍ ARITMETIKA

Definice 5. Nechť $a \in \mathbb{Z}$, $r \in \mathbb{N}_0$, $m \in \mathbb{N}$. Zbytek r po dělení čísla a číslem m budeme značit

$$r = a \pmod{m}.$$

(časová náročnost: 5 min)

Věta 6. Nechť $a \in \mathbb{Z}$, $m \in \mathbb{N}$. Potom zbytek po dělení čísla a číslem m je

$$a \pmod{m} = a - m \cdot \left\lfloor \frac{a}{m} \right\rfloor.$$

Důkaz. Podle věty 2 platí: $a = m \cdot q + r$, kde $q \in \mathbb{Z}$ a pro zbytek po dělení r platí: $0 \leq r < m$. Potom

$$a \pmod{m} = a - m \cdot \left\lfloor \frac{a}{m} \right\rfloor = a - m \cdot \underbrace{\left\lfloor \frac{m \cdot q}{m} + \underbrace{\frac{r}{m}}_{0 \leq \frac{r}{m} < 1} \right\rfloor}_q = a - m \cdot q = r.$$

□

(časová náročnost: 10 min)

$$\text{Například } 198 \pmod{13} = 198 - 13 \cdot \left\lfloor \frac{198}{13} \right\rfloor = 198 - 13 \cdot 15 = 3$$

Příklad 7. Vypočítejte:

(a) $36 \pmod{7} =$

(b) $1\,256 \pmod{12} =$

Řešení.

(a) $36 \pmod{7} = 36 - 7 \cdot \left\lfloor \frac{36}{7} \right\rfloor = 36 - 7 \cdot 5 = 1$

(b) $1\,256 \pmod{12} = 1\,256 - 12 \cdot \left\lfloor \frac{1\,256}{12} \right\rfloor = 1\,256 - 7 \cdot 104 = 8$

□

(časová náročnost: 10 min)

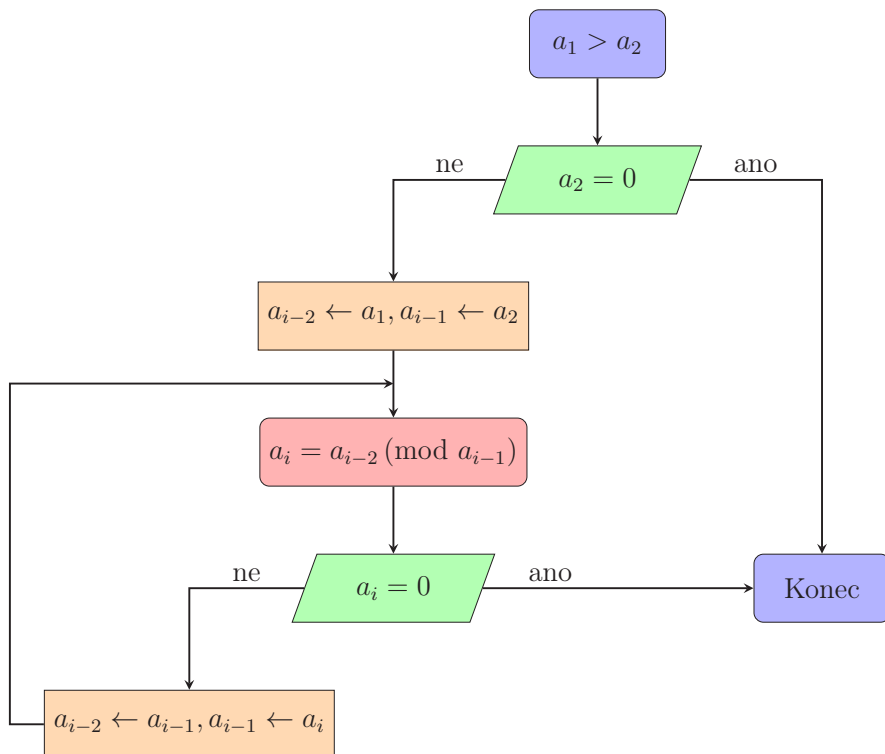
Věta 8 (Euklidův algoritmus). *Nechť a_1, a_2 jsou přirozená čísla. Pro každé $n > 3$, pro které $a_{n-1} \neq 0$ označme $a_n = a_{n-2} \pmod{a_{n-1}}$. Pak po konečném počtu kroků dostaneme $a_k = 0$ a platí:*

$$a_{k-1} = \text{NSD}(a_2, a_1).$$

(časová náročnost: 10 min)

Důkaz věty lze najít například v knize [3] na stranách 28–29.

Příklad 9. Pomocí Euklidova algoritmu (obr. 2) nalezněte $\text{NSD}(6\,840, 6\,426)$.



Obr. 2: Schéma Euklidova algoritmu

Řešení.

$$6\,840 = 1 \cdot 6\,426 + 414 \quad (2)$$

$$6\,426 = 15 \cdot 414 + 216 \quad (3)$$

$$414 = 1 \cdot 216 + 198 \quad (4)$$

$$216 = 1 \cdot 198 + 18 \quad (5)$$

$$198 = 11 \cdot 18 + 0 \quad (6)$$

$$\text{NSD}(6\,426, 6\,840) = 18.$$

□

(časová náročnost: 10 min)

Věta 10 (Rozšířený Euklidův algoritmus). *Pro libovolná přirozená čísla a_1, a_2 existuje největší společný dělitel $NSD(a_2, a_1)$ a přitom existují celá čísla a'_1, a'_2 tak, že*

$$a_1 \cdot a'_1 + a_2 \cdot a'_2 = NSD(a_2, a_1).$$

(časová náročnost: 5 min)

Důkaz věty lze najít například v knize [3] jako Lemma 1.21 a Lemma 1.22 na stranách 34–35.

Příklad 11. Pomocí rozšířeného Euklidova algoritmu nalezněte čísla a'_1 a a'_2 , pro která platí:

$$a'_1 \cdot 6\,840 + a'_2 \cdot 6\,420 = NSD(6\,420, 6\,840).$$

Řešení. Využijeme postup hledání $NSD(6\,420, 6\,840)$ z příkladu 9. Z rovnosti 5 vidíme, že $NSD(6\,426, 6\,480) = 18$ a vyjádříme jej jako

$$18 = 216 - 1 \cdot 198. \quad (7)$$

Z rovnosti 4 vyjádříme

$$198 = 414 - 1 \cdot 216$$

a dosadíme do rovnosti 5. Obdržíme

$$\begin{aligned} 18 &= 216 - (414 - 1 \cdot 216) \\ 18 &= -414 + 2 \cdot 216. \end{aligned} \quad (8)$$

Z rovnosti 3 vyjádříme

$$216 = 6\,426 - 15 \cdot 414$$

a dosadíme do rovnosti 8. Obdržíme

$$\begin{aligned} 18 &= -414 + 2 \cdot (6\,426 - 15 \cdot 414) \\ 18 &= 2 \cdot 6\,426 - 31 \cdot 414. \end{aligned} \quad (9)$$

Z rovnosti 2 vyjádříme

$$414 = 6\,840 - 1 \cdot 6\,426$$

a dosadíme do rovnosti 9. Obdržíme

$$\begin{aligned} 18 &= 2 \cdot 6\,426 - 31 \cdot (6\,840 - 1 \cdot 6\,426) \\ 18 &= -31 \cdot 6\,840 + 33 \cdot 6\,426. \end{aligned} \quad (10)$$

□

(časová náročnost: 15 min)

KONGRUENCE

Definice 12 (Kongruence). Mějme přirozené číslo m a celá čísla a, b . Říkáme, že čísla a a b jsou kongruentní modulo m právě tehdy, když jejich rozdíl je dělitelný číslem m .

$$a \equiv b \pmod{m} \Leftrightarrow m \mid (a - b)$$

(časová náročnost: 5 min)

Příklad 13. Rozhodně, zda platí následující kongruence.

(a) $93 \equiv 21 \pmod{6}$

(c) $785 \equiv 105 \pmod{17}$

(b) $312 \equiv 1\,204 \pmod{222}$

(d) $986 \equiv 9\,137 \pmod{627}$

Řešení. Kongruence ověříme z definice 12 a věty 2.

(a) $93 - 21 = 72 = 6 \cdot 12 + 0$

ANO

(b) $312 - 1\,204 = -892 = 222 \cdot (-5) + 218$

NE

(c) $785 - 105 = 680 = 17 \cdot 40 + 0$

ANO

(d) $986 - 9\,137 = -8\,151 = 627 \cdot (-13) + 0$

ANO

□

(časová náročnost: 5 min)

Věta 14. *Relace kongruence modulo m je relací ekvivalence na množině celých čísel. Tedy pro všechna celá čísla a, b, c a pro každé přirozené číslo m platí:*

1. $a \equiv a \pmod{m}$ (*reflexivnost*),

2. $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$ (*symetrie*),

3. $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$ (*tranzitivnost*).

(časová náročnost: 5 min)

Větu i s jejím důkazem lze nalézt v knize [3] na stranách 122 a 123.

