

M&M číslo 3 ročník IV

Ahojte řešitelé!

První poznámka se týká soustředění. Jak jste si jistě všichni všimli, neuskutečnilo se. Bylo to kvůli nezájmu účastníků. V daném termínu nám došlo asi 12 přihlášek, dloouho po termínu (ač jsme na to upozorňovali) asi další 4 přihlášky. Celkem bylo potřeba zaplnit chaloupku o kapacitě asi 25 lidí. Snad se vás příště přihlásí víc a hlavně dříve.

Letní konferenci plánujeme na počátek prázdnin, protože v době před prázdninami je neobyčejně narváno (olympiády, olympiádní soustředění, soustředění korespondenčních seminářů, maturity, zkouškové, ...) Uvažujte už nyní, zda byste se chtěli účastnit. Konference proběhne pravděpodobně v přírodě na nějaké lesní chatě.

V první sérii jsme vyhlásili soutěž o logo časopisu. Bylo by tedy slušné se o tom alespoň trochu zmínit. Nejdůležitější naše výtku se týká druhu dodaných obrázků. Poněvadž se jedná o jednoduché logo, které bude možná někdy v budoucnosti zdobit záhlaví časopisu, mělo by se skládat výhradně z několika jednoduchých křivek. Naprosto nepřipustné jsou barevné obrázky, nepraktické jsou také stínované přechody mezi černou a bílou. Logo by mělo být jednoduché a hezké, nehodí se moc složité přepíácané obrázky.

Jistá nejmenovaná řešitelka nám poslala mnoho návrhů na logo, které obsahovaly různé zvířátka, mimo jiné ptáky. Myslíme si, že když má seminář FKS v logu pterodaktyla, bylo by nemístné je napodobovat.

Všechna loga samozřejmě nebyla špatná, ale ještě jsme si žádné nevybrali. Pokud vás múza ještě neopustila, zkuste nám poslat nějaké další návrhy.

Jelikož někteří nejmenovaní řešitelé (však on bude vědět kdo) píší články tak, že to po nich při nejlepší vůli není nikdo schopen přečíst, jsme nuceni napsat několik pokynů, které je třeba dodržet, aby lidé, kteří budou článek číst neutrpěli vážnou duševní újmu.

1. Je důležité, aby jste pro *každé použité písmenko* uvedli, jaká *fyzikální veličina* se za ním skrývá. (pro některé veličiny se používá více označení (např. W , A pro práci), některá písmenka naopak znamenají více fyzikálních veličin (např. t může znamenat jak čas, tak teplotu, krom toho často se používá více označení stejné veličiny za různých podmínek: t_1, t_2, \dots).
2. Zkontrolujte si, zda odkazy na rovnice, obrázky, ... odkazují tam, kam mají (je dost pracné toto dohledávat).
3. Je-li význam nějaké veličiny jasný z obrázku, je stejně dobré to výslovně uvést (např. "Význam φ, θ viz obr. 3"). Je poměrně nepohodlné číst text a sledovat všechny obrázky – zvláště, je-li jich hodně –, jestli se tam náhodou dané písmenko nevyskytuje.
4. Pokud možno nepoužívat ve stejném textu jedno písmenko pro více proměnných. Pokud upravujete nějaký velice složitý výraz, rovněž by se slušelo uvést alespoň některé mezitvary. Nestačí uvést poznámku: "Jednoduchými úpravami dostaneme", zvláště pokud tyto úpravy vůbec nejsou jednoduché.

Nějak se vám zalíbily odpočinkové úlohy – jak snadno zjistíte nahlédnutím do výsledkové listiny. Jsme samozřejmě rádi, že se vám líbí, ale už méně se nám líbí, že kvůli nim zanedbáváte mnohem zajímavější témata. Proto bude od dalšího kola zvýšen bodový limit na příspěvky k tématům.

redaktoři časopisu

Téma 1 – Neukončená čísla

Bc. Petr Zima: r-adická neukončená čísla

Problém neukončených čísel (dále NČ) jsem zobecnil do libovolné r -adické soustavy. Celou teorii buduji od počátku včetně zavedení nových definic sčítání a násobení, které se ukázaly být vhodnější; jsou samozřejmě ekvivalentní s definicí původní. Některé důkazy jsou uvedeny na konci textu, aby nerušily plynulost výkladu.

V článku je použito značení NČ velkými písmeny a celých čísel písmeny malými. Pro zkrácení místa jsou na některých místech vynechány kvantifikátory (\exists, \forall). Ze stejných důvodů je zápis kongruencí zkrácen z původního $a \equiv b \pmod{10}$ na $a \equiv_{10} b$. Článek je rozdělen do 5 částí:

- I. Základní vlastnosti NČ
- II. Inverzní prvky vzhledem k násobení
- III. Odmocniny
- IV. Speciální případ $r = 10$
- V. Důkazy

Část 1. Základní vlastnosti NČ

Definice 1. *Neukončeným číslem rozumíme posloupnost čísel z množiny $\{0, 1, \dots, r-1\}$ pro pevně dané r . Zapišme $A = \dots a_n a_{n-1} \dots a_2 a_1 a_0$.*

Pro účel zkoumání NČ dále zavedme pojem Z -čísli A , značeno $[A]_Z$.

Definice 2. *Z -čísli NČ $A = \dots a_n a_{n-1} \dots a_2 a_1 a_0$ je celé nezáporné číslo definované $[A]_Z = \sum_{k=0}^{Z-1} a_k \cdot r^k$, neboli číslo, jehož r -adický zápis se shoduje s prvními Z ciframi NČ A .*

Věta 1.1. *Pro Z -čísli platí následující 2 tvrzení:*

- (a) posloupnost $\{x_Z \bmod r^Z\}_{Z=1}^{\infty}$ tvoří Z -čísli nějakého NČ, právě tehdy když $(\forall A \leq B \in \mathbb{N}) x_B \equiv_{r^A} x_A$. Toto NČ je posloupností jednoznačně určeno.
- (b) $A = B \iff (\forall Z \in \mathbb{N}) [A]_Z \equiv_{r^Z} [B]_Z$.

Důkaz. *Je zřejmý z jednoznačnosti r -adického zápisu.*

Díky zavedení pojmu Z -čísli můžeme vytvořit relativně přirozené definice součtu a součinu.

Definice 3. *Sčítání a násobení na množině NČ definujeme:*

$$A + B: (\forall Z \in \mathbb{N}) [A + B]_Z \equiv_{r^Z} ([A]_Z + [B]_Z)$$

$$A \cdot B: (\forall Z \in \mathbb{N}) [A \cdot B]_Z \equiv_{r^Z} ([A]_Z \cdot [B]_Z)$$

Použitím těchto definic snadno dokážeme věty charakterizující strukturu NČ.

Věta 1.2. *(a) NČ tvoří komutativní okruh s jednotkovým prvkem. (b) speciálně pro r prvočíslo je okruh r -adických NČ také oborem integrity.*

Důkaz. *Část (a) viz. dodatek, pro názornost zde uveďme pouze důkaz distributivity:*

$$\begin{aligned} [A \cdot (B + C)]_Z &\equiv_{r^Z} [A]_Z \cdot [B + C]_Z \equiv_{r^Z} [A]_Z \cdot ([B]_Z + [C]_Z) \equiv_{r^Z} \\ &\equiv_{r^Z} [A]_Z \cdot [B]_Z + [A]_Z \cdot [C]_Z \equiv_{r^Z} [A \cdot B]_Z + [A \cdot C]_Z \equiv_{r^Z} [A \cdot B + A \cdot C]_Z, \end{aligned}$$

a podle V1.1(b) platí $A \cdot (B + C) = A \cdot B + A \cdot C$ **q.e.d.** Pro důkaz části (b) dokažme nejprve následující Lemma 1.

Lemma 1. $(\forall Z \in \mathbb{N}) r^Z \mid [A]_Z \iff A = 0$.

$$r^Z \mid [A]_Z \iff [A]_Z \equiv_{r^Z} 0 \text{ a podle V1.1(b) } A = 0. \text{ **q.e.d.**}$$

Důkaz (b). *Provedeme sporem. Předpokládejme, že $(\exists A, B \neq 0) A \cdot B = 0$.*

Potom podle Lemmatu 1 (jelikož $A, B \neq 0$) $(\exists X, Y \in \mathbb{N}) r^X \nmid [A]_X$ & $r^Y \nmid [B]_Y$, a tedy vzhledem k tomu, že r je prvočíslo, musí platit $r^{X+Y} \nmid [A \cdot B]_{X+Y}$, což je ve sporu s Lemma 1 a předpokladem $A \cdot B = 0$. **q.e.d.**

Následuje velmi důležitá věta převádějící r -adická NČ na K -tici NČ o prvočíselných základech. V těchto základech lze počítat většínu výpočtů velmi jednoduše. Tento převod je podobný převodu čísla $x \in \{0, 1, \dots, N-1\}$ na K -tici čísel $x_i \in \{0, 1, \dots, a_i - 1\}$, kde $\prod_{i=1}^K a_i = N$, který znají řešitelé loňského ročníku jakožto modulární aritmetiku.

Při tomto převodu musejí být jednotlivá a_i po dvou nesoudělná čísla a pak existuje vzájemně jednoznačné zobrazení těchto dvou množin na sebe. Toto zobrazení zachovává aritmetiku, takže např. místo složitějšího násobení stačí pouze velká čísla x, y převést na několik menších čísel x_i, y_i , která mezi sebou snadno znásobíme na z_i , jehož opačným převodem získáme výsledek Z .

