Tételsor a Véges testek c. tárgyhoz

2012. őszi félév

1. Test, ferdetest fogalma, Wedderburn tétele, bővítés fogalma, test vektortér részteste fölött, bővítés foka, algebrai ill. transzcendens elem, minimálpolinom és annak tulajdonságai, elem foka, véges bővítés algebrai.

2. Testbővítések konstrukciója, kommutatív egységelemes gyűrű maximális ideálja szerinti faktorgyűtű test, Euklidészi gyűrűk főideálgyűrűk, maximális ideálok főideálgyűrűkben, testbővítésnek létezése, melyben egy irreducibilis polinomnak van gyöke, ill. melyben egy tetszőleges polinom faktorokra bomlik, felbontási test fogalma, felbontási test egyértelműsége.

3. Véges testek: karakterisztika, nullosztómentes gyűrű karakterisztikája, prímtest fogalma és létezése, véges testek elemszáma, résztest elemszáma, véges testek karakterizációja (létezésük és egyértelműségük). Frobenius automorfizmus.

4. Véges test additív és multiplikatív csoportja. Diszkrét logaritmus fogalma és alapvető tulajdonságai. Index kalkulus. Kriptográfiai alkalmazások: Diffie-Hellman kulcscsere protokoll, ElGamal titkosítás és digitális aláírás.

5. Véges test feletti polinomok: adott fokú ireducibilis főpolinomok szorzata, egyenlet a n-ed fokú irreducibilis polinomok számára, Möbius függvény, Möbius inverziós formula, n-ed fokú irreducibilis polinomok száma, ill. létezésük. Véges testek fölötti polinomok faktorizációja, Berlekamp algoritmus.

6. Elem nyoma véges tesben, a nyom alapvető tulajdonságai. Nyom és lineáris leképzések kapcsolata. Nyom magja. Norma és alapvető tulajdonságai.

7. Polinomok gyökeinek keresése kis prímtestben, nagy prímtestben és kis karakterisztikájú nagy testben.

8. Lineáris rekurzív sorozatok. Periódikus sorozatok, küszöbszám, minimális periódus, a minimális periódus hossza osztja az összes periódus hosszát. Véges test fölött minden lineáris rekurzív sorozat periódikus. Elégséges feltétel, hogy a küszöbszám 0 legyen. A sorozatot generáló mártix, és kapcsolata a sorozat minimális periódus hosszával. Inhomogén sorozatok.

9. IRS fogalma. IRS periódusa, annak kapcsolata a generáló mátrixhoz. Lineáris rekurzív sorozat és a hozzá tartozó IRS minimális periódusának kapcsolata. Tisztán periódikus sorozatok, elégséges feltétel a tisztán periódikusságra. Rekurzió karakteriszikus polinomja, annak kapcsolata a generátor mátrixszal. Lineáris rekurzív sorozatok előállítása zárt formulával.

10. Lineáris komplexitás fogalma. Explicit inverz generátor és annak lineáris komplexitása. A sorozat kezdőszeleteinek lineáris komlexitása közötti kapcsolat. Sorozatok lineáris komplexitásának kiszámolása a Berlekamp-Massey algoritmussal.

11. Legendre és Jacobi szimbólum fogalma, és alapvető tulajdonságaik. Kvadratikus maradékok, nemmaradékok és pszeudo-maradékok. Kvadratikus pszeudo-maradékok problémája. Goldwasser-Micali titkosítás.