

Diskuse k Teorii čísel 2024/25

Sem můžete psát dotazy k teorii čísel na přednášejícího a cvičící.

A samozřejmě i diskutovat navzájem nebo vést monology :)

[Web přednášky](#)

[Web cvičení](#)

OBECNÉ

Víťa: jak to tady funguje?

Víťa: přesně takto, napíšete dotaz a my vám odpovíme.

Víťa: letošní předtermín je tu

[Vzorová písemka \(z předtermínu\)](#)

Bodové hranice byly 43-36-27

Všichni uspěli, 7x 1, 2x 2, 3x 3.

“Zbytečné” bodové ztráty byly

- za nezduvodnění toho, že grupa není cyklická ve 4 (dalo se mluvit o řádech prvků, nebo i jenom odkázat na důsledek 5.6, ale nějaké zdůvodnění bylo potřeba).
- v 5 za nedostatečné zdůvodnění, např. proč $q < Q$ v důkazu první části Dirichletovy věty nebo jak přesně se z první části odvodí tvrzení, které chceme (proč dostaneme fakt nekonečně různých zlomků?)
- Ještě taky zopakuju varování, že to, že se nějaké téma (ne)objevilo na předtermínu nijak nekoreluje s tím, jestli se (ne)objeví v dalších písemkách.

Víťa: vypsal jsem ještě termíny na 5. a 15. září (víc zkouškových termínů už nebude).

Víťa: tu je vzorová písemka z 2022/23 a nějaké komentáře k ní (psané před 2 lety)

[Vzorová písemka \(z předtermínu\)](#)

Přiznám se, že jsem čekal, že písemka dopadne výrazně líp (ale možná to bylo souběhem se zkouškou z logiky?).

Každopádně bodové hranice jsem velmi lehce posunul na 43-35-28.

Známky byly 5x 1, 2x 2, 5x 3, 7x 4 (což samozřejmě z pohledu povinných předmětů není taková tragédie, ale za TČ radši dávám jedničky než čtyřky).

Komentáře:

- Lidé poztráceli netriviální množství bodů na úlohách 1 a 2: když máte něco zformulovat nebo zadefinovat a máte to trochu špatně, tak za to holt strhnu docela dost bodů (když v úloze o nic jiného než o tu formulaci nejde).
- Taky byl celkem častý problém, že jste přehlídli část zadání, zvlášť, ale nejenom, zase v 1 a 2 (když se ptám na víc věcí, tak je potřeba odpovědět na každou z nich...)
- Zvlášť u početních příkladů 3, 4 (ale nejenom u nich) vysvětlujte, co a proč děláte. Jenom za výpočet bez komentářů moc bodů nedostanete (zvlášť když se třeba ještě přepočítáte).
- Jinak mě překvapilo, jak málo lidí umělo důkazy 5 a 6. Pro příští písemky varuju, že tento “těžký důkaz” v 6 byl spíš z těch lehčích (viz třeba tu starší [písemku](#)).
- Ještě taky zopakuju varování, že to, že se nějaké téma (ne)objevilo na předtermínu nijak nekoreluje s tím, jestli se (ne)objeví v dalších písemkách.

Dotaz: Zdravím, rád bych se zeptal, zdali bude vypsán i termín v září? Díky.

Víťa: jasně, s tím by neměl být problém. (Můžete počítat s jedním termínem v září.)

Víťa: přehled látky ze skript, kterou **nezkouším**:

- tvrzení 2.6e) a jeho důkaz
- důkaz věty 2.13
- důkazy v sekci 3.4
- důkaz věty 4.14d); důkaz 4.14c) nezkouším pro $(2/n)$, ani nezkouším příslušnou část lemmatu 4.15
- důkaz v sekci 4.7
- sekci 5.3
- důkaz věty 5.1
- sekci 5.6* (nepřehlédněte hvězdičku! Sekci 5.6 zkouším.)

(upozorněte mě prosím, kdybych na něco zapomněl nebo to tu bylo blbě)

Víťa: Zkouška bude písemná s několika teoretickými i početními otázkami pokrývajícími látku probranou na přednášce a cvičení. Písemka bude na 90 minut, **nesmí** se u ní používat kalkulačky.

Omlouvám se, na webu byla informace o kalkulačkách špatně, už jsem ji opravil - děkuji za upozornění.

