

STUDENTSKÝ ČASOPIS A KORESPONDENČNÍ SEMINÁŘ

Ročník XXXII

Číslo 2



MATEMATIKA

FYZIKA

INFORMATIKA



Uvnitř najdete několik témat a s nimi souvisejících úloh. Zamyslete se nad nimi a pošlete nám svá řešení. My vám je opravíme a ta nejzajímavější z nich otiskneme. Nejlepší řešitele zveme na podzim a na jaře na soustředění.

Milí řešitelé,

vítejte u čtení již druhého letošního čísla časopisu M&M. Na listech tohoto podzimního čísla na vás čekají pokračování starých známých témat, na která se již jistě těšíte od prvního čísla. Zároveň tu pro vás máme jedno zbrusu nové: Šifrování! V něm se podíváme na šifrovačky z pohledu tvůrce šifer.

Tématko o grupách nabralo v tomto čísle poněkud nečekaný směr. Matematické symetrie nás zavedou do světa fyziky a budeme se zatajeným dechem sledovat, kolik jich tam najdeme. Jako bonus se na konci dozvíte řešení úloh z předchozího čísla. V tématku Brainfuck jsme si pro vás nachystali možnost nasimulovat jednoduchý počítač.

Než se pustíte do čtení, ještě vás pozveme na Den otevřených dveří na Matfyzu. Ten bude letos ve čtvrtek 27. listopadu a najdete tam prezentace různých částí Matfyzu.

Dále vás srdečně zveme na tradiční vánoční víkendovku, která proběhne 12. až 14. prosince. Tak si to zapište do kalendáře, ať si užijete hraní, výlet a setkání s ostatními řešiteli i orgy. Více informací obdržíte později e-mailem.

A teď už hurá do čtení témat! Přejeme vám příjemný zážitek z řešení a objevování.

Vaši orgové M&M

Obsah

Téma 1 – Grupy aneb Kterak matika k souměrnosti přišla	3
Téma 2 – Brainfuck	17
Téma 26 – Šifrování	20



Zadání a řešení témat

1. deadline: 4. listopadu 2025 | 2. deadline: 2. prosince 2025

Téma 1 – Grupy aneb Kterak matika k souměrnosti přišla

Díl 2: Pohled fyzika na symetrii.

„I byl řekl Bůh: ‚Buďtež grupy.‘ A grupy byly.“ vskutku není příliš vhodný způsob, kterak uvést následující text, jenž tě, čtenáři, osvítl ryze povrchním pohledem na standardní model částicové fyziky a jeho matematickou podstavu v podobě součinu maticových grup.

V minulém díle jsme ledabykle tvrdili, že grupy mají svá místa v modelech rozličných přírodních jevů. Těžko hledati ladnější představy takového tvrzení než právě v modelu těch nejjednodušších stavebních kamínků reality, jež lidstvo bylo s to odkrýt, a zákonů jejich interakcí – v tzv. *standardním modelu* částicové fyziky.

Své pojednání o krásném poutu mezi grupami, jakožto matematickým vyjádřením symetrie, a základními silami, jež drží náš vesmír pospolu, rozdělíme do dvou dílů. V tomto – dějme úvodním a primárně fyzikálním – díle představíme pohled fyziky na symetrii a způsob, jakým se symetrie fyzikálních systémů projevuje v jejich chování.

K povrchnímu pochopení předložených principů je třeba pouze fantasmie a základů klasické mechaniky, jimž jste se, předpokládáme, draží čtenáři, učili. Ovšem, zájemci o matematický základ vyřčených faktů a vysvětlení jsou dlužni chápat částečně formální stránku, ale především fyzikální pojetí, diferenciálního počtu.¹ Rovněž budeme plně využívat pravidel manipulace s vektory a maticemi. V tomto směru směle doporučíme tématko *Vektory a matice* z 31. ročníku, především jeho pátý díl.



¹Stránka na anglické Wikipedii účelu pochopení diferenciálního počtu dobře poslouží. Česká je poněkud skromná. Odkaz zde: <https://en.wikipedia.org/wiki/Calculus>.

Lagrangeovská mechanika

V této sekci stroze objasníme – snad spíše uvedeme – fyzikální teorii známou jako *lagrangeovská mechanika*. Zjednodušeně řečeno je tato popisem fyzikálního systému jako dvojice $(\mathcal{M}, \mathcal{L})$, kde $\mathcal{M}$ je zván *konfiguračním prostorem* a $\mathcal{L}$ *lagrangianem*.

O konfiguračním prostoru budeme hovořit jen výjimečně a okrajově. V podstatě je jím soustava souřadnic vyjadřující *pozici a orientaci* těles tvořících daný systém. Souřadnicím prostoru $\mathcal{M}$ se často přezdívá *stupně volnosti*, neboť představují v zásadě výčet nezávislých způsobů, kterými se systém může vyvíjet. Uvedeme dva malé příklady.

Možným konfiguračním prostorem pro popis pohybu částice (bezrozměrného tělesa) v prostoru je přesně onen prostor, tedy množina $\mathbb{R}^3$ – systém souřadnic o třech směrech, třech stupních volnosti. Když místo částice uvážíme těleso mohoucí se v prostoru otáčet, potřebujeme do konfiguračního prostoru zahrnout i souřadnice udávající jeho natočení. Rozšíříme jej pročež na množinu $\mathbb{R}^3 \times SO(3)$, kde $SO(3)$ je přesně množina všech rotací v 3D prostoru (více se o ní dozvíte v příštím díle). Lze si představovat, že tato množina sestává z trojic úhlů a každý úhel značí velikost otočení kolem jedné ze souřadnicových os. Pohyb tělesa v prostoru je tak systém s šesti stupni volnosti – třemi souřadnicemi pro pozici a třemi pro rotaci (vizte obrázek 1).

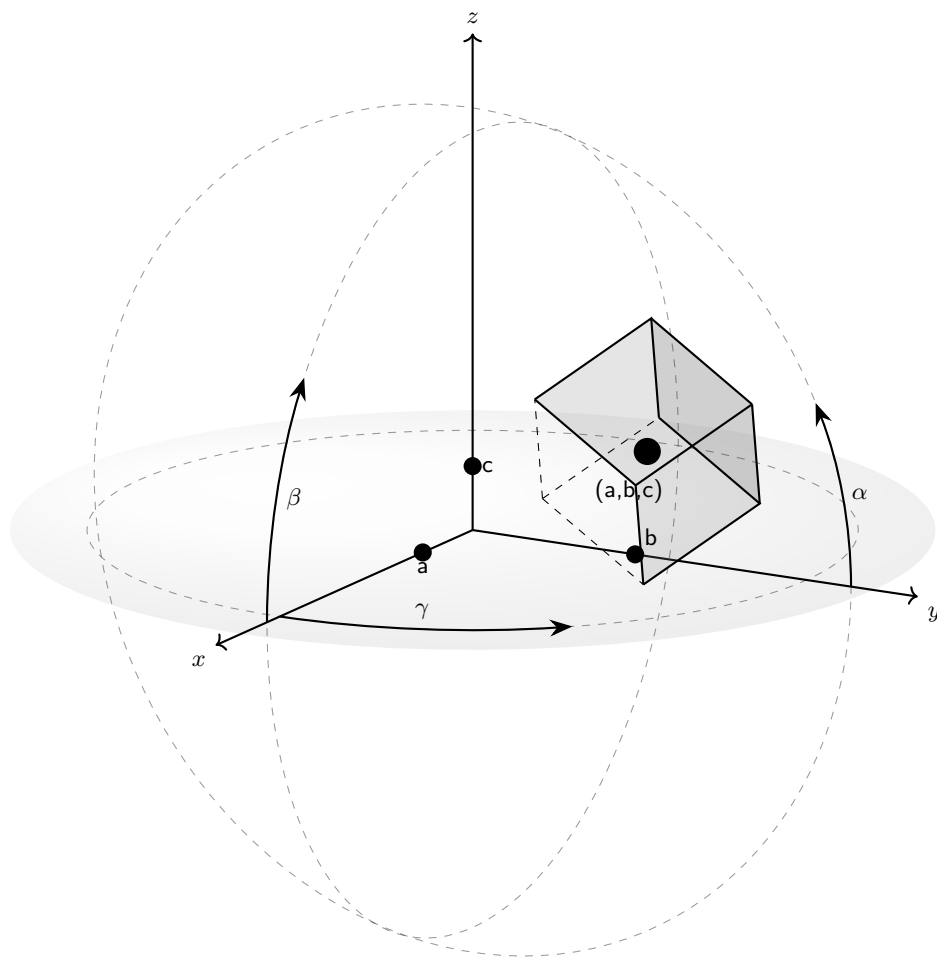


Úloha 2.1 [2b]: *Vymyslete možný konfigurační prostor, který lze použít k popisu fyzikálního systému dvojitého kyvadla², tedy systému, kde je na jednom kyvadle zavěšeno druhé. Nemusíte být rigorózní; stačí uvést množinu s intuitivním objasněním důvodu její volby.*

