Matematika pro informační technologie (Mgr.) - SZZ

Ústní část státní závěrečné zkoušky studijního oboru Matematika pro informační technologie se skládá z dvou tematických okruhů. Z tematického okruhu 1 dostane student jednu otázku. Z tematického okruhu 2 si student zvolí buď dvě z variant 2A, 2B, 2C pro zaměření *Matematika pro informační bezpečnost*, nebo dvě z variant 2D, 2E, 2F, 2G pro zaměření *Počítačová geometrie*. Z každé zvolené varianty dostane jednu otázku.

1.Základní matematické obory

(Společný tématický okruh)

Předměty potřebné k pokrytí požadované látky

NMMB403	Počítačová algebra 2
NMMB405	Složitost pro kryptografii
NMMB407	Pravděpodobnost a kryptografie
NMMB409	Konvexní optimalizace

Témata

Složitostní třídy a výpočetní modely.
Definice Turingova stroje. Výpočtový problém jako funkce nebo jazyk. Časová a prostorová složitost výpočtu. Koncept přijímání jazyka nedeterministickým strojem. Determinizace pomocí vektoru voleb. Simulace vícepáskového stroje jednopáskovým. Random Access Machine, srovnání s Turingovým strojem a současnými počítači. Nerozhodnutelné problémy (nerozhodnutelnost HALTING). Definice třídy NP pomocí nedeterministického stroje a pomocí svědecké relace, jejich ekvivalence. Popis problému P vs. NP.

Náhodnost a pseudonáhodnou.
Definice pravděpodobnostního Turingova stroje. Třída BPP. Amplifikace pravděpodobnosti v BPP. Definice zanedbatelné funkce. Jednosměrné funkce, definice a příklady kandidátů. Pseudonáhodné generátory a jejich konstrukce z jednosměrných funkcí. Výpočetně nerozlišitelné distribuce. Důkazy s nulovou znalostí, definice a příklady.

Algoritmy pro práci s algebraickými strukturami.
Výpočet NSD pro polynomy jedné proměnné: Eukleidův algoritmus a jeho praktická použitelnost, posloupnosti polynomiálních zbytků. Faktorizace polynomů nad konečnými tělesy (bezčtvercová faktorizace; Berlekampův algoritmus). Gröbnerovy báze a Buchbergerův algoritmus. Princip přepisovacích algoritmů. Řešení soustav polynomiálních rovnic.

Konvexní optimalizace.
Vlastnosti konvexních množin, kalkulus konvexních funkcí, základní typy úloh konvexní optimalizace.

2. Užší zaměření

Zaměření Matematika pro informační bezpečnost

Student zaměření *Matematika pro informační bezpečnost* zvolí dvě z variant 2A, 2B, 2C 2G a z každé zvolené varianty dostane jednu otázku.

2A Informace a kódy

Předměty potřebné k pokrytí požadované látky

MMB534	Kvantová informace
NMMB401	Automaty a konvoluční kódy

Témata

Klasická a kvantová informace a její přenos. Důsledky kvantové Fourierovy transformace pro kryptografii. Konvoluční kódy. Práce se skrytou a poškozenou informací.

2B Číselné algoritmy

Předměty potřebné k pokrytí požadované látky

NMMB402	Číselné algoritmy

Témata

Faktorizace: metody Pollard rho a Pollard p-1, algoritmus CFRAC (včetně aproximace odmocniny pomocí řetězových zlomků a řešení Pellovy rovnice), a kvadratické síto (včetně Tonelli-Shanksova algoritmu). Základní metody řešení diskrétního logaritmu: Pohlig-Hellman, Baby steps-giant steps a indexový kalkul.

2C Eliptické křivky

Předměty potřebné k pokrytí požadované látky

NMAG436	Křivky a funkční tělesa
NMMB538	Eliptické křivky a kryptografie

Témata

Základní vlastnosti algebraických funkčních těles a jejich grupy divisorů. Weierstrassova normální forma eliptické křivky - ekvivalence a odvození. Picardova grupa a sčítání bodů eliptické křivky. Morfismy, endomorfismy a izogenie. Využití v kryptografii.

Zaměření Počítačová geometrie

Student zaměření *Počítačová geometrie* zvolí dvě z variant 2D, 2E, 2F, 2G a z každé zvolené varianty dostane jednu otázku.

2D Počítačové vidění a robotika

Předměty potřebné k pokrytí požadované látky

NMMB440	Geometrie počítačového vidění
NMMB442	Geometrické problémy v robotice

Témata

Matematický model perspektivní kamery. Výpočet pohybu kalibrované kamery z obrazů neznámé scény. 3D rekonstrukce ze dvou obrazů neznámé scény. Geometrie tří kalibrovaných kamer. Denavit-Hartenbergův popis kinematiky manipulátoru. Inverzní kinematická úloha pro šestistupňový sériový manipulátor – formulace a řešení. Kalibrace parametrů manipulátoru – formulace a řešení.

2E Zpracování obrazu a počítačová grafika

Předměty potřebné k pokrytí požadované látky

NMMB535	Komprimované snímání
NPGR013	Speciální funkce a transformace ve zpracování obrazu
NPGR010	Počítačová grafika III
NMMB433	Geometrie pro počítačovou grafiku

Témata

Modelování inverzních problémů, regularizační metody, digitalizace obrazu, zaostřování a odšumování obrazu, detekce hran, obrazová registrace, komprese, syntéza obrazu, metody compressed sensing, analytická, kinematická a diferenciální geometrie.

2F Aproximace a optimalizace

Předměty potřebné k pokrytí požadované látky

NMMB409	Konvexní optimalizace
NMAG563	Úvod do složitosti CSP
NMMB536	Optimalizace a aproximace CSP

Témata

Konvexní optimalizační problémy, dualita, Lagrangeova duální funkce. Algoritmy pro řešení úloh konvexní optimalizace, metoda vnitřního bodu. Problém splnitelnosti omezení (CSP), algebraický přístup k řešení dichotomické hypotézy. Vážený problém splnitelnosti omezení (vCSP). Příklady výpočetních problémů, které lze popsat v jazyku vCSP, algebraická teorie. Řešení problémů s extrémně velkým vstupem.

2G Numerická lineární algebra

Předměty potřebné k pokrytí požadované látky

NMNV531	Inverzní úlohy a regularizace
NMNV407	Maticové iterační metody 1
NMNV438	Maticové iterační metody 2
NMNV534	Numerické metody optimalizace

Témata

LU a Choleského rozklad matice, metody nejmenších čtverců, Krylovovské prostory, maticové iterační metody (Arnoldiho, Lanczosova metoda, metoda sdružených gradientů,

zobecněná metoda minimálních reziduí), QR algoritmus, regularizační metody pro řešení lineárních inverzních problémů, numerická stabilita.