Věta 1.3. *Nechť $r = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ je kanonický rozklad r . Potom okruh r -adických neukončených čísel (dále NČ _{r}) je izomorfní s okruhem uspořádaných n -tic $(A_{p_1}, A_{p_2}, \dots, A_{p_n})$, kde $(\forall K) A_{p_K}$ je obor integrity NČ _{p_K} . Tyto n -tice se sčítají a násobí po složkách.*

Důkaz. Provedeme jej nalezením zobrazení $f(A_r) = (A_{p_1}, A_{p_2}, \dots, A_{p_n})$, které jednotlivé prvky NČ _{r} převede na prvky okruhu n -tic.

Zobrazení f definujeme takto: $[A_{p_K}]_{Z \cdot \alpha_K} \equiv [A]_Z \pmod{p_K^{Z \cdot \alpha_K}}$ pro $K \in \{1, 2, \dots, n\}$. Podle V1.1(a) jsou A_{p_K} jednoznačně definována, takže f je zobrazení. Na druhou stranu podle Čínské zbytkové věty má předchozí soustava kongruencí právě jedno řešení na soustavě zbytků r^Z , které dále splňuje podmínku V1.1.(a), takže A je jednoznačně definováno a tedy f je bijekce. Z definice součtu a součinu je již zřejmé, že obojí se zobrazením zachovává. **q.e.d.**

K tomuto vysoce matematickému textu si dovoluji poznámku, která doufám nebude zatemňující. Tato věta tvrdí, že mám-li např. NČ vyjádřené v soustavě 10 (= 2 · 5), pak je to ekvivalentní, jako kdybych měl dvě NČ – jedno v soustavě 2 a druhé soustavě 5. Pro každé $A \in \text{NČ}_{10}$ najdu právě jednu dvojici $B \in \text{NČ}_2, C \in \text{NČ}_5$ a naopak pro každou dvojici B, C najdu právě jedno odpovídající A . Toto zobrazení z jedné množiny na druhou navíc zachovává aritmetické operace. Závěrem této úvahy je to, že např. místo hledání odmocniny v soustavě 10 se stačí omezit na hledání odmocnin v soustavách {2, 5}, které již dovedeme provést (viz. dále).

Posledně dokázaná věta nám dává jasnou představu o struktuře NČ. Je to komutativní okruh, který je oborem integrity, právě když $r = p^\alpha$, kde p je prvočíslo (pak je opravdu součin nenulových čísel číslo nenulové). Dále snadno najdeme netriviální dělitele nuly – jsou to n -tice, jejichž alespoň jedna složka je nulová (vynásobíme-li ji po složkách s jinou n -ticí, která má nuly na opačných místech, dostaneme nulovou n -tici, což je podle Lemma 1 nula). Dále máme jednoznačný postup pro řešení rovnic – obvyklými metodami rovnic vyřešíme v oborech integrity NČ _{p_K} a libovolná kombinace řešení v NČ _{p_K} bude řešením v NČ _{r} .

Část 2. Inverzní prvky vzhledem k násobení

Problematika inverzních prvků byla již pro $r = 10$ uspokojivě vyřešena a tak jen pro úplnost uvádím následující analogické tvrzení.

Věta 2.1. *K danému NČ A existuje $A^{-1} : AA^{-1} = 1 \iff (a_0, r) = 1$.*

Dále uvedu výpočet a^{-1} pro $a \in \mathbb{N}$, neboť publikované tvrzení není správné. Kromě toho toto tvrzení platí i pro obecné $r \neq 10$.

Věta 2.2. *Nechť je dáno $A = a \in \mathbb{N}$ a platí $\frac{a-1}{a} = 0, \overline{b_1 b_2 \dots b_{n_r}}$. Pak $A^{-1} = \overline{b_1 b_2 \dots b_{n_r}} + 1$.*

Důkaz. *Vezměme předpoklad $a \cdot 0, \overline{b_1 b_2 \dots b_{n_r}} = a - 1$. Vynásobíme-li tuto rovnici r^n a odečteme-li rovnici původní, dostaneme $a \cdot b_1 b_2 \dots b_n = (a-1)(r^n - 1)$. Pro jistotu zopakujeme označení $[A]_z \equiv_{r^z} a$ a hlavně $[\overline{b_1 b_2 \dots b_n}]_{k \cdot n} \equiv_{r^{k \cdot n}} \sum_{j=0}^{k-1} r^{jn} \cdot b_1 b_2 \dots b_{n_r}$. Dosazením do součinu $a \cdot \overline{b_1 b_2 \dots b_{n_r}}$ dostaneme:*

$$\begin{aligned} [A \cdot \overline{b_1 b_2 \dots b_{n_r}}]_{k \cdot n} &\equiv_{r^{k \cdot n}} [A]_{k \cdot n} \cdot [\overline{b_1 b_2 \dots b_{n_r}}]_{k \cdot n} \equiv_{r^{k \cdot n}} a \cdot \sum_{j=0}^{k-1} r^{jn} \cdot b_1 b_2 \dots b_{n_r} = \\ &= (a \cdot b_1 b_2 \dots b_n) \cdot \sum_{j=0}^{k-1} r^{j \cdot n} = (a-1)(r^n - 1) \cdot \frac{r^{k \cdot n} - 1}{r^n - 1} = (a-1)(r^{k \cdot n} - 1) \equiv_{r^{k \cdot n}} 1 - a. \end{aligned}$$

Použitím V1.1(b) dostáváme, že $A \cdot \overline{b_1 b_2 \dots b_{n_r}} = 1 - A$. Pak je zřejmé, že $A \cdot (\overline{b_1 b_2 \dots b_{n_r}} + 1) = A \cdot \overline{b_1 b_2 \dots b_{n_r}} + A = 1 - a + A = 1$. **q.e.d.**

Nyní ještě ukáží, že tvrzení *Bc. Luboše Dostála* “Výpočet inverzního čísla pro čísla přirozená” platí pouze pro $a = r + 1 = 11_r$. Tvrzení jsem pochopil (*redakce taky*) takto: $A^{-1} = B = \overline{b_1 b_2 \dots b_n b_0}_r$, kde $b_0 \equiv_r a_0^{-1}$, $d = 0, b_1 b_2 \dots b_n r = \frac{d}{a}$.

Analogicky důkaz V2.2 dostaneme $[A \cdot \overline{b_1 b_2 \dots b_n r}]_{k \cdot n} \equiv_{r^k} -b_0$ a tedy platí $A \cdot B = A \cdot (\overline{b_1 b_2 \dots b_n 0_r + b_0}) = -r b_0 + a b_0 = (a - r) b_0$. Aby bylo $AB = AA^{-1} = 1$, musí být $(a - r) b_0 = 1$, což nastává pro $a = r + 1 = 11_r$. **q.e.d.**

Část 3. Odmocniny

V této části se omezím na hledání odmocnin v oborech integrity $\mathbb{N}\mathbb{C}_p$. Získané poznatky pak bude možno pomocí V1.3 aplikovat na libovolný okruh $\mathbb{N}\mathbb{C}_r$. Nejprve zde ukáží dvě důležité věty o kvadratických kongruencích, které pak poslouží pro hledání odmocnin v $\mathbb{N}\mathbb{C}$.

Každou větu je nutno vyslovit a dokázat ve dvou případech – pro lichá prvočísla a pro prvočíslo 2. Je to způsobeno tím, že hledáme druhou odmocninu. Kdybychom vyšetřovali obecně n . odmocninu, museli bychom vyšetřit zvlášť případ $p|n$.

Věta 3.1. *Nechť p je liché prvočíslo. Potom kongruence $x^2 \equiv_p a$, $(a, p) = 1$, $Z \in \mathbb{N}$ má řešení, právě když má řešení kongruence $x^2 \equiv_p a$. Řešení jsou případně dvě: x a $-x$.*

Věta 3.2. *Kongruence $x^2 \equiv_{2^z} a$, $(a, 2) = 1$, $Z \in \mathbb{N}$, $Z \geq 3$ má řešení, právě když má řešení kongruence $x^2 \equiv_8 a$, což nastává právě pro $a \equiv_8 1$. Řešení jsou případně čtyři: $\pm x, 2^{Z-1} \pm x$.*

Důsledkem těchto tvrzení jsou následující věty o odmocninách:

Věta 3.3. *Nechť p je liché prvočíslo. Potom rovnice $X^2 = A$, $(a_0, p) = 1$ má v $\mathbb{N}\mathbb{C}_p$ řešení, právě když má řešení kongruence $x^2 \equiv_p a_0$. Řešení jsou případně dvě: X a $-X$.*

Důkaz. Řešit rovnici $X^2 = A$ znamená řešit soustavu kongruencí $(\forall Z \in \mathbb{N}) x_Z^2 \equiv_p [A]_Z$. Podle V3.1 má každá z těchto kongruencí 2 řešení: x_Z a $-x_Z$, právě když má řešení $x^2 \equiv_p [A]_Z \equiv_p a_0$. Dále zřejmě platí: $(\forall M \leq N \in \mathbb{N}) x_N^2 \equiv_{p^M} [A]_N \equiv_{p^M} [A]_M$, & $x_N \not\equiv_{p^M} -x_N$, takže musí platit: $x_N \equiv_{p^M} \pm x_M$, tedy při vhodné volbě $x_N \equiv_{p^M} x_M$ a podle V1.1(a) určují posloupnosti x_Z a $-x_Z$ Z -číslí nějakých $\mathbb{N}\mathbb{C}$, která pak řeší rovnici $X^2 = A$. **q.e.d.**