Přestože konfiguračního prostoru budeme využívat jen implicitně, lagrangian se nám v dalším aktu stane nezanedbatelným nástrojem. Definován jest jako rozdíl kinetické energie $T(t)$ a potenciální energie $V(t)$ fyzikálního systému v čase t . Proč je užitečné popisovat systém pomocí *rozdílu* kinetické a potenciální energie spíše než pomocí jejich součtu (též *celkové energie*), zde vysvětlovat nebudeme, neboť vzniklý obchvat by nabyl délky nemalé.³ Pro náš text spočívá jeho význam hlavně ve skutečnosti, že lagrangian s sebou nese vysoce elegantní definici *symetrie* fyzikálního systému, jež právě následuje.

²Vizte např. https://en.wikipedia.org/wiki/Double_pendulum.

³Výklad lagrangeovské mechaniky na anglické Wikipedii je dosti uplný: https://en.wikipedia.org/wiki/Lagrangian_mechanics.



Obrázek 1: Těleso v prostoru jako systém s šesti stupni volnosti. Každá šestice $(a, b, c, \alpha, \beta, \gamma)$ udává jinou *pozici* nebo *orientaci* tělesa.

Vesmírné symetrie

V roce 1918 vydala německá matematická Emmy Noether článek s názvem *Invariante Variationsprobleme*, ve kterém předala jednu z nejdůležitějších idejí teoretické fyziky. Objevila až zázračnou korespondenci mezi symetriemi časoprostoru a zákony zachování veličin.

Slovem „symetrie“ zde – jako i v minulém díle tématka – myslíme více než pouhou osovou souměrnost či rotační symetrii. V lagrangeovské mechanice znamená symetrie fyzikálního systému transformaci souřadnic takovou, že ponechá jeho lagrangián neměnný.

Představme si fyzikální systém o pouze jedné částici v pohybu. Tato částice má pochopitelně nulovou potenciální energii, takže leckterá transformace je symetrií takového systému. Například, můžeme částici *posunout* o libovolnou konstantu λ a energii systému tím nijak neovlivníme. Řekneme, že systém vykazuje *translační symetrii*. Podobně, těleso můžeme otočit kolem libovolného bodu o libovolný úhel θ a opět tím energii neovlivníme; náš fyzikální systém je pročež *rotačně symetrický*.

Fakt, že fyzikální systém o jedné částici je skutečně translačně symetrický, můžeme dokonce snadno ověřit výpočtem. Ať značí $\mathbf{x}(t)$ pozici částice v čase t . Výraz $\mathbf{x}(t)$ zde bereme jako *vektor* o třech složkách odpovídajících třem dimenzím prostoru. Možná víte, že derivace pozice částice podle času je její rychlost. Přeci, derivací jakékoli funkce je rychlost, s jakou se mění její hodnota v daném bodě. Tedy, derivací pozice je rychlost, s jakou se pozice mění. Rychlosti změny pozice říkáme zkrátka ... no ... *rychlost*. Derivaci pozice $\mathbf{x}(t)$ označíme po newtonovsku jako $\dot{\mathbf{x}}(t)$, její druhou derivaci (též *zrychlení*) jako $\ddot{\mathbf{x}}(t)$ a tak dále. Připomínáme, že je-li $\mathbf{x}(t) = (x_1(t), x_2(t), \dots, x_n(t))$, pak derivací $\dot{\mathbf{x}}(t)$ myslíme vektor $(x'_1(t), x'_2(t), \dots, x'_n(t))$, tedy vektor derivací funkcí $x_i(t)$.

Přesněji řečeno udává vektor $\dot{\mathbf{x}}(t)$ rychlost a *směr pohybu* částice s pozicí $\mathbf{x}(t)$, protože každá ze složek vektoru $\dot{\mathbf{x}}(t)$ značí rychlost pohybu v jedné z dimenzí. Pro výpočet kinetické energie částice však potřebujeme její „absolutní“ rychlost, tím pádem velikost či normu vektoru $\dot{\mathbf{x}}(t)$, kterou označíme jako $\|\dot{\mathbf{x}}(t)\|$. Komu je příjemnější používat pro rychlost tradičního značení v , nechť dosadí $v = \|\dot{\mathbf{x}}(t)\|$.

Kinetická energie zkoumané částice je v čase t rovna $T(t) = \frac{1}{2}m\|\dot{\mathbf{x}}(t)\|^2$, kde m je její hmotnost. Protože je částice samotná, její potenciální energie je nulová, a tedy její lagrangián roven $\mathcal{L}(t) = \frac{1}{2}m\|\dot{\mathbf{x}}(t)\|^2$. Tvrdíme, že posunutí částice o konstantu λ (opět tříložkový vektor) nezmění lagrangián. Ať je tedy vektor $\mathbf{y}(t) = \mathbf{x}(t) + \lambda$ pozicí posunuté částice. Jelikož je derivace konstanty nulová (tj. rychlost změny konstantní hodnoty je 0, neb se nemění), dostaneme rovnost $\dot{\mathbf{y}}(t) = \dot{\mathbf{x}}(t)$ a odtud $\|\dot{\mathbf{y}}(t)\| = \|\dot{\mathbf{x}}(t)\|$. Čili

$$\mathcal{L}(t) = \frac{1}{2}m\|\dot{\mathbf{x}}(t)\|^2 = \frac{1}{2}m\|\dot{\mathbf{y}}(t)\|^2.$$

Dokázat, že týž fyzikální systém je rovněž rotačně symetrický, dá více práce. Jelikož však budeme svá tvrzení doprovázet podobnými výpočty i v následujícím

díle, soudíme, že je záhodno důkaz uvést. Omezíme se však na případ, kdy částici rotujeme kolem pouze jedné ze souřadnicových os.

Matice rotace o úhel θ kolem osy x v 3D prostoru má tvar

$$R_x(\theta) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \theta & -\sin \theta \\ 0 & \sin \theta & \cos \theta \end{pmatrix},$$

tedy vektor $\mathbf{y}(t) = R_x(\theta)\mathbf{x}(t)$ vyjadřuje pozici částice, jež byla původně na pozici $\mathbf{x}(t)$ a pak otočená o úhel θ kolem osy x . Matice $R_x(\theta)$ má jednu zásadní vlastnost: její transpose $R_x(\theta)^T$ je otočení o úhel $-\theta$ kolem osy x . To ovšem znamená, že $R_x(\theta)^T R_x(\theta) = I$ (I značí identickou matici), neboť matice $R_x(\theta)$ způsobí otočení o úhel θ a matice $R_x(\theta)^T$ pak otočí zase zpět o úhel $-\theta$.

