Komputeralgebra
vizsgatematika
2003/2004

1. A p-adikus számok
2. Többváltozós polinomgyűrű, Gröbner bázis (monomiális rendezés; maradékos osztás; monomiális ideál; Dickson lemma, a Gröbner bázis tulajdonságai; szükséges és elégséges feltétel arra, hogy valamely ideál bázisa Gröbner bázis legyen, Gröbner bázis keresése; minimális redukált Gröbner bázis)
3. Kínai maradéktétel
3. Algoritmus annak eldöntésére, hogy p prím esetén $M_p=2^p-1$ prímszám legyen.
4. Hosszú számok szorzása, Karacuba algoritmus
5. Gyors Fourier Transzformáció (FFT), polinomok szorzása
7. Polinom felbontása négyzetmentes polinomok szorzatára
8. Differenciálbővítés
9. Racionális törtfüggvények integrálása
10. Véges testekben polinomok faktorizációja
11. Polinomok és algebrai egészek különböző mértékei
12. Egész együtthatós polinomok faktorizációja
13. Primitív gyök a p-elemű véges testben
14. Dirichlet-karakterek
15. Dirichlet-tétel: Az $n \equiv l \pmod k$-ban végtelen sok prímszám van, ha $(l,k)=1$