Definice 15 (Zbytková třída). Nechť je dáno přirozené číslo m a celé číslo a . Potom zbytkovou třídou modulo m nazveme množinu

$$[a]_m = \{z \in \mathbb{Z} \mid z \equiv a \pmod{m}\}.$$

- V případě, kdy je zřejmé, že se jedná o zbytkovou třídu modulo m , použijeme místo označení $[a]_m$ pouze $[a]$.
- Množinu všech zbytkových tříd modulo m označíme $\mathbb{Z}_m$.

Například $[2]_7 = \{\dots, -12, -5, 2, 9, 16, 23, 30, 37, 44, \dots\}$

$$7 \mid (16 - 44)$$

$$7 \mid (-28) \dots$$

(časová náročnost: 5 min)

Věta 16. *Mějme čísla m, n a čísla a, b, c, d . Platí:*

$$1. \ a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \Rightarrow a \pm c \equiv b \pm d \pmod{m},$$

$$2. \ a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \Rightarrow a \cdot c \equiv b \cdot d \pmod{m}.$$

Například $2 \equiv 7 \pmod{5}$ a $6 \equiv 11 \pmod{5}$. Potom:

$$2 + 6 \equiv 7 + 11 \pmod{5} \quad 2 \cdot 6 \equiv 7 \cdot 11 \pmod{5}$$

$$8 \equiv 18 \pmod{5} \quad 12 \equiv 77 \pmod{5}$$

$$3 \equiv 3 \pmod{5} \quad 2 \equiv 2 \pmod{5}.$$

(časová náročnost: 10 min)

Příklad 17. Dokažte, že posloupnost (v desítkovém zápise)

$$11, 111, 1\,111, 11\,111, \dots$$

neobsahuje žádnou druhou mocninu.

Řešení. Nejprve si všimněme, že číslo 11 lze zapsat jako

$$11 = 4 \cdot 2 + 3 \equiv 3 \pmod{4}.$$

Všechna ostatní čísla z posloupnosti lze zapsat jako součet čísla 11 a čísla, které je násobkem čísla 100, tedy čísla, které je bezezbytku dělitelné číslem 4.

$$111 = 100 + 11 = 4 \cdot 25 + 4 \cdot 2 + 3 \equiv 3 \pmod{4}$$

$$1\,111 = 1\,100 + 11 = 4 \cdot 275 + 4 \cdot 2 + 3 \equiv 3 \pmod{4}$$

$$11\,111 = 11\,100 + 11 = 4 \cdot 2\,775 + 4 \cdot 2 + 3 \equiv 3 \pmod{4} \text{ atd.}$$

Dále dokážeme, že žádná druhá mocnina nemůže být kongruentní s číslem 3 modulo 4. Zvolme vhodné reprezentanty ze zbytkových tříd modulo 4. Například $0 \in [0]_4$, $1 \in [1]_4$, $2 \in [2]_4$, $3 \in [3]_4$. Platí:

$$\begin{aligned} 0^2 &\equiv 0 \equiv 0 \pmod{4} & 1^2 &\equiv 1 \equiv 1 \pmod{4} \\ 2^2 &\equiv 4 \equiv 0 \pmod{4} & 3^2 &\equiv 9 \equiv 1 \pmod{4}. \end{aligned}$$

Odtud je vidět, že žádné číslo naší posloupnosti nemůže být čtvercové. $\square$

(časová náročnost: 15 min)

Definice 18 (Multiplikativní inverze). Multiplikativní inverzí čísla a v modulu m nazveme každé a^{-1} , pro které platí:

$$a \cdot a^{-1} \equiv 1 \pmod{m}.$$

(časová náročnost: 5 min)

Podívejme se nyní na tabulku 1, kde nalezneme multiplikativní tabulky modulo 5 a modulo 6.

Tabulka 1: Multiplikativní tabulky

$\odot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(a) Modulo 5

$\odot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	4
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(b) Modulo 6

Tabulky získáme postupným násobením čísel v záhlaví a přepočtením výsledného součinu v daném modulu. V tabulce 1a vidíme, že každý prvek má multiplikativní inverzi. V tabulce 1b si můžeme všimnout, že existují čísla, která multiplikativní inverzi nemají. Konkrétně se jedná o čísla 2, 3 a 4, tedy čísla, která jsou s modulem 6 soudělná. Modul 5 je prvočíselný a žádné z čísel v záhlaví s ním soudělné být nemůže. Skutečně platí, že prvek a má multiplikativní inverzi a^{-1} pouze, pokud je s modulem m nesoudělný. Proto můžeme multiplikativní inverzi a^{-1} čísla a modulo m nalézt pomocí rozšířeného Euklidova algoritmu, jak je znázorněno v následujícím příkladu.

Příklad 19. Pokud existuje, nalezněte multiplikativní inverzi čísla 119 modulo 1 881. Využijte rozšířený Euklidův algoritmus.

Řešení. Nejprve pomocí Euklidova algoritmu ověříme, že $\text{NSD}(119, 1\,881)$ je roven číslu jedna, a tudíž jsou čísla 119 a 1 881 nesoudělná.

$$1\,881 = 15 \cdot 119 + 96$$

$$119 = 1 \cdot 96 + 23$$

$$96 = 4 \cdot 23 + 4$$

$$23 = 5 \cdot 4 + 3$$

$$4 = 1 \cdot 3 + 1$$

$$3 = 3 \cdot 1 + 0$$

Skutečně tedy platí, že $\text{NSD}(119, 1\,881) = 1$. Nyní použijeme postup z příkladu 11.

$$1 = 4 - 1 \cdot 3 = 4 - 1 \cdot (23 - 5 \cdot 4)$$

$$1 = -1 \cdot 23 + 6 \cdot 4 = -1 \cdot 23 + 6 \cdot (96 - 4 \cdot 23)$$

$$1 = 6 \cdot 96 - 25 \cdot 23 = 6 \cdot 96 - 25 \cdot (119 - 96)$$

$$1 = -25 \cdot 119 + 31 \cdot 96 = -25 \cdot 119 + 31 \cdot (1\,881 - 15 \cdot 119)$$

$$1 = 31 \cdot 1\,881 - 490 \cdot 119$$

Z poslední rovnosti vidíme, že platí

$$119 \cdot (-490) \equiv 1 \pmod{1\,881}$$

a číslo -490 je hledaná multiplikativní inverze. □

(časová náročnost: 15 min)

V dalším textu však budeme často potřebovat nalézt kladnou multiplikativní inverzi. To provedeme tak, že k záporné multiplikativní inverzi, která nám vyšla, přičteme modul.

Zkusme to ověřit na číslech, která nám vyšla v příkladu 19.

Příklad 20. Nalezněte kladnou multiplikativní inverzi čísla 119 modulo 1 881, když víte, že platí:

$$-490 \cdot 119 \equiv 1 \pmod{1\,881}.$$

Řešení. Kladnou multiplikativní inverzi obdržíme součtem

$$-490 + 1\,881 = 1\,391.$$

Pokud se skutečně jedná o multiplikativní inverzi, můžeme psát:

$$\begin{aligned} 1\,391 \cdot 119 &\equiv 1 \pmod{1\,881} \\ 165\,529 &\equiv 1 \pmod{1\,881}. \end{aligned}$$

Podle definice 12 platí:

$$\begin{aligned} 1\,881 &\mid (165\,529 - 1) \\ 1\,881 &\mid (165\,528). \end{aligned}$$

A podle věty 1 můžeme psát

$$165\,528 = 88 \cdot 1\,881 + 0.$$

Číslo 1 391 je tedy skutečně multiplikativní inverzí čísla 119 modulo 1 881. $\square$

(časová náročnost: 5 min)

ŠIFROVÁNÍ RSA

Název RSA je odvozen z iniciálů objevitelů algoritmu (Rivest, Shamir, Adelman). Jedná se o asymetrickou šifru, která k zašifrování zprávy využívá veřejný klíč (e, m) a k jejímu dešifrování využívá jiný, soukromý klíč (d, m) .

Velká výhoda asymetrických šifer spočívá právě ve využití různých klíčů k zašifrování a dešifrování zprávy. Odpadá tím potřeba distribuovat klíč bezpečným kanálem.

Definice 21 (Eulerova funkce φ). Pro každé přirozené číslo n udává Eulerova funkce $\varphi(n)$ počet všech přirozených čísel k takových, že $1 \leq k \leq n$ a $\text{NSD}(k, n) = 1$.

Platí:

- $\varphi(1) = 1$,
- $\varphi(p) = p - 1$ pro p prvočíslo,
- $\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p - 1) \cdot (q - 1)$, pro p, q nesoudělná,
- $\varphi(p^m) = (p - 1) \cdot p^{m-1}$ pro p prvočíslo a m přirozené číslo.

(časová náročnost: 5 min)

Příklad 22. Určete hodnoty Eulerovy funkce.

1. $\varphi(7) =$
2. $\varphi(95) =$
3. $\varphi(675) =$

Řešení.

