

Algebra és számelmélet (MBLK13)

2025 tavaszi félév

Követelmények

- Az előadás (MBLK13E) és a gyakorlat (MBLK13G) csak együtt vehető fel és csak együtt teljesíthető. Előfeltétel a Diszkrét matematika (MBLK12) kurzus.
- Öt elektronikus tesztet kell kitölteni a szorgalmi időszakban, ezekkel $5 \cdot 4 = 20$ pont szerezhető.
- A félév végén, május 23-án lesz egy zárthelyi dolgozat, amelyen 40 pont szerezhető.
- Pluszpontokat lehet szerezni az online órákon való aktív részvétellel (alkalmanként 1 pontot), illetve szorgalmi feladatok beadásával (feladatonként 1 pontot, egy feladatsorról legfeljebb három feladat adható be). Az így kapott pluszpontok száma nem lehet több, mint 6.
- A fenti módokon összegyűjtött pontok alapján a következő ponthatárok szerint alakul a megajánlott jegy.

53 – 60	jeles
45 – 52	jó
37 – 44	közepes
30 – 36	elégéses
0 – 29	elégtelen

- Ha valaki nem fogadja el ezt a megajánlott jegyet, akkor szóbeli vizsgát kell tennie. A végső eredménybe a félévközi pontok ekkor is beleszámítanak.
- Javítás, pótlás: Az elektronikus tesztek a teszt lezárta után nem javíthatók és nem is pótolhatók. A zárthelyi dolgozat a vizsgaidőszak elején egy alkalommal javítható vagy pótolható.

Tematika

Műveletek (asszociatív, kommutatív, idempotens, egységelem, zéruselem, inverz, disztributív tulajdonságok, nevezetes példák). A csoport, mint absztrakt struktúra, műveletábrázlat, izomorfia, izomorfizmus. Nevezetes példák: számok, (redukált) maradékosztályok, mátrixok, lineáris csoportok, diéderscsoportok, kvaterniócsoport. Páros és páratlan permutációk, szimmetrikus és alternáló csoportok. Permutációs játékok (ismertetés). Hatványozás, elem rendje, ciklikus csoport és részcsoportjai. Részcsoport, generálás. Mellékosztályok, Lagrange tétele. Alkalmazás összeszámlálási feladatokra. A gyűrű, az integritástartomány és a test fogalma, nevezetes példák (számgyűrűk és számtestek, maradékosztály-gyűrűk és maradékosztálytestek, mátrixgyűrűk).

A polinom fogalma, test feletti polinomgyűrű. Oszthatóság, maradékos osztás, lko és lkkt, euklideszi algoritmus, kétismeretlenes lineáris diofantoszi egyenlet, kongruencia, maradékosztályok, maradékosztály-gyűrű, lineáris kongruencia, multiplikatív inverz mod f . Polinom és polinomfüggvény, Lagrange-interpoláció, polinomok (többszörös) gyökei, Bézout tétele, (iterált) Horner-módszer. Irreducibilis polinomok, egyértelmű irreducibilis faktorizáció. Viéte-formulák, irreducibilis faktorizáció a komplex, valós és racionális számtest fölött, Schönemann–Eisenstein-tétel, Rolle-tétel. Polinomgyűrű faktorteste mint egyszerű algebrai bővítés, véges testek konstrukciója. Derivált, polinomok közös, ill. többszörös gyökei.

Teljes és redukált maradékrendszerek, az Euler-féle φ függvény, Euler–Fermat-tétel, rend modulo m , primitív gyökök, index. Négyzetes maradékok, Legendre-szimbólum. Titkosítások, nevezetes számelméleti problémák (ismertetés).

Algebrai struktúrák (példák, hálószerűen rendezett halmazok és hálók ekvivalenciája).

Irodalom

- Freud Róbert, Gyarmati Edit: Számelmélet, Nemzeti Tankönyvkiadó, 2000, 2006.
- Kalmárné Németh Márta, Katonáné Horváth Eszter, Kámán Tamás: Diszkrét matematikai feladatok, Polygon, 2003, 2005.
- Kiss Emil: Bevezetés az algebraiba, Typotex, 2007.
- Megyesi László: Bevezetés a számelméletbe, Polygon, 1997, 2005.
- Sárközy András, Surányi János: Számelmélet - Feladatgyűjtemény, Tankönyvkiadó, 1977, 1983, 1990, 1995, Nemzeti Tankönyvkiadó, 1996, 1999.
- Szendrei Ágnes: Diszkrét matematika, Polygon, 1994, 1996, 1998, 2000, 2002, 2004.