MASARYKOVA UNIVERZITA

PŘÍRODOVĚDECKÁ FAKULTA

ŽÁDOST O AKREDITACI

Navazujícího magisterského studijního programu

Matematika

Obor

Matematika s informatikou

Brno, říjen 2011

OBSAH

A – Žádost o akreditaci / rozšíření nebo prodloužení doby platnosti akreditace bakalářského / magisterského stud. Programu

Vysoká škola	Masarykova univerzita					
Součást vysoké školy	Přírodovědecká fakulta			**STUDPROG**	**st. doba**	**titul**
Název studijního programu	Matematika			N-MA	2 roky	Mgr.
Původní název SP	Matematika		**platnost předchozí akreditace**	15. 8. 2012		
Typ žádosti		prodloužení akreditace	**druh rozšíření**			
Typ studijního programu	Navazující magisterský			**rigorózní řízení**		
Forma studia	prezenční				**KKOV**	
Obor v tomto dokumentu	**Matematika s informatikou– prodloužení akreditace**			ano	**1103T016**	
Obory v jiných dokumentech	Finanční matematika – prodloužení akreditace			ano	1103T024	
	Matematická analýza – prodloužení akreditace			ano	1101T014	
	Geometrie - prodloužení akreditace			ano	1101T009	
	Algebra a diskrétní matematika – prodloužení akreditace			ano	1101T002	
	Aplikovaná matematika pro víceoborové studium – prodloužení akreditace			ano	1103T037	
	Matematické modelování a numerické metody – prodloužení akreditace			ano	1101T031	
	Statistika a analýza dat – prodloužení akreditace			ano	1101T021	
	Učitelství matematiky pro střední školy – prodloužení akreditace			ano	7504T089	
	Učitelství deskriptivní geometrie pro střední školy – prodloužení akreditace			ano	7504T045	
Adresa www stránky	http://www.sci.muni.cz/akreditace2011		**jméno a heslo k přístupu na www**	kom, akred2011		
Schváleno VR /UR /AR	VR PřF MU	**podpis**				**datum**
Dne	5.10.2011	**rektora**				
Kontaktní osoba	doc. RNDr. Jan Paseka, CSc.		**e-mail**	paseka@math.muni.cz		
Garant studijního programu	doc. RNDr. Jan Paseka, CSc.			paseka@math.muni.cz		

Představení navrhovaných změn v magisterském programu Matematika

Důvodem pro předložení akreditační žádosti je skutečnost, že převážné většině akreditovaných oborů v magisterských programech Matematika a Aplikovaná matematika končí k 15.8.2012 stávající akreditace.

Přírodovědecká fakulta Masarykovy univerzity považuje za vhodné upravit stávající nabídku magisterských oborů Ústavu matematiky a statistiky zejména z důvodu zvýšení propustnosti stávajících programů Matematika a Aplikovaná matematika. Proto navrhuje spojit programy Matematika a Aplikovaná matematika do nově koncipovaného programu Matematika s tím, že se pro budoucí výuku počítá s obory

- Finanční matematika,
- Statistika a analýza dat,
- Matematická analýza,
- Geometrie,
- Algebra a diskrétní matematika,
- Aplikovaná matematika pro víceoborové studium,
- Matematické modelování a numerické metody,
- Matematika s informatikou,
- Učitelství matematiky pro střední školy,
- Učitelství deskriptivní geometrie pro střední školy.

Při návrhu změn jsme vycházeli z praktických zkušeností s provozováním výše uvedených oborů již od roku 2002 (vyjma oboru Finanční matematika, který byl akreditován v roce 2008, a oboru Aplikovaná matematika víceoborová, který byl akreditován v roce 2011 jako náhrada za stávající jednooborové studium Matematika-Ekonomie). Přitom se zejména v bakalářském studiu programů Matematika a Aplikovaná matematika ukazuje, že současné rozdělení na dva programy vytváří zbytečnou psychologickou a administrativní bariéru pro studenty, kteří si při vstupu na naši univerzitu vyberou matematický obor z jednoho programu a během prvních semestrů zjistí, že by jim byl býval více vyhovoval matematický obor z druhého programu.

Domníváme se, že při nově předloženém návrhu bude studium na oborech magisterského programu, s návazností na obdobné změny v bakalářských programech Matematika a Aplikovaná matematika, pro studenty přehlednější a mj. jim umožní snazší přechod mezi obory. Studium je navrženo tak, že bez problémů umožní absolventovi bakalářského programu Matematika následující pokračování v magisterském programu Matematika.

Z hlediska realizace není zamýšlené spojení obou programů do jednoho náročné, protože se úpravou nemění stávající studijní plány jednotlivých oborů a následně tedy ani skladba povinných a povinně volitelných předmětů, nebo jejich rozsah či vyučující.

Každý obor programu specifikuje profil absolventa, který není nikterak dotčen navrhovanými změnami a který lze pro celý program stručně charakterizovat následujícícm způsobem. Absolvent magisterského programu Matematika získá solidní všeobecné znalosti matematických disciplín a hlubší znalosti podle své specializace. Má rozvinuté abstraktní myšlení, samostatný a tvůrčí přístup k formulaci a řešení problémů a schopnost si rychle

doplňovat nové poznatky. Dobře se uplatní všude tam, kde jsou tyto vlastnosti potřeba; v základním výzkumu, ve výuce na středních i vysokých školách, při vytváření matematických modelů v jiných oborech, při algoritmizaci, programování, ale i v manažerských profesích.

Obor: Matematika s informatikou

B – Charakteristika studijního programu a jeho oborů, pokud se na obory člení	
Vysoká škola	Masarykova univerzita
Součást vysoké školy	Přírodovědecká fakulta
Název studijního programu	Matematika (magisterský)
Název studijního oboru	Matematika s informatikou
Údaje o garantovi studijního oboru	doc. RNDr. Roman Šimon Hilscher, DSc.
Zaměření na přípravu k výkonu regulovaného povolání	

Charakteristika studijního oboru (studijního programu)

Studijní obor Matematika s informatikou má multidisciplinární charakter. Je zaměřen na studium matematických disciplín, které nacházejí uplatnění v informatice. Profilující předměty se zabývají matematickými metodami řešení algoritmických otázek a prohlubováním vědomostí v nejdůležitějších oblastech informatiky. Kromě širších základů bude mít absolvent hlubší znalosti oboru své diplomové práce, která určuje výběr volitelných předmětů a směr samostatného studia speciálních partií.

Profil absolventa studijního oboru (studijního programu) & cíle studia

Absolvent oboru bude schopen

- posoudit kvalitu návrhu počítačového systému,
- konstruovat efektivní algoritmy,
- dokazovat korektnost algoritmů,
- formulovat ideje formálním matematickým jazykem,
- kombinovat metody používané v různých oblastech informatiky,
- vytvořit počítačový program založený na hlubších teoretických znalostech,
- aplikovat nové teoretické výsledky při návrhu programů.

Hlavním cílem studia tohoto oboru je získání hlubších znalostí matematických disciplín, které tvoří teoretické základy metod používaných v informatice, a současně detailnější seznámení s nejdůležitějšími oblastmi teoretické i aplikované informatiky. Absolvent získá dobrou představu o tom, které matematické techniky lze v informatice aplikovat, a schopnost rychle si osvojovat nové poznatky a metody. Uplatní se především tam, kde je potřeba koncepční přístup k řešení problémů a týmová práce na hranicích jednotlivých oborů, zejména v základním a aplikovaném výzkumu, při tvorbě matematických modelů a softwaru.

Charakteristika změn od předchozí akreditace (v případě prodloužení platnosti akreditace)

Ve srovnání s předchozí akreditací (http://www.sci.muni.cz/akreditace/2002/m/Mt-MDO.htm) se z některých povinných předmětů staly předměty volitelné a naopak, některé předměty byly zařazeny mezi povinné. Nejde však o zásadní změny.

Prostorové zabezpečení studijního programu

Budova ve vlastnictví VŠ	**ANO**	**Budova v nájmu – doba platnosti nájmu**	

Informační zabezpečení studijního programu

Informační zdroje jsou zabezpečeny dvěma samostatnými knihovnami:

1) Ústřední knihovna Přírodovědecké fakulty umístěna v areálu na Kotlářské ulici.
2) Knihovna univerzitního kampusu, nově vzniklá v roce 2007 transformací Ústřední knihovny Lékařské fakulty MU, Knihovny Fakulty sportovních studií a integrací části Ústřední knihovny PřF MU. Knihovna je umístěna v areálu univerzitního kampusu v Bohunicích a slouží zejména studijním programům chemie a biochemie.