1. $\varphi(7) = 7 - 1 = 6$
2. $\varphi(95) = \varphi(5 \cdot 19) = \varphi(5) \cdot \varphi(19) = (5 - 1) \cdot (19 - 1) = 4 \cdot 18 = 72$
3. $\varphi(675) = \varphi(3^3 \cdot 5^2) = \varphi(3^3) \cdot \varphi(5^2) = (2 \cdot 3^2) \cdot (4 \cdot 5^1) = 18 \cdot 20 = 360$

□

(časová náročnost: 5 min)

Věta 23 (Eulerova věta). *Nechť $a, m \in \mathbb{N}$ a $\text{NSD}(a, m) = 1$. Potom*

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

kde $\varphi(m)$ je Eulerova funkce.

(časová náročnost: 10 min)

Větu i s jejím důkazem lze najít v knize [3] na stranách 142–143.

Věta 24. *Nechť $a, k, l, m \in \mathbb{N}$, $a, m > 1$. Dále mějme množiny:*

$$\begin{aligned} C &= \{c \in \mathbb{Z}_m \mid \exists j \in \mathbb{N}: c \equiv a^j \pmod{m}\}, & |C| &= g \\ D &= \{d \in \mathbb{Z}_m \mid \exists ! j \in \mathbb{N}: d \equiv a^j \pmod{m}\}, & |D| &= i. \end{aligned}$$

Označme $q = g - i$, potom

$$[(\forall k, l > i)(a^k \equiv a^l \pmod{m})] \Leftrightarrow [k \equiv l \pmod{q}].$$

Důkaz. Budeme-li postupně přepočítávat mocniny a^j v modulu m , získáme množinu C různých zbytků. Počet těchto zbytků bude $g < m$.

Může se stát, že některé z těchto zbytků obdržíme pouze jednou. Tyto zbytky tvoří množinu D . Počet zbytků z množiny D může být i nulový a označíme jej i .

Bude tedy existovat $q = g - i$ různých zbytků, které budeme stále získávat.

Zřejmě tedy pro první zbytek, který získáme dvakrát, bude platit:

$$a^{(i+1)} \equiv a^{(i+1)+q} \pmod{m}. \quad (11)$$

1. Nejprve dokážeme, že q zbytků z množiny C se bude pravidelně opakovat. Důkaz provedeme matematickou indukcí vzhledem k $n \in \mathbb{N}$ a budeme dokazovat

$$a^{(i+1)+n} \equiv a^{(i+1)+n+q} \pmod{m}. \quad (12)$$

- (a) Nechť $n = 0$.

$$\begin{aligned} a^{(i+1)+0} &\equiv a^{(i+1)+0+q} \pmod{m} \\ a^{(i+1)} &\equiv a^{(i+1)+q} \pmod{m}. \end{aligned}$$

Vidíme, že poslední kongruence je stejná jako kongruence 11.

- (b) Předpokládejme nyní, že $n > 0$ a že $a^{(i+1)+n} \equiv a^{(i+1)+n+q} \pmod{m}$. Potom kongruenci $a^{(i+1)+n+1} \equiv a^{(i+1)+n+1+q} \pmod{m}$ upravíme a ukážeme, že rovněž platí.

$$\begin{aligned} a^{(i+1)+n+1} &\equiv a^{(i+1)+n+1+q} \pmod{m} \\ a^{(i+1)+n} \cdot a &\equiv a^{(i+1)+n+q} \cdot a \pmod{m} \end{aligned}$$

Poslední kongruence platí podle indukčního předpokladu a věty 16.2. Tím jsme dokázali platnost kongruence 12.

2. Dále nechť $s \in \mathbb{Z}_m$ a $t, u \in \mathbb{N}_0$, $t \leq u$. Dokážeme, že

$$a^{(i+1)+s+t \cdot q} \equiv a^{(i+1)+s+u \cdot q} \pmod{m}. \quad (13)$$

Podle věty 2 můžeme libovolné n z kongruence 12 vyjádřit jako

$$n = s + t \cdot q.$$

Obdržíme tak

$$a^{(i+1)+s+t \cdot q} \equiv a^{(i+1)+s+(t+1) \cdot q} \pmod{m}.$$

Dosaďme $t = 0$ a postupným násobením obou členů kongruence podle věty 16.2 číslem a^q obdržíme

$$\begin{aligned} a^{(i+1)+s+0 \cdot q} &\equiv a^{(i+1)+s+1 \cdot q} \pmod{m} \\ a^{(i+1)+s+1 \cdot q} &\equiv a^{(i+1)+s+2 \cdot q} \pmod{m} \\ a^{(i+1)+s+2 \cdot q} &\equiv a^{(i+1)+s+3 \cdot q} \pmod{m} \\ &\vdots \\ a^{(i+1)+s+(u-1) \cdot q} &\equiv a^{(i+1)+s+u \cdot q} \pmod{m}. \end{aligned} \quad (14)$$

Opakovaným použitím věty 14.3 na kongruence 14 obdržíme kongruenci 13.

3. Nakonec budeme dokazovat následující implikace.

$$a^k \equiv a^l \pmod{m} \Rightarrow k \equiv l \pmod{q} \quad (15)$$

$$k \equiv l \pmod{q} \Rightarrow a^k \equiv a^l \pmod{m} \quad (16)$$

Bez újmy na obecnosti můžeme vyjádřit

$$k = (i + 1) + s + t \cdot q$$

$$l = (i + 1) + s + u \cdot q.$$

(a) Nejprve ukážeme platnost implikace 15. Přepíšeme ji do tvaru

$$\begin{aligned} a^{(i+1)+s+t \cdot q} &\equiv a^{(i+1)+s+u \cdot q} \pmod{m} \Rightarrow \\ (i + 1) + s + t \cdot q &\equiv (i + 1) + s + u \cdot q \pmod{q}. \end{aligned} \quad (17)$$

Levá strana implikace platí podle kongruence 13. Pravou stranu implikace můžeme podle definice 12 přepsat jako

$$\begin{aligned} q &\mid [(i + 1) + s + t \cdot q] - [(i + 1) + s + u \cdot q] \\ q &\mid (t - u) \cdot q. \end{aligned}$$

Poslední výraz platí podle definice 1.

(b) Dále ukážeme platnost implikace 16. Přepíšeme ji do tvaru

$$\begin{aligned} (i + 1) + s + t \cdot q &\equiv (i + 1) + s + u \cdot q \pmod{q} \Rightarrow \\ a^{(i+1)+s+t \cdot q} &\equiv a^{(i+1)+s+u \cdot q} \pmod{m}. \end{aligned} \quad (18)$$

Platnost levé strany implikace jsme ukázali v předchozím případě jako pravou stranu implikace 17. Pravá strana implikace platí podle kongruence 13.

□

(časová náročnost: 20 min)

Příklad 25. Určete zbytek po dělení čísla $3^{235\,842\,671}$ číslem 15. Použijte větu 24.

Řešení. Nejprve budeme postupně počítat $3^j \pmod{15}$, abychom určili i a q .

$$3^1 \equiv 3 \pmod{15}$$

$$3^2 \equiv 3 \cdot 3 \equiv 9 \pmod{15}$$

$$3^3 \equiv 9 \cdot 3 \equiv 27 \equiv 12 \pmod{15}$$

$$3^4 \equiv 12 \cdot 3 \equiv 36 \equiv 6 \pmod{15}$$

$$3^5 \equiv 6 \cdot 3 \equiv 18 \equiv 3 \pmod{15}$$

Odtud je vidět, že $3^1 \equiv 3^5 \pmod{15}$. Existují tedy čtyři zbytky, které se periodicky opakují $\{3, 9, 12, 6\}$, $q = 4$ a $i = 0$.

Podle věty 6 určíme $235\,842\,671 \pmod{4}$.

$$\begin{aligned} 235\,842\,671 \pmod{4} &= 235\,842\,671 - 4 \cdot \left\lfloor \frac{235\,842\,671}{4} \right\rfloor \\ 235\,842\,671 \pmod{4} &= 235\,842\,671 - 4 \cdot 58\,960\,667 \\ 235\,842\,671 \pmod{4} &= 235\,842\,671 - 235\,842\,668 \\ 235\,842\,671 \pmod{4} &= 3 \end{aligned}$$

Podle věty 24 tedy platí

$$3^{235\,842\,671} \equiv 3^3 \equiv 12 \pmod{15}.$$

□

(časová náročnost: 15 min)

POSTUP ŠIFROVÁNÍ RSA

Představme si situaci, ve které potřebujeme adresátovi bezpečně odeslat zprávu z . Adresát tedy vygeneruje sadu klíčů. Veřejný klíč (e, m) a soukromý klíč (d, m) , přičemž pro koeficienty e a d platí

$$e \cdot d \equiv 1 \pmod{\varphi(m)}. \quad (19)$$

Následně nám svůj veřejný klíč (e, m) zašle. Zprávu z zašifrujeme jako

$$z^e \equiv c \pmod{m}$$

a adresátovi bezpečně zašleme zprávu c . Adresát obdrží zprávu c a dešifruje ji pomocí svého soukromého klíče jako

$$c^d \equiv z \pmod{m}. \quad (20)$$

Nyní zdůvodníme kongruenci 20.