Po písemce může velmi výjimečně následovat ústní dozkoušení, zejména při nejasnostech v prezenční písemce nebo hraničním počtu bodů.

Zápočet není potřeba ke konání zkoušky.

Další [vzorová písemka \(z předtermínu 2019/20\)](#)

V písemkách půjde celkem získat 50 bodů a bodové hranice na známky budou podobné jako tady.

Pozor, další písemky se od této (samozřejmě!) budou lišit. Například v tom, ze kterých sekcí budou důkazy, resp. početní příklady.

Jinak upozorňuju, že plánuju otázky do písemky částečně losovat, takže to, že se např. nějaký důkaz už objevil ve vzorové písemce nebo v dřívějším termínu, nic neříká o tom, jestli se (ne)objeví znovu.

Pro jistotu taky upozorním, že se na předtermínu (samozřejmě) mohou objevit i věci, které teprve budou na poslední přednášce nebo cviku.

Jo a nebojte se o kapacitu na zkouškových termínech - když bude potřeba, tak ji zvýším (takže se nemusíte preventivně přihlašovat na termíny, na které vlastně nejspíš nepůjdete).

Dotaz: Budou zkoušena znění vět/definic, které byly napsány jen na cviku? Když je například použijeme k výpočtu? Např. cvičení 2 Cauchyho věta.

Víťa: ne, Fareyho zlomky nezkoušíme (ani příklady na ně).

Ale zkusíme důkaz tvrzení 2.1, který byl na cvičení.

Jinak mě vyloženě nenapadá něco, co by bylo explicitně jenom ze cvičení, když tak se radši zeptejte konkrétně.

Dotaz: Mohu se zeptat ktere pocetni prikladi ze cviceni se taky nezkouseji resp. neobjevi na predterminu? Dekuji.

Víťa: jednak obecně: předtermín bude obsahově zcela standardní zkouška, tedy včetně látky až do konce semestru. Ke cvičením se podívejte na příklady před 2 lety, letos jsou cvičení hodně podobná:

<https://sites.google.com/view/krasensky/archive-of-teaching-in-czech/ls-2223-teorie-%C4%8D%C3%ADsel>

A “početní” příklady na zkoušce odpovídají standardním příkladům ze cvičení (typicky ty, které byly na tabuli nebo mají v zadání vykřičník) nebo z dů. Nebudu dělat žádné cílené chytáky nebo zákeřnosti, ale zároveň negarantuji, že jiný příklad (např. bez vykřičníku) ve zkouškové písemce nemůže být. Obtížnost ale bude podobná.

Ale opět, klidně se zeptejte na něco konkrétního, pokud vám to není jasné.

Smutný dotaz: Přejde ještě někdy na přednášku hroch?

Víťa: no jo, to bych se měl nad sebou zamyslet, když takto hrocha zanedbávám...

Dotaz: Můžou ve zkoušce být i důkazy lemmat? A části důkazů, které jsou ve skriptech ponechány jako cvičení?

Víťa: důkazy lemmat rozhodně ano. Stejně tak části důkazů, které jsou jako cvičení, ale tak nějak rozumně. Klidně se tu ale zeptejte na konkrétní části důkazů, u kterých by Vás to zajímalo.

Obecně ale rozhodně chci, aby Vámi sepsané důkazy na zkoušce prokázaly, že tomu rozumíte, čili nespolehejte na to, že když se nazpaměť naučíte důkaz ze skript a na zkoušce ho doslova “opíšete”, tak že za něj dostanete plný počet bodů (ale velkou většinu bodů dostanete). Skripta jsou leckdy stručnější než pořádně vysvětlené důkazy.

PŘEDNÁŠKY

Jak jste se dostal k pití vody z lahve od rajčatového protlaku?

Víťa: díky moc za hodnotný první dotaz, pobavil mě, takže jen tak dál :) (zodpověděl jsem ho na přednášce)

Dotaz: Na straně 17 ve skriptech je poznámka, že posloupnost čísel p_n je rostoucí od $n = 0$. Podle mě by tam mělo být až od $n = 2$; když si vezmu třeba $\frac{1}{2}$, $\frac{2}{3}$.

Víťa: děkuji, máte pravdu, opravím.

Dotaz: V důkazu tvrzení 4.4: Jak $z(2/p) = (-1)^{(p+1)/4}$ plyne $z(2/p) = (-1)^{(p^2-1)/8}$? Proč to ještě násobíme $(-1)^{(p-1)/2}$?