	Ústřední knihovna PřF MU	Knihovna univerzitního kampusu MU
Celkový počet svazků	357 310	31 741
Roční přírůstek knižních jednotek	5 070	798
Počet odebíraných titulů časopisů	603	79
Jsou součástí fondu kompaktní disky?	ano	ano
Jsou součástí fondů videokazety?	ano	ano
Otevírací hodiny knihovny/studovny v týdnu	42 hod týdně	47 hod týdně
Provozuje knihovna počítačové inform. služby?	ano	ano
Zajišťuje knihovna rešerše z databází?	ne, uživatelé samoobslužně	ano
Je zapojena na CESNET/INTERNET?	ano	ano
Počet stanic na CESNETu/INTERNETu	90	110
Počet počítačů v knihovně/studovně	79	91
Z toho počítačů zapojených v síti	79	91

Citační databáze:
Zentralblatt Math Database
MathSciNet
Web of Science, Web of Knowledge
Journal Citation Report
Scopus
Seznam recenzovaných neimpaktovaných periodik vydávaných v ČR

Elektronické časopisy:
Archivum Mathematicum
Časopisy z databáze SUWECO CZ
Electronic Journals Library
JSTOR
ScienceDirect
Zpravodaj Ústavu výpočetní techniky MU

Knihovní služby:
Knihovna matematických dokumentů

C – Pravidla pro vytváření studijních plánů SP (oboru) a návrh témat prací					
Vysoká škola	Masarykova univerzita				
Součást vysoké školy	Přírodovědecká fakulta				
Název studijního programu	Matematika (magisterský)				
Název studijního oboru	Matematika s informatikou				
Název předmětu	**rozsah**	**způsob zák.**	**druh před.**	**přednášející**	**dop. roč.**
Seznam předmětů je uveden v doporučeném studijním plánu, viz část C1.					

Obsah a rozsah SZZk

Státní závěrečná zkouška sestává z obhajoby diplomové práce a z ústní zkoušky.

Charakteristika závěrečné práce a její obhajoba

Zpracováním diplomové práce student prokazuje orientaci v problematice dané tématem práce a schopnost odborné práce pod vedením vedoucího. U obhajoby diplomové práce se hodnotí porozumění tématu a úroveň prezentace.

Charakteristika ústní zkoušky

Účelem zkoušky je prověřit, že absolvent je schopen vést debatu na jisté odborné úrovni. Cílem ústní zkoušky není opakovat zkoušky z jednotlivých předmětů a zkoušet detailní znalost teorie a důkazů. Smyslem je prokázat všeobecný přehled o základních pojmech a výsledcích z jednotlivých oborů a širších souvislostech mezi nimi.

Vymezení rozsahu otázek k ústní zkoušce

1. Matematická logika

Výroková logika, predikátová logika prvního řádu, věta o úplnosti, věta o kompaktnosti.

2. Matematická analýza

- **Diferenciální a integrální počet funkcí více reálných proměnných:** derivace, parciální derivace, diferenciál, Riemannův a Lebesgueův integrál, Fubiniho věta, transformace integrálu, křivkové a plošné integrály, Greenova věta, Gaussova-Ostrogradského věta.
- **Řady:** absolutní konvergence, mocninné řady.
- **Metrické prostory:** spojitost, kompaktnost, úplnost, Banachova věta o kontrakci.

3. Lineární algebra a geometrie

Vektorové prostory, báze, souřadnice, lineární zobrazení, skalární součin, ortonormální báze, ortogonální a unitární operátory, samoadjungované operátory, vlastní čísla a vektory, Jordanův kanonický tvar, bilineární a kvadratické formy, Sylvesterova věta o setrvačnosti, pozitivně a negativně definitní kvadratické formy.

4. Základy algebry

- **Základní algebraické struktury:** monoidy, grupy, okruhy, obory integrity, tělesa, svazy.
- **Univerzální algebra:** podalgebry, součiny, homomorfismy, variety algeber.

5. Pravděpodobnost a statistika

- **Pravděpodobnost:** pravděpodobnostní prostor, náhodné veličiny a jejich charakteristiky, nezávislost náhodných veličin, diskrétní a spojité náhodné veličiny, důležitá rozdělení pravděpodobnosti, zákon velkých čísel, centrální limitní věta.
- **Statistika:** náhodný výběr, bodové a intervalové odhady, testování hypotéz.

6. Matematická optimalizace

Dualita v lineárním programování, simplexová metoda, základy kvadratického programování, variační úloha s pevnými konci.

7. Grafové algoritmy

Prohledávání grafu, nejkratší cesty z jednoho vrcholu a mezi všemi dvojicemi vrcholů, maximální toky v sítích, bipartitní párování, minimální kostry.

8. Geometrické algoritmy

- **Algoritmy založené na metodě zametací přímky:** průnik úseček a překryv map, triangulace mnohoúhelníka a diagramy Voronoia.
- **Náhodnostní přírůstkové algoritmy:** lokalizace bodu pomocí lichoběžníkové mapy, Delaunayova triangulace.
- **Ortogonální vyhledávání:** kd-trees a range trees. Konvexní obaly v rovině.

9. Algoritmy teorie čísel

- **Teoretický základ:** grupa bodů eliptické křivky, věty o rozložení prvočísel (Čebyšev, Hadamard & de la Vallée Poussin), dobré aproximace reálných čísel.
- Rabinův-Millerův test, Lehmannova metoda, Lenstrova metoda eliptických křivek.

10. Teorie her

- **Hry v normální formě:** rovnováha, antagonistické hry, řešení maticových her, úlohy o dohodě.
- **Hry ve tvaru charakteristické funkce:** jádro, von Neumannovo-Morgensternovo řešení, Shapleyho hodnota.

11. Formální jazyky a automaty

Konečné automaty, regulární jazyky, zásobníkové automaty, bezkontextové gramatiky a jazyky, Turingovy stroje, rekurzivní a rekurzivně vyčíslitelné jazyky, uzávěrové vlastnosti tříd jazyků v Chomského hierarchii.

12. Operační systémy

Principy operací výpočetních systémů, modely procesů a vláken a jejich implementace, algoritmy plánování činnosti procesoru a jejich hodnocení, synchronizace procesů, algoritmy a metodologie ochran proti uváznutí, virtualizace paměti, V/V podsystémy.

13. Analýza a návrh systémů

Životní cyklus softwaru, softwarové architektury, metody a modely strukturované analýzy, strukturovaný návrh, objektově-orientovaná analýza a návrh.

14. Počítačové sítě

Architektura ISO/OSI a TCP/IP, mechanismy využívané v soudobých sítích, používané grafy a grafové algoritmy, nároky síťových aplikací, síťová bezpečnost, správa a monitoring, multicast, IPv6, P2P systémy, ad hoc sítě, senzorové sítě.

15. Počítačová grafika

Vzorkování a rekonstrukce obrazového signálu, Fourierova analýza, jev alias a jeho omezení. Objemové a povrchové modely těles, jejich zobrazení. Lokální úpravy modelů, volné deformace. Rovnice globálního osvětlení scény a její přibližné řešení.

Požadavky na přijímací řízení
Předpokladem pro přijetí je složení přijímací zkoušky v rozsahu bakalářské státní závěrečné zkoušky v programu Matematika.

Další povinnosti / odborná praxe

Návrh témat prací a obhájené práce	Vypracování a obhajoba diplomové práce je povinnou součástí všech studijních oborů v magisterském studijním programu Matematika.

Standardní doba zadání diplomové práce je v 1. semestru magisterského studia. Zadáním magisterské práce se učitel, který téma vypsal, stává pro studenta, který si ho vybral, vedoucím magisterské práce. Ústav matematiky a statistiky písemné zadání magisterských prací registruje a archivuje. Student může kterémukoliv učiteli Ústavu matematiky a statistiky navrhnout téma své magisterské práce nebo se na tomto tématu dohodnout. V tomto případě navrhuje učitel téma magisterské práce pro konkrétního studenta.

Obhájená závěrečná práce:

Logické a fyzikální aplikace ortosvazů, http://is.muni.cz/th/207863/prif_m/

V současnosti vedené práce:

Průsečíková čísla grafů

Vedoucí: doc. RNDr. Petr Hliněný, Ph.D.

Zadání: Průsečíkové číslo grafu G udává minimální možný počet průsečíků dvojic hran při nakreslení G do roviny. Jedná se o výpočetně velmi obtížný parametr (NP-úplný), avšak mající zajímavé aplikace. Blíže viz http://en.wikipedia.org/wiki/Crossing_number_(graph_theory).

Diplomant bude studovat třídy grafů majících omezenou hodnotu průsečíkového čísla, jejich strukturální vlastnosti a případně tzv kritické grafy těchto tříd. Vedle toho se dotkne i souvisejících algoritmických otázek v teoretické rovině.

Literatura:

Mohar, Bojan - Thomassen, Carsten. Graphs on surfaces. Baltimore : The Johns Hopkins University Press, 2001. xi, 291 s. ISBN 0-8018-6689-8.

Beineke, Lowell - Wilson, Robin. Topics in Topological Graph Theory. : Cambridge University Press, 2009. ISBN 978-0-521-80230-7.

Tvorba matematické grafiky pomocí programu Asymptote

Vedoucí: RNDr. Roman Plch, Ph.D.

Zadání: Popište instalaci a použití programu Asymptote při tvorbě matematické grafiky. Zaměřte se zejména na spolupráci s LaTeXem a na tvorbu PDF dokumentů s vloženou interaktivní 3D grafikou, popište matematický základ algoritmů pro generování této grafiky. Vygenerujte interaktivní 3D grafiku pro podporu výuky Integrálního počtu funkcí více proměnných.

Literatura:

Plch, Roman - Šarmanová, Petra - Sojka, Petr. Integrální počet funkcí více proměnných. Elportál: portál Masarykovy univerzity [online], Brno : Masarykova univerzita, 2009, 1, 160 s. ISSN 1802-128X. 2009.