Věta 3.4. *Rovnice $X^2 = A$, $(a_0, 2) = 1$ má v $\mathbb{N}\mathbb{C}_2$ řešení, právě když má řešení kongruence $x^2 \equiv_8 [A]_3$, což nastává právě pro $[A]_3 \equiv_8 1$. Řešení jsou případně dvě: X a $-X$.*

Důkaz. Řešit rovnici $X^2 = A$ znamená řešit soustavu kongruencí $(\forall Z \in \mathbb{N}) x_Z^2 \equiv_{2^z} [A]_Z$. Omezme se na $Z \geq 3$. Podle V3.2 má každá z těchto kongruencí 4 řešení $\pm x_Z, 2^{Z-1} \pm x_Z$, právě když má řešení $x^2 \equiv_8 [A]_Z \equiv_8 [A]_3$. Dále platí: $(\forall M < N \in \mathbb{N}) 2^{N-1} \pm x_N \equiv_{2^M} \pm x_N \not\equiv_{2^M} \mp x_N$, takže zbytky $\pm x_N, 2^{N-1} \pm x_N \pmod{2^M}$ probíhají jen dvě řešení kongruence $x_M^2 \equiv_{2^M} [A]_M$. Nechť to jsou $\pm x_M$. Soustava má tedy jen dvě řešení, pro která platí $(\forall M \leq N \in \mathbb{N}) x_N \equiv_{2^M} x_M$, a tedy podle V1.1(a) určují nějaká $\mathbb{N}\mathbb{C}$, která řeší rovnici $X^2 = A$. **q.e.d.**

Nyní snadno rozešíme i na čísla soudělná s r .

Věta 3.5. *Nechť $A \neq 0$. Potom A se dá jednoznačně zapsat ve tvaru $A = B \cdot p^2$, kde $p = r$ je prvočíslo a $(b_0, p) = 1$. Řešením rovnice $X^2 = A$ jsou právě všechna $X = Y \cdot p^r$, kde $Y^2 = B$ a $2^r \gamma = \beta$ (to předpokládá, že $2|\beta$).*

Důkaz. První část věty vyplývá z Lemmatu důkazu V1.2(b) a druhá část je jejím triviálním důsledkem.

Nyní můžeme také dokázat následující tvrzení o uspořádání $\mathbb{N}\mathbb{C}_p$, které je další důležitou vlastností $\mathbb{N}\mathbb{C}$:

Věta 3.6. $\mathbb{N}\mathbb{C}_p$ se nedají uspořádat $\implies \mathbb{N}\mathbb{C}_p$ nejsou izomorfní s žádným podoborem integrity \mathbb{R} .

Důkaz. Je-li $p = 2$, pak podle V3.4 $(\exists X) X^2 = -7$. Je-li p liché, pak podle V3.3 $(\exists X) X^2 = 1 - p$. V obou případech dostáváme spor s uspořádáním, neboť každé uspořádání musí splňovat $(\forall X) X^2 \geq 0$. **q.e.d.**

Zjistili jsme, že existují i odmocniny ze záporných čísel (pro $p = 4k + 1$ je prvkem $\mathbb{N}\mathbb{C}_p$ přímo $i = \sqrt{-1}$), a tak zbývá otázka, zda jsou $\mathbb{N}\mathbb{C}_p$ izomorfní s nějakým podoborem integrity množiny \mathbb{C} komplexních čísel.

Pokud by chtěl někdo namítnout, že $-7 = \overline{9993}$ a to můžeme zadefinovat jako kladné, pak by to byl spor s tím, že $X > 0$ & $-X > 0$.

Část 4. Speciální případ $r = 10$

Okruh $\mathbb{N}\check{C}_{10}$ je podle V1.3 izomorfní s okruhem uspořádaných dvojic $(A_2, A_5) \in \mathbb{N}\check{C}_2 \times \mathbb{N}\check{C}_5$. Netriviální dělitelé nuly tedy jsou tvaru $(A_2, 0)$ a $(0, A_5)$ pro libovolná $A_2 \in \mathbb{N}\check{C}_2, A_5 \in \mathbb{N}\check{C}_5$. (pokud byste si je chtěli vyčíslit, musíte pro nějaké A_2 (resp. A_5) počítat dané A_{10} podle čínské zbytkové věty).

Kvadratické rovnice tvaru $(X - A)(X - B) = 0$ mají na $\mathbb{N}\check{C}_{10}$ čtyři řešení $(A_2, A_5), (A_2, B_5), (B_2, A_5), (B_2, B_5)$, kde A_2, B_2 a A_5, B_5 jsou řešení na oborech integrity $\mathbb{N}\check{C}_2$ a $\mathbb{N}\check{C}_5$. Speciálně rovnice $X^2 = X$ má na oborech integrity $\mathbb{N}\check{C}_2, \mathbb{N}\check{C}_5$ řešení 0, 1, takže řešení na $\mathbb{N}\check{C}_{10}$ jsou:

$$\begin{aligned} (0_2, 0_5) &= \dots 0000_{10} & (1_2, 0_5) &= \dots 918212890625_{10} \\ (1_2, 1_5) &= \dots 0001_{10} & (1_2, 0_5) &= \dots 081787109376_{10} \end{aligned}$$

Inverzní prvek existuje podle V2.1 k číslům, která končí cifrou nesoudělnou s 10, tedy konkrétně 1, 3, 7 nebo 9.

Rovnice $X^2 = A, (a_0, r) = 1$ má v $\mathbb{N}\check{C}_2$ řešení, právě když $[A]_3 \equiv_{\pm 1}$, a v $\mathbb{N}\check{C}_5$ právě když $a_0 \equiv_{\pm 1}$, podle V3.3. a V3.4. V $\mathbb{N}\check{C}_{10}$ potom $\exists \sqrt{A}$, právě když $A = B \cdot 4^\alpha \cdot 25^\beta$, kde $[B]_3 \equiv_{\pm 1}$ nebo 9, pro nedělitelé nuly. Odmocniny jsou pro nedělitelé nuly čtyři $(\pm\sqrt{A_2}, \pm\sqrt{A_5})$, pro netriviální dělitele nuly dvě $(\pm\sqrt{A_2}, 0_5)$ nebo $(0_2, \pm\sqrt{A_5})$ a pro nulu jediná $(0_2, 0_5)$. Existují tedy i netriviální odmocniny, např.:

$$\begin{aligned} \sqrt{1} &= (1_2, 1_5) = \dots 0001_{10}, & (-1_2, 1_5) &= \dots 163574218751_{10}, \\ &(-1_2, -1_5) = \dots 9999_{10}, & (1_2, -1_5) &= \dots 836425781249_{10}, \\ \sqrt{41} &= \dots 736758703821_{10}, & & \dots 519473547571_{10}, \\ &\dots 263241296179_{10}, & & \dots 480526452429_{10}, \\ \sqrt{-39} &= \dots 632469189531_{10}, & & \dots 611473095781_{10}, \\ &\dots 367530810469_{10}, & & \dots 388526904219_{10}, \end{aligned}$$

That's all.

Část 5. Důkazy

Věta 1.2. (a) $\mathbb{N}\check{C}$ tvoří komutativní okruh s jednotkovým prvkem. Důkaz tohoto tvrzení sestává z důkazů komutativity a asociativity obou operací (sčítání a násobení), existenci nulového a jednotkového prvku vzhledem k těmto operacím, existenci inverzního prvku vzhledem ke sčítání (**POZOR, nikoliv násobení**) a důkazu distributivity těchto 2 operací.

Jedná se bez výjimky o naprosto mechanické důkazy bez myšlenky, které se zapíší stejně jako důkaz distributivity uvedený v textu článku.

Věta. Čínská zbytková věta: Soustava kongruencí $x \equiv_{m_1} a_1, x \equiv_{m_2} a_2, \dots, x \equiv_{m_n} a_n$, kde m_1, m_2, \dots, m_n jsou po dvou nesoudělná čísla, má na soustavě zbytků mod $m_1 m_2 \dots m_n$ právě jedno řešení.

Důkaz. Indukcí podle n :

- I. $n = 1, x \equiv_{m_1} a_1$, není co řešit.
- II. $n = k$. Soustava $x \equiv_{m_1} a_1, x \equiv_{m_2} a_2, \dots, x \equiv_{m_k} a_k$ má jedno řešení $x \equiv_m a$, kde $m = m_1 m_2 \dots m_k$. Kongruence $x \equiv_{m_{k+1}} a_{k+1}$ má na soustavě zbytků mod $m \cdot m_{k+1}$ celkem m řešení $n \cdot m_{k+1} + a_{k+1}$, pro která platí: $(m, m_{k+1}) = 1 \implies (n_1 \not\equiv_m n_2 \implies n_1 m_{k+1} + a_{k+1} \not\equiv_m n_2 m_{k+1} + a_{k+1})$, takže $n m_{k+1} + a_{k+1}$ pro $n \in \{0, 1, \dots, m-1\}$ probíhá úplnou soustavu zbytků mod m , na které má kongruence $x \equiv_m a$ jedno řešení. **q.e.d.**

Věta 2.1. K danému $\mathbb{N}\check{C} A$ $(\exists A^{-1}) AA^{-1} = 1 \iff (a_0, r) = 1$.

