Véges testek és alkalmazásaik

választható tantárgy alkalmazott matematikus és doktoranduszhallgatóknak

Küronya Alex egyetemi adjunktus (Algebra tanszék) / 2006 ősz

Hely és időpont: H. épület 46., csütörtök 16-18.
Email: kalex@math.bme.hu

Irodalom:

- Siegfried Bosch: Algebra (5. kiadás), Springer, 2004.
- Ireland–Rosen: A classical introduction to modern number theory, Springer, 1982
- Victor Shoup: A computational introduction to number theory and algebra (letölthető a www.shoup.net/ntb címről)

Ajánlott irodalom:

- Iványi Antal (szerk.): Informatikai algoritmusok 2, Eötvös Kiadó, 2005
- Scheja–Storch: Lehrbuch der Algebra I.-II., Teubner, 1988.
- Ivanyos Gábor honlapja: www.math.bme.hu/∼ig/vegtest

Előfeltételek: Két félév absztrakt algebra, vagy azzal ekvivalens tudás. Abban az esetben, ha valakinek kétségei vannak, keressen meg engem.

Tárgyleírás: A félév első harmadában megismerkedünk a véges testek szerkezetével, majd ezután sok, a matematika különféle ágait érintő, illetve gyakorlati alkalmazást fogunk tárgyalni. Sor kerül véges test feletti egyenletek megoldásszámainak elemzésére, az ún. Weil-sejtés egyszerűbb eseteinek bizonyítására, titokmegosztási algoritmusra polinominterpoláció segítségével, kombinatórikai alkalmazásokra. A félév végén részletesen megismerkedünk véges testek feletti polinomok faktorizálására szolgáló algoritmusokkal, amelyeknek a gyakorlatban igen fontos szerepük van.

Házi feladatok és osztályozás: Kétféleképpen lehet jegyet szerezni: vagy a félévközi hetente kiadott házi feladatok beadásával (én ezt javasolnám), vagy pedig a félév végén írásbeli vizsga során.