Důkaz. Protože platí

$$\begin{aligned} c &\equiv z^e \pmod{m} \\ c^d &\equiv (z^e)^d \equiv z^{e \cdot d} \pmod{m}, \end{aligned}$$

ukážeme, že

$$z^{e \cdot d} \equiv z \pmod{m}. \quad (21)$$

Kongruenci 19 můžeme podle definice 12 přepsat jako

$$\varphi(m) \mid (e \cdot d - 1).$$

Podle definice 1 existuje $k \in \mathbb{Z}$ tak, že

$$\begin{aligned} \varphi(m) \cdot k &= e \cdot d - 1 \\ \varphi(m) \cdot k + 1 &= e \cdot d. \end{aligned} \quad (22)$$

Podle věty 23 můžeme psát

$$z^{\varphi(m)} \equiv 1 \pmod{m}. \quad (23)$$

Podle věty 16.2 můžeme psát

$$\begin{aligned} \underbrace{z^{\varphi(m)} \cdot z^{\varphi(m)} \cdot \dots \cdot z^{\varphi(m)}}_k &\equiv \underbrace{1 \cdot 1 \cdot \dots \cdot 1}_k \pmod{m} \\ z^{k \cdot \varphi(m)} &\equiv 1 \pmod{m} \\ z^{k \cdot \varphi(m)} \cdot z &\equiv 1 \cdot z \pmod{m} \\ z^{k \cdot \varphi(m) + 1} &\equiv z \pmod{m}. \end{aligned}$$

Dosaďme podle rovnosti 22 za $k \cdot \varphi(m) + 1$ výraz $e \cdot d$. Můžeme psát

$$z^{k \cdot \varphi(m) + 1} \equiv z^{e \cdot d} \equiv (z^e)^d \equiv c^d \equiv z \pmod{m}.$$

□

TVORBA KLÍČOVÉHO PÁRU

Příklad 26. Vygenerujte sadu klíčů podle návodu.

1. Zvolte „nepříliš blízka“ prvočísla p a q .

Řešení. $p = 11, q = 13$

□

2. Spočítejte modul šifrovací a dešifrovací transformace, $m = p \cdot q$.

Řešení.

$$m = p \cdot q$$

$$m = 11 \cdot 13$$

$$m = 143$$

□

3. Vypočítejte Eulerovu funkci pro m , $\varphi(m)$.

Řešení.

$$\varphi(143) = \varphi(11 \cdot 13) = \varphi(11) \cdot \varphi(13) = 10 \cdot 12 = 120$$

□

4. Zvolíme **šifrovací exponent** e takový, že

$$1 < e < \varphi(m) \wedge \text{NSD}(e, \varphi(m)) = 1.$$

Použijte Euklidův algoritmus.

Řešení. Zvolme například šifrovací exponent $e = 17$.

Protože $e = 17$ jsme zvolili prvočíselné, je zřejmé, že $\text{NSD}(17, 120) = 1$, ale výpočty z Euklidova algoritmu budeme potřebovat v následujícím úkolu.

$$120 = 7 \cdot 17 + 1$$

$$17 = 17 \cdot 1 + 0$$

□

5. Dopačítejte **dešifrovací exponent** d tak, aby d bylo multiplikativní inverzí k e modulo $\varphi(m)$,

$$d \cdot e \equiv 1 \pmod{\varphi(m)}.$$

Řešení. K nalezení multiplikativní inverze čísla e modulo $\varphi(m)$ pomocí rozšířeného Euklidova algoritmu využijeme výpočty z předchozího úkolu a postup z příkladu 11.

$$1 = 120 - 7 \cdot 17$$

Multiplikativní inverze čísla 17 modulo 120 je tedy -7 . K dalším výpočtům však budeme potřebovat kladnou multiplikativní inverzi, kterou nalezneme podle příkladu 20.

$$-7 + 120 = 113$$

Nakonec ověříme, že číslo 113 je multiplikativní inverzí čísla 17 modulo 120.

$$113 \cdot 17 = 1921$$

$$1921 = 16 \cdot 120 + 1$$

Dešifrovací exponent $d = 113$. □

Získali jsme tedy sadu klíčů. Veřejný klíč $(17, 143)$ a soukromý klíč $(113, 143)$.

(časová náročnost: 20 min)

Příklad 27. Ověřte, že vygenerované klíče fungují.

1. Vygenerovaným veřejným klíčem zašifrujte číslo 5. Využijte kongruenci $c \equiv 5^e \pmod{m}$ a větu 24.

Řešení.

$5^1 \equiv 5 \pmod{143}$	$5^7 \equiv 47 \pmod{143}$	$5^{13} \equiv 70 \pmod{143}$
$5^2 \equiv 25 \pmod{143}$	$5^8 \equiv 92 \pmod{143}$	$5^{14} \equiv 64 \pmod{143}$
$5^3 \equiv 125 \pmod{143}$	$5^9 \equiv 31 \pmod{143}$	$5^{15} \equiv 34 \pmod{143}$
$5^4 \equiv 53 \pmod{143}$	$5^{10} \equiv 12 \pmod{143}$	$5^{16} \equiv 27 \pmod{143}$
$5^5 \equiv 122 \pmod{143}$	$5^{11} \equiv 60 \pmod{143}$	$5^{17} \equiv 135 \pmod{143}$
$5^6 \equiv 38 \pmod{143}$	$5^{12} \equiv 14 \pmod{143}$	

□

2. Výsledek dešifrujte soukromým klíčem. S využitím věty 24 ověřte kongruenci $5 \equiv c^d \pmod{m}$.

Řešení.

$135^1 \equiv 135 \pmod{143}$	$135^8 \equiv 27 \pmod{143}$	$135^{15} \equiv 34 \pmod{143}$
$135^2 \equiv 64 \pmod{143}$	$135^9 \equiv 27 \pmod{143}$	$135^{16} \equiv 14 \pmod{143}$
$135^3 \equiv 60 \pmod{143}$	$135^{10} \equiv 12 \pmod{143}$	$135^{17} \equiv 31 \pmod{143}$
$135^4 \equiv 92 \pmod{143}$	$135^{11} \equiv 47 \pmod{143}$	$135^{18} \equiv 38 \pmod{143}$
$135^5 \equiv 122 \pmod{143}$	$135^{12} \equiv 53 \pmod{143}$	$135^{19} \equiv 125 \pmod{143}$
$135^6 \equiv 25 \pmod{143}$	$135^{13} \equiv 5 \pmod{143}$	$135^{20} \equiv 1 \pmod{143}$
$135^7 \equiv 86 \pmod{143}$	$135^{14} \equiv 103 \pmod{143}$	

Podle věty 24 je $g = q = 20$, $i = 0$.

$$113 \pmod{20} = 113 - 20 \cdot \left\lfloor \frac{113}{20} \right\rfloor = 113 - 20 \cdot 5 = 13$$

$$113 \equiv 13 \pmod{20} \Rightarrow 135^{113} \equiv 135^{13} \equiv 5 \pmod{143}.$$

□

(časová náročnost: 15 min)

ŠIFRÁTOR A DEŠIFRÁTOR

Jedná se o počítačové programy, které nalezneme pod názvy „Sifrator“ a „Desifrator“, v dalším textu je však budeme nazývat Šifrátor a Dešifrátor.

Symbody použité v programech pro přehlednost uvádíme v tabulce 2. Šifrátor si po spuštění vyžádá zadání veřejného klíče a zprávy, kterou má zašifrovat. Zprávu v programu zapisujeme bez diakritiky a jednotlivá slova oddělujeme symbolem „-“. Nepoužíváme mezerník.

Následně program postupně po jednom přečte symbody, které zpráva obsahuje a nalezne je v tabulce 2. Nahraje index čteného symbolu a podle věty 24 je přepočítá jako

$$index^c \equiv c \pmod{m}.$$

Každé získané číslo pak vypíše na vlastní řádek v poznámkovém bloku a uloží jej pod názvem „zasifrovaná_zpráva“. Na první řádek však zapíše veřejný klíč, kterým byla zpráva zašifrována. Tuto informaci budeme potřebovat při řešení posledního úkolu.

Poznámkový blok se zašifrovanou zprávou lze adresátovi zaslat pomocí e-mailu, sociálních sítí nebo ji můžeme předat na externím disku. Adresát, který zašifrovanou zprávu přijme, ji uloží do složky s Dešifrátorem a program spustí. Program si vyžádá zadání adresátova soukromého klíče. Následně začne po řádcích načítat čísla ze zašifrované zprávy a opět podle věty 24 provede výpočet

$$c^d \equiv index \pmod{m}.$$

Následně v tabulce 2 nalezne příslušný $index$ a symbol vypíše.

Příklad 28. Obdrženým veřejným klíčem zašifrujte zprávu pomocí Šifrátoru. Vygenerovaný poznámkový blok odešlete adresátovi.

Řešení. Obdrželi jsme veřejný klíč (17, 437). Spustíme program Šifrátor. Zobrazí se následující instrukce.