Plch, Roman - Šarmanová, Petra. Interaktivní 3D grafika v HTML a PDF dokumentech. Zpravodaj Československého sdružení uživatelů TEXu, Praha : Československé sdružení uživatelů TEXu, 18, 1-2, od s. 76-92, 16 s. ISSN 1211-6661. 2008.

Kinematická geometrie

Vedoucí: RNDr. Jan Vondra, Ph.D.

Zadání: Student napíše srozumitelný text o kinematické geometrii (účelem textu je zaujmout studenta VŠ/maturanta). Vysvětlí základní pojmy a vztahy a vyřeší příklady k jejich demonstraci. Dále ve vhodném softwaru předvede vznik jednotlivých objektů. Za vhodný výstup je považován jednoduchý web s java aplety.

Literatura:

Kadeřávek, František - Klíma, Josef - Kounovský, Josef. Deskriptivní geometrie. Díl 1. [Kadeřávek, 1945]. Vyd. 2. Praha : Jednota československých matematiků a fyziků, 1945. 420 s.

Urban, Alois. Deskriptivní geometrie. II [Urban, 1967]. Vyd. 1. Praha : SNTL - Nakladatelství technické literatury, 1967. 267 s. : i.

Příklad tématu závěrečné práce:

Součiny pologrup v teorii regulárních jazyků

Vedoucí: doc. Mgr. Michal Kunc, Ph.D.

Zadání: Přehledně prezentujte definice a základní vlastnosti různých součinů pologrup používaných k rozpoznávání regulárních jazyků a popište jim odpovídající operace na jazycích, automatech a varietách. Vše ilustrujte na příkladech.

Literatura:

Eilenberg, Samuel. Automata, languages and machines. Volume A. New York : Academic Press, 1974. 451 s.

Eilenberg, Samuel. Automata, languages and machines. Volume B. New York : Academic Press, 1976. 387 s.

Další obhájená témata lze nalézt v Informačním systému Masarykovy univerzity - viz http://is.muni.cz/thesis, (položky Fakulta studia="Přírodovědecká fakulta", Pracoviště="14311010 ÚMS Ústavy PřF")

Návaznost na další stud. program

Absolvent tohoto oboru může pokračovat ve studiu oboru Algebra, teorie čísel a matematická logika doktorského programu Matematika nebo některého z oborů doktorského programu Informatika.

C1 -Doporučený studijní plán

Vytvoření studijního plánu podle pravidel studijního programu je zákonným právem studenta. Při sestavení studijního plánu musí student dodržet ustanovení Studijního a zkušebního řádu fakulty a Pravidla a podmínky pro vytváření studijního plánu v daném studijním programu. Jako východisko k tvorbě studijního plánu může student využít Doporučeného studijního plánu. Doporučený studijní plán rovnoměrně rozkládá studium do standardní doby dvou let a může se stát závazným jedině volbou studenta. Zaručuje studentům, kteří podle něho studují, splnění povinností nutných k ukončení vysokoškolského studia během standardní doby. Fakultní rozvrh (časová a prostorová alokace výuky předmětů pro daný semestr) je zpracován v návaznosti na doporučené studijní plány.

Ze 120 kreditů, které je student povinen během svého studia získat, musí být 75 kreditů za povinné předměty (z toho 30 za diplomovou práci), 10 kreditů za volitelné předměty z nabídky Fakulty informatiky a 9 kreditů za volitelné předměty z nabídky Ústavu matematiky a statistiky. Předložený studijní plán je pro povinné předměty rozepsán do jednotlivých semestrů. Následuje seznam doporučených volitelných předmětů, z nichž si student může vybírat kdykoliv během studia.

Doporučený studijní plán oboru Matematika s informatikou

1. rok studia

kód	název předmětu	kredit	rozsah	ukončení	vyučující
Podzimní semestr					
Povinné předměty					
FI:MA015	Grafové algoritmy	3+2	2/1	zk	Polák
FI:PA010	Počítačová grafika	2+2	2/0	zk	Sochor
FI:PA150	Principy operačních systémů	2+2	2/0	zk	Staudek,Říha
M71XF	Diplomová práce 1 (FINA, MINF)	5	0/0	z	vedoucí práce
M7130	Geometrické algoritmy	2+2	2/0	zk	Čadek
Jarní semestr					
Povinné předměty					
FI:PV112	Programování grafických aplikací	3+2	2/1	zk	Tobola
M0160	Teorie optimalizace	2+2	2/1	zk	Došlý
M7190	Teorie her	3+2	2/1	zk	Polák
M81XF	Diplomová práce 2 (FINA, MINF)	5	0/0	z	vedoucí práce
M8190	Algoritmy teorie čísel	2+2	2/0	zk	Kučera

2. rok studia

kód	název předmětu	kredit	rozsah	ukončení	vyučující
Podzimní semestr					
Povinné předměty					
JA002	Pokročilá odborná angličtina - zkouška	2	0/0	zk	Ševečková
M91XF	Diplomová práce 3 (FINA, MINF)	10	0/0	z	vedoucí práce
Jarní semestr					
Povinné předměty					
FI:PA103	Objektové metody návrhu informačních systémů	2+2	2/0	zk	Ošlejšek
FI:PA151	Soudobé počítačové sítě	2+2	2/0	zk	Staudek,Říha
MA1XF	Diplomová práce 4 (FINA, MINF)	10	0/0	z	vedoucí práce

Doporučené volitelné předměty

kód	název předmětu	kredit	rozsah	ukončení	vyučující
Podzimní semestr					
M5110	Okruhy a moduly	3+2	2/1	zk	Rosický
M7150	Teorie kategorií	2+2	2/0	zk	Rosický
M7250	Pologrupy a formální jazyky	2+2	2/0	zk	Kunc
Jarní semestr					

M0170	Kryptografie	3+2	2/1	zk	Paseka
M7230	Galoisova teorie	3+2	3/0	zk	Kučera
M8170	Teorie kódování	3+2	2/1	zk	Paseka

E – Personální zabezpečení studijního programu (studijního oboru) – souhrnné údaje											
Vysoká škola	Masarykova univerzita										
Součást vysoké školy	Přírodovědecká fakulta										
Název studijního programu	Matematika (magisterský)										
Název studijního oboru	společné pro všechny obory										
Název pracoviště:	**celkem**	**prof. celkem**	**přepoč. počet p.**	**doc. celkem**	**přepoč. počet d.**	**odb. as. celkem**	**z toho s věd. hod.**	**lektoři**	**asistenti**	**vědečtí pracov.**	**THP**
Ústav matematiky a statistiky	70	8	7,500	15	13,400	11	11	6	1	11	18

F – Související vědecká, výzkumná, vývojová, umělecká a další tvůrčí činnost

Vysoká škola	Masarykova univerzita
Součást vysoké školy	Přírodovědecká fakulta
Název studijního programu	Matematika (magisterský)
Název studijního oboru	společné pro všechny obory

Informace o tvůrčí činnosti vysoké školy související se studijním oborem (studijním program)

Výzkum na Ústavu matematiky a statistiky (dále jen UMS) zahrnuje několik hlavních odvětví teoretické a aplikované matematiky, zejména algebru, geometrii, matematickou analýzu, historii matematiky a matematické vzdělávání, statistiku a matematické modelování.

Náš ústav dále zajišťuje výuku teoretické matematiky, finanční matematiky a matematiky pro učitele středních škol. UMS také nabízí matematické předměty pro ostatní vědní obory Přírodovědecké fakulty jako jsou fyzika, chemie, biologie, geografie. Učitelé našeho ústavu také vedou výuku všech hlavních matematických předmětů na Fakultě informatiky a některých předmětů na Ekonomicko-správní fakultě.

UMS má akreditaci doktorského studijního programu v následujících směrech
algebra, teorie čísel a matematická logika,
geometrie, topologie a globální analýza,
matematická analýza,
obecné otázky matematiky (historie matematiky a matematické vzdělávání),
pravděpodobnost, statistika a matematické modelování.

Ve spolupráci s Masarykovou univerzitou UMS vydává odborný časopis Archivum Mathematicum (http://emis.muni.cz/journals/AM/). Na našem ústavu také sídlí redakce odborného časopisu Differential Geometry and its Applications (http://dga.math.muni.cz/), který je publikován vydavatelstvím Elsevier. Oba časopisy jsou indexovány v mezinárodních databázích Mathematical Reviews, Zentralblatt für Mathematik a Scopus.

UMS v současné době řeší 1 výzkumný záměr – MSM0021622409 Matematické struktury a jejich fyzikální aplikace a na dalším výzkumném záměru participuje jako spoluvykonavatel – MSM0021622419 Vysoce paralelní a distribuované výpočetní systémy. Dále se UMS podílí na výzkumných centrech Centrum Jaroslava Hájka pro teoretickou a aplikovanou statistiku – LC06024 a Centrum Eduarda Čecha pro algebru a geometrii - LC505.

Mimo výše uvedené se na UMS řeší 10 projektů GAČR, 7 projektů MŠMT (1 Kontakt, 1 FRVŠ, 5 OPVK) a 4 projekty podpory studentů ve

vědecké činnosti na MU. UMS je také zapojena do 1 projektu 7.RP EU a 2 projektů Jihomoravského kraje (OPVK, SoMoPro). Na výzkumu UMS se podílí akademičtí pracovníci včetně školitelů, studentů doktorského i magisterského studia. UMS úzce spolupracuje s odbornými pracovišti ostatních vysokých škol i ústavy akademie věd. Výzkum není strukturován podle pracovišť.

