

B-IIa – Studijní plány pro bakalářské a magisterské SP

Označení studijního plánu Studijní plán - prezenční forma studia

P: Matematika pro informační technologie - povinné předměty

Název předmětu	rozsah	způsob ověření	počet kreditů	garant předmětu/vyučující	doporučený ročník /semestr	dvousemestrální předmět	PPZ	ZT PPZ
Konvexní optimalizace	4/2	Z+Zk	9	RNDr. Alexandr Kazda, Ph.D.	1/ZS	ne	ano	ne
Algoritmy na mřížích	2/1	Z+Zk	4	doc. Mgr. Pavel Příhoda, Ph.D.	1/ZS	ne	ano	ano
Algoritmy na polynomech	2/1	Z+Zk	4	doc. RNDr. David Stanovský, Ph.D.	1/ZS	ne	ano	ano
Automaty a výpočetní složitost	3/1	Z+Zk	6	doc. Mgr. Štěpán Holub, Ph.D.	1/ZS	ne	ano	ano
Celkem kreditů			23				23	

PV: Matematika pro informační technologie - povinně volitelný skupina 1

Název předmětu	rozsah	způsob ověření	počet kreditů	garant předmětu/vyučující	doporučený ročník /semestr	dvousemestrální předmět	PPZ	ZT PPZ
Číselné algoritmy	2/1	Z+Zk	4	doc. Mgr. Pavel Příhoda, Ph.D.	LS	ne	ano	ne
Kryptoanalýza	3/1	Z+Zk	6	Dr. rer. nat. Faruk Göloğlu	LS	ne	ano	ne
Geometrie pro počítačovou grafiku	2/0	Zk	3	doc. RNDr. Zbyněk Šír, Ph.D.	LS	ne	ano	ne
Geometrie počítačového vidění	2/2	Z+Zk	6	doc. Ing. Tomáš Pajdla, Ph.D.	LS	ne	ano	ne
Geometrické problémy v robotice	2/2	Z+Zk	6	doc. Ing. Tomáš Pajdla, Ph.D.	LS	ne	ano	ne
Algoritmy maticových iteračních metod	2/2	Z+Zk	5	RNDr. Iveta Hnětynková, Ph.D.	ZS	ne	ano	ne
Numerické metody optimalizace 1	3/1	Z+Zk	6	doc. RNDr. Václav Kučera, Ph.D.	ZS	ne	ano	ne
Rídící matice v numerické matematice	2/2	Z+Zk	5	prof. Ing. Miroslav Tůma, CSc.	ZS	ne	ano	ne
Speciální funkce a transformace ve zpracování obrazu	2/0	Zk	3	prof. Ing. Jan Flusser, DrSc. doc. RNDr. Barbara Zitová, Ph.D.	LS	ne	ano	ne
Variační metody ve zpracování obrazu	2/0	Zk	3	doc. Ing. Filip Šroubek, Ph.D.	LS	ne	ano	ne
Náhodnost a výpočty	2/1	Zk	4	Mgr. Pavel Hubáček, Ph.D.	LS	ne	ano	ne
Aproximační a online algoritmy	2/2	Z+Zk	5	prof. RNDr. Jiří Sgall, DrSc.	LS	ne	ano	ne
Pravděpodobnostní algoritmy	2/2	Z+Zk	5	prof. RNDr. Jiří Sgall, DrSc.	LS	ne	ano	ne
Matematická logika	2/0	Zk	3	doc. RNDr. David Stanovský, Ph.D.	ZS	ne	ano	ne
Algebraická geometrie	2/2	Z+Zk	5	doc. RNDr. Jan Šťovíček, Ph.D.	ZS	ne	ano	ne