Tabulka 2: Tabulka symbolů

index	0	1	2	3	4	5	6	7	8	9
symbol			1	2	3	4	5	6	7	8
index	10	11	12	13	14	15	16	17	18	19
symbol	9	0	a	b	c	d	e	f	g	h
index	20	21	22	23	24	25	26	27	28	29
symbol	i	j	k	l	m	n	o	p	q	r
index	30	31	32	33	34	35	36	37	38	39
symbol	s	t	u	v	w	x	y	z	A	B
index	40	41	42	43	44	45	46	47	48	49
symbol	C	D	E	F	G	H	I	J	K	L
index	50	51	52	53	54	55	56	57	58	59
symbol	M	N	O	P	Q	R	S	T	U	V
index	60	61	62	63	64	65	66	67	68	69
symbol	W	X	Y	Z	,	.	?	!	-	+
index	70	71	72	73	74	75	76	77	78	79
symbol	—	*	/	\$	<	>	(	)	[	]
index	80	81	82	83	84	85	86	87	88	89
symbol	{	}	=	~	'	°	“	”	'	-

- Zadej mensi clen verejneho klice a stiskni Enter:

Zadáme číslo 17.

- Zadej vetsi clen verejneho klice a stiskni Enter:

Zadáme číslo 437.

- Zadej zpravu:

1. bez diakritiky

2. mezeru zapis znakem: _

3. stiskni Enter

Zadáme zpravu: `The_Beacons_of_Minas_Tirith!_The_Beacons_are_lit!_Gondor_calls_for_aid.`

Program přepočítá jednotlivé znaky a výsledná čísla zapíše do poznámkového bloku. Situace je znázorněna na obrázcích 3 a 4. □

(časová náročnost: 10 min)

Obr. 3: Zašifrování zprávy Šifrátorem

Obr. 4: Zašifrovaná zpráva

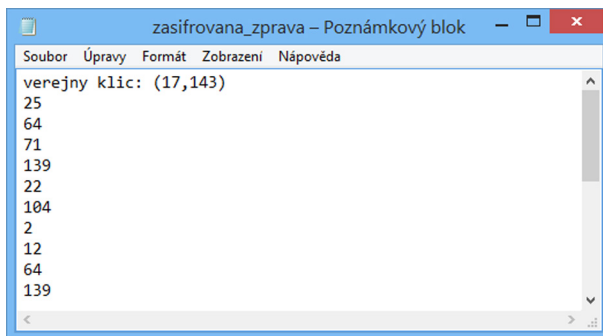
Příklad 29. Od odesílatele obdržíte zprávu. Dešifrujte ji pomocí Dešifrátoru svým soukromým klíčem.

Řešení. Zpráva je znázorněna na obrázku 5. Spustíme program Dešifrátor. Zobrazí se následující instrukce.

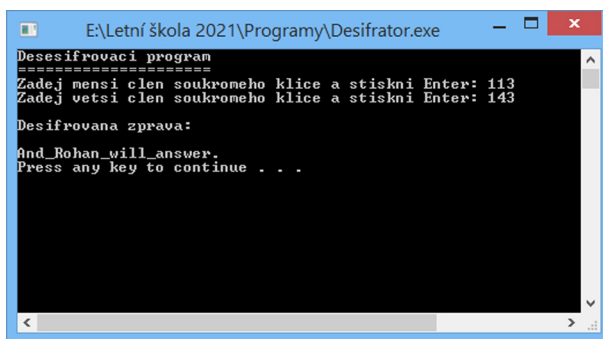
- Zadej mensi clen soukromeho klice a stiskni Enter:
Zadáme číslo 113.
- Zadej vetsi clen soukromeho klice a stiskni Enter:
Zadáme číslo 143.

Následně se zobrazí dešifrovaná zpráva. Situace je znázorněna na obrázku 6. □

(časová náročnost: 10 min)



Obr. 5: Zašifrovaná zpráva



Obr. 6: Dešifrovaná zpráva

Příklad 30. Zachytili jste cizí zprávu v poznámkovém bloku. Na prvním řádku zprávy naleznete veřejný klíč. Přepočítejte jej na soukromý klíč a zprávu dešifrujte pomocí Dešifrátoru.

Řešení. Zpráva je znázorněna na obrázku 7. Z prvního řádku zprávy vidíme, že byla zašifrována veřejným klíčem (23, 143). Musíme tedy provést faktorizaci čísla 143 a určit multiplikativní inverzi čísla 23 modulo $\varphi(143)$.

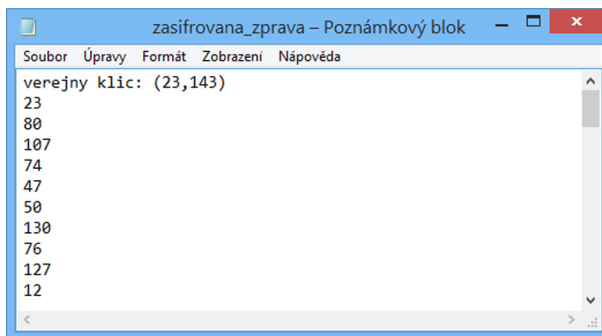
$$143 = 11 \cdot 13$$

Potom

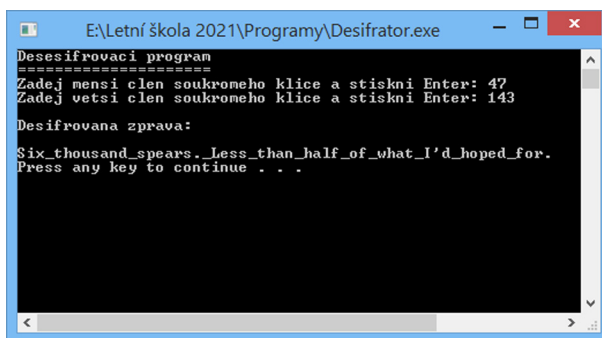
$$\varphi(143) = 10 \cdot 12 = 120.$$

Dále použijeme Euklidův algoritmus při hledání NSD(23, 120).

$$120 = 5 \cdot 23 + 5$$



Obr. 7: Dešifrovaná zpráva



Obr. 8: Dešifrovaná zpráva

$$23 = 5 \cdot 4 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

Dále určíme multiplikativní inverzi podle příkladu 19.

$$1 = 3 - 2$$

$$1 = 3 - (5 - 3) = -5 + 2 \cdot 3$$

$$1 = -5 + 2 \cdot (23 - 4 \cdot 5) = 2 \cdot 23 - 9 \cdot 5$$

$$1 = 2 \cdot 23 - 9 \cdot (120 - 5 \cdot 23) = -9 \cdot 120 + 47 \cdot 23$$

Multiplikativní inverze čísla 23 modulo 120 je tedy 47. Nyní můžeme zprávu dešifrovat pomocí Dešifrátoru. Situace je znázorněna na obrázku 8. $\square$

(časová náročnost: 20 min)

ZÁVĚR

Semináře šifrování RSA se zúčastnilo třináct dětí, jedenáct z nich studovalo gymnázium, dvě další studovaly jinou střední školu. Z toho čtyři ukončily druhý ročník, šest ukončilo třetí ročník a tři ukončily čtvrtý ročník. Účastníci vyplnili závěrečný dotazník následovně.

DATA Z DOTAZNÍKŮ

- Příklad 4** vyřešilo samostatně: 12,
samostatně nevyřešilo, ale užití definice 3 pochopilo: 1,
samostatně nevyřešilo a užití definice 3 nepochopilo: 0.
- Příklad 7** vyřešilo samostatně: 13,
samostatně nevyřešilo, ale užití věty 6 pochopilo: 0,
samostatně nevyřešilo a užití věty 6 nepochopilo: 0.
- Příklad 13** vyřešilo samostatně: 12,
samostatně nevyřešilo, ale užití definice 12 pochopilo: 1,
samostatně nevyřešilo a užití definice 12 nepochopilo: 0.
- Příklad 19** NSD samostatně určilo: 12,
NSD samostatně neurčilo, ale užití Euklidova algoritmu pochopilo: 1,
NSD samostatně neurčilo a užití Euklidova algoritmu nepochopilo: 0,
multiplikativní inverzi samostatně určilo: 8,
multiplikativní inverzi samostatně neurčilo, ale užití Euklidova algoritmu pochopilo: 5,
multiplikativní inverzi samostatně neurčilo a užití Euklidova algoritmu nepochopilo: 0.
- Příklad 22** vyřešilo samostatně: 8,
samostatně nevyřešilo, ale užití věty 21 pochopilo: 5,
samostatně nevyřešilo a užití věty 21 nepochopilo: 0.
- Příklad 25** vyřešilo samostatně: 8,
samostatně nevyřešilo, ale užití definice 24 pochopilo: 4,
samostatně nevyřešilo a užití definice 24 nepochopilo: 1.
- Příklad 26** samostatně vygenerovalo a princip generování klíčů pochopilo: 10,
samostatně nevygenerovalo, ale princip generování klíčů pochopilo: 3,
samostatně nevygenerovalo a princip generování klíčů nepochopilo: 0.

Příklad 27 při ověřování sady klíčů princip šifrování RSA pochopilo: 13,
při ověřování sady klíčů princip šifrování RSA nepochopilo: 0.