Důkaz. Pokud $(a_0, r) = d \nmid 1 \implies (\forall B) d \mid AB \nmid 1 \implies (\nexists A^{-1}) AA^{-1} = 1$. Na druhou stranu pokud $(a_0, r) = 1$, má každá z lineárních kongruencí $x_Z \cdot [A]_Z \equiv_{rZ} 1$ jediné řešení $x_Z \equiv_{rZ} [A]_Z^{-1}$. Dále zřejmě platí: $(\forall M \leq N \in \mathbb{N}) x_N \equiv_{rM} x_M$, takže podle V1.1(a) $(\exists X) [X]_Z = x_Z$ a tedy $AX=1$. **q.e.d.**

Věta 3.1. Nechť p je liché prvočíslo. Potom kongruence $x^2 \equiv_p z a, (a, p) = 1, Z \in \mathbb{N}$ má řešení, právě když má řešení kongruence $x^2 \equiv_p a$. Řešení jsou případně dvě: x a $-x$.

Důkaz. Indukcí podle z :

- I. $Z = 1, x^2 \equiv_p a$ má 0 nebo 2 řešení, protože \mathbb{Z}_p je těleso.

II. $Z = k, x^2 \equiv_p a$ má 2 řešení $\pm x_k$. Řešení kongruence $x^2 \equiv_{p^k} a$ bude tvaru $x_{k+1} = x_k + y \cdot p^k$. Pro y dostáváme lin. kongruenci:

$$\begin{aligned} x_k^2 + 2x_k y p^k + y^2 p^{2k} &\equiv_{p^{k+1}} a & / : p^k \\ 2x_k y &\equiv_p \frac{a - x_k^2}{p^k} & p \nmid 2, p \nmid x_k \Leftrightarrow (a, p) = 1 \\ y &\equiv_p x_k^{-1} 2^{-1} \left(\frac{a - x_k^2}{p^k} \right) \end{aligned}$$

Pro každé x_k dostaneme tedy jedno y . Zřejmě pro $x_k, = -x_{k_2}$ dostaneme $y_1 = -y_2$, a řešení tedy budou $\pm x_{k+1}$. **q.e.d.**

Pozn. Právě uvedený důkaz by šel snadno zobecnit i pro řešení $x^n \equiv_{p^k} a$, přičemž bychom museli opět jako zvláštní případ vyjmout $p|n$.

Věta 3.2. Kongruence $x^2 \equiv_{2^z} a, (a, 2) = 1, Z \in \mathbf{N}, Z \geq 3$ má řešení, právě když má řešení kongruence $x^2 \equiv_8 a$, což nastává právě pro $a \equiv_8 1$. Řešení jsou případně čtyři: $\pm x, 2^{Z-1} \pm x$.

Důkaz. Indukcí podle z :

I. $Z = 3, 1^2 \equiv_8 3^2 \equiv_8 5^2 \equiv_8 7^2 \equiv_8 1$. Máme tedy dvě dvojice řešení $\pm 1, 2^2 \pm 1$.

II. $Z = k, (2^{k-1} \pm x_k)^2 \equiv_{2^{k+1}} a, x_k^2 \pm 2^k x_k \equiv_{2^{k+1}} a, x_k^2 + 2^k \implies$ právě jedna z dvojic $\pm x_k, 2^{k-1} \pm x_k$ řeší i kongruenci $x^2 \equiv_{2^{k+1}} a$, označme ji $\pm x_{k+1}$. Dále se snadno přesvědčíme, že i zbylá dvě řešení mod 2^{k+1} splňující $x \equiv_{2^k} \pm x_{k+1}$, totiž $2^k \pm x_{k+1}$, řeší: $(x + 2^k)^2 \equiv_{2^{k+1}} x^2 + 2^{k+1}x + 2^{2k} \equiv_{2^{k+1}} x^2$. **q.e.d.**

Tímto důkazem končí tento příspěvek. Jako redaktor bych k němu chtěl dodat pár věcí. Za celou dobu, co opravuji seminář, jsem se nesešel s tak důkladně zpracovaným článkem. Vše, co jsem zde vysázel, je téměř doslovný přepis autorova rukopisu, na některých místech jsem pouze (kurzívou) vysázel vysvětlující poznámky. Autorův příspěvek je zpracován matematicky naprosto přesně, výklad je prost jakéhokoliv "okecávání", neobsahuje žádné nezodpovězené otázky, prostě je jednoznačně vynikající. Nezbývá mi, než vám všem popřát, abyste v budoucnu posílali stejně dobře zpracované články.

Zdeněk Dvořák: Důkaz asociativity a distributivity

Zavedme si speciální označení NČ: libovolnou posloupnost $a_0, a_1, a_2, \dots \in \mathbf{N}$ zobrazme na jedno NČ $A = \dots A_2 A_1 A_0$ takto:

$$\begin{aligned} A_0 &= a_0 \bmod 10, & z_0 &= a_0 \operatorname{div} 10 \\ A_n &= (a_n + z_{n-1}) \bmod 10, & z_n &= (a_n + z_{n-1}) \operatorname{div} 10 \end{aligned}$$

Je zřejmé, že číslu $A = \dots A_2 A_1 A_0$ odpovídá mimo jiné posloupnost $a_0 = A_0, a_1 = A_1, \dots$. Pomocí těchto posloupností snadno nadefinujeme součet $C = A + B$ takto: $c_n = a_n + b_n$, kde a_i, b_i, c_i jsou libovolné posloupnosti odpovídající daným NČ.

V článku *Bc. Luboš Dostála* chybí důkaz asociativity násobení a distributivity. Tyto důkazy se velmi snadno dokáží použitím sum. Označme si $A = \dots a_2 a_1 a_0$, a stejným způsobem také proměnné B, C, D, E . Nechť $D = (AB)C, E = A(BC)$. Pak platí:

$$\begin{aligned} d_n &= \sum_{i=0}^n (AB)_i \cdot c_{n-i} = \sum_{i=0}^n \sum_{j=0}^i a_j b_{i-j} c_{n-i} \\ e_n &= \sum_{i=0}^n a_i (BC)_{n-i} = \sum_{i=0}^n a_i \sum_{j=0}^{n-i} b_j c_{n-i-j} = \sum_{i=0}^n \sum_{j=0}^{n-i} a_i b_j c_{n-i-j}, \end{aligned}$$

je vidět, že $d_n = e_n$, neboť suma se počítá přes všechny trojice $a_k b_l c_m$ takové, že $k + l + m = n$. Sumy se liší pouze způsobem zápisu. **q.e.d.** Důkaz distributivního zákona je ještě jednodušší, nebudeme ho zde ani uvádět.

Zdeněk Dvořák: Jsou NČ o daném základu oborem integrity?

Víme, že pro libovolný základ r jsou r -adická NČ okruhem. Dále víme jsme, že desítková NČ nejsou oborem integrity (existují netriviální dělitelé nuly). Z minulého příspěvku vyplývá, že $(\forall A) (\exists A^{-1}) \Leftrightarrow (a_0, r) = 1$. Je zřejmé, že pro prvočíselný základ soustavy r existuje inverzní číslo ke každému A , které nekončí na nulu.

Vyšetřeme existenci netriviálních dělitelů nuly, tj. $A \neq 0, B \neq 0, AB = 0$. Stačí se omezit na A, B nekonečné na nulu, je zřejmé, že pokud $A = 10C, AB = 0 \Rightarrow 10CB = 0 \Rightarrow CB = 10$. Jistě musí platit $a_0 b_0 \equiv 0 \pmod{r}$. To lze splnit pouze pro r složené. Pro vyšší řády musí být splněna podmínka

$$c_n = 0 \equiv \sum_{i=0}^n a_i b_{n-i} + z_n \pmod{r}$$

$$a_0 b_n + b_0 a_n \equiv - \left(\sum_{i=1}^{n-1} a_i b_{n-i} + z_n \right) \pmod{r}$$

Neznámé jsou a_n, b_n , ostatní čísla lze z nižších řádů vypočítat. Jak snadno nahlédneme, rovnice má řešení právě tehdy, když $(a_0, b_0, r) | z$, kde z je pravá strana (neboť kongruence se dá zapsat jako $a_0 b_n + b_0 a_n + Kr = z$). Tato podmínka bude zcela jistě splněna, pokud a_0, b_0 budou nesoudělná. Takže má-li r alespoň dva prvočíselné dělitele, lze taková a_0, b_0 najít a okruh \mathbb{N}_r není oborem integrity. Zbývá nám vyšetřit případ $r = p^n, p$ je prvočíslo.

Uvažujme $a_0 b_0 \equiv 0 \pmod{r} \Rightarrow a_0 b_0 = Kr \Rightarrow a_0 = a \cdot p^m, b_0 = b \cdot p^l, p \nmid a, p \nmid b, m + l \geq n, m < n, l < n$, BÚNO $l \geq m$. Pak pro druhé cifry A, B platí: $a_1 b p^l + b_1 a p^m + a b p^{m+l} / p^n \equiv 0 \pmod{p^n}$. Aby toto mělo řešení, musí platit $(b p^l, a p^m, p^n) | a b p^{m+l-n}$, ale $(b p^l, a p^m, p^n) = (p^l, p^m, p^n) = p^m$, podle předpokladů tedy $p^m | p^{m+l-n}$, což nelze, neboť $l < n \Rightarrow l - n < 0$. Takže taková a_0, b_0 nelze sestrojít, \mathbb{N}_{p^n} nemá netriviální dělitele nuly a tedy je oborem integrity.