Evidence aktuálních projektů a projektů z předchozích období je přístupná na adrese

http://www.muni.cz/sci/311010/projects

Přehled řešených grantů a projektů (závazné jen pro magisterské programy) - VZHLEDEM K VELKÉMU POČTU JSOU UVEDENY POUZE PŘÍKLADY

Pracoviště	Názvy grantů a projektů získaných pro vědeckou, výzkumnou, uměleckou a další tvůrčí činnost v oboru	Zdroj	Období
Ústav matematiky a statistiky	Matematické struktury a jejich fyzikální aplikace (MSM0021622409)	MŠMT	1/2005 - 12/2011
Ústav matematiky a statistiky	Kvalitativní vlastnosti řešení diferenciálních rovnic a jejich aplikace	GAČR	1/2011 - 12/2015
Ústav matematiky a statistiky	Matematické struktury (MUNI/A/0964/2009)	MU	1/2010 - 12/2012
Ústav matematiky a statistiky	Globální analýza a geometrie fibrovaných prostorů (GA201/09/0981)	GAČR	1/2009 - 12/2013
Ústav matematiky a statistiky	Centrum Jaroslava Hájka pro teoretickou a aplikovanou statistiku (LC06024)	MŠMT	1/2006 - 12/2011
Ústav matematiky a statistiky	Matematická statistika a modelování (MUNI/A/1001/2009)	MU	1/2010 - 12/2012
Ústav matematiky a statistiky	Diferenční rovnice a dynamické rovnice na time scales III (GAP201/10/1032)	GAČR	1/2010 - 12/2014
Ústav matematiky a statistiky	Algebraické metody v geometrii s potenciálem k aplikacím (CZ.1.07/2.3.00/20.0003)	MŠMT	5/2011 - 4/2014
Ústav matematiky a statistiky	Algebraické metody v kvantové logice (CZ.1.07/2.3.00/20.0051)	MŠMT	7/2011 - 6/2014
Ústav matematiky a statistiky	Algebraické metody v teorii automatů a formálních jazyků II (GA201/09/1313)	GAČR	1/2009 - 12/2011
Ústav matematiky a statistiky	Grupy tříd ideálů algebraických číselných těles (GAP201/11/0276)	GAČR	1/2011 - 12/2014

I – Uskutečňování akreditovaného stud. programu mimo sídlo vysoké školy	
Vysoká škola	Masarykova univerzita
Součást vysoké školy	Přírodovědecká fakulta
Název studijního programu	Matematika
Název instituce nebo pobočky VŠ, kde probíhá výuka SP mimo sídlo VŠ nebo fakulty	
Výuka veškerých programů je uskutečňována výhradně v sídle fakulty.	

D-Charakteristika studijních předmětů

Seznam předmětů oboru Matematika s informatikou

FI:MA015 Grafové algoritmy
FI:PA010 Počítačová grafika
FI:PA103 Objektové metody návrhu informačních systémů
FI:PA150 Principy operačních systémů
FI:PA151 Soudobé počítačové sítě
FI:PV112 Programování grafických aplikací
JA002 Pokročilá odborná angličtina - zkouška
MA1XF Diplomová práce 4 (FINA, MINF)
M0160 Teorie optimalizace
M0170 Kryptografie
M5110 Okruhy a moduly
M71XF Diplomová práce 1 (FINA, MINF)
M7130 Geometrické algoritmy
M7150 Teorie kategorií
M7190 Teorie her
M7230 Galoisova teorie
M7250 Pologrupy a formální jazyky
M81XF Diplomová práce 2 (FINA, MINF)
M8170 Teorie kódování
M8190 Algoritmy teorie čísel
M91XF Diplomová práce 3 (FINA, MINF)

Anotace předmětů oboru Matematika s informatikou

FI:MA015 Grafové algoritmy

Vyučující: doc. RNDr. Libor Polák CSc.
Rozsah: 2/1. 3 kr. (plus ukončení). Doporučované ukončení: zk. Jiná možná ukončení: k.
Cíle předmětu: Jsou prezentovány základní grafové algoritmy: průzkumy, hledání minimální kostry a rozličné algoritmy pro hledání nejkratších cest a maximálních toků v sítích. Ve všech případech dokazujeme korektnost a odhadujeme složitost.
Osnova:

- Elementární grafové algoritmy (reprezentace grafů, prohledávání do šířky, prohledávání do hloubky, topologické uspořádání, silně souvislé komponenty).
- Minimální kostry (růst minimální kostry, algoritmy Kruskala a Prima).
- Nejkratší cesty z jediného vrcholu (nejkratší cesty a relaxace, Dijkstrův algoritmus, Bellman-Fordův algoritmus, nejkratší cesty v orientovaných acyklických grafech).
- Nejkratší cesty mezi všemi dvojicemi vrcholů (nejkratší cesty a násobení matic, Floyd-Warshallův algoritmus, Johnsonův algoritmus pro řídké grafy).
- Maximální toky v sítích (sítě, Ford-Fulkersonova metoda, maximální párování v bipartitních grafech).
- Datové struktury pro grafové algoritmy (binární haldy, prioritní fronty, datové struktury pro systémy disjunktních množin).

Výukové metody: Jednou týdně klasická dvouhodinová přednáška. V navazujícím hodinovém semináři studenti referují řešení předem zadaných úloh.
Metody hodnocení: Zkouška je písemná. 30% bodů tvoří řešení konkrétní úlohy některým se známých algoritmů. Podstatná část je předpracovaná nová úloha. Studenti doplňují vynechané části algoritmu, demonstrují ho na konkrétních datech, dokazují jeho korektnost a odhadují složitost.
Literatura:

- Cormen, Thomas H. - Leiserson, Charles E. - Rivest, Ronald L. *Introduction to algorithms*. Cambridge : MIT Press, 1989. xvii, 1028. ISBN 0-07-013143-0. info

FI:PA010 Počítačová grafika

Vyučující: doc. Ing. Jiří Sochor CSc.
Rozsah: 2/0. 2 kr. (plus ukončení). Ukončení: zk.
Cíle předmětu: Na přednáškách jsou podrobně probírány klasické poznatky ze stěžejních oblastí počítačové grafiky a porovnávány s nejnovějšími výsledky výzkumu. Studenti získají přehled o klíčových problémech a směrech vývoje v dané oblasti. Po absolvování kurzu budou studenti - rozumět a být schopni vysvětlit teoretické základy současné počítačové grafiky; - posoudit a vyhodnotit výzkumné a vývojové směry v dané oblasti; - s využitím získaných znalostí by měli být schopni navrhovat složité grafické systémy v různých aplikačních oblastech.
Osnova:

- Vzorkování a rekonstrukce obrazu, alias a vyhlazování.
- Proměny a míchání rastrových obrazů.
- Textury.
- Globální osvětlování, zobrazovací rovnice.
- Rekostrukce a zjednodušování ploch.
- Přímá vizualizace objemových dat.
- Vykreslování v reálném čase.
- Zobrazování terénu.
- Zobrazování založené na obrazech.
- Speciální modelování, lokální a globální deformace těles.
- Dělené povrchy.
- Datové struktury pro prostorové vyhledávání.
- Kolizní metody.

Výukové metody: Teoretické přednášky pokrývající fundamentální i "žhavá" témata, diskuze během přednášek.
Metody hodnocení: Přednášky podle prezentací zveřejněných na stránkách předmětu. Písemná zkouška, 5 otázek z předem zveřejněného seznamu, 90 minut.
Literatura:

- Watt, Alan H. *3D Computer Graphics*. 2nd ed. Wokingham : Addison-Wesley Publishing Company, 1993. 500 s., ob. ISBN 0-201-63186-5. info
- Žára, Jiří - Beneš, Bedřich - Sochor, Jiří - Felkel, Petr. *Moderní počítačová grafika*. 2. vyd. Praha : Computer Press, 2005. 609 s. I 1. ISBN 80-251-0454-0. info

FI:PA103 Objektové metody návrhu informačních systémů

Vyučující: Mgr. Radek Ošlejšek Ph.D.
Rozsah: 2/0. 2 kr. (plus ukončení). Ukončení: zk.
Cíle předmětu: Na konci tohoto kurzu bude student schopen: pochopit funkce a strukturu objektového systému popsaného pomocí UML diagramů; zachytit požadavky uživatelů na systém pomocí UML; vytvořit analytické modely systému pomocí UML; vytvořit návrhové modely systému pomocí UML; zvolit vhodné postupy a metodiky při analýze a návrhu systému; použít Unified Process v životním cyklu softwaru; využít analytické a návrhové vzory při vývoji softwaru; využít softwarové architektury a navrhnout komponentové systémy;
Osnova:

- Objektové paradigma, vlastnosti objektů, principy abstrakce a dekompozice.
- UML, tvorba modelů, použití UML.
- Etapy vývoje, iterativní a inkrementální vývoj, agilní versus model-driven vývoj, RUP -- Rational Unified Process.
- Zachycení požadavků, Use Case modelování.
- Analytické modely, objekty a třídy, analytické balíky, realizace případů užití.
- Návrhové modely, návrhové třídy, rozhraní, komponenty, stavové diagramy.
- Implementace, diagram nasazení.
- Analytické a návrhové vzory, výběr a použití vzoru, katalogy vzorů.
- Heuristiky a metriky, OCL, případové studie.
- Softwarové architektury, komponentové systémy.