Na základě odpovědí z dotazníku se zdá, že zadané úkoly účastníkům semináře nečinily velké potíže. Je však nutné podotknout, že se nejedná o reprezentativní vzorek běžné třídy.

PODĚKOVÁNÍ

Děkuji PhDr. Magdaleně Krátké, Ph.D., za to, že mi umožnila na letní škole vystoupit a téma ověřit v praxi.

Dále děkuji Bc. Pavlíně Matysové za zapůjčení notebooků, na kterých jsme s dětmi mohli provádět šifrování a dešifrování zpráv.

LITERATURA

- [1] Huraj, J. (2002). *Nebojme sa šifrovania*. 1. vyd. Bratislava: Metodicko-pedagogické centrum.
- [2] Kořínek, V. (1956). *Základy algebry*. 2. vyd. Praha: Nakladatelství Československé akademie věd.
- [3] Jahoda, P. (2011). *Základy teorie čísel a jejích aplikací pro nematematiky*. Ostrava: VŠB–TU.

GEOMETRICKÁ KONSTRUKCE LOMENÉHO PAPRSKU

Tomáš Vlasák

ABSTRAKT

Při lomu na rozhraní dvou optických prostředí lze lomený paprsek najít výpočtem ze Snellova zákona. Příspěvek ukazuje, jak lze úhel lomu a tím pádem i lomený paprsek najít čistě geometricky bez nutnosti výpočtů ze Snellova zákona.

KLÍČOVÁ SLOVA: Snellův zákon, lomený paprsek, geometrická optika.

ÚVOD

Sledujme paprsek světla dopadající na rozhraní dvou prostředí s jinými optickými vlastnostmi. Po dopadu paprsku na rozhraní pozorujeme jednak odražený paprsek, za určitých okolností též lomený paprsek.

Pro popis chování dopadajícího paprsku je klíčová rychlost, s jakou se světlo pohybuje v obou dvou prostředích. Rychlost šíření světla v prostředí je charakterizována veličinou index lomu n , která udává, kolikrát je rychlost světla ve vakuu c větší než rychlost světla v daném prostředí v :

$$n = \frac{c}{v}.$$

Kolmice dopadu je přímka kolmá na optické rozhraní procházející bodem, v němž se dopadající paprsek rozhraní dotýká. Úhel dopadu α je poté úhel, který svírá dopadající paprsek s kolmicí dopadu. Úhel odrazu α' je úhel, který svírá odražený paprsek s kolmicí dopadu. Podle zákona odrazu se velikosti úhlu dopadu a úhlu odrazu rovnají, tedy $\alpha = \alpha'$. Jako úhel lomu β se označuje úhel, který svírá lomený paprsek s kolmicí dopadu.

Uvažujme nyní situaci, kdy dopadající paprsek dopadá pod úhlem dopadu α na rozhraní dvou optických prostředí s indexy lomu n_1 a n_2 a do druhého prostředí se láme pod úhlem lomu β . Index lomu a úhly dopadu a lomu jsou pak svázány

vztahem, který se nazývá Snellův zákon, a který se dá matematicky vyjádřit vztahem

$$n_1 \sin \alpha = n_2 \sin \beta.$$

Ze známých indexů lomu a známého úhlu dopadu lze tedy pomocí Snellova zákona dopočítat úhel lomu.

Ze Snellova zákona vyplývá, že pro případ kdy $n_1 > n_2$ může nastat situace, kdy je úhel lomu roven 90° a lomený paprsek by se tedy měl šířit v rovině rozhraní. V této situaci říkáme, že nastal totální odraz. Úhel dopadu v tomto případě označujeme jako mezní úhel dopadu a značíme ho α_m . Pozorujeme pouze odražený paprsek, rovinou rozhraní se šíří rychle utlumená evanescentní vlna. Rovněž pro větší úhly dopadu než je mezní úhel dopadu pozorujeme pouze odražený paprsek. [1]

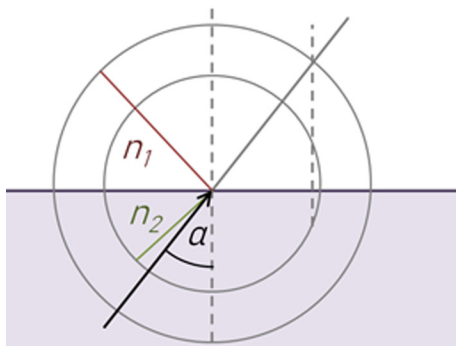
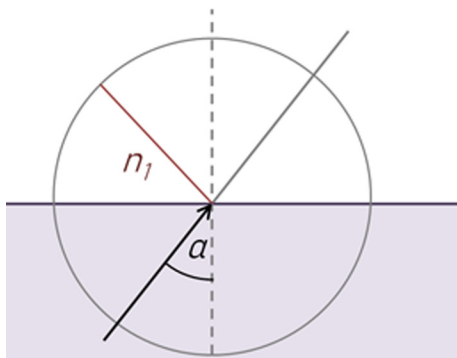
Potíž s tímto přístupem k lomu světla spočívá v tom, že Snellův zákon obsahuje goniometrické funkce a v praktických případech nelze snadno výsledek rychle spočítat. Často bývá velmi obtížné rychle odhadnout, jak velký bude úhel lomu nebo rozhodnout, zda nastane totální odraz. To může činit potíže, pokud chcí například rychle načrtnout nějakou konkrétní situaci na tabuli.

V tomto příspěvku bude vysvětlena konstrukce, kterou lze lomený paprsek najít bez výpočtů čistě geometrickým způsobem. Konstrukce je natolik jednoduchá, že ji lze provádět i čistě mentálně a rychle načrtnout se slušnou přesností lomený paprsek i v případě exotičtějších kombinací indexů lomů dvou prostředí. Konstrukce je běžně popisovaná ve francouzských učebnicích fyziky, například v [2]. Z autorových osobních zkušeností vyplývá, že u nás je téměř neznámá.

POSTUP KONSTRUKCE

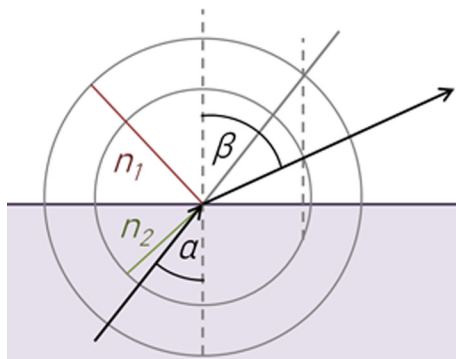
Geometrickou konstrukci určenou k načrtnutí lomeného paprsku (případně rozhodnutí, že nastal totální odraz) lze shrnout do následujících kroků:

1. Přicházející paprsek prodloužíme za rozhraní do druhého prostředí.
2. Do průsečíku přicházejícího paprsku a optického rozhraní umístíme střed kružnice, jejíž poloměr je úměrný indexu lomu prvního prostředí n_1 (viz obrázek 1).
3. Vedeme kolmici k rozhraní, která prochází průsečíkem kružnice s prodlouženým paprskem.
4. Do průsečíku přicházejícího paprsku a optického rozhraní umístíme střed kružnice, jejíž poloměr je úměrný indexu lomu druhého prostředí n_2 (viz obrázek 2).



Obr. 1: První krok geometrické konstrukce Obr. 2: Druhý krok geometrické konstrukce

5. Pokud pomocná kolmice k rozhraní protíná druhou kružnici, pak nenastal totální odraz. Průsečíkem pomocné kolmice a druhé kružnice v druhém prostředí vedeme lomený paprsek.

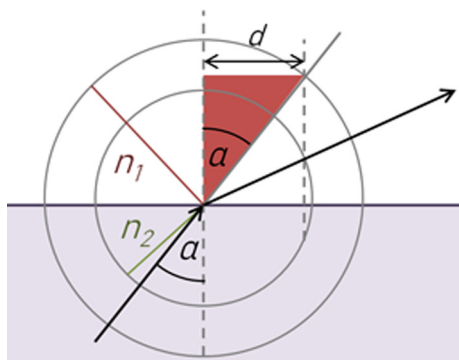


Obr. 3: Třetí krok geometrické konstrukce

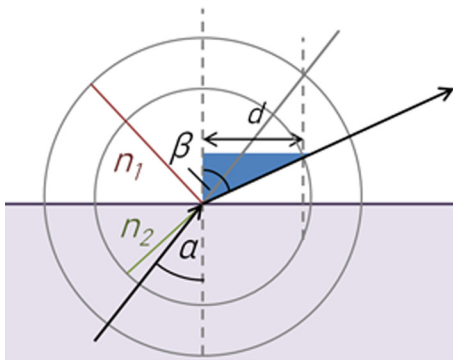
6. Pokud pomocná kolmice k rozhraní neprotíná druhou kružnici, pak nastal totální odraz. Pokud má pomocná kolmice s druhou kružnicí právě jeden společný bod, paprsek dopadá pod mezním úhlem dopadu.

PROČ TO FUNGUJE?