Přikročíme konečně k samotnému výpočtu lagrangiánu zrotované částice. Pro přehlednost vynecháme parametr t v zápisech vektorů pozic $\mathbf{x}(t)$ a $\mathbf{y}(t)$. Platí $\mathbf{y} = R_x(\theta)\mathbf{x}$, takže také $\dot{\mathbf{y}} = R_x(\theta)\dot{\mathbf{x}}$, a proto⁴

$$\begin{aligned} \|\dot{\mathbf{y}}\|^2 &= \langle \dot{\mathbf{y}} | \dot{\mathbf{y}} \rangle = \dot{\mathbf{y}}^T \dot{\mathbf{y}} = (R_x(\theta)\dot{\mathbf{x}})^T (R_x(\theta)\dot{\mathbf{x}}) \\ &= \dot{\mathbf{x}}^T R_x(\theta)^T R_x(\theta) \dot{\mathbf{x}} = \dot{\mathbf{x}}^T I \dot{\mathbf{x}} = \dot{\mathbf{x}}^T \dot{\mathbf{x}} = \langle \dot{\mathbf{x}} | \dot{\mathbf{x}} \rangle = \|\dot{\mathbf{x}}\|^2. \end{aligned}$$

Tím docházíme k závěru – stejně jako v případě posunutí – že rotace částice o úhel θ kolem osy x ponechá lagrangián stejným. Všimněte si však, že jsme vlastně dokázali poněkud hlubší výsledek. Dokonale stejný výpočet můžeme provést s libovolnou maticí M (namísto $R_x(\theta)$), která splňuje vztah $M^T M = I$. Aplikace každé takové matice na vektor pozice $\mathbf{x}(t)$ je symetrií systému o jedné částici v pohybu.

Úloha 2.2 [3b + 1b + 1b]:



1. Dokažte, že matice $R_x(\theta)$ je opravdu maticí rotace kolem osy x o úhel θ . Případný obrázek, prosíme, nezapomeňte doplnit rozumným argumentem.
2. Dokažte, že z rovnosti $\mathbf{y} = R_x(\theta)\mathbf{x}$ opravdu plyne rovnost $\dot{\mathbf{y}} = R_x(\theta)\dot{\mathbf{x}}$.
3. Dokažte, že platí $R_x(\theta)^T R_x(\theta) = I$.

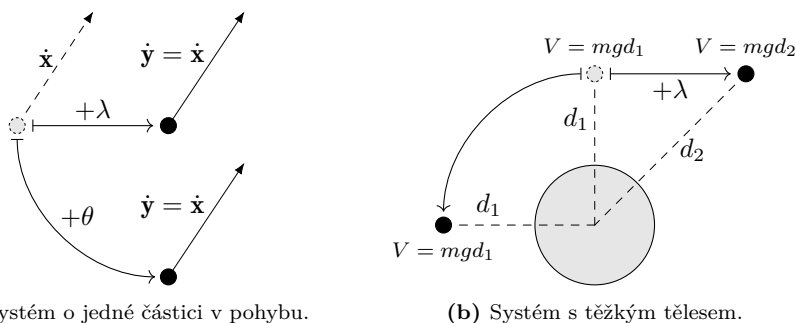
Problém 2.3: V odstavci výše tvrdíme, že násobení maticí M splňující $M^T M = I$ je symetrií fyzikálního systému o jedné částici v pohybu. Prozkoumejte, co je na těchto maticích zajímavé. Co násobení takovou maticí ve skutečnosti „dělá“ s oním systémem? Nemají jistou souvislost s grupami? Dokázali byste dokonce rozhodnout, které z těchto matic jsou symetriemi fyzikálních systémů s nenulovou potenciální energií?



Co když ale k této částici přidáme jiné těleso, třeba nějakou mnohem těžší kouli? Nyní už přiblížením částice k těžšímu tělesu změníme celkovou energii

⁴Použitě značení je stejné v jako již zmíněném pátém díle tématka *Vektory a matice*.

systému, protože částice ztratí část své gravitační potenciální energie. Avšak, budeme-li částici rotovat kolem středu velké koule, její energie zůstane nezměněna. Přišli jsme pročež o translační symetrii, ale nikoli o rotační.



Obrázek 2: Translační a rotační symetrie fyzikálního systému. Zde m je hmotnost částice, g gravitační zrychlení vlivem velké koule a d_1, d_2 vzdálenosti středu částice od středu tělesa.

Místo posunutí pouze malého tělesa můžeme však posunout celý systém. Tím je přeci energie celého systému opět nezměněna, protože vzájemná poloha částice a tělesa se rovněž nemění. Nač ale meškat u jednoduchých systémů! Po stejném proudu myšlenek doplujeme třeba k translační a rotační symetrii sluneční soustavy nebo – jako Emmy Noether – k symetriím celého vesmíru.

Nyní zpět k ideji z prvního odstavce. Totiž, fakt, že vesmír jako fyzikální systém vykazuje jisté symetrie, se odráží ve fyzikálních zákonech. Plné formální znění výsledku Emmy Noether je mimo rozsah (aspoň tohoto dílu) tématka, ale jeho princip si ukážeme na ještě jednom příkladě.⁵

Rozmyslíme si, že zákon zachování hybnosti (tedy součinu hmotnosti s rychlostí⁶) je ekvivalentní translační symetrii systému. Prostorem v onom příkladném systému budiž nekonečná dokonale rovná ledová plocha bez jakéhokoli tření. Když na tuto plochu položíme puk, zůstane na místě, a když do něj cvrkne, bude se navždy pohybovat určenou rychlostí. Translační symetrii systému si lze vyložit jako pravidlo, že dokonale tentýž experiment provedený na dvou různých místech bude mít dokonale tentýž výsledek.

Nejprve nahlédneme, že zákon zachování hybnosti implikuje translační symetrii; to je vcelku jednoduché odvodit. Například, pošleme-li proti sobě dva různé puky, pak zákon zachování hybnosti říká, že součet jejich hybností musí zůstat konstantní i po jejich srážce. Z toho vyplývá, že rychlost obou puků je závislá pouze na *relativním* vztahu mezi jejich hmotnostmi a rychlostmi před srážkou,

⁵Pro stručné objasnění s doprovodnými výpočty doporučíme například video https://www.youtube.com/watch?v=00NYa0_OnH4.

⁶Rychlostí zde míníme *vektor rychlosti*, vlastně „rychlost a směr“.

a tedy můžeme oba puky současně posunout libovolným směrem o libovolnou vzdálenost, aniž výsledek srážky ovlivníme.

Abychom viděli, že naopak translační symetrie s sebou již nutně nese zachování hybnosti, uvažme, co by se stalo, kdyby hybnost zachována nebyla. Čili, místo „důkazu“ zákona zachování hybnosti za předpokladu existence translační symetrie, uvidíme, že porušení tohoto zákona již nutně znamená, že pracujeme se systémem, který translačně symetrický *není*.

Řekněme, že položený puk se začne bez aplikace vnější síly pohybovat jistým daným směrem. V zájmu intuice si můžeme představit onu nekonečnou ledovou plochu nakloněnou na nějakou ze stran. Možná vás napadá, že takový systém přeci vykazuje translační symetrii: totiž, bez ohledu na to, kam puk položíme, začne se pohybovat tímž směrem. Zde přijde vhod pohled na translační symetrii jako na nemožnost určit polohu experimentu podle jeho výsledku. Toto pravidlo totiž v systému bez translační symetrie neplatí. Uvažme, že na řečené nahnuté ledové ploše sedí nad sebou Yveta a Zbyšek. Položí-li oba ve stejný čas puk na ledovou plochu, tento přirozeně doputuje za tím, kdo je níž. Pokud sedí třeba Zbyšek pod Yvetou, v jistý čas se dozví, že Yveta sedí nad ním. Je pročež schopen zjistit něco o její poloze, čímž je translační symetrie porušena.