Závěr. \mathbb{N}_r jsou oborem integrity $\Leftrightarrow r = p^n, n \in \mathbb{N}, p$ je prvočíslo. **q.e.d.**

Zdeněk Dvořák: Řešení rovnice $AX + B = 0$

- I. Existuje-li A^{-1} (což nastane, pokud a_0 není dělitelné 2 ani 5), pak celou rovnici tímto číslem vynásobíme a dostaneme jediné řešení $X = -B \cdot A^{-1}$. Toto číslo je jediné, což plyne z vlastností komutativního okruhu.
- II. Pokud je poslední číslice a_0 dělitelná 2 nebo 5 a poslední číslice b nikoliv, rovnice nemá řešení, protože $(VK) (KA)_0$ je dělitelné 2 nebo 5.
- III. V opačném případě obě čísla A, B jsou dělitelné 2 (resp. 5) a rovnici $AX + B = 0$ tedy můžeme pozměnit na $(kM)X + kN = 0$. Pokud k není nula ani její dělitel, pak se dá tato rovnice číslem k vykrátit a řešit rovnici $MX + N = 0$. Je tedy nutné prokázat, že žádné z čísel 2, 5 není netriviálním dělitelem nuly, a posléze nalézt čísla $M = A/2, N = B/2$ (resp. $/5$).
Číslo 2 netriviální dělitel nuly není, protože je-li $2X = 0$, pak pro první nenulovou cifru x_k platí $2x_k \equiv 0 \pmod{10} \Rightarrow x_k = 5$ a pro další cifru x_{k+1} musí platit $2x_{k+1} + 1 \equiv 0 \pmod{10}$, což samozřejmě nelze.
Analogicky číslo 5 není netriviální dělitel nuly, neboť první nenulová číslice $x_k \in \{2, 4, 6, 8\}$, přenos $z_{k+1} \in \{1, 2, 3, 4\}$ a $5x_{k+1} + z_{k+1} \equiv 0 \pmod{10}$, což evidentně nelze.
Zbývá nám nalézt polovinu (resp. pětinu) daného \mathbb{N}_C . Platí zřejmá rovnost $A/2 = 5A/10$, takže stačí dané \mathbb{N}_C vynásobit 5 (resp. 2) a odstranit počáteční nulu. Takže postupným dělením dokážeme převést rovnici na jiný tvar.
- IV. Tímto postupem však nelze vyřešit všechny rovnice. Existují rovnice, které takto nevyřešíme, např. ty, které souvisejí s netriviálními děliteli nuly. Máme-li rovnici $AX = 0$, kde $A|0$, pak stačí nalézt příslušný sdružený dělitel nuly, ale naším postupem to nevyřešíme, protože A může být dělitelné 2 (resp. 5) donekonečna a postup by nikdy neskončil (viz. řešení rovnice $x^2 = x$ z minulého čísla).

Náměty k dalšímu bádání. Jsou opravdu všechna čísla z odstavce IV vždy netriviálními děliteli nuly? Jak rovnice IV rozpoznat a řešit? Snadno nahlédneme, že mají nekonečně mnoho řešení, neboť všechny násobky řešení X jsou také řešení.

V \mathbb{N}_{p^n} nemůže bod IV nastat, jelikož jediné netriviální dělení je dělení číslem p , které ale po n krocích znamená dělení základem soustavy, tj. odstranění počáteční nuly, což nelze pro nenulová čísla opakovat donekonečna. Speciálně pro prvočíselný základ je kritérium řešitelnosti rovnice $AX + B = 0$ jednoduché: počet nul na začátku B musí být větší nebo rovno počtu nul na začátku A .

Téma 2 – Lednička

Doc. Pavol Habuda: Peltierova lednička

Zaujal mě článek *Bc. Tomáše Nečase*: Peltierova lednička, tak jsem se pokusil něco spočítat. Předpokládejme, že máme termoelektrický článek s velkým součinitelem termoelektrického napětí α . Dále nechť má elektrickou vodivost σ a měrnou tepelnou vodivost λ . Předpokládejme, že článek se velmi neochladí, tj. tyto veličiny nejsou funkcí teploty.

Ze zákona zachování energie bude platit

$$Q_{\text{Peltierovo}} = Q_{\text{prostředí}} + Q_{\text{vodivostní}} + Q_{\text{Jouleovo}} \quad (1)$$

Pro jednotlivé složky platí: $Q_J = \frac{1}{2}RI^2t$ – polovina tepla jde k chladnějšímu a polovina k teplejšímu konci. Dále

$$Q_{\text{vod}} = \frac{\lambda_1 S_1 + \lambda_2 S_2}{l} \Delta T t = \Lambda \Delta T t$$

kde ΔT je rozdíl teplot, S_i průřez a l délka sloupků. $Q_{\text{Peltierovo}} = \alpha IT_2 t$ ($T_2 > T_1$). Odtud dostáváme

$$\frac{Q_{\text{prostředí}}}{t} = P = \alpha IT_2 - \Lambda \Delta T - \frac{1}{2}RI^2 \quad (2)$$

Teď zavedeme účinnost $\eta = \frac{P}{P'}$, kde $P' = RI^2 + (\alpha_1 - \alpha_2)\Delta T I$ je příkon chladícího článku. Dosazením dostáváme

$$\eta = \frac{\alpha T_2 I - \frac{1}{2}RI^2 - \Lambda \Delta T}{\alpha \Delta T I + RI^2} \quad (3)$$

Určíme teď proud, při kterém dosahuje η maxima:

$$\frac{d\eta}{dI} = 0 \Rightarrow I_\eta = \frac{2\Lambda}{\alpha} \cdot \frac{T_1 - T_2}{T_1 + T_2} \cdot \left[\sqrt{1 + \frac{1}{2} \frac{\alpha^2 (T_1 + T_2)}{R\Lambda}} - 1 \right] \quad (4)$$

Úpravami dojdeme ke vztahu

$$I_\eta = \frac{\alpha \Delta T}{R(k-1)} \quad (4.1)$$

kde k značí odmocninu v rovnici (4). Dosazením do rovnice (3) dostaneme pro maximální účinnost

$$\eta_{\text{max}} = \frac{T_2}{T_1 - T_2} \cdot \frac{k - T_1/T_2}{k + 1} \quad (5)$$

Pro dva polovodičové válečky zapojené podle této teorie pak platí

$$R\Lambda = \left(\frac{1}{\sigma_1} \cdot \frac{l_1}{S_1} + \frac{1}{\sigma_2} \cdot \frac{l_2}{S_2} \right) \cdot \left(\frac{\lambda_1 S_1}{l_1} + \frac{\lambda_2 S_2}{l_2} \right) \quad (6)$$

Jestliže $l_1 = l_2$; $S_1 = S_2$, tak $R\Lambda = (\rho_1 + \rho_2)(\lambda_1 + \lambda_2)$.

Předpokládejme teď, že $k \rightarrow 1$. Pak pro napětí článku plyne z (4.1)

$$U_\eta = \frac{4(\rho_1 + \rho_2)(\lambda_1 + \lambda_2)\Delta T}{\alpha(T_1 + T_2)}$$

Podívejme se ještě jednou na vztah (5). Vidíme, že $R\Lambda$ musí být minimální, takže je třeba konstruovat články s co největší vodivostí a s co nejmenší tepelnou vodivostí. Já jsem si za svůj článek zvolil $Bi_2Te_3 + Sb_2Te_3$ a $Bi_2Te_3 + Bi_2Se_3$. Po dosazení konstant $\Delta T = 50^\circ C$; $k - 1 = 37 \cdot 10^{-3}$ (literatura) dostaneme $\eta_{\text{max}} = -0.61 = 61\%$. Záporný výsledek vyšel proto, že se jedná o chlazení.

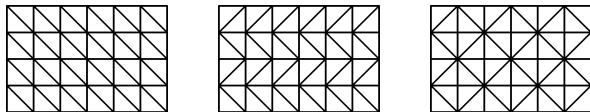
Téma 3 – Rovinné dláždění

Dr. Jan Holeček: Specifikace typů dláždění

Zkusme si navrhnout všechny možné typy dláždění, co nás napadnou, a pak z nich vyházet ty, které mají shodné vlastnosti. Rovina se dá vyplnit trojúhelníky, čtyřúhelníky a šestiúhelníky, klasifikace bude vycházet z tohoto rozdělení.

Trojúhelníky.

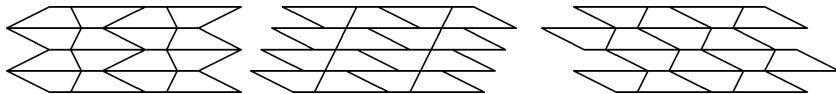
- I. rovnostranné trojúhelníky,
- II. rovnoramenné pravoúhlé trojúhelníky můžeme rozdělit na 3 izomerie α, β, γ :



- III. rovnoramenné trojúhelníky,
- IV. pravoúhlé trojúhelníky, mají opět 3 izomerie,
- V. obecné trojúhelníky, opět ve 3 izomeriích.

Čtyřúhelníky.

- I. čtverce,
- II. obdélníky,
- III. kosočtverce,
- IV. kosočtělíky,
- V. rovnoramenné lichoběžníky,
- VI. obecné lichoběžníky, mají 3 izomerie α, β, γ :



Šestiúhelníky.

- I. pravidelné,
- II. "rovnoramenné", tj. dvě dvojice protějších stran mají všechny stejnou délkou,
- III. "kosé", pouze protější strany jsou stejně dlouhé.

