6 Dedekindovy řezy (30 bodů)

V této úloze se pokusíme seznámit s *Dedekindovými řezy*, pomocí nichž zavedeme reálná čísla. Tuto konstrukci vymyslel a publikoval Dedekind v roce 1872. Poznamenejme, že ve stejném roce Cantor publikoval alternativní zavedení reálných čísel jako limit Cauchyovských posloupností.

Samotnou konstrukci neprovedeme do nejmenších detailů, ostatně to by formálně zabralo několik stránek. Naším cílem bude poznat, jak tyto řezy fungují a proč mají vlastnosti, které po reálných čísel požadujeme. Tou nejklíčovější vlastností bude existence suprema každé neprázdné shora omezené množiny.

Na začátku máme uspořádané těleso racionálních čísel $\mathbb{Q}$, které splňuje následující vlastnosti: Sčítání a násobení je komutativní, asociativní, existují inverzní prvky a operace jsou svázané distributivitou, navíc máme definované lineární uspořádání (tedy tranzitivní antisymetrickou relaci). Budeme chtít toto těleso rozšířit, tedy vytvořit těleso reálných čísel $\mathbb{R}$ rozšiřující $\mathbb{Q}$, které bude splňovat velice silný axiom o supremu. Další veledůležitou vlastností racionálních čísel, kterou budeme potřebovat, je, že jsou *husté*, tedy že mezi každými dvěma racionálními čísly je jedno další. Formálně: Pokud $a, b \in \mathbb{Q}$ a $a < b$, potom existuje $c \in \mathbb{Q}$, že $a < c < b$.

6.1 Definice řezu

Budeme chtít využít faktu, že reálných čísel je přesně tolik, kolik je podmnožin racionálních čísel. Tedy reálná čísla budeme reprezentovat jako podmnožiny racionálních čísel. Ovšem ne ledajaké podmnožiny, budeme uvažovat pouze podmnožiny, které jsou *řezy*.

Řez α je podmnožina $\mathbb{Q}$, která splňuje tři podmínky:

1. α je neprázdná a rozdílná od celého $\mathbb{Q}$,
2. pokud $p \in \alpha$, $q \in \mathbb{Q}$ a $q < p$, potom i $q \in \alpha$,
3. pokud $p \in \alpha$, potom existuje r, že $p < r$ a $r \in \alpha$.

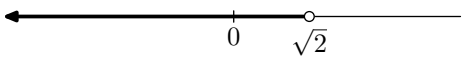
První podmínka říká, že řez je netriviální podmnožina. Druhá říká, že řez obsahuje s každým reálným číslem i všechna menší. Třetí naopak říká, že řez neobsahuje největší racionální číslo.

V dalším textu budeme řeckými písmeny $\alpha, \beta, \gamma, \ldots$ označovat řezy a normálními písmeny racionální čísla.

Úloha 6.1. Pro lepší seznámení s řezy dokažte:

1. Pokud $p \in \alpha$ a $q \notin \alpha$, potom $p < q$,
2. Pokud $r \notin \alpha$ a $r < s$, potom i $s \notin \alpha$.

Pan Dedekind nebyl cukrář, a tedy řezy se nejmenují řezy podle cukrárny. Tento název dostaly, neboť odpovídají rozříznutí reálné osy na dvě části. Reálné číslo r je reprezentováno tak, že vezmeme reálnou osu a rozřízneme ji v bodě r na dvě části. Řez reprezentující r jsou potom všechna racionální čísla menší než r. Například řez, který bude reprezentovat $\sqrt{2}$ bude množina všech racionálních čísel q menších než $\sqrt{2}$ (tedy to jsou buď čísla záporná nebo ty, že $q^2 < 2$). Tento řez je naznačen tučně na obrázku.



Abychom pomocí řezů vytvořili uspořádané těleso reálných čísel, budeme muset udělat čtyři věci:

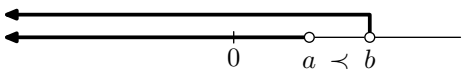
1. Zadefinovat na řezech uspořádání,
2. zadefinovat operaci sčítání,
3. zadefinovat operaci násobení a

4. ukázat, že v sobě obsahují racionální čísla jako podtěleso.

