

Okruhy ke státní závěrečné zkoušce	
Název studijního programu	Informatika se zaměřením na vzdělávání
Kód studijního programu	B0114A300065IF(M)
Typ studia	bakalářský
Forma studia	prezenční/kombinovaná
Specializace	----
Platnost od	1. 9. 2019

Jedna otázka je položena z infromatických okruhů, jedna otázka pak z didaktiky informatiky. Jedna otázka je položena z matematiky. Pokud je program sdružen s matematikou, pak je místo toho položena ještě jedna otázka z infromatických okruhů.

## Matematika

Základy maticového počtu. Inverzní matice, výpočet. Determinant, výpočet. Vlastní vektory a čísla. Soustavy lineárních algebraických rovnic, maticový zápis, Frobeniova věta, Gaussova eliminace. Vektorový prostor, základní pojmy. Souřadnice vektoru vzhledem k bázi, matice přechodu. Lineární zobrazení, operace, maticová reprezentace, změna při změně báze. Skalární součin, kolmost vektorů, ortogonální báze, Gramův-Schmidtův algoritmus. Ortogonální matice.

Kombinatorika. Princip inkluze a exkluze, Dirichletův princip. Variace, permutace, kombinace (bez/s opakováním). Základní kombinatorické identity, zobecnění kombinačních čísel. Binomická věta.

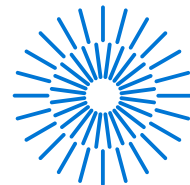
Lineární rekurentní vztahy – (ne)homogenní, jejich řešení. Neorientované grafy, zadání. Skóre grafu, Havlův algoritmus. Souvislost (sled, tah, cesta). Eulerovské grafy, Fleuryho algoritmus.

Hamiltonovské grafy. Rovinné grafy. Stromy a minimální kostra grafu.

Dělitelnost – Eukleidův algoritmus, jeho využití. Řetězové zlomky, přibližné zlomky, konstrukce, vlastnosti. Základní věta aritmetiky, využití. Eulerova funkce. Relace  $a \equiv b \pmod{m}$  a její vlastnosti. Počítání v  $(\mathbb{Z}_m, +, \cdot)$ . Malá Fermatova věta. Řešení kongruencí 1. stupně a jejich soustav (zobecněná Čínská věta o zbytku).

Základní algebraické struktury. Cyklické grupy. Symetrická grupa. Okruhy, dělitelé nuly, eukleidovské obory integrity. Polynomy nad tělesem, dělení polynomů se zbytkem, Eukleidův algoritmus.

Ireducibilita nad  $\mathbb{R}$ ,  $\mathbb{C}$ ,  $\mathbb{Z}_p$ . Tělesa, charakteristika, konečná tělesa. Kódování, jednoznačně dekódovatelný/prefixový/blokový kód. Kraftova nerovnost, McMillanova věta. Nejkratší kód, Huffmanova konstrukce nejkratšího kódu. Šifrování, základní pojmy, Kerckhoffsův princip. Klasifikace metod – symetrické šifry (substituce, transpozice) × asymetrické šifry (RSA). Substituce – afinní, jednoduchá substituce, Hill, Vigenère, Feistel.



## Informatika

### Algoritmizace a programování

Algoritmus a program. Časová a paměťová složitost algoritmu, vysvětlení časové složitosti na řadících algoritmech: na některém z kvadratických (výběrem – selectsort, vkládáním – insertsort, bublinkovém – bubblesort) a některém z rychlejších (sléváním – mergesort, quicksort). Metoda rozděl a panuj, programování rekurzí, vysvětlení na algoritmech mergesort a quicksort. Jednoduché a strukturované datové typy, pole, spojový seznam, zásobník, fronta. Vybrané grafové algoritmy: prohledávání do šířky (použití fronty), prohledávání do hloubky (použití zásobníku); pro grafy s ohodnocenými hranami: nejkratší cesta (Dijkstrův algoritmus, Bellman-Fordův algoritmus), minimální kostra (Jarníkův algoritmus). Základní programové konstrukce – sekvence, větvení, cykly.

### Architektura počítačů

Číselné soustavy. Aritmetické operace ve dvojkové soustavě. Booleova algebra, základní logické funkce a minimalizace logických funkcí, kombinační logické obvody (návrh a realizace logických funkcí). Von Neumannova a harvardská architektura. Blokové schéma procesoru, instrukční sada, procesory CISC a RISC. Paměťové členy a registry, sekvenční logické obvody (čítače). Cache. Počítače a typy sběrnic.

### Operační systémy

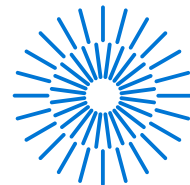
Účel, funkce a struktura OS. Jádro OS a jeho funkce. Režimy procesoru a využití v OS. Přerušení a jeho využití v OS. Proces a jeho stavy, životní cyklus procesu, vlákna. Přepínání procesů – strategie a realizace. Spolupráce mezi procesy, sdílená paměť. Souběh, uváznutí – jejich důsledky a prevence; souvislost s OS. Správa paměti, virtuální paměť. Správa úložišť a systém souborů. Druhy operačních systémů podle způsobu užití a související vlastnosti: systémy serverů, vestavné systémy, mobilní systémy a RTOS další.

### Databázové systémy

Relační model dat, základní konstrukty, integritní omezení. Normalizace, normální formy (první, třetí a BCNF), bezztrátová dekompozice. SQL, DDL a DML, množinové operace, vnořené dotazy, spojení; realizace integritních omezení. Transakce, ACID, stupně izolace, uváznutí (deadlock).

### Automaty a formální jazyky

Základní pojmy: abeceda, symbol, řetězec nad abecedou, jazyk nad abecedou. Konečné automaty. Nedeterministické konečné automaty a převod na deterministické konečné automaty. Redukce konečného automatu. Zásobníkové automaty, přijímání prázdným zásobníkem a koncovým stavem, porovnání síly automatů. Gramatika, Chomského hierarchie, souvislost mezi gramatikami a automaty. Turingův stroj.



## Počítačové sítě

Základní pojmy – topologie, architektura, LAN, WAN, spojované a nespojované služby. Referenční model OSI. Ethernet. IEEE 802.11 (Wi-Fi). Rodina protokolů TCP/IP (IP, TCP, UDP). Směrování. Domain Name System. Služby sítě Internet – elektronická pošta, WWW.

## Didaktika informatiky

Informatické myšlení a digitální gramotnost v RVP ZV. Specifika výuky informatiky – učebnice, výukové metody, hodnocení, učebny a vybavení. ICT koordinátor / ICT metodik. Didaktická transformace konkrétních témat z oblasti digitálních technologií (hardware, software, počítačové sítě, internet, nové technologie), vytváření digitálního obsahu (text, obrázek, multimédia, prezentace, webové stránky), zpracování dat a informačních systémů, modelování, kódování.

### Obsahová správnost

<b>Předkládající katedra</b>	katedra geoinformatiky a didaktiky informatiky
<b>Jméno předkladatele</b>	doc. RNDr. Pavel Satrapa, Ph.D.