Výukové metody: Teorie ve formě přednášek, praktické příklady předváděné na přednáškách, diskuse, studium literatury.
Metody hodnocení: Přednášky s příklady, diskuse v hodině. Závěrečná písemná zkouška 90 minut (4 otázky po 10 bodech): příklady a vysvětlení probraných pojmů a metod.
Literatura:

- Arlow, Jim - Neustadt, Ila. *UML 2.0 and the unified process :practical object-oriented analysis and design*. 2nd ed. Boston : Addison-Wesley, 2005. xxiii, 592. ISBN 0321321278. info
- Page-Jones, Meilir. *Fundamentals of object-oriented design in UML*. New York : Dorset House Publishing, 2000. xxi, 458 s. ISBN 0-201-69946-. info
- Oestereich, Bernd. *Developing software with UML :object-oriented analysis and design in practice*. Harlow : Addison-Wesley, 1997. xiii, 321. ISBN 0-201-39826-5. info
- *Design patterns :elements of reusable object-oriented software*. Edited by Erich Gamma. Reading, Mass. : Addison-Wesley, 1995. xv, 395 p. ISBN 0-201-63361-2. info
- Larman, Craig. *Applying UML and patterns :an introduction to object-oriented analysis and design*. Upper Saddle River : Prentice Hall PTR, 1998. xix, 507 s. ISBN 0-13-748880-7. info

FI:PA150 Principy operačních systémů

Vyučující: doc. Ing. Jan Staudek CSc., Ing. Mgr. Zdeněk Říha Ph.D.
Rozsah: 2/0. 2 kr. (příf plus uk plus > 4). Ukončení: zk.
Cíle předmětu: Na konci tohoto kurzu bude student schopen rozumět složitým aplikačním systémům orientovaným na transakční zpracování založeným na multitaskingových operačních systémech, navrhovat aplikační systémy orientované na transakční zpracování odolné vůči poruchám, vyvíjet middlewarové systémy orientované na distribuované a transakční zpracování, rozumět dokumentaci složitých softwarových aplikačních

systémů budovaných pro middlewarové prostředí, ilustrovat architekturu navrhovaných a vyvíjených systémů a hodnotit výkonnostní a bezpečnostní vlastnosti složitých softwarových systémů
Osnova:

- Role a principy operačních systémů
- Uváznutí
- Transakce
- Řízení souběžných transakcí
- Systémy obnovy transakcí po poruše
- Čas a stav v distribuovaném prostředí
- Koordinace a dosažení dohody v distribuovaném prostředí
- Transakce a souběžnost v distribuovaném prostředí

Výukové metody: přednášky
Metody hodnocení: písemná zkouška
Literatura:

- Silberschatz, Abraham - Galvin, Peter Baer - Gagne, Greg. *Operating system concepts with Java*. 6th ed. Hoboken : John Wiley & Sons, 2004. xxiii, 952. ISBN 0-471-48905-0. info
- Coulouris, George - Dollimore, Jean - Kindberg, Tim. *Distributed systems :concepts and design*. 3rd ed. Harlow : Addison-Wesley, 2001. xiii, 772. ISBN 0-201-61918-0. info

FI:PA151 Soudobé počítačové sítě

Vyučující: doc. Ing. Jan Staudek CSc., Ing. Mgr. Zdeněk Říha Ph.D.
Rozsah: 2/0. 2 kr. (příf plus uk plus > 4). Ukončení: zk.
Cíle předmětu: Na konci tohoto kurzu bude student schopen aplikovat techniky řízení přístupu k bezdrátovému médiu popsat a vysvětlit principy WPAN, Wireless Personal Area Networks, Bluetooth, Zigbee, ... popsat a vysvětlit principy WLAN, Wireless Local Area Networks, Wi-Fi, 802.11 popsat a vysvětlit principy mobilních sítí, GSM, GPRS, EDGE, UMTS popsat a vysvětlit principy satelitních komunikací popsat a vysvětlit principy WMAN, Metropolitan Networks (WiMAX/802.16) popsat a vysvětlit principy bezšňůrová telefonie (DECT), FWA
Osnova:

- Základy (bezdrátového) přenosu dat
- Řízení přístupu k bezdrátovému médiu
- WPAN, Wireless Personal Area Networks, Bluetooth, Zigbee, ...
- WLAN, Wireless Local Area Networks, Wi-Fi, 802.11
- Mobilní sítě,GSM, GPRS, EDGE, UMTS
- Satelitní komunikace
- WMAN, Metropolitan Networks (WiMAX/802.16)
- Bezšňůrová telefonie (DECT), FWA

Výukové metody: přednášky
Metody hodnocení: přednáška, písemná zkouška
Literatura:

- Schiller, Jochen H. *Mobile communications*. 2nd ed. London : Addison-Wesley, 2003. xviii, 492. ISBN 0-321-12381-6. info
- Stallings, William. *Wireless Communications and Networks*. : Prentice Hall, 2002. 584 s. ISBN 0130408646. info

FI:PV112 Programování grafických aplikací

Vyučující: Mgr. Petr Tobola Ph.D.
Rozsah: 2/1. 3 kr. (plus ukončení). Doporučované ukončení: zk. Jiná možná ukončení: z.

Cíle předmětu: Cílem předmětu je získat všeobecný přehled o grafických aplikačních rozhraních a současně získat praktické zkušenosti s použitím standardního rozhraní OpenGL. Po absolvování předmětu budou studenti schopni programovat široké spektrum grafických aplikací, animací.
Osnova:

- Aplikační rozhraní počítačové grafiky.
- Základní principy zobrazování pomocí výkonných grafických akcelerátorů
- Zobrazovací řetězec
- Struktura a funkce grafického API
- Datové typy a grafická primitiva
- Souřadné systémy, transformace
- Osvětlování
- Antialiasing, mapování textur, alfa míchání
- Použití evaluátorů pro Bézierovy křivky a plochy.
- Nadstavby pro práci s 3D objekty a pro tvorbu GUI.
- OpenGL Shading Language
- Příklady API, OpenGL a jeho nadstavby, knihovny GLU a GLUT.

Výukové metody: Přednášky a navazující cvičení.
Metody hodnocení: Před závěrečnou zkouškou je požadováno odevzdání individuálního projektu. Závěrečná zkouška má písemnou formu.
Literatura:

- *OpenGL reference manual :the offical reference document for OpenGL, release 1*. Reading, Mass. : Addison-Wesley Publishing Company, 1992. ix, 388 s. ISBN 0-201-63276-4. info
- Neider, Jackie - Davis, Tom - Woo, Mason. *OpenGL programming guide :the official guide to learning OpenGL, release 1*. Reading, Mass. : Addison-Wesley Publishing Company, 1993. xxxiii, 51. ISBN 0-201-63274-8. info
- Hill, Francis S. *Computer graphics using OpenGL*. 2nd ed. Upper Saddle River : Prentice Hall, 2001. xxxi, 922. ISBN 0-02-354856-8. info

JA002 Pokročilá odborná angličtina - zkouška

Vyučující: Mgr. Hana Ševečková M.A.
Rozsah: 0/0. 2 kr. Ukončení: zk.
Cíle předmětu: Zkouška prověří, že student je schopen zvládat následující dovednosti odpovídající úrovni B2 ERR - odborný jazyk porozumět odbornému textu/mluvenému projevu identifikovat hlavní myšlenky formulovat hlavní myšlenky interpretovat informaci z textu/mluveného projevu shrnout náročnější odborný text klasifikovat, porovnávat, určit příčiny a důsledky, popsat proces, definovat prezentovat odborný text vztahující se ke studovanému oboru za použití pokročilých prezentačních technik diskutovat o obecných a odborných tématech hovořit o svém oboru - disponovat základní slovní zásobou svého oboru argumentovat
Osnova:

- 1.Písemná část
- a) Akademická část - gramatika odborného textu viz
- http://www.sci.muni.cz/main.php?stranka=Jazyky&podtext=A2
- b) Odborný text - slovník k dispozici (porozumění textu, shrnutí)
- 2. Ústní část
- Prezentace odborného textu vztahujícího se ke studovanému oboru - téma dle vlastního výběru, ale obsah srozumitelný i pro posluchače jiných oborů, v rozsahu 10 minut s využitím veškerých prezentačních technik, popř. názorných pomůcek. Je třeba prokázat i schopnost reagovat na otázky publika.

Výukové metody: Zkouška
Metody hodnocení: Písemný test, ústní zkouška
Literatura:

- Jeremy Comfort. Effective Presentations.OUP 2000.

