**1. Teorie grup: Grupoidy, pologrupy, monoidy a grupy. Podgrupy, cyklické grupy a jejich generátory.**

NI-MPI

* **Grupoid** – uspořádaná dvojice
  + = libovolná neprázdná množina
  + = binární operace nad (tzv. kule)
* **Pologrupa** – grupoid, pro který je asociativní
* **Monoid** – pologrupa, ve které existuje neutrální prvek
  + V monoidu existuje právě jeden neutrální prvek
* **Grupa** – monoid, ve kterém ke každému existuje inverzní prvek
  + V grupě má každý prvek právě 1 inverzní prvek
* **Abelovská grupa** – grupa, kde je komutativní

Uzavřená grupoid asociativní pologrupa monoid inverze grupa komutativní Abel. grupa

* **Podgrupa grupy** je je grupa
  + V každé grupě s alespoň 2 prvky existují alespoň 2 podgrupy
    - **Triviální podgrupy**
    - Ostatní podgrupy jsou **vlastní podgrupy**
  + **Průnik** podgrup je podgrupa
  + **Kritérium** podgrupovosti: je podgrupa , právě když
  + **Neutrální prvek** podgrupy je roven neutrálnímu prvku grupy
  + **Inverze** prvku v podgrupě je stejná, jako inverze stejného prvku v grupě
* **Řád grupy** – počet prvků množiny –
  + Podle řádu se dělí na **konečné a nekonečné grupy** (nekonečná )
  + **Lagrangeova věta** – buď podgrupa konečné grupy , potom žád dělí řád
  + **Sylowova věta** – buď grupa konečného řádu a číslo prvočíselný dělitel čísla . Pokud dělí (pro přirozené), pak grupa obsahuje podgrupu řádu
* je podgrupou obsahující
* **Grupa generovaná množinou** – podgrupa grupy
  + Množina je **generující množina** grupy
  + Pro jednoprvkovou množinu zavádíme značení , = generátor
  + je nejmenší podgrupa
  + Všechny prvky lze získat pomocí „**grupového obalu**“
  + **Generátor** = prvek, jehož **mocněním** dostaneme všechny prvky grupy
* Grupa je rovna právě když a jsou nesoudělná čísla
* **Cyklická grupa** – existuje prvek
  + = **generátor** cyklické grupy
  + Buď prvek grupy . Pokud existuje , pak **nejmenší**  s touto vlastností je **řád prvku** . Pokud takové neexistuje, řád prvku je nekonečno
    - Řád se značí
    - Řád prvku je roven řádu grupy
    - je cyklická, právě když , kde je liché prvočíslo a
* **Jak najít všechny generátory**
  + Je-li cyklická grupa řádu a nějaký její generátor, potom je také generátor tehdy, a jen tehdy, když a jsou nesoudělná
  + V cyklické grupě řádu je počet generátorů roven
    - = **Eulerova funkce** – každému přiřazuje počet přirozených čísel menších než , které jsou s ním nesoudělná
    - Takže pro prvočíslo je cyklická grupa řádu a má generátorů
    - Algoritmus na to není
* Libovolná podgrupa cyklické grupy je opět cyklická grupa
* **Malá Fermatova věta** – pro libovolné a libovolné
  + Z důsledku Lagrangeovy věty: , kde je neutrální prvek
* **TODO přidat příklad**

**2. Tělesa a okruhy: Základní definice a vlastnosti. Konečná tělesa. Okruhy polynomů, ireducibilní polynom.**

NI-MPI

* **Okruh** – , kde je neprázdná množina a binární operace na ní a platí:
  1. je **abelovská grupa** = **aditivní grupa** okruhu
     + Neutrální prvek = **nulový prvek** – značí se
     + Inverzní prvek vůči k  značíme
     + Lze definovat odčítání:
  2. je monoid = **multiplikativní monoid** okruhu
     + Je-li komutativní, je komutativní okruh
     + Neutrální prvek = **jednička**, značení 1
  3. Platí **distributivní zákon:**
* Základní vlastnosti okruhu
  + Násobení nulovým prvkem dává nulový prvek
  + Levý i pravý distribuční zákon pro odečítání:
* **Obor integrity** – okruh, ve kterém neexistují dělitelé nuly
  + **Dělitelé nuly** = nenulové prvky
* **Těleso** – okruh kde je abelovská grupa
  + Tuto grupu nazýváme **multiplikativní grupou** tělesa T
  + Pokud pro z tělesa platí , potom , nebo
    - Každé těleso je oborem integrity
* **Zobrazení** z okruhu/tělesa do okruhu/tělesa je **homomorfismus** těchto okruhů/těles, jestliže je homomorfismem příslušných aditivních a multiplikativních grupoidů/grup a platí
  + Je-li navíc **bijekce** (prosté a na), jedná se o **izomorfismus** těchto okruhů/těles
  + Tělesa a nazýváme izomorfní, právě když existuje izomorfismus . V tomto případě je těleso izomorfní s tělesem
* **Konečné těleso** – těleso, které má konečný počet prvků
* **Řád tělesa** = počet prvků tělesa
* Základní příklad konečného tělesa – množina s operacemi **modulo prvočíslo** 
  + **-** aditivní grupa , multiplikativní grupa
    - - řád
      * Každý nenulový prvek je její **generátor**
      * Je grupou i pro neprvočíselné
    - - řád – není prvočíslo
      * Je **cyklická**
      * Počet generátorů závisí na řádu, je roven
* **Řád konečného tělesa** musí být mocnina prvočísla , kde je prvočíslo a je kladné celé číslo
  + Všechna tělesa řádu jsou **navzájem izomorfní**
* **Galois field** – těleso s prvky -
  + Prvočíslo = charakteristika tělesa
  + – aditivní grupa
    - Řád
    - Neutrální prvek
    - Pro není cyklická
  + – multiplikativní grupa
    - Řád
    - Neutrální prvek:
    - Inverzi lze nalézt pro každý prvek s REA v polynomiálním čase
    - Je vždy cyklická
* **Polynom nad okruhem**
  + Nad okruhem
  + … koeficienty polynomu
  + … **formální proměnná** polynomu
  + Pokud pro existuje , pak největší z  = **stupeň polynomu** , značeno
  + … nulový polynom – nedefinovaný stupeň
  + Abychom mohli dělat operace s polynomy, potřebujeme je umět s jejich koeficienty – lze vybudovat okruh polynomů nad libovolným okruhem (i tělesem)
* **Okruh polynomů** – množina všech polynomů nad okruhem spolu s operacemi **sčítání** a **násobení** definovanými předpisy