Pokud bychom chtěli definici ověřit do všech detailů, museli bychom ukázat, že splňuje všechny axiomy uspořádaného tělesa. Takový důkaz by byl moc pracný, a proto ověříme jenom některé axiomy. I tak získáme dobrý náhled do toho, jak řezy fungují, díky čemuž by dokázání ostatních vlastností už nebylo obtížné.

6.2 Uspořádání na řezech

Na řezech nadefinujeme uspořádání zcela přirozeně. Řezy uspořádáme inkluzí, tedy $\alpha \prec \beta$, pokud $\alpha \subsetneq \beta$.



Úloha 6.2. Dokažte, že pro každé dva řezy nastane právě jedna z možností $\alpha \prec \beta$, $\alpha = \beta$ nebo $\alpha \succ \beta$.

Úloha 6.3. Dokažte, že je uspořádání tranzitivní: Pro každé tři řezy α, β, γ platí, že $\alpha \prec \beta$ a $\beta \prec \gamma$ implikuje $\alpha \prec \gamma$.

Úloha 6.4. Ukažte, že platí axiom o supremu. Tedy ukažte, že pro libovolnou neprázdnou shora omezenou podmnožinu řezů M existuje $\sup(M)$, nejmenší horní závora množiny M.

Nápověda. Uvažte množinu všech horních závor, každá z nich je řez. Definujte $\sup(M)$ jako průnik všech horních závor. Budete muset ukázat, že $\sup(M)$ je řez a že neexistuje žádná menší horní závora.

6.3 Sčítání řezů

Pro dva řezy α a β definujeme sčítání takto:

$$\alpha \oplus \beta = \{x + y \mid x \in \alpha, y \in \beta\}.$$

Pokud chceme něco dokázat o sčítáni řezů, potřebujeme využít vlastností sčítání v racionálních číslech. Jak by se dalo čekat, struktura racionálních čísel se přenese i na řezy.

Úloha 6.5. Dokažte, že sčítání $\oplus$ je komutativní a asociativní.

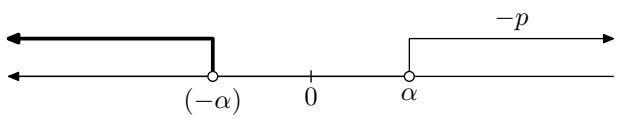
Neutrální prvek $0^\star$ definujeme jako množinu všech záporných racionálních čísel.[1]

Úloha 6.6. Dokažte, že $0^\star$ je skutečně neutrální prvek vůči operaci $\oplus$, tedy $\alpha \oplus 0^\star = \alpha$ pro každý řez α.

Definovat inverzní prvek bude maličko komplikovanější. Nechť α je libovolný řez. Definujme

$$(-\alpha) = \{p \mid p \in \mathbb{Q} \text{ a } \exists r > 0, \text{ že } -r - p \notin \alpha\}.$$

Jinými slovy, p leží v $(-\alpha)$, pokud nějaké racionální číslo menší než $-p$ neleží v α. Následující obrázek ilustruje definici. Množina všech $-p$ z definice odpovídá všem „větším racionálním číslům“ než těm obsažených v řezu α. Množina $(-\alpha)$ obsahuje racionální čísla k nim opačná.



Korektnost definice dokážeme ve dvou krocích:

Úloha 6.7. Dokažte, že pro každý řez α je množina $(-\alpha)$ řez, tedy splňuje podmínky (1) až (3) z definice řezu.

Úloha 6.8. Dokažte pro každý řez α, že $(-\alpha)$ je skutečně inverzní prvek ke sčítání, tedy $\alpha + (-\alpha) = 0^\star$.

[1] Značíme s hvězdičkou, abychom odlišili od neutrálního prvku $0 \in \mathbb{Q}$.

6.4 Násobení řezů

Definovat násobení je kvůli znaménku maličko složitější než definovat sčítání. Omezíme se proto nejprve jenom na kladné řezy. Nechť $\alpha \succ 0^\star$ a $\beta \succ 0^\star$, potom definujeme

$$\alpha \odot \beta = \{p \mid \exists r \in \alpha, \exists s \in \beta, \text{ že } r \geq 0 \text{ a } p < rs\}.$$

Úloha 6.9. Ukažte, že pro libovolné dva řezy $\alpha \succ 0^\star$ a $\beta \succ 0^\star$ je $\alpha \odot \beta$ řez.