- Douglas Bell: Passport to Academic Presentations.Garnet 2008.
- *Academic vocabulary in use*. Edited by Michael McCarthy - Felicity O'Dell. Cambridge : Cambridge University Press, 2008. 176 s. ISBN 978-0-521-68939. info
- Keith Kelly: Science.Macmillan 2008
- *Key words in science & technology :helping learners with real English*. Edited by Bill Mascull. 1st ed. London : Harper Collins Publishers, 1997. xii, 210 s. ISBN 0-00-375098-1. info
- *Academic writing course :study skills in English*. Edited by R.R Jordan. 1st ed. Essex : Longman, 1999. 160 s. ISBN 0-582-40019-8. info
- English for science. Edited by Fran Zimmerman. New Jersey : Regents/Prentice Hall, 1989
- Donovan, Peter. *Basic English for Science*. 10. vyd. Oxford : University Press, 1994. 153 s. ISBN 0-19-457180-7. info
- *Nucleus ; English for science and technology*. Edited by Martin Bates - Tony Dudley-Evans. info
- Physics:Reader.Ivana Tulajová, Masarykova univerzita Přírodovědecká fakulta 2000
- Plummer, Charles C. - McGeary, David. *Physical geology :student study art notebook*. 7th ed. Dubuque : Wm. C. Brown Communications, 1996. 161 s. ISBN 0-697-28732-7. info
- Strahler, Alan H. - Strahler, Arthur Newell. *Introducing physical geography*. 4th ed. Hoboken, N.J. : J. Wiley, 2006. xxv, 728 s. ISBN 0-471-67950-X. info
- Murphy, Raymond. *English grammar in use :a self-study reference and practice book for intermediate students of English : with answers*. 3rd ed. Cambridge : Cambridge University Press, 2004. x, 379 s. ISBN 0-521-53762-2. info
- Cunningham, Sarah - Bowler, Bill. *Headway : intermediate : pronunciation*. 1. vyd. Oxford : Oxford University Press, 1990. xi, 112 s. ISBN -19-433968-8. info
- +Any materials aimed at preparation for B2 level examinations(e.g. FCE, TOEFL)

MA1XF Diplomová práce 4 (FINA, MINF)

Vyučující: vedoucí práce
Rozsah: 0/0/0. 10 kr. Ukončení: z.
Cíle předmětu: Předmět je koncipován jako kurz motivující studenta k napsání diplomové práce splňující veškeré požadavky na ni kladené. Absolvování tohoto kurzu zajistí, že student odevzdá diplomovou práci odsouhlasenou vedoucím. Po absolvování tohoto kurzu by student měl být připraven k úspěšné obhajobě diplomové práce, která je součástí státní závěrečné zkoušky.
Osnova:

- Individuální konzultace v průběhu zpracování diplomové práce.

Výukové metody: Individuální konzultace v průběhu zpracování diplomové práce.
Metody hodnocení: Zápočet je udělen za odevzdání práce se souhlasem vedoucího.
Literatura:

- Literatura použitá v diplomové práci / Literature used in diploma thesis.
- Lomtatidze, Lenka - Plch, Roman. *Sázíme v LaTeXu diplomovou práci z matematiky*. 1. vyd. Brno : Masarykova univerzita, 2003. 122 s. ISBN 80-210-3228-6. info

M0160 Teorie optimalizace

Vyučující: prof. RNDr. Ondřej Došlý DrSc.
Rozsah: 2/1. 2 kr. (příf plus uk k 1 zk 2 plus 1 > 4). Ukončení: zk.
Cíle předmětu: Kurs je volným pokračováním kursu Matematiké programování (M5170) a jsou zde probírány některé další optimalizační metody.
Osnova:

- I. Kvadratické programování v ekonomickém rozhodování, doplnění metod kvadratiockého programování z kursu Matematické programování. II. Dynamické programování: Bellmanův princip optimality, konečněkrokové deterministické a pravděpodobnostní rozhodovcí procesy, nekonečněkrokové rozhodovací procesy - funkcionální rovnice dynamického programování. III. Základy variačního počtu a diskrétní optimalizace: historická motivace, Euler-Lagrangeova rovnice a první variace, druhá variace, elementární diferenční rovnice a rekurentní relace, diskrétní variační počet.

Výukové metody: Teoretická přednáška
Metody hodnocení: Přednáška je zakončena ústní zkouškou.
Literatura:

- Kauman, A. - Cruon, R. *Dynamické programovanie*. Bratislavaa, 1969. 312 s. Matematické metódy v ekonomike, Alfa. ISBN 302 - 063 - 69. info
- Nemhauser, George, L. *Introduction to Dynamic Programming*. New York : John Wiley, 1966. 350 s. ISBN 0-8247-8245-3. info
- Škrášek, Josef - Tichý, Zdeněk. *Základy aplikované matematiky*. Vyd. 1. Praha : SNTL - Nakladatelství technické literatury, 1990. 853 s. ISBN 80-03-00111-0. info

M0170 Kryptografie

Vyučující: doc. RNDr. Jan Paseka CSc.
Rozsah: 2/1/0. 3 kr. (příf plus uk k 1 zk 2 plus 1 > 4). Ukončení: zk.
Cíle předmětu: Základním cílem přednášky je seznámení studenta s matematickými základy šifrování - kryptografie. Jsou rovněž zmíněny aplikace teorie šifrování, zejména v oblasti computer science. Absolvováním disciplíny získá student tyto základní znalosti a dovednosti: * Pochopení základních principů kryptografie, formulace perfektní bezpečnosti. * Pochopení podstaty a variant perfektního šifrovacího systému one-time pad. * Zvládnutí praktických výpočetních postupů při řešení rovnic vyplývajících z použití posouvacích registrů. * Pochopení pojmů výpočetní složitost, integrita a autentičnost. * Pochopení a vysvětlení podstaty asymetrického šifrovacího systému. * Použití kryptografických metod při řešení konkrétních úloh z oblasti bezpečnosti a šifrování dat.
Osnova:

- Úvod. Shrnutí - přehled. Historie. Obsah a záměr přednášky. Kryptosystémy a jejich aplikace v computer science. Základní principy. Narušení kryptosystému. Perfektní šifra. One time-pad a lineární posouvací registry. One time-pad. Narušitelnost lineárních posouvacích registrů. Jednosměrné funkce. Neformální přístupy; problém rozesílání hesel. Použití NP-těžkých problémů jakožto kryptosystémů. Data Encryption Standard (DES). Diskrétní logaritmy. Kryptosystémy s veřejným klíčem. Myšlenka funkce s vlastností padacích dveří. Rivest-Shamir-Adlemanův (RSA) systém. Kryptosystém s veřejným klíčem založený na diskrétním logaritmu. Autentikace a digitální podpisy. Authentikace v komunikačním systému. Použití veřejných klíčů v síti pro zasílání podepsaných zpráv. Dvoustranné protokoly. Vícestranné protokoly. Pseudonáhodné generátory.

Výukové metody: Přednáška: teoretická výuka kombinovaná s praktickými příklady Cvičení: teoretické cvičení zaměřené na procvičení základních pojmů a tvrzení, samostatné řešení úloh, včetně úloh komplexnějšího charakteru,domácí úlohy. Je nutná aktivní účast na cvičeních nebo zpracování písemného referátu, který bude následně přednesen na některém ze cvičení. Téma bude stanoveno po dohodě s vyučujícím.
Metody hodnocení: Přednáška se cvičením. Zkouška je ústní s písemnou přípravou. Uspěšné složení zkoušky předpokládá předvedení přehledu k vybrané kapitole.
Literatura:

- Menezes, A. J. - Oorschot, Paul van - Vanstone, Scott A. *Handbook of applied cryptography*. Boca Raton : CRC Press, 1997. xiii, 780. ISBN 0-8493-8523-7. info
- Porubský, Š. a Grošek, O. Šifrovanie. Algoritmy, Metódy, Prax. Grada, Praha 1992. ISBN 80-85424-62-2
- Schneier, Bruce. *Applied cryptography :protocols, algorithms, and source code in C*. New York : John Wiley & Sons, 1996. xxiii, 758. ISBN 0-471-12845-7. info
- Welsh, D., Codes and Cryptography, Oxford University Press, New York 1989.
- Salomaa, Arto. *Public-key cryptography*. 2nd ed. Berlin : Springer, 1996. x, 271 s. ISBN 3-540-61356-0. info

M5110 Okruhy a moduly

Vyučující: prof. RNDr. Jiří Rosický DrSc.
Rozsah: 2/1. 3 kr. (příf plus uk k 1 zk 2 plus 1 > 4). Ukončení: zk.
Cíle předmětu: Přednáška seznamuje s jednou ze základních oblastí moderní algebry. Přirozeně navazuje na známý pojem vektorového prostoru a ukazuje, co se stane, když skaláry netvoří těleso, ale okruh. Prezentuje vznikající pojmy projektivního, plochého a injektivního modulu a jejich strukturní vlastnosti. Využívá přitom

základní modulové konstrukce, t.j., součiny, přímé součty, jádra, kojádra a tenzorové součiny. Připravuje na použití modulů v geometrii a topologii.
Osnova:

- 1. Moduly: moduly, podmoduly, homomorfismy, faktorové moduly, součiny, přímé součty, jádra, kojádra 2. Volné a projektivní moduly: volné moduly, projektivní moduly, polojednoduché moduly, vektorové prostory 3. Tenzorový součin: tenzorový součin a jeho vlastnosti 4. Ploché moduly: ploché moduly, direktní kolimity, Lazardova věta, regulární okruhy 5. Krátké exaktní posloupnosti: krátké exaktní posloupnosti, grupa Ext 6. Injektivní moduly:injektivní moduly, injektivní obal

Výukové metody: Přednáska prezentuje potřebné znalosti a způsoby uvažování; ukazuje jejich využití; stimuluje diskuzi o problematice předmětu.
Metody hodnocení: Přednáška ukončena ústní zkouškou.
Literatura:

- L.Rowen, Ring theory I, Academic Press 1988
- A.J.Berrick, M.E.Keating, An introduction to rings and modules, Cambridge Univ. Press 2000

M71XF Diplomová práce 1 (FINA, MINF)

Vyučující: vedoucí práce
Rozsah: 0/0/0. 5 kr. Ukončení: z.
Cíle předmětu: Předmět je koncipován jako kurz motivující studenta k napsání diplomové práce splňující veškeré požadavky na ni kladené. Absolvování tohoto kurzu (a kurzů navazujících) zajistí, že student odevzdá diplomovou práci odsouhlasenou vedoucím. Po absolvování tohoto kurzu (a kurzů následujících) by student měl být připraven k úspěšné obhajobě diplomové práce, která je součástí státní závěrečné zkoušky.
Osnova:

- Individuální konzultace v průběhu zpracování diplomové práce.