Podívejme se nyní, proč tato konstrukce vlastně funguje. Vysvětlení založíme na obrázcích 4 a 5, na kterých jsou v konstrukci barevně vyznačeny dva pravouhlé trojúhelníky.



Obr. 4: První náčrtek k vysvětlení konstrukce



Obr. 5: Druhý náčrtek k vysvětlení konstrukce

Z červeného pravoúhlého trojúhelníku na obrázku 4 vyplývá, že pro vzdálenost d platí

$$d = n_1 \sin \alpha.$$

Z modrého trojúhelníku na obrázku 5 pro vzdálenost d vyplývá, že musí být rovněž rovna

$$d = n_2 \sin \beta.$$

Pokud vložíme pravé strany těchto rovnic do rovnosti, získáme Snellův zákon

$$n_1 \sin \alpha = n_2 \sin \beta.$$

ZÁVĚR

V příspěvku byl shrnut postup, jak najít lomený paprsek na základě úhlu dopadu a indexů lomů obou prostředí čistě geometrickým způsobem.

LITERATURA

- [1] Lepil, O. (2015). *Fyzika pro gymnázia – Optika*. Praha: Prometheus.
- [2] Maurel, A. & Malbec, J.M. (2002). *Optique géométrique. Rappels de cours et exercices*. Paris: Éditions Belin.

ZÁKONY IDEÁLNÍHO PLYNU

Zuzana Vlasáková

ABSTRAKT

Příspěvek vysvětluje koncept ideálního plynu a jeho stavové rovnice. V hlavní části se zabývá historickým odvozením této rovnice a zejména jednotlivými dílčími zákony, které k němu vedly.

KLÍČOVÁ SLOVA: ideální plyn, stavová rovnice, Boyleův zákon, Gay-Lussacův zákon, Charlesův zákon.

IDEÁLNÍ PLYN

Pokusíte-li se najít ve vašem okolí ideální plyn, budete hledat marně. Jedná se totiž, jak název napovídá, o idealizaci, zjednodušený model plynu reálného. V čem toto zjednodušení spočívá? V následujících třech vlastnostech [1]:

- Rozměry jeho molekul se považují za zanedbatelné.
- Kromě okamžiku srážek na sebe molekuly nepůsobí silami.
- Srážky molekul jsou dokonale pružné.

Zavedením těchto podmínek se nám značně zjednodušují výpočty a rovnice, které plyn popisují. Jednoduché rovnice by nám ale nebyly k ničemu, kdyby se tento model nedal použít k popisu reálného světa – naštěstí se ale ukazuje, že se ve skutečnosti za vhodných podmínek většina běžných plynů přibližně jako ideální chová. Problémy nastanou, pokud se dostaneme do oblastí vysokých tlaků nebo nízkých teplot nebo pokud bychom se snažili popsat chování těžších plynů, jako jsou např. freony.

A o jakých rovnicích popisujících ideální plyn to vlastně mluvíme? Bude se jednat hlavně o jednu rovnici, tzv. stavovou rovnici popisující vztah mezi tlakem, teplotou, objemem a látkovým množstvím, tedy stavovými veličinami (veličinami popisujícími stav daného plynu). Ukážeme si, že přestože má tato rovnice velmi jednoduchý tvar, cesta k jejímu objevení trvala zhruba 200 let a zahrnovala několik dílčích výsledků.

, vlasakova.zuzka@seznam.cz

BOYLEŮV ZÁKON

Robert Boyle (1627–1691) byl irský chemik a fyzik, někdy považován za „zakladatele moderní chemie“ [2]. Zabýval se různorodými experimenty, jeho asistent byl přitom Robert Hooke, kterého můžete znát jako autora Hookova zákona. Mimo jiné zdokonalil vakuovou pumpu, a díky tomu mohl zkoumat vzduch při nižším tlaku. Přitom ho nezajímal vzduch jen z fyzikálního a chemického hlediska, ale např. i fyziologický vliv vzduchu a jeho nedostatku na živé tvory. Na obraze Josepha Wrighta z roku 1768 (viz obrázek 1) je vidět jeden z těchto poněkud krutých pokusů.



Obr. 1: Experiment na ptáku ve vývěvě od Josepha Wrighta, 1768 [3]

Ve svém díle *New Experiments Physico-Mechanical, Touching the Spring of the Air, and its Effects* z roku 1660 [4] detailně zdokumentoval 43 různých pokusů a dva roky poté publikoval druhé vydání [5] se svou reakcí na různé připomínky k jeho závěrům. V rámci jedné této reakce sepsal měření, jehož výsledky jsou uvedeny na obrázku 2.

A table of the condensation of the air.

<i>A</i>	<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>	<i>E</i>
48	12	00	Added to 22½ makes	29½	29½
46	11½	01½		30½	33½
44	11	02½		31½	31½
42	10½	04½		33½	33½
40	10	06½		35½	35 -
38	9½	07½		37	36½
36	9	10½		39½	38½
34	8½	12½		41½	41½
32	8	15½		44½	43½
30	7½	17½		47½	46½
28	7	21½		50½	50 -
26	6½	25½		54½	53½
24	6	29½		58½	58½
23	5½	32½		61½	60½
22	5½	34½		64½	63½
21	5¼	37½		67½	66¼
20	5	41½		70½	70 -
19	4¾	45 -		74½	73½
18	4½	48½		77½	77½
17	4¼	53½		82½	82¼
16	4	58½		87½	87½
15	3¾	63½		93½	93½
14	3½	71½		100½	99½
13	3¼	78½		107½	107½
12	3	88½		117½	116¼

AA. The number of equal spaces in the shorter leg, that contained the same parcel of air diversly extended.

B. The height of the mercurial cylinder in the longer leg, that compressed the air into those dimensions.

C. The height of the mercurial cylinder, that counterbalanced the pressure of the atmosphere.

D. The aggregate of the two last columns *B* and *C*, exhibiting the pressure sustained by the included air.

E. What that pressure should be according to the hypothesis, that supposes the pressures and expansions to be in reciprocal proportion.

Obr. 2: Výsledky Boyleova experimentu [5]

Experiment provedl následovně [5]: připravil si dlouhou zkumavku, kterou na jednom konci ohnul tak, aby její tvar připomínal písmeno J. Do každého ramene vložil papír s měřítkem, jehož nejmenší dílek byl 1/4 palce. Na začátku experimentu nalil do zkumavky opatrně rtuť tak, aby byla v obou ramenech ve stejné výšce (tím pádem byl v uzavřené části atmosférický tlak). Sloupec A v tabulce na obrázku 2 obsahuje výšku vzduchového sloupce v kratším rameni, přitom první sloupec A je uvedený v počtu dílků stupnice, druhý sloupec A je potom v palcích. Protože průměr zkumavky by měl být konstantní, tento sloupec vlastně reprezentuje objem vzduchu. Sloupec B je výška rtuťového sloupce v delším rameni, reprezentuje tedy hydrostatický tlak tohoto sloupce podle známého vzorce

$$p = h\rho g. \quad (1)$$

Sloupec C je pak vlastně atmosférický tlak vyjádřený jako výška rtuťového sloupce (na základě vztahu 1, přesnou hodnotu této výšky lze jednoduše určit dosazením hodnoty atmosférického tlaku, hustoty rtuti a tíhového zrychlení). Sloupec D obsahuje výsledný tlak vzduchu určený jako součet sloupců B a C (tedy hydrostatického a atmosférického tlaku). V sloupci E je potom vypočtená hodnota, která by odpovídala tomu, že by platil vztah

$$p = \frac{\text{konst.}}{V}. \quad (2)$$

Boyle sloupce D a E ručně porovnával a dospěl k závěru, že tato hypotéza platí. Vztah 2 ukazuje, že za konstantní teploty je objem nepřímo úměrný tlaku plynu a nazývá se Boyleův zákon¹.

GAY-LUSSACŮV A CHARLESŮV ZÁKON

Jacques Charles (1746–1823) byl vynálezce a fyzik, který ale zřejmě vlastnosti plynů nezkoumal čistě z teoretického zájmu, nýbrž kvůli svému nadšení do létání balónem. Byl jeden z jeho prvních průkopníků a v roce 1783 dokonce spolu s bratry Robertovými sestavil a vypustil první vodíkem plněný balon [6].

Charles zkoumal vlastnosti různých plynů při jejich zahřívání, svoje výsledky ale nikdy nepublikoval. O jeho poznatcích víme tedy jen z publikací Josepha Gay-Lussaca (1778–1850) [7, 8], který, jak sám tvrdí, se o nich dozvěděl pouhou náhodou. Gay-Lussac byl významný fyzik a chemik, který opakoval Charlesovy

¹Někdy (obzvlášť ve Francii) také zvaný Mariottův zákon po francouzském fyzikovi Edme Mariottovi (1620–1684), který ho nezávisle objevil.

experimenty se zahříváním plynů (konkrétně s kyslíkem, dusíkem, vodíkem, oxidem uhličitým a vzduchem) a zároveň prováděl svoje vlastní experimenty. S Charlesem měli zřejmě společný i zájem o lety balónem – sám Gay-Lussac balonem letěl až do výšky 7 km, aby mohl měřit vlastnosti vzduchu za různých podmínek.