Podobně jako výše, lze snadno ukázat, že násobení splňuje všechny axiomy tělesa. Jako neutrální prvek $1^\star$ se použije množině všech racionálních čísel menších než jedna. Pro $\alpha \succ 0^\star$ se definuje inverzní prvek jako

$$\alpha^{-1} = \left\{p \mid p \leq 0 \text{ nebo } \exists r > 0, \text{ že } \tfrac{1}{p} - r \notin \alpha\right\}.$$

Protože však důkaz by byl hodně podobný výše uvedeným důkazům pro sčítání, detaily si zde odpustíme.

Dodefinovat násobení pro všechny řezy je jednoduché. Pro libovolný řez α platí, že $\alpha \odot 0^\star = 0^\star \odot \alpha = 0^\star$. Dále definujeme

$$\alpha \odot \beta = \begin{cases} -((-\alpha) \odot \beta), & \text{pokud } \alpha \prec 0^\star \text{ a } \beta \succ 0^\star, \\ (-\alpha) \odot (-\beta), & \text{pokud } \alpha \prec 0^\star \text{ a } \beta \prec 0^\star, \\ -(\alpha \odot (-\beta)), & \text{pokud } \alpha \succ 0^\star \text{ a } \beta \prec 0^\star, \\ \alpha \odot \beta, & \text{jinak platí původní definice.} \end{cases}$$

Inverzní prvky se dodefinují podobně, pro $\alpha \prec 0^\star$ definujeme $\alpha^{-1} = (-((-\alpha)^{-1}))$. Opět vynecháme detaily důkazů, že násobení splňuje axiomy tělesa.

Úloha 6.10. Ukažte, že pro libovolné dva řezy α a β je $\alpha \odot \beta$ řez.

Tím je odvození téměř dokončeno. Víme, že takto sestrojené řezy tvoří uspořádané těleso, které má supremum pro libovolnou neprázdnou shora omezenou množinu.

6.5 Vnoření racionálních čísel

Zbývá dokázat, že vzniklé těleso obsahuje racionální čísla jako podtěleso. Pro racionální číslo r uvažujme množinu $r^\star$ definovanou takto:

$$r^\star = \{p \mid p \in \mathbb{Q}, p < r\}.$$

Úloha 6.11. Pro libovolné racionální číslo r platí, že $r^\star$ je řez.

Úloha 6.12. Sčítání řezů reprezentujících racionální čísla odpovídá sčítání racionálních čísel, tedy pro libovolná dvě racionální čísla r a s je $r^\star \oplus s^\star = (r + s)^\star$.

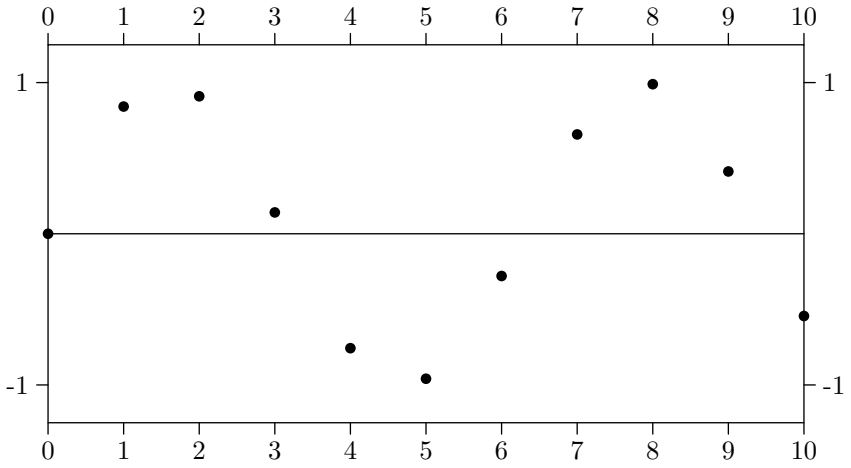
Podobně lze dokázat, že pro libovolná dvě racionální čísla r a s platí, že $r^\star \odot s^\star = (rs)^\star$ a $r^\star \prec s^\star$, právě když $r < s$. Z toho vyplývá, že každé racionální číslo r můžeme zidentifikovat s řezem $r^\star$.