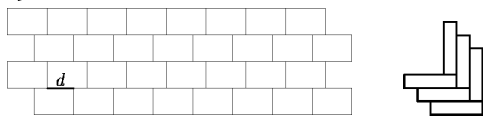
Probíral jsem každé jednotlivé z uvedených dláždění a studoval, kolik má osových souměrností, zda lze (nějak) rotovat ve středech stran, středech útvaru, či ve vrcholech. Posunutí jsem nepovažoval za směrodatné, protože nebereme-li v úvahu jen sousedící kostičky, má jich každé nekonečně rozlehlé dláždění nekonečně mnoho (samozřejmě jsem mohl brát v úvahu jen sousedící kostičky, je však velmi obtížné jednoznačně určit, které to jsou a které ne).

Poznatky jsem poskládal do přiložené tabulky.

Při dělení do skupin jsem bral v úvahu různý počet jen u osových souměrností, u RSÚ a RV jsem počítal jen orientačně, rozlišoval jsem jen nulu a ostatní, zápis RSS o rozlišování jasně vypovídá (stejně lze rotovat jen o 180°); konec konců počet RSÚ a RV by stejně rozhodoval jen v několika málo případech.

Pozn. Použitá dláždění považuji za základní, protože namátkově zkušeno tvary složitější šly všechny na tyto zjednodušit BÚNO.

Dospěl jsem ke skupinám a, b, \dots, p (viz. tabulka), myslím tedy, že existuje 16 tříd dláždění “neposunutého” typu. Do 17. třídy (q) jsem souhrně zařadil všechna dláždění, jejichž kostičky tvoří nezávislé pásy, a ty jsou posunuty (kostičky nemají společně vrcholy) o konstantní vzdálenost d . Osmnáctou třídu (r) pak tvoří “parkety”. Obě třídy jsou nakresleny na následujícím obrázku.



Závěr. Celkem tedy existuje 18 tříd dláždění.

Tvar kostičky dláždění POS RSS RSÚ RV SK

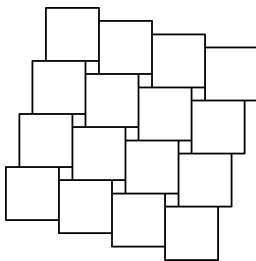
čtverec	4	+	2	2	a
obélník	2	+	1	1	b
kosočtverec	2	-	1	1	c
kosodélník	0	+	1	1	d
lichoběžník rovnoramenný	2	+	0	0	e
lichoběžník obecný	α	1	-	0	f
	β	0	+	0	g
	γ	0	+	0	g
šestiúhelník pravidelný	6	+	1	1	h
rovnoramenný	2	+	1	0	i
kosý	0	-	1	0	j

Vysvětlivky zkratk:

POS = počet osivých souměrností
 RSS = rotace ve středu hran
 RSÚ = rotace ve středu útvaru
 RV = rotace ve vrcholech
 SK = skupina (třída), do níž dláždění patří

Trojúhelníky

rovnostanný	6	+	1	2	h
rovnoramenný pravoúhlý	α	2	+	0	1
	β	1	+	0	0
	γ	4	-	0	2
rovnoramenný	2	+	0	1	k
pravoúhlý	α	0	+	0	1
	β	1	+	0	0
	γ	2	-	0	1
obecný	α	0	+	0	1
	β	0	+	0	0
	γ	0	+	0	1



Poznámka redakce. Do které skupiny tedy patří dláždění vedle tabulky?

Téma 4 – Dělení lupu

Bc. Lenka Zdeborová, Robert Vácha: Dělení lupu 1

Mějme skupinu N lupičů, kteří si mají rozdělit lup o hodnotě n . Nechť dále je lup dělitelný na N částí bez znehodnocení. Algoritmus dělení je tento:

- Zloději si rozlosují jednoznačné pořadí.
- Ten, který si podle pořadí bude vybírat poslední, rozdělí lup na N částí.

Pokud by lup rozdělil na nestejně díly, neměl by jistotu, že na něj zbyde alespoň $\frac{1}{N}$ lupu, a proto lup ve vlastním zájmu rozdělí na stejné díly.

Tento algoritmus bude fungovat, jen když se např. první s posledním nedomluví, aby poslední na nějakou hromádku dal víc, tu by si první vybral a pak by se spolu rozdělili.

Takového podvádění se můžeme zbavit, když po rozdělení hromádky očíslováme a každý z lupičů si vylosuje číslo hromádky, která mu připadne.

Doc. Jan Mysliveček: Podělme se (ne)přátelé

Mějme N lupičů a poklad o hodnotě 1. Nejprve budeme uvažovat, že loupežníci netvoří spolky s cílem okrást ostatní, pouze se každý snaží okrást ostatní pro svůj zisk. Pro jednoduchost předpokládejme, že poklad lze rozdělit právě na N dílů. První loupežník rozdělí lup na dvě části. V první bude poklad hodnoty $\frac{p}{N}$ a v druhé $1 - \frac{p}{N}$. Tyto části definitivně oddělíme (odneseme je aspoň 50m od sebe). Loupežníci se po řadě začínou rozhodovat, ke které části půjdou a to tak, aby tam na ně připadal větší díl lupu. Nechť je $p < \frac{N}{2}$ a je již rozděleno k loupežníků, u první části je jich p . U druhé jich pak je $k - p$. Loupežník s číslem $N - k - 1$, tedy ten, který je na řadě, půjde k druhé části, protože u první části je poklad na osobu $\frac{1}{N}$, po jeho příchodu by to ale bylo už jen $\frac{p}{N(p+1)} < \frac{p}{pN} = \frac{1}{N}$, zatímco u druhé části na něj čeká po jeho příchodu poklad $\frac{N-p}{N(k-p+1)}$, což je víc než u části první. Z toho plyne, že nakonec bude u první části p loupežníků, zatímco u druhé části $N - p$. Tento postup budeme aplikovat tak dlouho, dokud nebudou všichni účastníci spokojeni, tj. budou mít díl $\frac{1}{N}$.

Důležitější je situace, kdy je poklad dělitelný více méně do nekonečna. Rozdělení, které nebude rovnoměrné, bude ale nevýhodné právě pro dělitele, což dokážu sporem. Nechť hodnota pokladu v první části je $\frac{z+z}{N}$, kde $0 \leq z < 1$. Pak nastane situace, kdy u první hromádky bude p loupežníků, hodnota pokladu v druhé části je $\frac{N-p+(1-z)}{N}$ a nechť je u této části $N - p - 1$ loupežníků. Je tedy rozděleno $N - 1$ loupežníků. Na řadě je dělitel, ale je zřejmé, že na něj bude čekat poklad o hodnotě menší než $\frac{1}{N}$.

Tohoto by se dalo využít k tomu, aby se k loupežníků dohodlo a okradlo zbytek. Při daném postupu musí být $k > \frac{N}{2}$. Pak by ale měli jednodušší ten menší zbytek zmlátit a se vším utéct. Myslím si, že všechny, a tedy i tento, algoritmy řeší situaci, kdy všichni se chtějí podělit, ale mají strach, že ti ostatní je chtějí okrást, nedochází tedy ke společným dohodám.

Antonín Lejsek, Bc. Karel Kyrián, Doc. Pavol Habuda: Dělení lupu 2

První lupič rozdělí lup na dvě části a druhý si od něj jednu vybere. Pak oba rozdělí svůj díl na tři části a třetí si od každého jednu vybere. Je zřejmé, že vždy může získat alespoň $\frac{1}{3}$ lupu, bez ohledu na rozdělení mezi první a druhým lupičem. Takto se pokračuje dál až $N - 1$ lupičů rozdělí své podíly na N částí a poslední lupič si od každého jednou vybere.

Bc. Karel Kyrián: Důkaz správnosti algoritmu

Tímto způsobem může první lupič zřejmě získat pro sebe $\frac{1}{N}$ lupu. Když rozdělí svůj podíl vždy přesně na stejné části, ztratí při prvním dělení $\frac{1}{2}$ lupu, při druhém $\frac{1}{3} \cdot \frac{1}{2}$ lupu, po $k - 1$ děleních tedy má

$$1 - \frac{1}{2} - \frac{1}{2} \cdot \frac{1}{3} - \frac{1}{2} \cdot \frac{1}{3} \cdot \frac{1}{4} - \dots = 1 - \frac{1}{1 \cdot 2} - \frac{1}{2 \cdot 3} - \frac{1}{3 \cdot 4} - \dots - \frac{1}{(k-1) \cdot k} = \frac{1}{k}.$$

Uvažujme k -tého lupiče. Lupiči před ním nechť mají po řadě $\frac{1}{a_1}, \frac{1}{a_2}, \dots, \frac{1}{a_{k-1}}$ lupu, kde $\sum_{i=1}^{k-1} \frac{1}{a_i} = 1$. Tento lupič si od každého může vybrat minimálně $\frac{1}{k}$ jeho části, tedy celkově $\frac{1}{k}$ lupu. Může tedy mít po $k - 1$ děleních $\frac{1}{k}$ majetku stejně jako první lupič, a ten může skončit s $\frac{1}{N}$ majetku, takže i tento lupič může skončit s $\frac{1}{N}$ majetku. K podvodu nemůže dojít.

Doc. Pavol Habuda: Dělení kořisti

Složitější je případ, kdy mezi loupežníky je hierarchie, první lupič má dostat N_1 kořisti, druhý N_2 , třetí N_3, \dots až poslední N_n kořisti.

