Požadavky ke zkoušce z Algebry I pro informatiky, 2020/21

David Stanovský

Předmět zkoušky:

Vše potřebné k úspěšnému vykonání zkoušky se nachází v učebním textu. Přečíst a pochopit byste měli vše, i když na některé níže uvedené drobnosti se ptát nebudu. Měli byste znát postupy řešení úloh ze cvičení.

Nebudu zkoušet:

- složitější výpočty v oborech $\mathbb{Z}[\sqrt{s}]$ (NSD, ireducibilní rozklady)
- technické důkazy tvrzení 2.3, 3.2, 4.2, 7.2, 7.5
- důkaz Gaussova lemmatu a Eisensteinova kritéria (ale znění a princip důkazu se naučte!)
- formulaci algoritmu na čínskou větu o zbytcích (poznámka pod důkazem v sekci 8.1), ale měli byste umět spočítat konkrétní příklad
- cvičení 8.4
- šifra AES, Hammingovy kódy (ale kódy obecně ano), sekce 9.4 (latinské čtverce)
- dodatek o permutacích (ale pracovat s permutacemi samozřejmě musíte umět)

Naopak, explicitně upozorňuji, že se budou zkoušet

- informatické aplikace (protokoly sdílení tajemství, Reed-Salomonovy kódy, protokoly založené na diskrétním logaritmu),
- řešení cvičení 6.1-6.3

Průběh zkoušky:

- zkouška bude písemná, na papír, společná pro obě varianty, 6 úloh dohromady za 90 bodů, k tomu se přičte 0-10 za kvízy
- každý si může volně vybrat, zda se zapíše na prezenční nebo distanční termín.
- prezenční: 120 minut; distanční: 3x 45 minut (včetně odeslání řešení), na každou etapu dostanete pouze 2 úlohy
- hodnocení *(předběžně)*: hranice známek 55-67-80
- otázky se budou pídit po znění definic a vět, příkladech ilustrujících definice a věty, otázky kvízového typu, jednoduché početní úlohy, důkazy ze skript či popisy algoritmů, může tam být nějaká nestandardní úloha (nealgoritmický výpočet, důkaz tvrzení, které nemusí být doslovně ve skriptech, apod.)
- přesné pokyny pro on-line zkoušení viz str. 3

Nevím, jak to půjde organizačně. Pokud se první termín neosvědčí, počítejte s tím, že může dojít ke změnám.

Máte-li jakékoliv otázky nebo nápady, jak něco dělat lépe, neváhejte se (včas) ozvat.

Vzorový test

Pozor!! Jde o koncept, není to úplně bodově vyvážené, některé početní úlohy možná vycházejí složitě, možná se to nedá stíhat atd. Se skutečným testem si dám víc práce. Jde mi hlavně o to, abyste viděli typ otázek, které kladu. Pokud se tento typ testu neosvědčí v on-line, udělám změny.

1. (15 bodů) Spočtěte $3^{3^{3^{3}}} \bmod 33$. (Připomínám, že $a^{b^c} = a^{(b^c)}$.) Pokud používáte k výpočtu nějakou větu, formulujte ji.

2. (12 bodů)

(a) Definujte, co přesně znamená, že jsou v daném oboru jednoznačné ireducibilní rozklady.
(b) Uveďte příklad oboru, který tuto vlastnost nemá, včetně konkrétního protipříkladu.
(c) Existuje obor, který tuto vlastnost má, ale neplatí v něm Bézoutova věta? Pokud ano, uveďte příklad. Pokud ne, dokažte.

3. (15 bodů) Popište princip Reed-Salomonových kódů: jaké je zadání úlohy, jak vypadá vstupní text, jak vypadá zakódovaný text, jak se (teoreticky) najde opravená zpráva.

4. (15 bodů) Napište nějaké těleso s 81 prvky a dokažte, že to je opravdu těleso, včetně popisu výpočtu inverzního prvku. Zvolte si libovolný prvek různý od ± 1 a najděte jeho inverz. Využít můžete cokoliv z teorie eukleidovských oborů.

5. (15 bodů) Napište všechny podgrupy grupy $\mathbb{Z}_{19}^*$. Kolik jich je, jak jsou velké? Odpovědi zdůvodněte, formulujte všechny věty, které používáte.

6. (18 bodů) Formulujte a dokažte Burnsideovu větu, vysvětlete značení. Dosaďte do vzorce z věty konkrétní hodnoty při následujícím působení: grupa D_{10} působí na množinu vrcholů pětiúhelníka.

Pokyny pro distanční zkoušku

Co potřebujete:

- tužka, papír
- nějaké zařízení s kamerou a mikrofonem, aplikace zoom
- nějaké zařízení, které umí skenovat, například mobil s aplikací AdobeScan
- průkazka studenta

Přihlašovací údaje pošlu emailem.

Průběh testu:

- v daný čas se přihlásíte pod svým jménem, budu pouštět přes waiting room
- ukážete mi na kameru studentskou průkazku
- ukážete mi na kameru, že jste v místnosti sami a nikde neleží studijní materiály
- po dobu testu musíte mít zapnutou kameru a mikrofon (aby bylo slyšet, že se s nikým nedomlouváte)
- po dobu testu se nesmíte vzdálit z místa, odskočit si můžete mezi odevzdáním části testu a novým zadáním
- test má tři části po 45 minutách (včetně odeslání řešení)
- zadání testu nasdílím přes zooom
- na email stanovsk@karlin.mff.cuni.cz mi pošlete naskenované řešení testu v daném časovém limitu
- po dobu testu nesmíte manipulovat s žádným elektronickým zařízením z jiného důvodu, než sken řešení – po jakékoliv manipulaci s mobilem/tiskárnou očekavám v krátkém okamžiku email s řešením
- po skončení poslední části testu zůstáváte přihlášeni, v breakout místnostech rychle projdeme (já nebo jiný zkoušející) kritické části testu s jednotlivými studenty
- v případě výpadku techniky či spojení na delší než krátkou chvíli:
  - v jiné než poslední části: zkouška se anuluje, termín vám nepropadá
  - v poslední části:
    - pokud předchozí části nasvědčují, že zkoušku nemáte šanci složit, jste hodnoceni nedostatečně
    - pokud předchozí části nasvědčují, že výsledek bude nevalný (3–4), zkouška se anuluje a termín vám nepropadá
    - pokud předchozí části nasvědčují, že výsledek bude pěkný (1–2), dohodneme se na náhradním dozkoušení
  - buďte připraveni na emailové instrukce ke znovunavázaní spojení (pokud bude chyba na mé straně)

Podmínky jsou adaptací obecných instrukcí UK, viz https://karlovkaonline.cz/