kde , tvoří okruh polynomů nad okruhem -

* + **Násobení** polynomů: buď těleso a nenulové polynomy. Platí
  + **Dělení** polynomů: buď těleso a nenulové polynomy. Pak existují jednoznačně určené polynomy takové, že

kde je buď nulový, nebo má stupeň ostře menší než stupeň

* + **Bézoutova rovnost** pro polynomy: Buďte a nenulové polynomy nad tělesem . Pak existují polynomy tak, že:
  + Buď těleso a polynom stupně . Prvek je **kořen polynomu** právě tehdy, když:

kde je stupně

* **Ireducibilní polynom** – buď stupně alespoň 1. Řekneme, že je ireducibilní nad okruhem , jestliže :
  + Mějme celé a prvočíslo . Označme počet monických polynomů stupně ireducibilních nad . Potom
    - **Monický polynom** – má za koeficient u nejvyšší mocniny jedničku
    - – **Möbiova funkce** definovaná pro celé :

**3. Funkce více proměnných: gradient, Hessián, definitnost matic, extrémy funkcí více proměnných bez omezení a s rovnostními omezeními.**

NI-MPI

**4. Integrál funkcí více proměnných (Darbouxova konstrukce).**

NI-MPI

**5. Numerická matematika: reprezentace čísel v počítači, chyby vznikající při výpočtech s pohyblivou řádovou čárkou, podmíněnost a stabilita numerických algoritmů.**

NI-MPI

**6. Testování statistických hypotéz. T-testy, testy nezávislosti, testy dobré shody.**

NI-VSM

**7. Základy teorie informace a kódování, entropie.**

NI-VSM

**8. Markovské řetězce s diskrétním časem. Jejich limitní vlastnosti.**

NI-VSM

**9. Markovské řetězce se spojitým časem. Souvislost s Markovskými řetezci s diskrétním časem a s Poissonovým procesem.**

NI-VSM

**10. Systémy hromadné obsluhy a jejich limitní vlastnosti. Souvislost s Markovskými řetězci se spojitým časem.**

NI-VSM

**11. Význam tříd NP a NPH pro praktické výpočty.**

NI-KOP

**12. Experimentální vyhodnocení algoritmů, zejména randomizovaných.**

NI-KOP

**13. Princip lokálních heuristik, pojem globálního a lokálního minima, obrana před uváznutím v lokálním minimu.**

NI-KOP

**14. Princip genetických algoritmů, význam selekčního tlaku pro jejich funkci.**

NI-KOP

**15. Princip simulovaného ochlazování, význam parametrů a způsoby jejich řízení.**

NI-KOP

**16. Výkonnostní měřítka paralelních algoritmů, PRAM model, APRAM model, škálovatelnost.**

NI-PDP

**17. Programování nad sdílenou pamětí, programový model OpenMP, datový a funkční paralelismus, synchronizace vláken, vícevláknové algoritmy (násobení polynomů, násobení matic, řazení).**

NI-PDP

**18. Programování nad distribuovanou pamětí, programový model MPI (vícevláknové procesy, komunikátory, 2-bodové blokující a neblokující komunikační operace, kolektivní operace), paralelní násobení hustých matic, paralelní mocninná metoda.**

NI-PDP

**19. Přímé ortogonální a hyperkubické propojovací sítě paralelních počítačů (definice, vlastnosti, vnořování).**

NI-PDP

**20. Paralelní algoritmy pro redukci, prefixový součet a segmentový prefixový součet na PRAM, v ortogonálních, hyperkubických a obecných topologiích, aplikace.**

NI-PDP