Co se teď stane, když přijde $k + 1$. lupič. Aby nebyl nikdo škodný, musí platit, že části se přeskupí tak, že všechny aktuální poměry budou stejné jako poměry konečné, tj.

$$\frac{N_1}{N'_1} = \frac{N_2}{N'_2} = \dots = \frac{N_k}{N'_k} \quad (1)$$

Určitě platí $N_1 + N_2 + \dots + N_k = 1$, a zároveň $N'_1 + N'_2 + \dots + N'_{k+1} = 1$, kde N'_{k+1} je díl, který získal $(k+1)$ -ní lupič. Také platí

$$\frac{N'_1}{N'_{k+1}} = \frac{L_1}{L_{k+1}}; \frac{N'_2}{N'_{k+1}} = \frac{L_2}{L_{k+1}}; \dots \text{ atd.} \quad (2)$$

kde L_k je konečná hodnota lupičova lupu po všech děleních.

Máme určit, jaký díl si vezme $k+1$. lupič od každého předchozího.

$$\begin{aligned} P_1 &= N_1 - N'_1 = N_1 - \frac{L_1}{L_{k+1}} \cdot N'_{k+1} \\ P_2 &= N_2 - N'_2 = N_2 - \frac{L_2}{L_{k+1}} \cdot N'_{k+1} \\ &\dots\dots\dots \\ P_k &= N_k - N'_k = N_k - \frac{L_k}{L_{k+1}} \cdot N'_{k+1} \end{aligned} \tag{P}$$

Sečtením těchto rovnic dostaneme

$$N'_{k+1} = \sum_{i=1}^k N_i - \frac{N'_{k+1}}{L_{k+1}} \cdot \sum_{j=1}^k L_j$$

Zřejmě $\sum_{j=1}^k N_j = 1$, odkud pro N'_{k+1} dostaneme

$$N'_{k+1} = \frac{L_{k+1}}{L_{k+1} + \sum_{j=1}^k L_j} \tag{3}$$

Dosažením (3) do rovnic (P) dostaneme obecně

$$P_i = N_i - \frac{L_i}{L_{k+1} + \sum_{j=1}^k L_j} = N_i - \frac{L_i}{\sum_{j=1}^{k+1} L_j} \tag{4}$$

P_i nechť má tvar $\frac{\Pi_i}{\Pi}$. Potom i -tý loupežník si rozdělí svůj lup na Π_i částí a $(k+1)$ -ní loupežník si Π_i částí vezme.

Michal Tarana: Nepoctivá spravedlnost

Mějme N lupičů, kteří si mají rovnoměrně rozdělit lup, tj. každý má dostat minimálně $\frac{1}{N}$ lupu. Jeden lupič bude lup dělit. Uvažme, že se chce obohatit o část x , kterou přidá k svému dílu. To může udělat tak, že z jedné z ostatních částí odebere x , nebo z každé z ostatních částí odebere $\frac{x}{N-1}$. V tomto případě si lupiči zabezpečí svůj podíl tak, že nakradou co nejvíc, protože čím víc nakradou, tím méně jim "děliče" ukradne.

Dále autor navrhuje algoritmus, který umožňuje každému lupiči ovlivnit stav částí natolik, že znemožní jakýkoliv pokus o podvod ze strany ostatních.

- každý z lupičů vyčlení z lupu $\frac{1}{N}$ (všechny části budou vedle sebe a budou vypadat stejně)
- každý z lupičů všechny části navzájem promíchá (změní jejich pořadí), samozřejmě náhodně
- každý z lupičů změni náhodně pořadí ostatních lupičů
- každý lupič si vybere odpovídající část (první lupič první část atd.)

Poznámka opravovatele: Navrhli jste několik způsobů, jak zamezit podvodu ze strany některých lupičů, ale jediný algoritmus (uvedený v článku Dělení lupu 2) umožňuje každému lupiči nezávisle na ostatních získat pro sebe aspoň $\frac{1}{N}$ lupu.

Úloha 4 – Barvení obrazce

Jak se všichni řešitelé přesvědčili, je obsah systému obdélníků nekonečný: $P = 1 + 1 + 1 + \dots = \infty$. Natíráme-li tento systém obdélníků barvou, spotřebujeme nekonečné množství barvy, protože vrstva nátěru není nekonečně

Úloha 2. Hodinář

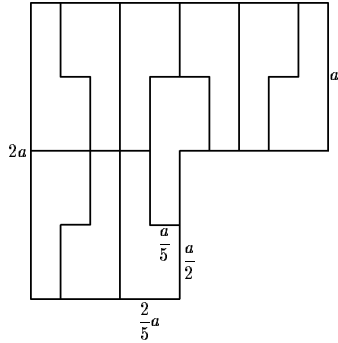
Antonín Lejsek: Řešení

Povšimněme si, za jak dlouho se setkají ručičky jdoucí stejným směrem, ale jedna z nich $12\times$ pomaleji. Pokud je postavíme na stejné místo a pustíme, rychlejší se dostane na stejné místo za 12 hodin $12\times$, pomalejší jen jednou. Pomalejší ručička "utíká" rychlejší a tak se za 12 hodin potkají jen $11\times$. Od spuštění se poprvé potkají za 12/11 hod.

Porovnejme chování pokažených a správně jdoucích hodin. Velké ručičky jdou jedním směrem, jedna $12\times$ rychleji než druhá. Potkají se za 12/11 hod. Stejně je to s malými ručičkami. Špatně nastavené hodiny budou ukazovat správný čas za 12/11 hod. Tedy v 7 : 05 hod. a 27, $\overline{27}$ s.

Úloha 3. Dělení na 10 dílů

Tato úloha původně nevyžadovala komentář, stačil by správný přehledně nakreslený obrázek, ale Petr Zima si všiml zajímavého problému: Kam patří hranice? "U uvedeného řešení se snadno přesvědčíme, že z hranice nelze vybrat část, která by náležela právě 1 dílu tak, aby disjunktivním sjednocením byl celý obrazec."

**Úloha 4. Číslo násobené dvěma**

Pokud dané číslo existuje ve tvaru $a_n a_{n-1} a_{n-2} \dots a_1 2$, pak platí

$$\begin{array}{r} a_n a_{n-1} a_{n-2} \dots a_1 2 \\ \times 2 \\ \hline 2 a_n a_{n-1} a_{n-2} \dots a_2 a_1 \end{array}$$

Je zřejmé, že $a_1 = 2 \cdot 2 = 4$, pak $a_2 = a_1 \cdot 2 = 8$ a tak dále, dokud nedostaneme $a_n = 1$ (samozřejmě ještě musí být přechod z nižšího řádu roven 0).

Takže nejmenší možné takové číslo je

$$\begin{array}{r} 105263157894736842 \\ \times 2 \\ \hline 210526315789473684 \end{array}$$

Zadání nových témat

Téma 5. Pokus R. P. Feynmana

Nechali jsme se inspirovat jednou příhodou z autobiografie známého amerického fyzika *R. P. Feynmana*: To snad nemyslíte vážně? Cituji:

Jednou jsem experimentoval v princetonské cyklotronové laboratoři s dosti otřesným výsledkem. V jedné knize o hydrodynamice se vyskytoval problém, který tenkrát rozebírali všichni studenti fyziky. Problém zní takhle: máte rozprašovač vody na trávnický – kus trubky ve tvaru S, který se může otáčet kolem svého středu –, voda stříká ven v pravém úhlu k ose a způsobuje otáčení trubky v určitém směru. Každý ví ve kterém: v opačném, než má tryskající voda. Otázka zní takto: Kdybyste měli jezero nebo bazén – spoustu vody – a ponořili rozprašovač zcela do vody a nasávali jím vodu dovnitř, místo abyste ji stříkali ven – kterým směrem se roztočí? Bude se otáčet stejně, jako když rozprašujete vodu na vzduchu, nebo opačně?

Na první pohled je odpověď úplně jasná. Potíž byla v tom, že jedněm bylo jasné, že se bude otáčet takhle, a druhým bylo stejně jasné, že se bude otáčet naopak. Všichni to tedy rozebírali a pamatují se, že na jednom semináři nebo čaji šel někdo k profesoru Johnu Wheelerovi a zeptal se ho: “Jakým směrem si vy myslíme, že se to bude točit?”

Načež Wheeler řekl: “Včera mě Feynman přesvědčil, že se to bude točit jedním směrem. Dneska mě zase přesvědčil, že se to bude otáčet právě naopak. Jak se to bude točit zítra – to nevím.”

Řeknu vám důvody, které vás přesvědčí o otáčení jedním směrem, a jiné důvody, které vás přesvědčí, že to má být právě naopak.

Prvé zdůvodnění spočívá v tom, že když sajete vodu, tak ji vlastně vtahujete dovnitř tryskou, a tryska se tedy bude pohybovat dopředu, vstříc přicházející vodě.

Jednomže přijde někdo jiný a řekne: “Představme si, že rozprašovač držíme nehybně – jaký silový moment k tomu potřebujeme? Když voda tryská ven, tak všichni víme, že musíme tlačit na vnějším oblouku trubky, vzhledem k odstředivé síle vody, která její zakřivení sleduje. Když teď voda poteče podél stejné křivky, ale opačně, bude působit stejnou odstředivou silou směrem k vnějšmu okraji oblouku. Proto jsou oba případy vlastně totožné a rozprašovač se bude otáčet stejným směrem, ať z něj vodu stříkáte, nebo ať ji sajete dovnitř.”

Nějakou dobu jsem si s tím lámal hlavu a pak jsem se konečně rozhodl, která z odpovědí je správná, a abycho to prokázal, chtěl jsem provést experiment.