Výukové metody: Individuální konzultace v průběhu zpracování diplomové práce.
Metody hodnocení: Zápočet je udělen za úspěšný postup v přípravě práce.
Literatura:

- Literatura použitá v diplomové práci / Literature used in diploma theses
- Lomtatidze, Lenka - Plch, Roman. *Sázíme v LaTeXu diplomovou práci z matematiky*. 1. vyd. Brno : Masarykova univerzita, 2003. 122 s. ISBN 80-210-3228-6. info

M7130 Geometrické algoritmy

Vyučující: doc. RNDr. Martin Čadek CSc.
Rozsah: 2/0/0. 2 kr. (plus 2 za zk). Doporučované ukončení: zk. Jiná možná ukončení: k.
Cíle předmětu: Cílem kurzu je seznámit studenty se základními geometrickými algoritmy. Po absolvování předmětu budou studenti znát *základní algoritmické metody (sweeping line, randomized incremental, rozděl a panuj) používané v této oblasti, *základní datové a vyhledávací struktury(connected edge list, kd-trees, range trees), *časovou a paměťovou náročnost v oblasti geometrických algoritmů. *Dále budou schopni samostatně implementovat probírané algoritmy.
Osnova:

- 1. Konvexní obaly 2. Průsečíky úseček 3. Triangulace mnohoúhelníků 4. Lineární programování v rovině 5. Ortogonální vyhledávání 6. Lokalizace bodu 7. Diagramy Voronoia 8. Dualita 9. Delauneyovy triangulace 10. Konvexní obal v dimenzi 3

Výukové metody: Přednášky.
Metody hodnocení: Písemná zkouška.
Literatura:

- učební text na www.math.muni.cz/~slovak

- de Berg, M. - van Kreveld, M. - Overmars, M. - Schwarzkopf, O. *Computational Geometry*. 1. vyd. Berlin : Springer-Verlag, 1997. 365 s. ISBN 3-540-61270-X. info

M7150 Teorie kategorií

Vyučující: prof. RNDr. Jiří Rosický DrSc.
Rozsah: 2/0/0. 2 kr. (přif plus uk k 1 zk 2 plus 1 > 4). Ukončení: zk.
Cíle předmětu: Přednáška seznámí se základy teorie kategorií a s jejím významem pro matematiku. Na konci kurzu student: porozumí základním kategoriálním pojmům; zvládne kategoriální způsob uvažování; umí analyzovat kategoriální kontext matematických pojmů a tvrzení; uvědomí si možnosti konceptuálního přístupu k matematice.
Osnova:

- 1. Kategorie: definice, příklady, konstrukce kategorií, speciální objekty a morfismy 2. Součiny a součty: definice, příklady 3. Funktory: definice, příklady, diagramy 4. Přirozené transformace: definice, příklady, Yonedovo lemma, reprezentovatelné funktory 5. Kartézsky uzavřené kategorie: definice, příklady, souvislost s typovaným lambda-kalkulem 6. Limity: (ko)ekvalizátory, pullbacky, pushouty, limity, kolimity, limity pomocí součinů a ekvalizátorů 7. Adjungované funktory: definice, příklady, Freydova věta 8. Monoidální kategorie: definice, příklady, souvislost s lineární logikou, obohacené kategorie.

Výukové metody: Přednáska: prezentuje potřebné znalosti a způsoby uvažování; ukazuje jejich využití; stimuluje diskuzi o problematice předmětu.
Metody hodnocení: Přednáška zakončena ústní zkoušku. Účast na přednášce žádoucí. Domácí práce zadávána, neodevzdávána.
Literatura:

- Awodey, Steve. *Category theory*. 1st. pub. Oxford : Clarendon Press, 2006. xi, 256 s. ISBN 0-19-856861-4. info
- J.J.Adámek, Matematické struktury a kategorie, Praha 1982
- Barr, Michael - Wells, Charles. *Category theory for computing science*. 2nd ed. London : Prentice-Hall, 1995. xvii, 325. ISBN 0-13-323809-1. info

M7190 Teorie her

Vyučující: doc. RNDr. Libor Polák CSc.
Rozsah: 2/1/0. 3 kr. (přif plus uk k 1 zk 2 plus 1 > 4). Doporučované ukončení: zk. Jiná možná ukončení: k.
Cíle předmětu: Základní kurs teorie her zaměřený zejména na ekonomické aplikace. Věnujeme se obvyklým třem matematickým modelům (normální tvar, charakteristická funkce, poziční hry). Diskutují se různé koncepty rovnováhy a jejich existence. Řeší se řada praktických úloh.
Osnova:

- Hry n hračů v normální formě (koncepty rovnováhy, jejich existence). Hry 2 hračů v normální formě (antagonistické hry, optimalní stratégie, řešení maticových her, hry na čtverci, víceetapové hry). Neantagonistické hry 2 hráčů (bimaticové hry, teorie užitečnosti, úlohy o dohodě, vyhrožování). Hry n hračů ve tvaru charakteristické funkce (jádro, jeho existence, von Neumann-Morgensternovo řešení, Shapleyho hodnota, aplikace v ekonomii). Poziční hry.

Výukové metody: Jednou týdně dvouhodinová klasická přednáška zahrnující teorii i praktické úlohy. V navazujícím hodinovém semináři se řeší další úlohy většinou předem oznámené. U náročnějších se předem určují i referující.
Metody hodnocení: Písemná zkouška zahrnující řešení rozsáhlejší úlohy v normálním tvaru plus další dvě úlohy týkající se jiných typů her. U všech částí úloh je oznámen maximální počet bodů; je třeba získat celkově polovinu. Kolokvium: řeší se část úloh pro zkoušku či jejich zjednodušení, tak, aby stačila běžná rutina; opět se vyžaduje polovina.
Literatura:

- *Handbook of game theory with economic applications.* Edited by Robert J. Aumann - Sergiu Hart. Amsterdam : North-Holland, 1994. 1520 s. ISBN 0-444-89427-6. info

- G. Owen, Game Theory, Sounders Company 1983

M7230 Galoisova teorie

Vyučující: prof. RNDr. Radan Kučera DSc.
Rozsah: 3/0. 3 kr. (příf plus uk k 1 zk 2 plus 1 > 4). Ukončení: zk.
Cíle předmětu: Výklad Galoisovy teorie včetně jejích některých aplikací v algebře i geometrii. Na konci tohoto kurzu bude student schopen: porozumět hlavním výsledkům Galoisovy teorie; vysvětlit základní pojmy a souvislosti mezi nimi.
Osnova:

- Rozšíření teles: jednoduché algebraické rozšíření, stupeň rozšíření, algebraické a transcendentní rozšíření.
- Konstruovatelnost pravítkem a kružítkem: nemožnost konstrukce řešení následujících úloh zformulovaných v antice: zdvojení krychle, trisekce úhlu a kvadratury kruhu (bez důkazu, že "pi" je transcendentní).
- Normální a separabilní rozšíření, lineární nezávislost vnoření těles, normální uzávěr, Galoisova korespondence.
- Řešitelné a jednoduché grupy.
- Řešitelnost algebraických rovnic v radikálech: radikálová rozšíření.
- Jednotný pohled na řešení rovnic kvadratických, kubických a rovnic čtvrtého stupně, konstrukce rovnice pátého stupně neřešitelné v radikálech nad racionálními čísly.
- Galoisova grupa kruhových teles, konstrukce pravidelných mnohoúhelníků pravítkem a kružítkem.

