

Diszkrét matematika tematika BSc, középszint
2010 őszi szemesztertől
I. félév

- **Logikai alapok:** logikai jelek predikátumok, formulák.
- **Halmazelméleti alapfogalmak:** halmazok, részhalmazok, unió, metszet, különbség, komplementer és tulajdonságai, hatványhalmaz.
- **Relációk:** rendezett pár, koordináták, binér reláció, értelmezési tartomány, értékészlet, kiterjesztés, leszűkítés. Relációk kompozíciója, ekvivalencia reláció és osztályozás, részben rendezés, rendezés. Legkisebb, legnagyobb, minimális és maximális elem. Korlátok és pontos korlátok.
- **Függvények:** injektív, szürjektív és bijektív függvények, monoton függvények. Indexelt családok. Reláció és Descartes-szorzat általános esetben, kapcsolat adatbázis kezeléssel. Műveletek, logikai műveletek, műveletek függvényekkel, művelettartó leképezések.
- **Valós számok:** félcsoport, csoport, gyűrű, integritási tartomány, rendezés, rendezett test. Arkhimédészi rendezettség, a valós számok. A természetes, az egész, és a racionális számok, mint a valós számok részhalmaza. Teljes indukció, rekurzió, a természetes számok rendezésének tulajdonságai, jólrendezés. Sorozatok, többváltozós függvények, szorzatok és összegek. Logikai függvények és megvalósításuk, a maradékos osztás tétele, számrendszerek. Számítógépes számábrázolás. Intervallumaritmetika.
- **Komplex számok:** a komplex számok teste, konjugálás, abszolút érték, argumentum, trigonometrikus alak. Gyökvonás komplex számból. Az algebra alaptétele.
- **Kombinatorika:** halmazok ekvivalenciája, véges és végtelen halmazok, véges halmazok tulajdonságai. A skatulya elv. Permutációk, variációk, kombinációk, ismétléssel is. Binomiális és polinomiális tétel. Logikai szita formula.
- **Végtelen halmazok:** halmazok összehasonlítása, Schröder-Bernstein-tétel, Cantor-tétele (bizonyítás nélkül). Megszámlálható halmazok és jellemzéseik, megszámlálható halmazok egyesítése. Kontinuum számosságú halmazok.
- **Oszthatóság:** oszthatóság a természetes és az egész számok körében. Törzsszám és prímszám, legnagyobb közös osztó, legkisebb közös többszörös, relatív prímelek. Bővített euklideszi algoritmus egész számokra és következményei. A számelmélet alaptétele. Prímszámok, szita.
- **Kongruenciák:** maradékosztályok, teljes és redukált maradékrendszerek, Z/mZ szerkezete, Komplementens számábrázolás. Diszkrét logaritmus probléma, Diffie-Hellmann-Merkle-kulcscsere. Az Euler-féle függvény, Euler-Fermat-tétel, Fermat-tétel. Lineáris kongruencia rendszer megoldása. A kínai maradéktétel. Az RSA-eljárás és alkalmazásai. Számelméleti függvények, egyszerű példák, az Euler-féle függvény számítása.