Úloha 2.4 [3b]: *Možná jste, sečtělí čtenáři, slyšeli o zákonech zachování jiných veličin než hybnosti. Mezi nimi je například zákon zachování tzv. „momentu hybnosti“⁷. V závěsu předchozího textu snad není překvapující, že je i tento zákon ekvivalentní jistě symetrii fyzikálního systému, v němž platí. Nás by zajímalo vědět, která symetrie to je a hlavně (co vám výmluvnost dovolí) proč.*



Standardní model částicové fyziky

Záměrem tématka není podat zevrubnou přednášku o standardním modelu na dřevě kosti, ale poukázat na roli, kterou grupy hrají v našich snahách o zachycení podstaty vesmíru.⁸

Standardní model je teorie popisující tři ze čtyř základních sil – silnou nukleární sílu, slabou nukleární sílu a elektromagnetismus.⁹ Činí to prostřednictvím výčtu subatomárních částic (zvaných *elementární*), jejich vlastností a vzájemného působení.

Částice vystupující ve standardním modelu můžeme hrubě rozdělit do dvou kategorií: částice *tvořící hmotu* (oficiálně *fermiony*) a částice *zprostředkující základní síly* (oficiálně *bosony*). Pro snazší vyjádření si vymyslíme svoje vlastní názvosloví a budeme rozlišovat částice *hmototvorné* a částice *sílonosné*. V příštím

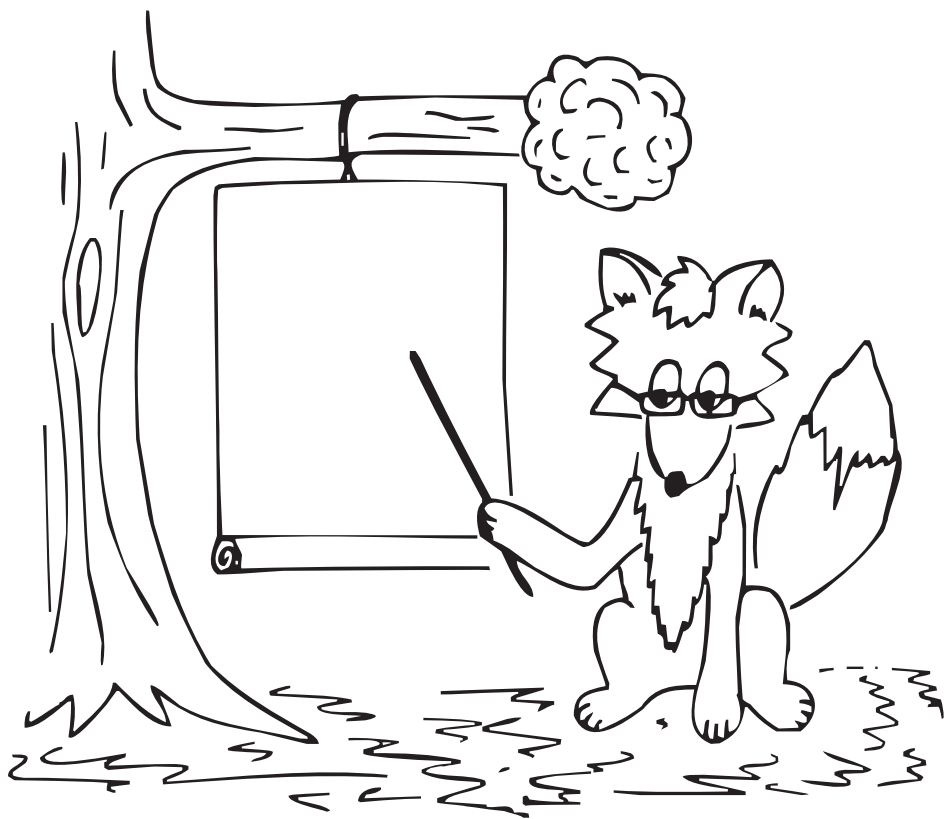
⁷Lze si o něm přečíst např. opět na Wikipedii: https://cs.wikipedia.org/wiki/Moment_hybnosti.

⁸Zájemce o tuto část fyziky odkážeme na knihy *The Theory of Almost Everything: The Standard Model, the Unsung Triumph of Modern Physics* od R. Oertera či *Deep Down Things: The Breathtaking Beauty of Particle Physics* od B. Schuma, do nichž jsme při přípravě tématka měli příležitost nahlédnout a jeví se přístupnými.

⁹Gravitace zatím není do této teorie začleněna, ačkoli pokusy o sesnutí standardního modelu a obecné teorie relativity stále trvají.

díle uvedeme, že hmototvorné částice jsou v jistém smyslu (především) rotačně symetrické. V duchu předchozího textu budou na druhé straně těchto symetrií zákony o zachování přidružených vlastností. V kvantové mechanice však tyto „zákony“ přejímají podobu základních sil.

*Adam, Jáchym; grupytematko@gmail.com
odevzdávejte do odevzdávátka*



Řešení 1. dílu

Úloha 1

Zadání:

- (a) Uvažte nejprve rotace v D_{18} , grupě symetrií pravidelného devítiúhelníku. Rozhodněte, které z jeho devíti rotačních symetrií generují všechny ostatní rotační symetrie, tj. pro které rotační symetrie $r \in D_{18}$ je pravda, že

$$\{r^1, r^2, r^3, r^4, r^5, r^6, r^7, r^8, r^9\}$$

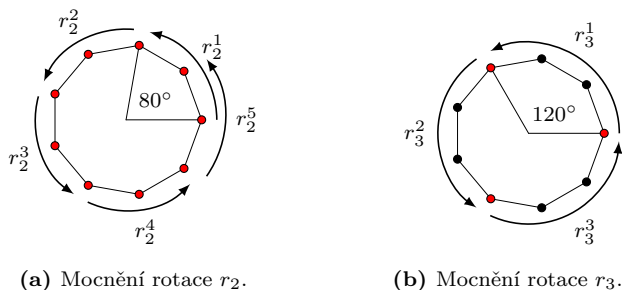
obsahuje všechny rotační symetrie v D_{18} .

- (b) Pokuste se postup z části (a) zobecnit na D_{2n} , čili na libovolný pravidelný n -úhelník. Pro které rotační symetrie $r \in D_{2n}$ je pravda, že

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

obsahuje všechny rotační symetrie v D_{2n} ? Může vám pomoci myšlenka, že rotace o nejmenší možný úhel (tím jest $360^\circ/n$) je vždy generátor. Tudíž, kterákoli rotační symetrie, jejíž (některou) mocninou je rotace o $360^\circ/n$, bude rovněž generátorem.

Řešení:



Obrázek 3: Mocnění různých rotací.

- (a) Pro pohodlí si označíme symbolem r_k rotaci o $k \cdot 360^\circ/9$ stupňů. Jak je z obrázku 3 jasné, rotace r_3 není generátorem všech rotací v D_{18} , neb ji stačí opakovat méně než devětkrát, abychom získali rotaci r_0 . Obecně: vrátíme-li se k rotaci r_0 po méně než devíti opakováních, tak jsme na generátor nenarazili. Jediné rotace mající tuto vlastnost jsou r_0, r_3 a r_6 , a tedy generátorkami jsou všechny ostatní: $r_1, r_2, r_4, r_5, r_7, r_8$.
- (b) Na pomoc s důkazem obecného případu si pozveme rigorosní řešení Doc.^{MM} Michaela Jarvise.



Řešení od Doc.^{MM} Michaela Jarvise:

Triviálně platí, že rotace „nedělej nic“, r_0 , nikdy (pokud $n > 1$) nebude generátorem.