Výukové metody: Přednášky: teoretická výuka s aplikacemi na konkrétní příklady.
Metody hodnocení: Zkouška má dvě části, písemnou a ústní.
Literatura:

- *Abstract algebra*. Edited by David Steven Dummit - Richard M. Foote. 3rd ed. Hoboken, N.J. : John Wiley & Sons, 2004. xii, 932 s. ISBN 0-471-45234-3. info
- Stewart, Ian. *Galois theory*. 2nd ed. London : Chapman & Hall, 1989. xxx, 202 s. ISBN 0-412-34550-1. info
- Procházka, Ladislav. *Algebra [Procházka, 1990]*. 1. vyd. Praha : Academia, 1990. 560 s. ISBN 80-200-301-0. info

M7250 Pologrupy a formální jazyky

Vyučující: doc. Mgr. Michal Kunc Ph.D.
Rozsah: 2/0. 2 kr. (příf plus uk k 1 zk 2 plus 1 > 4). Ukončení: zk.
Cíle předmětu: Přednáška seznamuje se dvěma úzce svázanými oblastmi teoretické informatiky a matematiky, s teorií regulárních jazyků a konečných pologrup. Po absolvování kurzu by studenti měli: být seznámeni s moderními metodami teorie regulárních jazyků; rozumět vztahu mezi třídami regulárních jazyků a konečných pologrup; být schopni použít pseudovariety pologrup k popisu vlastností regulárních jazyků; ovládat základní pojmy a techniky strukturní teorie konečných pologrup.
Osnova:

- 1. Rozpoznatelné a racionální množiny: definice, vztahy mezi nimi, uzávěrové vlastnosti.
- 2. Struktura konečných pologrup: Greenovy relace, 0-jednoduché pologrupy, faktorizační lesy.
- 3. Eilenbergova korespondence: pseudovariety, pseudoidentity, příklady.
- 4. Dobrá předuspořádání v teorii formálních jazyků.

Výukové metody: Přednáška: teoretická výuka, domácí cvičení.
Metody hodnocení: Ústní zkouška.
Literatura:

- Pin, J.-E. *Varieties of formal languages*. New York : Plenum Publishing Corporation, 1986. 138 s. Foundations of Computer Science. ISBN 0-306-42294-8. info
- Sakarovitch, Jacques. *Elements of Automata Theory*. Cambridge : Cambridge University Press, 2009. 782 s. ISBN 978-0-521-84425-3. info

- *Handbook of formal languages. Vol. 1 Word, language, grammar*. Edited by Grzegorz Rozenberg - Arto Salomaa. Berlin : Springer, 1997. xvii, 873. ISBN 3-540-60420-0. info
- Howie, John M. *Fundamentals of semigroup theory*. Oxford : The Clarendon Press, 1995. x, 351 s. ISBN 0-19-851194-9. info
- Grillet, Pierre Antoine. *Semigroups :an introduction to the structure theory*. New York : Marcel Dekker, 1995. ix, 398 s. ISBN 0-8247-9662-4. info
- Almeida, Jorge. *Finite semigroups and universal algebra*. Singapore : World Scientific, 1994. 511 s. ISBN 81-02-1895-8. info
- de Luca, Aldo - Varricchio, Stefano. *Finiteness and regularity in semigroups and formal languages*. Berlin : Springer, 1999. 240 s. EATCS Monographs on Theoretical Computer Science. ISBN 3-540-63771-0. info

M81XF Diplomová práce 2 (FINA, MINF)

Vyučující: vedoucí práce
Rozsah: 0/0/0. 5 kr. Ukončení: z.
Cíle předmětu: Předmět je koncipován jako kurz motivující studenta k napsání diplomové práce splňující veškeré požadavky na ni kladené. Absolvování tohoto kurzu (a kurzů navazujících) zajistí, že student odevzdá diplomovou práci odsouhlasenou vedoucím. Po absolvování tohoto kurzu (a kurzů následujících) by student měl být připraven k úspěšné obhajobě diplomové práce, která je součástí státní závěrečné zkoušky.
Osnova:

- Individuální konzultace v průběhu zpracování diplomové práce.

Výukové metody: Individuální konzultace v průběhu zpracování diplomové práce.
Metody hodnocení: Zápočet je udělen za úspěšný postup v přípravě práce.
Literatura:

- Literatura použitá v diplomové práci / Literature used in diploma thesis.
- Lomtatidze, Lenka - Plch, Roman. *Sázíme v LaTeXu diplomovou práci z matematiky*. 1. vyd. Brno : Masarykova univerzita, 2003. 122 s. ISBN 80-210-3228-6. info

M8170 Teorie kódování

Vyučující: doc. RNDr. Jan Paseka CSc.
Rozsah: 2/1/0. 3 kr. (přif plus uk k 1 zk 2 plus 1 > 4). Ukončení: zk.
Cíle předmětu: Základním cílem přednášky je seznámení studenta s matematickými základy teorie kódování. Jsou rovněž zmíněny aplikace teorie kódování, zejména v pblasti přenosu dat. Na konci tohoto kurzu bude student schopen: porozumět základům teorie kódování; vysvětlit základní pojmy a souvislosti mezi nimi. Na základě nabytých znalostí bude moci použít metody teorie kodování při řešení konkrétních úloh z oblasti přenosu dat.
Osnova:

- Úvod. Shrnutí - přehled. Historie. Obsah a záměr přednášky. Entropie. Nejistota. Entropie a nejistota. Informace. Komunikace mezi informačními kanály. Diskrétní kanál bez paměti. Kódování a dekódovací pravidla. Věta o kódování se šumem - Shannonova věta. Kódy opravující chyby. Problém kódování - potřeba pro opravu chyb. Lineární kódy. Binární Hammingovy kódy. Cyklické kódy. Reed-Mullerovy kódy. Obecné zdroje. Entropie obecného zdroje. Stacionární zdroje. Markovovy zdroje. Struktura přirozených jazyků. Angličtina jakožto matematický zdroj. Entropie anglického jazyka.

Výukové metody: Přednáška: teoretická výuka kombinovaná s praktickými příklady Cvičení: teoretické cvičení zaměřené na procvičení základních pojmů a tvrzení, samostatné řešení úloh, včetně úloh komplexnějšího charakteru,domácí úlohy. Je nutná aktivní účast na cvičeních nebo zpracování písemného referátu, který bude následně přednesen na některém ze cvičení. Téma bude stanoveno po dohodě s vyučujícím.
Metody hodnocení: Přednáška se cvičením. Zkouška je ústní s písemnou přípravou. Uspěšné složení zkoušky předpokládá předvedení přehledu k vybrané kapitole.
Literatura:

- Roman, Steven, Coding and Information Theory, Graduate Texts in Mathematics, Springer Verlag, 1992
- Hamming, R. W. Coding and information theory, Prentice-Hall, New-Jersey 1950
- Welsh D., Codes and cryptography, Oxford, University Press, New York, 1988
- Adámek, Jiří. *Kódování*. 1. vyd. Praha : SNTL - Nakladatelství technické literatury, 1989. 191 s. info
- Adámek, Jiří. Foundations of coding, John Wiley \& Sons, Inc. 1991

M8190 Algoritmy teorie čísel

Vyučující: prof. RNDr. Radan Kučera DSc.
Rozsah: 2/0/0. 2 kr. (příf plus uk k 1 zk 2 plus 1 > 4). Ukončení: zk.
Cíle předmětu: Cílem přednášky je ukázat, jak mohou výsledky teorie čísel pomoci při hledání rozkladu daného přirozeného čísla na prvočinitele, úloze, jejíž důležitost v poslední době roste kvůli aplikacím např. v teorii kódování. Na konci tohoto kurzu bude student schopen porozumět základním myšlenkám vyložených algoritmů.
Osnova:

- 1. Testy, zda je přirozené číslo N složené: Fermatův test a Carmichaelova čísla, Rabinův-Millerův test.
- 2. Testy, zda je přirozené číslo N prvočíslo: N-1 test Poclingtona-Lehmera, Metoda eliptických křivek.
- 3. Test Agarwala-Kayala-Saxeny
- 4. Hledání netriviálního dělitele přirozeného čísla N: Lehmannova metoda, Pollardova ρ metoda, Pollardova p-1 metoda, Metoda řetězových zlomků, Metoda eliptických křivek, Metoda kvadratického síta.

Výukové metody: Přednášky: teoretická výuka potřebného matematického základu, aplikace teorie na konstrukci konkrétních algoritmů.
Metody hodnocení: Zkouška má dvě části, písemnou a ústní.
Literatura:

- Cohen, Henri. *A Course in Computational Algebraic Number Theory*. : Springer-Verlag, 1993. 534 s. Graduate Texts in Mathematics 138. ISBN 3-540-55640-0. info

M91XF Diplomová práce 3 (FINA, MINF)

Vyučující: vedoucí práce
Rozsah: 0/0/0. 10 kr. Ukončení: z.
Cíle předmětu: Předmět je koncipován jako kurz motivující studenta k napsání diplomové práce splňující veškeré požadavky na ni kladené. Absolvování tohoto kurzu (a kurzu navazujícího) zajistí, že student odevzdá diplomovou práci odsouhlasenou vedoucím. Po absolvování tohoto kurzu (a kurzu následujícího) by student měl být připraven k úspěšné obhajobě diplomové práce, která je součástí státní závěrečné zkoušky.
Osnova:

- Individuální konzultace v průběhu zpracování diplomové práce.

Výukové metody: Individuální konzultace v průběhu zpracování diplomové práce.
Metody hodnocení: Zápočet je udělen za úspěšný postup v přípravě práce.
Literatura:

- Literatura použitá v diplomové práci / Literature used in diploma theses

  Lomtatidze, Lenka - Plch, Roman. *Sázíme v LaTeXu diplomovou práci z matematiky*. 1. vyd. Brno : Masarykova univerzita, 2003. 122 s. ISBN 80-210-3228-6. info