Kombinatorika	2/2	Z+Zk	5	prof. RNDr. Jan Kratochvíl, CSc.	ZS	ne	ano	ne
Algebraická teorie čísel	3/1	Z+Zk	6	Mgr. Vítězslav Kala, Ph.D.	LS	ne	ano	ne
Křivky a funkční tělesa	4/0	Zk	6	prof. RNDr. Aleš Drápal, CSc., DSc.	LS	ne	ano	ne
Výpočetní logika	1/1	KZ	3	RNDr. Jakub Bulín, Ph.D.	ZS	ne	ano	ne
Úvod do složitosti CSP	2/0	Zk	3	doc. Mgr. Libor Barto, Ph.D.	ZS	ne	ano	ne
Základy analýzy dat	2/2	Z+Zk	5	RNDr. Pavel Charamza, CSc.	ZS	ne	ano	ne
Právní aspekty ochrany dat	2/0	Zk	3	JUDr. Ján Matejka, Ph.D.	ZS	ne	ano	ne
Základy spojité optimalizace	2/2	Z+Zk	6	doc. Mgr. Milan Hladík, Ph.D. prof. RNDr. Martin Loebel, CSc.	LS	ne	ano	ne
Kryptoanalýza na úrovni instrukcí	0/2	Z	2	Dr. rer. nat. Faruk Göloğlu	LS	ne	ano	ne
Výběrová přednáška MIT 1	2/0	Zk	3	doc. Mgr. Pavel Příhoda, Ph.D.	ZS	ne	ano	ne
Výběrová přednáška MIT 2	2/0	Zk	3	doc. Mgr. Pavel Příhoda, Ph.D.	LS	ne	ano	ne
Zabezpečení síťových protokolů	2/2	Z+Zk	5	Dr. rer. nat. Faruk Göloğlu	ZS	ne	ano	ne
Číselné síto	2/0	Zk	3	doc. Mgr. Pavel Příhoda, Ph.D.	ZS	ne	ano	ne
Kvantová informace	3/1	Z+Zk	6	doc. Mgr. Štěpán Holub, Ph.D.	LS	ne	ano	ne
Eliptické křivky a kryptografie	3/1	Z+Zk	6	prof. RNDr. Aleš Drápal, CSc., DSc.	LS	ne	ano	ne
Sedlobodové úlohy a jejich řešení	2/2	Z+Zk	5	doc. Ing. Miroslav Rozložník, Dr.	LS	ne	ano	ne
Analýza maticových iteračních metod – principy a souvislosti	4/0	Zk	6	prof. Ing. Zdeněk Strakoš, DrSc.	LS	ne	ano	ne
Inverzní úlohy a regularizace	2/2	Z+Zk	5	RNDr. Iveta Hnětynková, Ph.D.	ZS	ne	ano	ne
Paralelní maticové výpočty	2/2	Z+Zk	5	prof. Ing. Miroslav Tůma, CSc.	LS	ne	ano	ne
Celočíselné programování	2/2	Z+Zk	5	doc. Mgr. Milan Hladík, Ph.D.	LS	ne	ano	ne
Hluboké učení	3/2	Z+Zk	7	RNDr. Milan Straka, Ph.D.	LS	ne	ano	ne
Pokročilá 3D grafika pro film a hry	2/2	Z+Zk	6	doc. Ing. Jaroslav Křivánek, Ph.D.	ZS	ne	ano	ne
Pravděpodobnostní techniky	2/2	Z+Zk	5	doc. Mgr. Robert Šámal, Ph.D. doc. RNDr. Martin Tancer, Ph.D.	ZS	ne	ano	ne
Foundations of theoretical cryptography	2/1	Z+Zk	4	Mgr. Pavel Hubáček, Ph.D.	LS	ne	ano	ne

Algoritmy na eliptických křivkách	2/1	Z+Zk	4	prof. RNDr. Aleš Drápal, CSc., DSc.	LS	ne	ano	ne
Výpočetní geometrie	2/2	Z+Zk	5	doc. RNDr. Martin Tancer, Ph.D.	LS	ne	ano	ne
Booleovské funkce	2/0	Zk	3	Dr. rer. nat. Faruk Göloglu	ZS	ne	ano	ne
Minimální počet kreditů			46					

PV: Matematika pro informační technologie - povinně volitelný seminář - skupina 3								
Název předmětu	rozsah	způsob ověření	počet kreditů	garant předmětu/vyučující	doporučený ročník /semestr	dvousemestrální předmět	PPZ	ZT PPZ
Kryptografické otázky současnosti	0/2	Z	2	Dr. rer. nat. Faruk Göloglu		ne	ano	ne
Aplikace matematiky v informatice	0/2	Z	3	doc. RNDr. Jirí Tůma, DrSc.		ne	ano	ne
Studentský logický seminář	0/2	Z	2	prof. RNDr. Jan Krajíček, DrSc.		ne	ano	ne
Výběrový seminář z MIT	0/2	Z	2	doc. RNDr. David Stanovský, Ph.D.		ne	ano	ne
Seminář z kombinatorické, algoritmické a finitní algebry	0/2	Z	2	doc. Mgr. Libor Barto, Ph.D. doc. Mgr. Štěpán Holub, Ph.D.		ne	ano	ne
Seminář numerické matematiky	0/2	Z	2	prof. RNDr. Vít Dolejší, Ph.D., DSc. prof. Ing. Zdeněk Strakoš, DrSc.		ne	ano	ne
Seminář z matematiky inspirované kryptografií	0/2	Z	3	Dr. rer. nat. Faruk Göloglu		ne	ano	ne
Minimální počet kreditů			4					

P: Matematika pro informační technologie - pro zpracování závěrečné práce								
Název předmětu	rozsah	způsob ověření	počet kreditů	garant předmětu/vyučující	doporučený ročník /semestr	dvousemestrální předmět	PPZ	ZT PPZ
Diplomová práce I	0/4	Z	6		1/LS	ne	ano	ne
Diplomová práce II	0/6	Z	9		2/ZS	ne	ano	ne
Diplomová práce III	0/10	Z	15		2/LS	ne	ano	ne
Celkem kreditů			30					

* případně uváděný ročník, nebo semestr je z hlediska studijního plánu pro účely akreditace SP považován za doporučený ročník, nebo doporučený semestr

30. Poznámky ke studijnímu plánu:

Některé předměty budou zajišťovány externisty, s nimiž budou uzavřeny dohody o provedení práce.