Dále budeme zkoumat, kolikrát musíme rotaci použít, abychom se vrátili do původního stavu. Tedy, jaké nejmenší k splňuje $r_i^k = r_0$ pro dané r_i . Všimněme si, že $r_i^k = r_{k \cdot i \bmod n}$, tedy k -krát opakovaná rotace o $i \cdot 360^\circ/n$ je ekvivalentní jedné rotaci o $(k \cdot i \bmod n) \cdot 360^\circ/n$ („ $\bmod n$ “ značí zbytek po dělení n). Rovnost $r_i^k = r_0$ pak můžeme napsat jako:

$$\begin{aligned} r_i^k &= r_0 \\ r_0 &= r_{k \cdot i \bmod n} \\ 0 &= k \cdot i \bmod n \\ i \cdot k &= c \cdot n, \quad c \in \mathbb{Z} \end{aligned}$$

Chceme najít nejmenší nenulové $k \in \mathbb{N}$, pro které rovnost platí. Není těžké si všimnout, že $c \cdot n = i \cdot k$ je společný násobek n a i – najdeme tedy nejmenší společný násobek těchto čísel. Rozlišme nyní dva případy.

V prvním případě $i \cdot k = \text{nsn}(i, n) < i \cdot n$ (což nastane pokud n a i mají alespoň jednoho společného dělitele), z čehož vyplývá $k < n$. Avšak, pokud se nám začnou rotace opakovat už po $k < n$ použití rotace r_i , tak r_i určitě není generátorem, protože jsme „navštívili“ pouze k různých rotací. Navíc si můžeme všimnout, že tím pádem musíme navštívit právě ty rotace, které generátory taky nejsou.

V druhém případě, kde $i \cdot k = \text{nsn}(i, n) = i \cdot n$, nám vyplývá $k = n$, tudíž musíme navštívit n různých stavů (tj. všechny), než se nám začnou stavy opakovat.

Summa summarum: rotace $r_i \in D_{2n}$ je generátorem právě tehdy, když největší společný dělitel i a n je 1. Navíc si můžeme všimnout hezké vlastnosti, že pro prvočíselná n jsou všechny rotace krom r_0 generátory.

Úloha 2

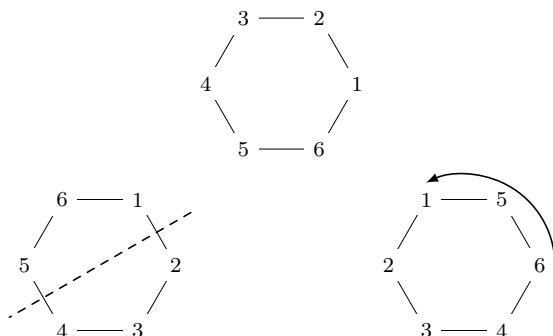
Zadání:

Dokažte (či argumentujte, objasněte, ...) následující tvrzení.

- Složením $r_1 \circ r_2$ dvou rotací $r_1, r_2 \in D_{2n}$ je vždy rotace a nikdy reflexe.*
- Jsou-li $r_1, r_2 \in D_{2n}$ různé rotace a $s \in D_{2n}$ kterákoli reflexe, pak $r_1 \circ s$ i $r_2 \circ s$ jsou navzájem různé reflexe.*

Řešení:

- Očíslujeme-li si vrcholy tvaru, jež rotujeme, zjistíme, že po každé rotaci zůstane pořadí vrcholů stejné a můžeme je přechít ve stejném směru jako předtím. U reflexí toto neplatí (zůstává sice zachováno pořadí, ale musíme číst vrcholy opačným směrem).



Obrázek 4: Vliv rotace a reflexe na pořadí vrcholů mnohoúhelníku.

- (b) Nejjednodušší způsob, jak nahlédnout tento fakt, je předpokládat, že výsledné reflexe jsou navzájem stejné a dojít ke sporu. To provedeme výpočtem. Předpokládejme, že

$$r_1 \circ s = r_2 \circ s.$$

Teď si jen stačí uvědomit, že opakování jedné reflexe dvakrát za sebou vyústí v identitu (každá reflexe je svým vlastním inversem). Čili,

$$r_1 \circ s \circ s = r_2 \circ s \circ s,$$

$$r_1 = r_2.$$

Což je ovšem ve sporu s tím, že jsou rotace r_1 a r_2 různé, a důkaz je hotov.

Úloha 3

Zadání:

Najděte množiny generátorů grup $(\mathbb{Q}, +, -, 0)$ a $(\mathbb{Q}, \cdot, ^{-1}, 1)$. Jsou konečné? Zkuste volit tyto množiny tak, aby žádné prvky nepřebývaly, tedy tak, aby tyto množiny obsahovaly pouze ty zlomky, které nezbytně musejí. Zlomek by byl v množině generátorů **přebytečný**, kdyby se dal vyjádřit pomocí ostatních generátorů.

Řešení:

Pro grupu $(\mathbb{Q}, +, -, 0)$ je množina generátorů například

$$\left\{ \frac{1}{n} \mid n \in \mathbb{N} \right\}.$$

Jakýkoliv zlomek $a/n \in \mathbb{Q}$ vytvoříme tak, že $|a|$ -krát sečteme zlomek $1/n$, respektive $-1/n$, se sebou samým, je-li a kladné, resp. záporné.

Druhým možným řešením (a mezi řešiteli rozhodně oblíbenějším) je generovat tuto grupu pomocí množiny

$$\left\{ \frac{1}{p^x} \mid p \in \mathbb{P}, x \in \mathbb{N} \right\},$$

kde $\mathbb{P}$ značí množinu všech prvočísel.

Pro jednoduchost předpokládejme, že vyjadřujeme zlomek a/b , kde $b = p^x \cdot q^y$ pro $p \neq q \in \mathbb{P}$. K obecnému případu, kdy se b rozkládá na více různých prvočísel, lze dojít přímočarou indukcí. Prvek $a/b \in \mathbb{Q}$ s pomocí zlomků ve tvaru $1/p^x$ vygenerujeme tak, že podle Bézoutovy rovnosti¹⁰ spočítáme $a, b \in \mathbb{Z}$ taková, že $ap^x + bq^y = 1$ (dvě různá prvočísla jsou vždy nesoudělná). Teď stačí spočítat

$$\frac{a}{q^y} + \frac{b}{p^x} = \frac{ap^x + bq^y}{p^x \cdot q^y} = \frac{1}{b}.$$

A tento zlomek sečteme (nebo odečteme pro záporné a) $|a|$ -krát sám se sebou.

Když přijde na přebytnost v této množině dojdeme děsivého uvědomění, je v ní nekonečno zbytečných prvků! Vždyť každé $1/p^x$ jsem schopný stvořit z $1/p^{x+1}$ (tak, že $1/p^{x+1}$ sečteme p -krát). Jak z toho ven? To úplně nejde; potřebovali bychom totiž „největší mocninu“ každého prvočísla (z které by šly vytvořit všechny menší, ale žádná větší by neexistovala), což je ovšem pouze sen, tak krásný, že se vždy rozplyne s probuzením.

V případě grupy $(\mathbb{Q} \setminus \{0\}, \cdot, {}^{-1}, 1)$ ¹¹ je množinou generátorů množina všech prvočísel (sjednocená s -1 , abychom získali i záporná čísla). Díky tomu, že každé přirozené číslo se dá zapsat jako součin prvočísel, můžeme na součin prvočísel rozložit i jmenovatele a čitatele jakéhokoliv zlomku. Stačí pak z každého prvočísla v rozkladu jmenovatele udělat jeho invers a máme výsledný zlomek. Například, zlomek $6/8$ získáme rozkladem

$$\frac{6}{8} = \frac{2 \cdot 3}{2 \cdot 2 \cdot 2} = 2 \cdot 3 \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = 2 \cdot 3 \cdot 2^{-1} \cdot 2^{-1} \cdot 2^{-1}.$$

V tomto případě máme nad přebytnými prvky vyhráno, prvočísla se ze své definice nedají vyjádřit jako násobek ničeho jiného než sama sebe a jedničky.