Víťa: Na první dotaz “Jak to plyne?” jste si odpověděl/a sam/a: vynásobením $(-1)^{(p-1)/2} = 1$ díky předpokladu, že $p \equiv 1 \pmod{4}$.

Ke druhému dotazu "Proč?": Všimněte si, že ten výsledek $s(p+1)/4$ vyšel jen v případě a) v důkazu (kdežto v případě b) to vyjde jinak). Výhodou toho vyjádření pomocí $(p^2-1)/8$ je, že kompaktním způsobem zahrnuje oba případy. Ale jak je napsané ve znění tvrzení, ten vzoreček je ekvivalentní s podmínkou na $p \bmod 8$, takže by si člověk taky mohl pamatovat tuto podmínku mod 8.

Dotaz: Jak z věty 4.1 plyne důsledek 4.3?

Víť: Podle věty 4.1 jsou čísla $(-1/p)$ a $(-1)^{(p-1)/2}$ kongruentní modulo p . Protože se oba rovnají ± 1 , z kongruence vyplývá rovnost stejně jako v důkaze důsledku 4.2.

Dotaz:

V důkazu 4.8:

Víť: díky za dotazy, odpovídám níže **oranžově**:

- Proč $\chi(y)$ komplexne sdruzené = $\chi(y^{-1})$? A podobná věc pro odmocniny z jedné?
Pro komplexní číslo z platí, že z^* (z s pruhem) = (absolutní hodnota z)². To se rovná 1, pokud z leží na jednotkové kružnici, což je případ $\chi(y)$ i odmocnin z jedné. Tedy z s pruhem je inverz k z .
- A v tomtéž důkazu, proč $(x,y) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ právě tehdy, když $(xy^{-1}, y) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$?

Zkoušela jste si to rozepsat? Máte dvě implikace, tak je dokažte jednu po druhé. Případně sem napište svůj pokus o důkaz a já Vám poradím podle toho, kde se zaseknete.

Tak toto je můj pokus o důkaz:

$$z = xy^{-1} \Rightarrow x = zy$$

$$(x,y) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^* \Leftrightarrow (xy^{-1}, y) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$$

DŮKAZ:

- " $\Rightarrow$ " $(x,y) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^* \Rightarrow x,y \in \mathbb{Z}_p^*$
 $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\} \dots$ invertibilní prvky
 $\bmod p: y \in \mathbb{Z}_p^* \Rightarrow y^{-1} \in \mathbb{Z}_p^*$
 $x \cdot y^{-1} \in \mathbb{Z}_p^*$, protože $x \nmid p$ a $y^{-1} \nmid p$, $p = 1 \cdot p$
 $\Rightarrow x \cdot y^{-1} \nmid p$.
- " $\Leftarrow$ " $xy^{-1}, y \in \mathbb{Z}_p^*$, $x \cdot y^{-1} \cdot y \in \mathbb{Z}_p^*$, $x \cdot y^{-1} \cdot y = x \Rightarrow x \in \mathbb{Z}_p^*$

To vypadá správně, ne? :) akorát dělitelnost píšete prohozeně, má být p nedělit x atd. Jinak všimněte si, že $\mathbb{Z}_p^*$ je grupa, což vlastně zdůvodňujete, když chcete xy^{-1} ležet v $\mathbb{Z}_p^*$.

Ještě pro tu substituci v důkazu 4.8 je potřeba, že takto dostáváte bijekci mezi množinou všech (x,y) a množinou všech (z,y) . To je vidět třeba z toho, že máte vzájemně inverzní zobrazení, a to

$$(x,y) \rightarrow (xy^{-1}, y),$$

$$(z,y) \rightarrow (zy, y).$$

- A proč je součet odmocnin z jedné v části b roven -1?

Aha, na tohle už jsem si odpověděla: je to vysvětlené nad zněním věty, protože je to rovné g. součtu triviálního charakteru.

- A potom součet $\chi(z)$ taky?

Není toto tvrzení 4.7?

- A v posledním řádku tohoto důkazu používáme tvrzení 4.7, ale pro aditivní grupu Z_p ?

Díky a omlouvám se, je tam překlep, má být součet přes Z_p^* .

Je takto už vše jasné?

Už ano, moc moc děkuji!!