6.6 Shrnutí

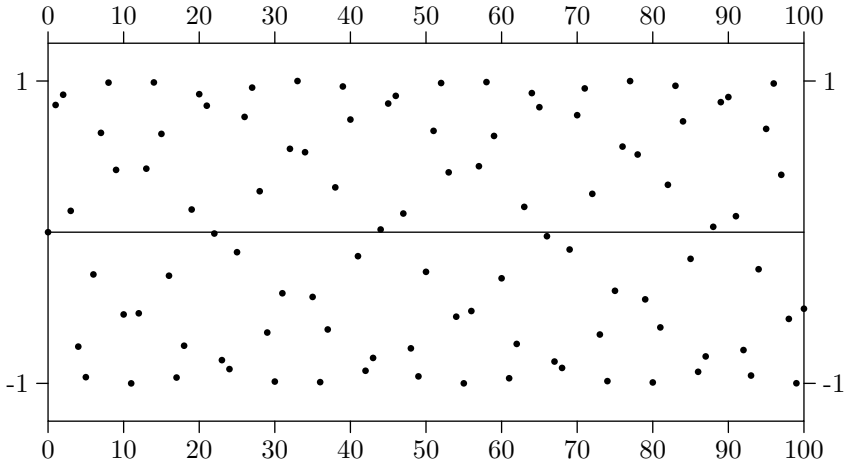
V této úloze jsme popsali, jak pomocí Dedekinových řezů zkonstruovat z uspořádaného tělesa $(\mathbb{Q}, +, \cdot, <)$ jiné uspořádané těleso $(\mathbb{R}, \oplus, \odot, \prec)$ splňující axiom o supremu. Navíc jsme ukázali, že lze těleso $\mathbb{Q}$ vnořit do nově zkonstruovaného tělesa $\mathbb{R}$.

7 Jen jeden sinus? (25 bodů)

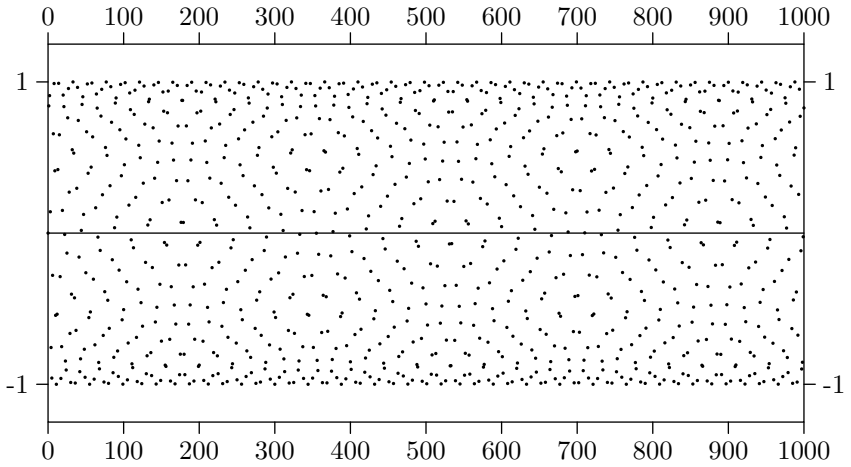
Čtenář určitě dobře zná křivku funkce $\sin x$. V této úloze se zaměříme na posloupnost $\{\sin n\}_{n=0}^{\infty}$ a její počáteční úsek. Ukážeme si, že změna měřítka může mít velký vliv. Prvních deset členů posloupnosti vypadá přesně tak, jak čtenář očekává.