Úloha 4

Zadání:

Ukažte, že množina $\mathfrak{U}_n = \{e^{i \cdot k \cdot \frac{2\pi}{n}} \mid 0 \leq k < n\}$ n -tých odmocnin z jedné spolu s operací násobení komplexních čísel tvoří grupu. Nezapomeňte uvést, co jsou inverzy a neutrální prvek (či identita).

¹⁰Pokud vůbec tuto rovnost neznáte nebo se chcete zahloubat do jejích útrob, ideálním vstupním bodem je Wikipedia: [https://cs.wikipedia.org/wiki/Bézoutova_rovnost](https://cs.wikipedia.org/wiki/B%C3%A9zoutova_rovnost).

¹¹Bedliví čtenář si mohl povšimnout, že jsme pozměnili množinu prvků této grupy. V minulém díle totiž nastala chyba: nula nemůže být v této grupě, protože vzhledem k násobení nemá invers. Děkujeme všem, kdo nás opravili.

Řešení:

Že je tato grupa uzavřená (součin kterýchkoliv dvou prvků je stále v $\mathfrak{U}_n$), dokážeme jednoduchým výpočtem. Součinem dvou prvků z $\mathfrak{U}_n$ jest

$$e^{i \cdot k_1 \cdot \frac{2\pi}{n}} \cdot e^{i \cdot k_2 \cdot \frac{2\pi}{n}} = e^{i \cdot \frac{2\pi}{n} \cdot (k_1 + k_2)}.$$

Je-li $k_1 + k_2$ menší než n , máme prvek v $\mathfrak{U}_n$ a jsme hotovi. Ovšem, může se stát, že $k_1 + k_2 = n + k_3$; v tomto případě pokračujeme v počítání.

$$e^{i \cdot \frac{2\pi}{n} \cdot (n + k_3)} = e^{i \cdot \left(\frac{2\pi n}{n} + \frac{2\pi k_3}{n} \right)} = e^{i \cdot 2\pi} \cdot e^{i \cdot \frac{2\pi k_3}{n}}.$$

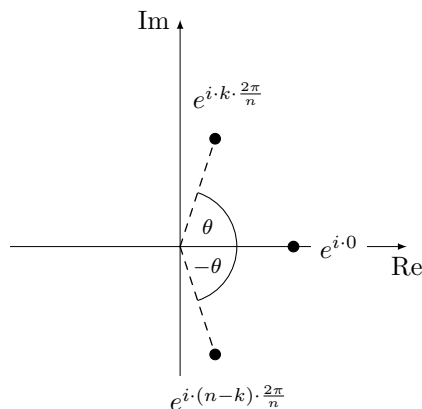
Teď si jen zbývá uvědomit, že $e^{i \cdot 2\pi} = 1$, a dospěli jsme ke kýženému výsledku.

Jak už to tak v grupách s klasickým násobením bývá, neutrálním prvkem je 1. Chceme-li najít invers nějakého prvku, velmi nám pomůže obrázek a vědomí, že násobit imaginárním číslem koresponduje s rotací v komplexní rovině (což je odpověď na jednu podotázku následující úlohy, ale pro intuitivní řešení se to hodí již teď). Abychom tento invers vyjádřili algebraicky, obrátíme se znovu na pravidla o součtu mocnin. Chceme, aby invers k $e^{i \cdot k \cdot \frac{2\pi}{n}}$ dal po vynásobení tímto číslem výsledek $1 = e^{i \cdot 2\pi}$. Dejme se tedy do počítání.

$$e^{i \cdot k \cdot \frac{2\pi}{n}} \cdot e^{i \cdot x \cdot \frac{2\pi}{n}} = e^{i \cdot 2\pi}$$

$$(k + x) \cdot \frac{2\pi}{n} = 2\pi$$

$$x = n - k$$



Obrázek 5: Geometrická interpretace inverzního prvku v $\mathfrak{U}_n$.

Z obrázku 5 je jasné, že invers má „opačný“ úhel. Prvek $e^{i \cdot (n-k) \cdot \frac{2\pi}{n}}$ je samozřejmě v $\mathfrak{U}_n$, protože $0 < n - k \leq n$ pro $k < n$.



Úloha 5

Zadání:

Dokažte, že grupa $\mathfrak{U}_n$ je cyklická, tedy lze generovat pouze jedinou n -tou odmocninou z jedné. Pro která $k < n$ je číslo $e^{i \cdot k \cdot \frac{2\pi}{n}}$ jejím generátorem? Vidíte souvislost s dihedrálními grupami (zamyslete se nad tím, jak násobení odmocninou z jedné „transformuje“ jinou odmocninu z jedné)?

Řešení:

Na důkaz toho, že $\mathfrak{U}_n$ je cyklická, nám postačí základní pravidla umocňování. Vezměme si pro jednoduchost prvek $e^{i \cdot \frac{2\pi}{n}} \in \mathfrak{U}_n$. Chceme-li s tímto prvkem vygenerovat nějaký jiný, dejme tomu $e^{i \cdot k \cdot \frac{2\pi}{n}}$, stačí ho umocnit na k ,

$$\left(e^{i \cdot \frac{2\pi}{n}}\right)^k = e^{i \cdot k \cdot \frac{2\pi}{n}}.$$

Získali jsme zatím jeden generátor, jak to je s těmi dalšími? Velmi podobně jako v úloze 1; $\mathfrak{U}_n$ dokonce v komplexní rovině „kreslí“ pravidelné n -úhelníky a každé komplexní číslo koresponduje s rotací. Propojení mezi komplexními odmocninami z jedné a rotacemi pravidelných mnohoúhelníků¹² je tak silné, až by si někdo mohl pomyslet, že mají úplně stejnou strukturu a liší se pouze jmény. Bohužel ke konceptu grup se stejnou strukturou se dostaneme až později v tomto tématku.

Adam, Jáchym; grupytematko@gmail.com
odevzdávejte do odevzdávátka

¹²Specificky tady uvádíme grupu rotací pravidelného mnohoúhelníku a ne dihedrální grupu, protože žádný ekvivalent reflexe mezi komplexními odmocninami z jedné nenajdeme.

Téma 2 – Brainfuck

Úvod

Vítejte v druhém díle tématku o Brainfucku. V minulém díle jsme se s jazykem seznámili a nyní je čas posunout se dále. Na Brainfuck se podíváme trochu jiným způsobem, a to tak, že se pokusíme postavit (nasimulovat) velmi jednoduchý počítač. Díky této abstrakci pak budeme schopni psát složitější programy bez nutnosti přemýšlet nad Brainfuckem. Počítač bude mít 8 registrů (paměťových buněk), zásobník a bude velmi pomalý. Nebudeme se ho snažit optimalizovat, ale napíšeme si pro něj jednoduchá makra připomínající příkazy v assembleru¹³. Poté budeme moct psát programy pouze pomocí našich nových příkazů a přeložit je do Brainfucku pomocí kousků kódu, které si v tomto tématku napíšeme.

Úlohy na procvičování

Ještě před vytvářením příkazů pro počítač tu pro vás mám pár jednodušších úloh na procvičení ;)

Úloha 2.1 [2b]:



1. Program načte dvě čísla a uloží do buňky jejich součin.
2. Program načte dvě čísla A a B , do buňky následně uloží $A // B$ (kde $//$ je celočíselný podíl).
3. Program načte dvě čísla A a B , do buňky uloží $A \bmod B$. Jednodušší verze – program načte jedno číslo a vypočítá jeho $\bmod 3$ (program bude umět počítat pouze $\bmod 3$, ne obecně jakýmkoliv číslem na vstupu).

$A \bmod B$ je celočíselný zbytek po dělení A/B (např. $25 \bmod 3 = 1$).

Připomínám, že interpret pro toto tématko je stále k dispozici na adrese https://ticvac.github.io/brainfuck_interpreter/.