Možnosti zmíněné u SZZ jsou typické možnosti volby, které očekáváme. Student si ale může zvolit jinou dvojici podle svého uvážení.

Následující povinně volitelné předměty tvoří skupinu povinně volitelných předmětů 2, ze které bude muset student získat minimálně 17 kreditů. Tyto předměty jsou také součástí skupiny povinně volitelných předmětů 1 a do celkového součtu kreditů jsou započítány pouze jedenkrát. Skupina 2 není z technických důvodů ve studijním plánu samostatně uvedena.

Booleovské funkce 2/0 Zk 3
Číselné algoritmy 2/1 Z+Zk 4
Kryptoanalýza 3/1 Z+Zk 6
Geometrie pro počítačovou grafiku 2/0 Zk 3
Geometrie počítačového vidění 2/2 Z+Zk 6
Geometrické problémy v robotice 2/2 Z+Zk 6
Algoritmy maticových iteračních metod 2/2 Z+Zk 5
Numerické metody optimalizace 1 3/1 Z+Zk 6
Řídké matice v numerické matematice 2/2 Z+Zk 5
Speciální funkce a transformace ve zpracování obrazu 2/0 Zk 3
Variační metody ve zpracování obrazu 2/0 Zk 3
Náhodnost a výpočty 2/1 Zk 4

Tato struktura studijního plánu stanovuje povinnost získat 46 kreditů ze skupiny povinně volitelných předmětů 1 tak, aby alespoň 17 z nich bylo ze skupiny povinně volitelných předmětů 2.

SP vyžaduje rovněž povinnost získat 4 kredity ze skupiny předmětů označených jako povinně volitelný seminář (skupina 3).

Část výuky probíhá v anglickém jazyce. Upozornění studentům, že musejí s výukou v angličtině počítat, bude uvedeno v podmínkách přijímacího řízení.

Rozložení kreditů	Kredity za předměty profilujícího základu (včetně základních teoretických předmětů profilujícího základu)	Kredity za všechny předměty
Povinné předměty	23	23
Povinné předměty - závěrečná práce	30	30
Povinně volitelné předměty	50	50
Kredity pro volbu studenta		17
Celkem	103	120

Státní závěrečná zkouška	<p>Státní závěrečná zkouška se skládá ze dvou částí, z obhajoby diplomové práce a z ústní zkoušky.</p> <p>Ústní část SZZ je tvořena dvěma tematickými okruhy. Z tematického okruhu 1 dostane student jednu otázku. Tematický okruh 2 je rozdělen na podokruhy 2A, 2B, 2C, 2D, 2E. Student si vybere dva z nich a ke každému zvolenému tématu dostane jednu otázku. Očekávané kombinace 2A + 2C, 2B + 2D, 2B + 2E odpovídají volbě zaměření.</p> <p>1 Matematika pro informační technologie Výpočetní modely, algoritmická rozhodnutelnost, základní složitostní třídy, regulární jazyky. Základní metody konvexní optimalizace. Gröbnerovy báze a Buchbergerův algoritmus. Mříže a algoritmus LLL.</p> <p>2A Algebraické a číselné algoritmy Rozklady polynomů: Berlekampův algoritmus, Henselovo zdvihání a Berlekampův-Henselův algoritmus. Aplikace Gröbnerovýchází v algebraické geometrii. Číselné algoritmy: Pollardova rho a p-1 metoda, algoritmus CFRAC, ECM, kvadratické síto. Souvislost faktorizace a diskrétního algoritmu.</p> <p>2B Algoritmy pro lineární algebru a optimalizaci Řídký Choleského a LU rozklad, řídký QR rozklad. Krylovovské iterační metody pro řešení soustav lineárních algebraických rovnic a lineárních aproximačních problémů, včetně konstrukce algebraických předpokládání. Metody pro řešení nelineárních algebraických rovnic a jejich soustav, metody pro minimalizaci funkcionálu bez omezení, lokální a globální konvergence metod.</p> <p>2C Kryptologie Základy Booleovských funkcí (ohnuté funkce, APN a AB funkce, ekvivalence, S-boxy, Walshova transformace a LAT, diferenční uniformita a DDT). Posloupnosti dané posuvnými registry. Základní kryptoanalytické útoky na blokové šifry (diferenciální a lineární kryptoanalýza, útoky vyšších řádů, meet-in-the-middle) a proudové šifry (korelace, algebraické útoky), útoky postranním kanálem. Aplikace mříží: NTRU, aplikace LLL (např. útok na RSA s malým veřejným exponentem). Pravděpodobnostní složitostní třídy, pseudonáhodné generátory.</p> <p>2D Počítačové vidění a robotika 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.</p> <p>2E Zpracování obrazu a počítačová grafika 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.</p>
--------------------------	--

61. Státní rigorózní zkouška - ústní část
<ol style="list-style-type: none"> 1. Konvexní optimalizace 2. Číselné algoritmy a algoritmy počítačové algebry 3. Automaty a výpočetní složitost 4. Booleovské funkce 5. Metody numerické lineární algebry 6. Geometrie v počítačovém vidění a robotice 7. Zpracování obrazu a počítačová grafika