Zahřívání plynu můžeme provádět tak, že udržujeme jeho objem konstantní (izochorické zahřívání) a necháme volně měnit tlak plynu, nebo tak, že udržujeme konstantní jeho tlak (izobarické zahřívání) a necháme měnit jeho objem.

Tyto dva druhy ohřívání popisují další dva zákony. Pravděpodobně díky podobnostem mezi experimenty Charlese a Gay-Lussaca a znalosti Charlesových experimentů jen z Gay-Lussacových referencí jsou ale dohledatelné informace o objevech těchto dvou zákonů značně chaotické a nekonzistentní, a to dokonce do té míry, že existuje rozdíl i v názvosloví. Zatímco zákon o izobarickém ději

$$\frac{V}{T} = \text{konst.}, \quad (3)$$

který matematicky vyjadřuje, že objem je přímo úměrný teplotě, se v anglické literatuře označuje jako Charlesův zákon (Charles's law), v české literatuře ho nalezneme pod názvem Gay-Lussacův zákon.

Asi už tušíte, že zákon o izochorickém ději

$$\frac{p}{T} = \text{konst.}, \quad (4)$$

který matematicky vyjadřuje, že tlak je přímo úměrný teplotě, se v anglické literatuře označuje jako Gay-Lussacův zákon (Gay-Lussac's law), v české literatuře ho ale nalezneme pod názvem Charlesův zákon.

AVOGADRŮV ZÁKON

V roce 1811 [9] publikoval italský vědec Amedeo Avogadro (1776–1856) hypotézu říkájící, že za konstantního tlaku a teploty obsahují stejné objemy různých plynů stejné množství molekul [10, 11]. S využitím jednotky látkové množství n (což není vlastně nic jiného než počet molekul udaný v jiných jednotkách) bychom v současnosti toto tvrzení, označované jako Avogadrův zákon, zapsali vztahem

$$\frac{V}{n} = \text{konst.} \quad (5)$$

STAVOVÁ ROVNICE

Spojením vztahů 2, 3, 4, 5 získáváme konečně finální stavovou rovnici ideálního plynu [12]

$$pV = nRT, \quad (6)$$

kde R je konstanta zvaná molární plynová konstanta. Tuto souhrnnou rovnici poprvé odvodil fyzik Benoît Clapeyron (1799–1864) [13], který ji publikoval ve svém článku z roku 1834 [14]. Clapeyron se velmi významně podílel na rozvoji termodynamiky, známá je po něm pojmenovaná Clausiova-Clapeyronova rovnice, kterou se popisují fázové přechody².

Přestože se tento příspěvek věnuje ideálnímu plynu, pojďme se na závěr podívat i na náznak zobecnění stavové rovnice pro plyny, které už za ideální považovat nemůžeme. Tímto zobecněním je tzv. Van der Waalsova rovnice [15]

$$\left(p + n^2 \frac{a}{V^2}\right) (V - nb) = nRT. \quad (7)$$

Při porovnání rovnic 6 a 7 vidíme, že rozdíl je jen ve dvou korekčních členech $\frac{n^2 a}{V^2}$ a $-nb$, které Van der Waalsova rovnice obsahuje. První z nich opravuje předpoklad, že molekuly plynu na sebe nepůsobí silami, a započítává tlak, který vytváří přitažlivé mezimolekulární síly. Druhý člen opravuje předpoklad, že rozměry molekul plynu jsou zanedbatelné – celkový objem zmenšuje o vlastní objem molekul (toto se projevuje hlavně při vyšším tlaku, kdy už vlastní objem vůči objemu plynu nelze zanedbat).

ZÁVĚR

Při hodinách středoškolské fyziky se nám může zdát divné, proč se musíme učit o různých zákonech se špatně zapamatovatelnými názvy, které přitom všechny jednoduše plynou ze stavové rovnice. Snad bylo v tomto článku čtenáři ukázáno, že důvod je jednoduchý – i k takovéto jednoduché rovnici se muselo dospět postupně během mnoha let a za každým dílčím poznatkem, který se nám z dnešního pohledu zdá jako samozřejmý, stála usilovná práce mnoha vědců.

²O fázových přechodech se v tomto příspěvku vůbec nezmiňujeme, stavová rovnice ideálního plynu totiž fázové přechody vůbec nezohledňuje (což je jedna z jejích dalších nevýhod).

LITERATURA

- [1] Reichl, J. & Všeticka, M. (22. 3. 2008). *Ideální plyn. Encyklopedie fyziky*. Citováno 15. 1. 2022.
Dostupné z <http://fyzika.jreichl.com/main.article/view/592-idealni-plyn>
- [2] Principe, L.M. (27. 12. 2021). *Robert Boyle. Encyclopedia Britannica*. Citováno 15. 1. 2022.
Dostupné z <https://www.britannica.com/biography/Robert-Boyle>
- [3] The National Gallery, London. *An Experiment on a Bird in the Air Pump*. Citováno 15. 1. 2022.
Dostupné z <https://www.nationalgalleryimages.co.uk/asset/1761/>
- [4] Boyle, R. (1660). *New Experiments Physico-Mechanicall, Touching the Spring of the Air, and its Effects*. Oxford: H. Hall for T. Robinson.
- [5] Boyle, R. (1662). *New Experiments Physico-Mechanical, Touching the Air: Whereunto is Added A Defence of the Authors Explication of the Experiments, Against the Objections of Franciscus Linus, and, Thomas Hobbes*. Oxford: H. Hall for T. Robinson
- [6] Science & Society Picture Library. *Medal commemorating Charles and Robert's balloon ascent, Paris, 1783*. Citováno 15. 1. 2022.
Dostupné z <https://www.scienceandsociety.co.uk/results.asp?image=10447673>
- [7] Crosland, M.P. (2. 12. 2021). *Joseph-Louis Gay-Lussac. Encyclopedia Britannica*. Citováno 15. 1. 2022. Dostupné z <https://www.britannica.com/biography/Joseph-Louis-Gay-Lussac>
- [8] Gay-Lussac, J. L. (1802). Recherches sur la dilatation des gaz et des vapeurs [Researches on the expansion of gases and vapors]. *Annales de Chimie* (43), s. 137–75. Anglický překlad.
Dostupné z <https://web.lemoyne.edu/~giunta/gaygas.html>
- [9] Avogadro, A. (1810). Essai d'une maniere de determiner les masses relatives des molecules elementaires des corps, et les proportions selon lesquelles elles entrent dans ces combinaisons [Essay on a Manner of Determining the Relative Masses of the Elementary Molecules of Bodies, and the Proportions in Which They Enter into These Compounds]. *Journal de Physique, de Chimie, et d'Histoire Naturelle* (73), s. 58–76. Anglický překlad.
Dostupné z <https://web.lemoyne.edu/giunta/avogadro.html>

- [10] Britannica, T. Editors of Encyclopaedia (12. 12. 2019). *Avogadro's law*. *Encyclopedia Britannica*. Citováno 15. 1. 2022.
Dostupné z <https://www.britannica.com/science/Avogadros-law>
- [11] Coley, N. G. (5. 8. 2021). *Amedeo Avogadro*. *Encyclopedia Britannica*. Citováno 15. 1. 2022.
Dostupné z <https://www.britannica.com/biography/Amedeo-Avogadro>
- [12] Reichl, J. & Všeticka, M. (28. 10. 2012). *Stavová rovnice ideálního plynu*. *Encyklopedie fyziky*. Citováno 15. 1. 2022.
Dostupné z <http://fyzika.jreichl.com/main.article/view/598-stavova-rovnice-idealniho-plynu>
- [13] Wikipedia contributors. (14. 12. 2021). *Benoît Paul Émile Clapeyron*. In Wikipedia, The Free Encyclopedia. Citováno 15. 1. 2022.
Dostupné z https://en.wikipedia.org/w/index.php?title=Beno%C3%AEt_Paul_%C3%89mile_Clapeyron&oldid=1060332599
- [14] Clapeyron, E. (1834). Mémoire sur la Puissance Motrice de la Chaleur [Memoir on the Motive Power of Heat]. *Journal de l'École Royale Polytechnique* (Tome XIV), s. 153–190. Anglický překlad.
Dostupné z https://en.wikisource.org/wiki/Scientific_Memoirs/1/Memoir_on_the_Motive_Power_of_Heat
- [15] Reichl, J. & Všeticka, M. (28. 10. 2012). *Stavová rovnice reálného plynu*. *Encyklopedie fyziky*. Citováno 15. 1. 2022.
Dostupné z <http://fyzika.jreichl.com/main.article/view/599-stavova-rovnice-realneho-plynu>

LETNÍ ŠKOLA MATEMATIKY A FYZIKY 2021
SBORNÍK PŘÍSPĚVKŮ

Editoři: Magdalena Krátká, Jiří Příbyl, Jana Kasperová
Sazba: Miloš Brejcha, Vydavatelský servis

Vydavatel: Vydavatelský servis,
Republikánská 28, Plzeň

1. vydání

Plzeň 2022