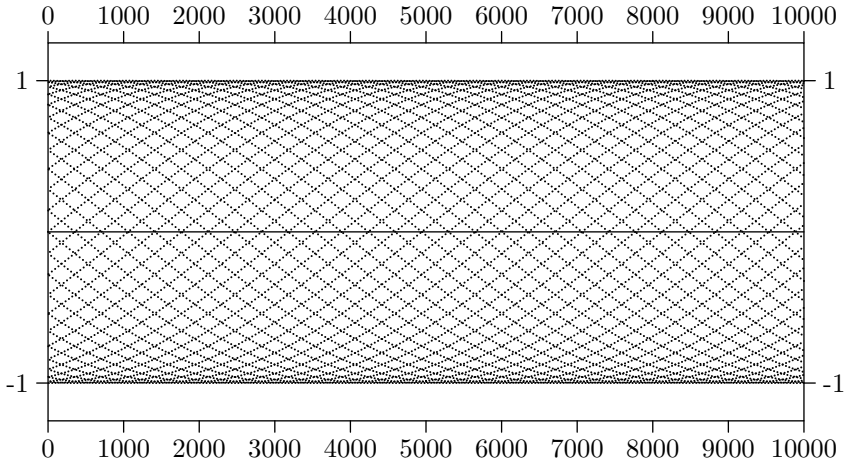


Pro prvních sto členů vypadá obrázek mnohem chaotičtěji. Ostatně to dává smysl, protože jsme hodnoty desetkrát více nahustili vedle sebe, tedy jednotlivé obloučky funkce $\sin x$ začnou splývat.



Zkusíme tedy zobrazit prvních tisíc a prvních deset tisíc členů, což vytvoří dva různé překvapivé vzory. Pro tisíc členů dostáváme jakýsi vzor šestiúhelníků. Ty vidíme kvůli našemu vnímání, které spojuje nesouvisející věci. Pro deset tisíc však dostáváme ještě překvapivější vzor, který vůbec nevypadá jako posloupnost; vidíme řadu sinusovek položených přes sebe.





Možná je překvapivé, že se obrázky pro tisíc a deset tisíc bodů tolik liší. Zkuste se však na obrázek pro tisíc bodů podívat ze strany a uvidíte posunuté sinusovky.

Úloha 7.1. Vaším úkolem je poslední obrázek pochopit a vysvětlit. Proč na obrázku vidíme přes sebe položené sinusovky? Kolik těch sinusovek je a jakou mají periodu? Proč obrázek vypadá symetricky kolem osy x?

Nápověda. Co víte o aproximaci čísla π? Můžete k analyzování posloupnosti používat libovolný matematický software a zkusit lépe pochopit, jak se hodnoty posloupnosti $\{\sin n\}_{n=1}^{\infty}$ chovají.

8 Konečná tělesa existují jen pro mocniny prvočísla (40 bodů)

V této úloze si ukážeme část z důkazu následující algebraické věty.

Věta. *Konečné těleso $\mathbb{F}$ řádu $ř$ existuje, právě když $ř$ je mocnina prvočísla p^k.*

Dokonce platí, že konečně těleso daného řádu je určeno jednoznačně (až na přejmenování prvků, kterému se odborně říká *isomorfismus*). Tato věta tedy opodstatňuje označení $\mathbb{GF}(p^k)$, neboť těleso řádu p^k je jednoznačně určené. V důkazu ukážeme, že každé takové těleso je vysoce symetrický objekt, který v sobě skrývá vektorový prostor. To je poměrně překvapivé, neboť v definici tělesa se vektorové prostory vůbec nevyskytují a naopak ty se definují pomocí těles.

Co o tělesech už známe ...

V samotném důkazu můžeme použít *pouze axiomy tělesa* a jejich důsledky! Připomeňme si, co říkají axiomy tělesa:

- Těleso je struktura s dvěma operacemi – sčítáním a násobením.
- Těleso obsahuje dva speciální prvky, neutrální prvek na sčítání (budeme značit 0) a neutrální prvek na násobení (značíme 1).
- Z hlediska sčítání se těleso chová jako grupa – máme inverzní prvky a neutrální prvek.
- Z hlediska násobení se těleso bez 0 chová jako grupa – opět máme inverze a neutrální prvek.
- Navíc operace sčítání a násobení jsou dohromady svázané distributivitou.

Z axiomů lze odvodit i další vlastnosti těles, některé jsme již viděli.

- Neutrální prvky 0 a 1 a inverze pro obě operace jsou určeny jednoznačně. Ostatně to platí obecně i v grupách.
- Libovolný násobek 0 je zase nula: $a \cdot 0 = 0$.
- Pokud $a + b = a + c$, potom $b = c$.
- Podobně pro násobení a $a \neq 0$, pokud $a \cdot b = a \cdot c$, potom $b = c$.
- Neexistují dvě nenulová čísla a a b, že $a \cdot b = 0$.

$\mathbb{Z}_p$ je podtěleso $\mathbb{F}$

Na rozjezd vyřešíme tělesa s prvočíselnou velikostí. Uvažujme strukturu $\mathbb{Z}_k$ tvořenou čísly $0, \ldots, k-1$ a operacemi sčítaní a násobení definovanými jako zbytek po celočíselném sčítání a násobení.