Dotaz: V lemmatu 4.15: jak funguje dělení dvěma, když počítáme modulo 2? A podobně s osmi?

Víťa: nikdy se tam modulo nedělí.

a_i jsou lichá, takže $(a_i - 1)/2$ je celé číslo, se kterým se tam pak pracuje. Podobně si rozmyslete, že $(a_i^2 - 1)/8$ je celé číslo.

Dotaz: Proč v důkazu Bertrandova postulátu můžeme pokračovat v odhadech pro $n \geq 18$? Nevidím, pro kterou z těch nerovností je to potřeba.

Víťa: Asi ne zcela rozumím dotazu - ptáte se, proč platí ty nerovnosti nebo proč je potřeba předpoklad $n \geq 18$?

Každopádně si ty nerovnosti prostě zkuste jednu po druhé detailně dokázat a když tak sem dejte svůj pokus o důkaz a vysvětlím Vám krok, kde jste se zasekl/a.

Nerozumím, pro kterou z těch nerovností je potřeba, aby n bylo alespoň 18. Vychází mi, že $(2n+1) < (2n)^2$ pro všechna n , a pak $\sqrt{2n} + 2 < 4/3 \sqrt{2n}$ pro $n > 6$.

Víťa: je to potřeba pro tu druhou nerovnost, nebo ne? Máme ekvivalentní úpravy

$$\sqrt{2n} + 2 \leq 4/3 \sqrt{2n}$$

$$2 \leq 1/3 \sqrt{2n}$$

$$6 \leq \sqrt{2n}$$

$$36 \leq 2n$$

$$18 \leq n$$

CVIČENÍ

Mohl byste nám prosím ukázat, jak se dá vyřešit 2. úloha z 5. cvičení? Není mi úplně jasné, jak se dá vyřešit pomocí definice, ta samotná definice je trochu neprůhledná.

Simča: Do piatka pribudnú na stránkach cvičení riešenia úloh z 5. cvičenia. Bude tam riešenie aj úlohy číslo dva. [Web cvičení](#)

Dotaz: Ve cvičení 7 v úloze 0 ve vzorovém řešení řešíme i případ $p = 2$. Jakto, když Legendrův symbol je definovaný pro lichá p ?

Víťa: díky, máte pravdu, nemá to tam být, protože Leg. symbol není definovaný pro $p=2$.

Dotaz: Jak určit řád charakteru modulo v grupě $X(Z_8^*)$? Je to nejmenší r takové, že $\chi(k)^r = 1$ pro všechna k ze Z_8^* ?

Víťa: ano, přesně tak.

Dotaz: Dobrý den, mám dotaz k 5. cvičení příklad 8, viz obrázek. Není mi úplně jasné, jak to ukázat. Souvisí nějak to, že pro $\{\alpha\} > \frac{1}{2}$ sblížený zlomek p_0/q_0 , což je dolní celá část z alfa, není dobrou aproximací s tím, že dolní celá část z alfa “je moc daleko” pro $\{\alpha\} > \frac{1}{2}$?

8. Ukažte, že pokud $\{\alpha\} > \frac{1}{2}$, pak sblížené zlomky $\frac{p_n}{q_n}$ pro $n \geq 1$ jsou všechny dobré aproximace α .

Víťa: napřed obecně: příklady z konce cvičení jsou spíš doplňující, nejedná se o klíčové věci.

Ale toto je v zásadě pokryto důkazem věty 2.10 ve skriptech. Jak se tam píše na začátku důkazu, tak “Dobré aproximace se jmenovatelem 1 je potřeba vyřešit samostatně.”

To je právě to, co píšete s $\{\alpha\} > \frac{1}{2}$: p_0/q_0 pak opravdu není dobrá aproximace (bo p_1/q_1) dává menší chybu. Zkuste si explicitně rozepsat a dokázat, jaké jsou tedy všechny d.a. se jmenovatelem 1.

Pro zlomky se jmenovatelem ≥ 2 projde důkaz podle skript.

Dobře, děkuji za odpověď.

ARCHÍV

Víťa: bavili jsme se o možnosti předtermínu už cca 29.4. Napište mi prosím email, pokud byste o něm uvažovali :) (jinak předběžně počítám s předtermínem místo poslední přednášky 20.5., ale můžeme se domluvit i na jindy)

– vypsal jsem předtermín 29.4. od 12.10, přihlašujte se v SISu.