Počítač

Počítač bude mít registry A, B, C až H představované buňkami $0, 3, 6, \dots, 21$. Ano, po každém registru jsou dvě buňky vynechány, a to z praktických důvodů. Před každým příkazem bude počítač ve skoro stejném stavu, obsahy registrů se mohou lišit, ale vynechané buňky $(1, 2, 4, 5, \dots)$ budou nastaveny na 0 a ukazatel ukazovat na registr A (buňka 0). Na tyto podmínky budete muset dávat pozor při vytváření příkazů. Během provádění příkazu tak můžete vynechané buňky volně využívat pro mezivýpočty.

Příkazy pro registry jsou parametrizované $(A, B, \dots)$. Stačí napsat příkaz pro jeden příklad registrů, je ale vhodné část kódu, kterou byste parametrizovali, nějak označit v komentářích ;)

¹³https://en.wikipedia.org/wiki/Assembly_language#%22Hello,_world!%22_on_x86_Linux

Operace s registry

1. načíst konstantní hodnotu do A
2. načíst vstup do D
3. přesun A do E
4. kopírovat H do B
5. vynulovat F
6. přičíst A k B (A obsahuje A , B obsahuje $B + A$)
7. odečíst F od G (F obsahuje F , G obsahuje $G - F$)
8. vynásobit A s B (uložit do B)
9. celočíselně vydělit B pomocí A (A obsahuje A , B obsahuje $B // A$)
10. zbytek po dělení B mod A (A obsahuje A , B obsahuje $B \bmod A$)
11. prohodit F a B
12. vypsat na výstup ASCII hodnotu B
13. vypsat na výstup hodnotu C v decimální soustavě.



Problém 2.2: *Naprogramujte tyto operace s registry v Brainfucku. Také zde si vyzkoušejte, že operace v libovolném pořadí dělají stále to, co bychom od nich očekávali.*

Operace pro větvení programu

Abychom mohli vytvářet podmínky a smyčky, potřebujeme větvení. Schopnost provést kus kódu, pokud je hodnota buňky nenulová, už máme jednoduše k dispozici v podobě `[ /* další kód */ [-] ]`. Takže potřebujeme ještě následující operace.

1. provést kus kódu, pokud je registr C nulový
2. provést kus kódu, pokud je registr C větší než registr A
3. provést kus kódu, pokud je registr B stejný jako registr G
4. provést kus kódu, pokud je registr A jiný než B
5. provést kus kódu, pokud je registr A nenulový (jako v příkladu o odstavci výše), ale nenulovat registr, aby se program vracel na začátek bloku (vytvoříme tak while cyklus)



Problém 2.3: *Naprogramujte tyto operace pro větvení v Brainfucku. Vyzkoušejte si, že operace v libovolném pořadí dělají stále to, co bychom od nich očekávali.*

Při převádění našich příkazů do Brainfucku si jen někde poznamenejme, k jak velkému následujícímu bloku příkazů se podmínka/cyklus vztahuje, například pomocí `{ }`.

Zásobník

Poslední věc, která by se nám ještě mohla hodit umět, je ukládat více dat i mimo registry. K tomu si nasimulujeme zásobník. Aktuální počet prvků zásobníku budeme ukládat do buňky 24 (jakoby na místo 9. registru) a data zásobníku budou v buňkách 27, 29, 31, ...

1. přidat hodnotu registru A na zásobník
2. načíst vršek zásobníku do registru B
3. smazat vršek zásobníku

Problém 2.4: *I toto bude na vás: Naprogramujte tento zásobník v Brainfucku. I zde si vyzkoušejte, že operace v libovolném pořadí dělají stále to, co bychom od nich očekávali.*



Závěr a poznámky k řešení

Ke svému řešení dodejte .pdf/.doc/.txt popisující vaše postupy k jednotlivým krokům. Pokud něco nezvládnete vyřešit, či vám to bude připadat nepřiměřeně těžké, napište to k dané úloze, nebo na Discord do #brainfuck, nebo mně přímo (Václav Tichý). Jelikož bude vaše řešení pravděpodobně obsahovat více souborů, odevzdejte prosím vše dohromady jako .zip s případnými poznámkami k organizaci ;)

Vašek; vaclav.tichy.mam@gmail.com
odevzdávejte do odevzdávátka

¹⁴<https://susi.trojsten.sk/>

Steganografie

Abychom zprávu pořád jen nekódovali, můžeme ji také prostě schovat tak, aby nebyla na první pohled vidět. Třeba ji napsat velmi malým či velmi světlým písmem nebo na zadní stranu papíru.

Hádanky

Nezbytným krok v řešení šifry může být vyřešení běžné hádanky, slovní hříčky nebo logické hádanky typu sudoku či Einsteinovy hádanky.

Kdo mě zná, ptá se na mé jméno, kdo mě nezná, odpovídá. Kdo jsem?

Znalostní

Obdobně může být šifra založená na vědomostech. Většinou je dobré vystačit si v šifře s běžnými středoškolskými znalostmi a dát dostatečně najevo, pokud by měl řešitel dohledávat něco více.

měkký lehce tavitelný kov, používaný k pokovování železa; jeho oxidy tvoří například safír; plyn tvořící zhruba pětinu zemské atmosféry; měkký, stříbřitý kov, jeho soli barví plamen výrazně červeně

Dobrá šifra

Co je to dobrá šifra, je často otázkou názoru, co se jednomu líbí, na to může druhý jen nechápavě zírat. Nicméně existuje pár pravidel, na kterých se shodnou snad všichni. Především by měla být luštitelná. Jejím řešením je tedy jedno nebo více smysluplných slov (nejčastěji podstatné jméno nebo slovní spojení), která navíc lze odhalit. Pokud je založená na tajném písmu, které jste vymysleli s kamarádem na základce, nejspíš ji nikdo nevyřeší. Měla by pracovat pouze se samotným zadáním, případně kontextem, který je známý všem řešitelům. Což může znamenat všeobecné znalosti, které lze relativně jednoduše dohledat na internetu, nebo třeba logo hry a podobné libůstky. Dále to mohou být i známé šifrovací postupy, jejichž přehled lze najít v šifrovacích pomůckách¹⁵. Kromě toho by také neměla obsahovat žádné informace navíc (takzvaný balast). Vše by mělo ideálně mít nějaký smysl. Samozřejmě, pokud se jedná například o prostý smysluplný text, nemusí být v každém slově něco schovaného. Může jít „jen“ o jeho význam a v takovém případě měl autor celkem volnost v tom, jak ho formulovat, a na přesné volbě slov tedy nezáleží. Pokud je ale z něčeho nic část šifry jinou barvou, můžete si být téměř jisti, že omylem to nebylo. Další vlastností dobré šifry je její jednoznačnost. Pokud existuje více způsobů, jak z šifry dostat nějaké heslo, nevěstí to nic dobrého.

¹⁵<https://sifrovacky.cz/pomucky/>

Tipy a triky k řešení šifer

Vyplatí se být systematicky kreativní. Házet nápady jeden přes druhý, ale nebýt líní je pak skutečně vyzkoušet. A když říkáme skutečně, myslíme skutečně. Úplně nejhorší, co se při luštění šifry může stát, je, že vyzkoušíte správný postup, uděláte chyбку, vyjdou vám nesmysly, vy princip zahodíte a už se k němu nevrátíte. A pokud jste to už fakt dořešili do konce a nějak nechápete, co vám vyšlo, zkuste si to přečíst znovu a nejlépe nahlas. Zkuste různě doplnit diakritiku, případně mezery, třeba je to fakt smysluplná tajenka, jen to tak na první pohled nevypadá.

Často se může vyplatit zkusit uvažovat jako autor. Ať už máte nějaký nápad, u nějž si nejste jisti správností, nebo zatím žádný nápad nemáte. Jaký princip by mohla šifra využívat, aby její finální verze vypadala takhle? Zkuste se zamyslet, jak by se mohlo stát, že jste takovou šifru vymysleli sami. Jaké všechny informace v sobě šifra nese a jak spolu vzájemně souvisí? Tyto a podobné otázky můžou proces luštění značně urychlit.