Příklad. Například pro $\mathbb{Z}_4$ a prvky $a = 2$ a $b = 3$ dostaneme, že $a + b = 1$ a $a \cdot b = 2$, neboť přesně takové zbytky mají čísla 5 a 6 po dělení 4.

Úloha 8.1. Dokažte, že $\mathbb{Z}_p$ je těleso, právě když p je prvočíslo.

Nápověda. Pokud p není prvočíslo, není těžké nalézt dvojici, která porušuje poslední vlastnost. Pro prvočísla to se sčítáním bude docela jednoduché. Je však třeba pro každý prvek a ukázat, že násobení tímto prvkem je prosté, tedy že neexistuje dvě rozdílná čísla b a c, aby $a \cdot b = a \cdot c$.

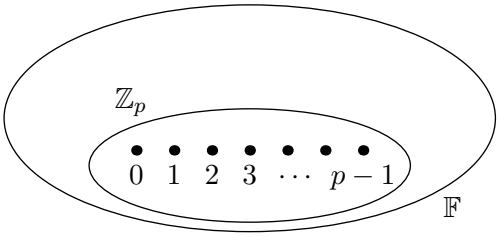
Charakteristika tělesa je nejmenší přirozené číslo k takové, že součet k jedniček $1+1+\cdots+1 = 0$, případně 0, pokud takové k neexistuje (třeba reálná čísla).

Úloha 8.2. Dokažte, že pro každé konečné těleso $\mathbb{F}$ je jeho charakteristika nějaké prvočíslo p.

Nápověda. Ukažte nejprve, že charakteristika je nenulová. Poté zkuste dokazovat sporem. Kdyby charakteristika nebyla prvočíselná, co by bylo špatně?

Označme součet k jedniček pomocí k. V tělese tedy máme prvky $0, \ldots, p-1$. O dalších prvcích zatím nic nevíme.

Úloha 8.3. Ukažte, že prvky $0, \ldots, p-1$ tvoří podtěleso totožné $\mathbb{Z}_p$.



Cože? Těleso je vektorový prostor?

Nyní využijeme získané znalosti o tělesech a dokončíme důkaz překvapivým úskokem, však posuďte sami.

Úloha 8.4. Dokažte, že každé konečné těleso $\mathbb{F}$ charakteristiky p je vektorový prostor $\mathbb{V}$ nad tělesem $\mathbb{Z}_p$. Operace $\mathbb{V}$ definujeme takto: sčítání vektorů odpovídá sčítání v tělese a skalární násobení násobením v tělese (protože $\mathbb{Z}_p$ je podtěleso $\mathbb{F}$, lze to takto definovat).

Nápověda. K tomu potřebujeme dokázat, že vzniklá struktura splňuje všechny axiomy vektorového prostoru. Neplyne to snadno z toho, že $\mathbb{F}$ je těleso?

Víme, že vektorové prostory tvoří silně předurčenou strukturu, pojďme toho tedy využít. Vektorový prostor $\mathbb{V}$ má totiž konečnou dimenzi k. Podle Steinitzovy věty víme, že existuje nějaká báze $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k$. Sice vůbec netušíme, jak vypadá, ale to nebudeme potřebovat – stačí vědět, že existuje.

Bude se hodit ještě jedno obecné tvrzení o bázích a lineárních kombinacích.

Úloha 8.5. Dokažte, že pokud $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k$ je báze vektorového prostoru, potom její různé lineární kombinace definují různé vektory. Tedy dokažte, že $\sum_{i=1}^{k} \alpha_i \boldsymbol{b}_i = \sum_{i=1}^{k} \bar{\alpha}_i \boldsymbol{b}_i$ implikuje, že $\alpha_i = \bar{\alpha}_i$.

Dokončení důkazu

A na závěr složme oba poznatky dohromady.

Úloha 8.6. Dokažte, že každé konečné těleso $\mathbb{F}$ má p^k prvků.

Nápověda. Kolik rozdílných lineárních kombinací vektorů $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k$ existuje?

Tím jsme ukázali neexistenci konečného tělesa velikosti, která není mocnina prvočísla. Také vám přijde trik hezký? Pokud jste se dostali až sem (a případně všechna tvrzení po cestě dokázali), máte můj obdiv (a zasloužíte si své body :)).