Tady náš vložený text končí. Pokud vás zajímá, jak to dopadlo, přečtěte si knížku. Vaším úkolem je zjistit, jakým směrem se tedy bude trubka točit. Pokud provedete pokus, budeme jen rádi.

Téma 6. Totální destrukce

Toto téma je neobyčejně rozsáhlé, každý může napsat příspěvek podle svého vlastního uvážení. Jednou větou bych téma shrnul na: “**Studujte destruktivní síly.**” Studovat můžete např.:

- jakou silou musíme působit, abycho roztrhli lano; materiál a tloušťku si můžete zvolit, nebo jaký musí být časový průběh síly, když chce člověk roztrhnout např. telefonní seznam,
- kolik tabulek skla rozbije kámen o dané hmotnosti m letící danou rychlostí v ,
- jaká síla je potřebná k ohnutí tyče o tloušťce d ,
- kolik cihel může pouhou rukou rozbít šikovný karatista,
- obecně co všechno je v čase t schopen zničit jeden jediný člověk (bez použití pomůcek),
- (...) a mnoho dalších nápadů.

Téma můžete studovat teoreticky, nebráníme se však ani praktickým pokusům.

Zadání rekreačních úloh

Příklad 7. Plusy a mínusy

Mějme tabulku 4×4 zaplněnou znaménky $+$ a $-$. Tato znaménka můžeme měnit takto: vybereme si libovolný sloupec, řádek nebo diagonálu (nemusí to být nutně hlavní diagonála) a na této úsečce změníme všechna znaménka na opačná.

Na počátku je tabulka plná znamének $+$ kromě jediné buňky: v prvním řádku je ve druhém sloupci (tedy na pozici $(1, 2)$) znaménko $-$. Zjistěte, zda je možné použitím povolených tahů změnit tabulku tak, aby obsahovala pouze znaménka $+$.

Pro pilné řešitele zadáváme jako téma rozšiřující úkol: zjistěte, jak vypadá situace v tabulce $n \times n$. Vaším úkolem je tedy charakterizovat množinu stavů do kterých se lze dostat pomocí těchto povolených úprav.

Příklad 8. Kondenzátor

Je dán kondenzátor se čtvercovými deskami. Ve směru rovnoběžném s deskami přiletá elektron rychlostí \vec{v}_0 . Provedeme následující úvahu: na elektron působí pole kondenzátoru silou konstantní velikosti, kolmou ke směru rychlosti \vec{v}_0 . To znamená, že po průletu kondenzátorem si elektron zachová složku rychlosti ve směru \vec{v}_0 , získá však navíc ještě nějakou rychlost ve směru kolmém (ve směru intenzity elektrického pole kondenzátoru \vec{E}), zvýší se tedy velikost jeho kinetické energie.

Energie kondenzátoru závisí pouze na jeho kapacitě a náboji. Ty se ale průletem elektronu nezmění, takže energie kondenzátoru bude po průletu elektronu stejná jako na počátku. A na vás je, abyste vysvětlili, jak je to vlastně s těmi zákony zachování (energie a hybnosti) – jak je možné, že se celková energie soustavy elektron-kondenzátor zvětšila?

Příklad 9. Odpočinkové úlohy

Opět vás čeká nová serie jednodušších úloh, bodovaných postupně 1, 2, 3, 4 body.

1. Ach ta maturita

V maturitních ročnících na gymnáziu se rozhodli propagovat významná povolání. Pozvali zástupce z vysoké školy hutní, hornické a dopravní, aby si pohovořili se skupinou studentů, kteří mají o tato povolání zájem. Nikdo se nehlásil na více než jednu školu. Když zástupce hutní školy odcházel z besedy, řekl: “Přihlásili se všichni, kromě tří.” Za chvíli přišel zástupce hornické školy a řekl: “Všichni kromě tří chtějí jít k nám studovat.” Totéž prohlásil i zástupce dopravní školy. Vaší úlohou je zjistit, kolik studentů se zúčastnilo besedy.

2. Tři mudrcové

Tři mudrcové se vydali na výlet. Jednoho večera ulehli do trávy a usnuli. V noci šel kolem nějaký vtípálek a namaloval každému z nich na čelo posměšný obrázek.

Dalšího rána se tito pánové probudili a vzájemně se na sebe podívali. Okamžitě se začali smát, protože ostatní vypadali velice legračně. Po chvíli jim ale úsměv ztuhl na rtech, protože si uvědomili, že toto posměšné znamení mají na čele také.

Jak to zjistili? Samozřejmě nepoužili zrcátko a ani se nesnažili rukou nahmatat barvu na svém čele.

3. Věčný věkový problém

Dvěma lidem je dohromady 86 let. Počet let jednoho z nich tvoří $15/16$ počtu let, kterého druhý dosáhne, až věk prvního bude tvořit $9/16$ počtu let, jehož by druhý dosáhl, kdyby se dožil věku, který je dvanáctkrát větší než počet let prvního z nich v okamžiku, kdyby první mohl být dvakrát tak starý jako druhý. Kolik let je prvnímu a kolik druhému?

4. Čtyři čtyřky

Použítím právě čtyř čísel 4 a libovolného množství závorek a operací $+$, $-$, \times , $/$ vyjádřete postupně všechna přirozená čísla z množiny $1, 2, \dots, 30$. Např. $0 = 4 + 4 - 4 - 4$. Pokud si opravdu nebudete vědět rady, můžete použít i odmocninu, faktoriál, ... Ale výrazy složené pouze ze 4 základních aritmetických operací budou hodnoceny lépe.

Náročnější řešitelé mohou jako téma řešit rozšíření tohoto příkladu: pokud bychom vám povolili používat také některé další funkce, jako jsou např. \sqrt{x} , \log , \exp , \sin , \cos , $x!$, ... dokázali byste vyjádřit libovolné přirozené číslo n ? Obecný vzorec je vítán. Zkuste také použitím těchto funkcí vyjádřit větší interval čísel, např. $1, 2, \dots, 100$.

Pořadí	Jméno	Škola	\sum_{-1}	Témata					Rekreační úlohy						\sum_0	\sum_1
				1	2	3	4	R1	4	5	6.1	6.2	6.3	6.4		
1.	Doc. Pavol Habuda	3.B,?	168	6	8	0		5	5	1	1	3	1	30	53	
2.	Bc. Petr Zima	4.A,GKlad	10	25								4		29	39	
3.	Dr. Jan Holeček	3.A,GKJB	71		8			5	1	2	3	4		23	38	
4.	Zdeněk Dvořák	VI.A,GNové	9	10				5	1	1	3	3		23	32	
5.	Bc. Lenka Zdeborová	3.A,GPlzeň	12		4			4	1	2		2		13	25	
6.-7.	Doc. Jan Mysliveček	3.A,GKJB	100		5			5				4		14	24	
	Antonín Lejsek	5B/6,GKojc	9		4			4	1	2		4		15	24	
8.	Bc. Karel Kyrián	3.A,GBudě	14		7									7	21	
9.	Robert Vácha	3.A,GJihl	5		2			4	1	2	3	3		15	20	
10.	Bc. Tomáš Nečas	3.B,GKJB	12					5	1	1				7	19	
11.	Václav Kučera	3.A,GSmích	8					3	1	2		3		9	17	
12.	Dr. David Holec	3.A,GKJB	72						0	1		4		5	16	
13.	Martin Netolický	3.B,GMedl	4					5	1		3	2		11	15	
14.	Jiří Chaloupka	kvinta,GŽldo	8					5				1		6	14	
15.	Jozef Gajdoš	4.A,SPŠS Žil	0					5	5	1	0	2	0	13	13	
16.-20.	Pavel Augustinský	V.B,GHavř	3					2		2		4		8	11	
	Dr. Ondřej Píbyla	3.A,GKJB	81											0	11	
	Bc. Martin Wokoun	3.A,GKJB	11											0	11	
	Jiří Vábek	kvinta,GŽďár	5						1	1		4		6	11	
	Svatava Stehlíková	sexta,GHust	4					3	1			3		7	11	
21.-22.	Jan Prokleška	oktáva B,GZlín	3									3	4	7	10	
	Bc. Luboš Dostál	septima,GStřb	10											0	10	
23.	Lenka Kučerová	septima,GJičín	7							0		2		2	9	
24.	Dr. Václav Račanský	3.A,GKJB	87											0	8	
25.-26.	Dr. Štěpánka Kučková	4.E,GArab	54											0	6	
	Vladislav Válek	?,?	6											0	6	
27.-31.	Michal Tarana	1.C,GVOza	0		4						1			5	5	
	Peter Hunana	4.,GBystr	5											0	5	
	Alena Kovárová	3.A,GBlava	5											0	5	
	Karel Honzl	3.,GPodb	5											0	5	
	Juraj Fedor	4.,GBystr	5											0	5	
32.-36.	Lucie Petráčková	4.L,GStraš	4											0	4	
	Miroslav Černý	3.,GKutn	4											0	4	
	Pavel Moravec	3.A,GKJB	4											0	4	
	Andrea Svinková	?,GUhr	4											0	4	
	Mgr. Jarmila Mulačová	4.,GMIBol	29											0	4	
37.	Braňo Bača	4.,GDubní	3											0	3	
38.	Tomáš Svatoň	1.,SPŠStav	0									1		1	1	

Uzávěrka dalšího čísla je **5. března. 1998.**

Adresa redakce je:

Robert Špalek B1506
VŠK 17. listopadu
Pátkova 3
182 00 Praha Holešovice