A že jste úplně bezradní, na šifru jen zíráte, v mozku prázdko a všechny předchozí tipy stojí za houbu? I to se stává (možná že častěji, než by bylo příjemné). V takovém případě může pomoci podívat se do šifrovacích pomůcek. Připomenout si, jaké všechny šifrovací principy vlastně existují, a třeba zjistíte, že by něco z toho mohlo vycházet. Nebo se zkuste na chvíli projít, vyčistit si hlavu a podívat se na šifru novým pohledem. Nahlas pojmenovat, co všechno na šifře vidíte a k čemu by to tak mohlo být dobré. A hlavně se nevzdávat, ono to půjde.

Jak vymýšlet šifry

Možná jste teď už o něco moudřejší v tom, jak takovou šifru vyřešit. Ale zamysleli jste se někdy nad tím, jaké to je dobrou šifru vymyslet? Možná jste někdy drželi v ruce šifru a říkali jste si: „Vždyť tohle musel vymyslet leda úplnej blázen!“ Díky nám se i vy můžete teď stát takovým bláznem.

Úlohy

 **Úloha 2.1** [2b]: Zjistěte princip a řešení každé ukázkové šifry z předchozích šesti podsekcí sekce *Typy šifer*.

 **Problém 2.2:** Zkuste vymyslet vlastní šifru.¹⁶ Společně se zadáním nám nezapomeňte poslat i návod, jak se šifra řeší :)

Olga a Pája; Olga.dvorakova17@gmail.com
odevzdávejte do odevzdávátka

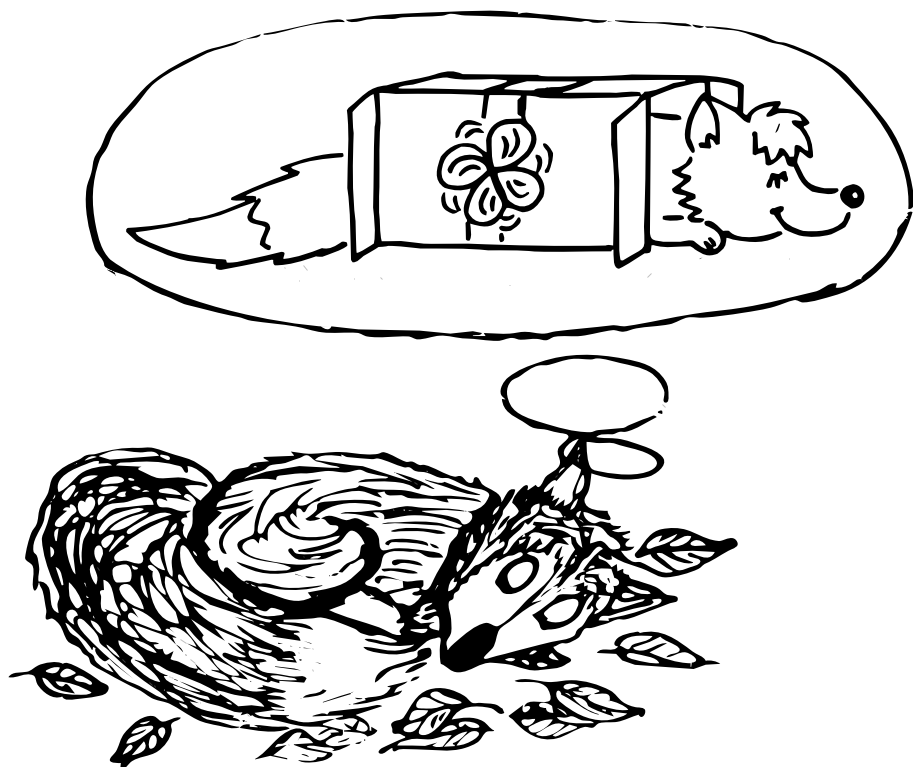
¹⁶Disclaimer: tato aktivita vás může dlouhodobě poznamenat. Vymýšlení šifer má silné vedlejší účinky. Dvacet šestku budete hledat všude. Myšlenka: „A nedala by se z toho udělat šifra?“ se stane vašim každodenním chlebem.

Výsledky 1. deadlinu 1. čísla

Poř.	Jméno	R.	$\sum_{-1}$	Témata				$\sum_0$	$\sum_1$
				1	2	3	4		
1.	Doc. ^{MM} M. Jarvis	4	441,3	14,0	20,5	19,0	12,5	66,0	66,0
2.	Bc. ^{MM} M. Hrubá	2	46,0	10,5	6,0	14,0	15,5	46,0	46,0
3.	Dr. ^{MM} P. Starý	4	149,6	12,5	11,5		11,3	35,3	35,3
4.	Doc. ^{MM} J. Klementová	4	394,1	10,0	3,0		20,0	33,0	33,0
5.	Mgr. ^{MM} J. Fišerová	3	58,7	13,0	4,0	15,0		32,0	32,0
6.	Bc. ^{MM} T. Holásek	3	28,2	11,7		16,5		28,2	28,2
7.	Bc. ^{MM} E. Ježek	4	22,8		11,5		11,3	22,8	22,8
8.–10.	M. Stroff	4	19,8	3,9	3,9	11,4	0,6	19,8	19,8
	A. Mouchová	3	19,8	3,9	3,9	11,4	0,6	19,8	19,8
	V. Kubrycht	4	19,8	3,9	3,9	11,4	0,6	19,8	19,8
11.	Mgr. ^{MM} V. Kučera	4	93,0				15,0	15,0	15,0
12.	R. Krzystek	3	13,9	9,1		4,8		13,9	13,9
13.	A. Ježková	2	13,0	13,0				13,0	13,0
14.–15.	P. Fiala	4	11,0	11,0				11,0	11,0
	Mgr. ^{MM} F. Nouza	4	79,1		11,0			11,0	11,0
16.	Mgr. ^{MM} P. Barták	2	72,4		10,5			10,5	10,5
17.	L. Mihola	1	9,5	6,5	3,0			9,5	9,5
18.	Mgr. ^{MM} N. Jochová	3	55,4	6,3	2,0			8,3	8,3
19.	Bc. ^{MM} Š. Swaczyna	1	45,2	3,0	3,0	2,0		8,0	8,0
20.	Š. Hrdý	4	7,0		3,0		4,0	7,0	7,0
21.	J. Kaplický	4	10,7		6,0			6,0	6,0
22.	Doc. ^{MM} O. Nevěril	4	269,4	5,0				5,0	5,0
23.	Mgr. ^{MM} A. Gauchet	4	85,0		4,5			4,5	4,5
24.	S. Bažantová	3	4,0	4,0				4,0	4,0
25.–26.	L. Koma	2	8,0		3,0			3,0	3,0
	K. Kučerová	1	3,0		3,0			3,0	3,0

Sloupecek $\sum_{-1}$ je součet všech bodů získaných v našem semináři, $\sum_0$ je součet bodů v tomto deadlinu a $\sum_1$ součet všech bodů v tomto ročníku. Tituly uvedené v předchozím textu slouží pouze pro účely M&M.





Časopis M&M je zastřešen Matematicko-fyzikální fakultou Univerzity Karlovy. S obsahem časopisu je možné nakládat dle licence CC BY 4.0. Autory textů jsou, není-li uvedeno jinak, organizátoři M&M. Realizace projektu byla podpořena Ministerstvem školství, mládeže a tělovýchovy. Pokud si časopis nepřejete dále dostávat v tištěné podobě, zrušte si prosím jeho odběr v nastavení svého účtu na webu.

Kontakty:

M&M, OPMK, MFF UK
Ke Karlovu 3
121 16 Praha 2

E-mail: mam@matfyz.cz
Web: mam.matfyz.cz
FB: [casopis.MaM](https://www.facebook.com/casopis.MaM)

