

BSc Matematika Alapszak, 2017.

Matematikai Intézet,
Természettudományi Kar,
Eötvös Loránd Tudományegyetem.

Számelmélet1 — normál változat

- **Óraszám** ($ea+gy$): $2 + 2$
- **Specializáció**: közös
- **Kredit** ($ea+gy$): $3 + 3$
- **Számonkérés**: kollokvium + gyak. jegy
- **Tárgykód** (ea, gy): szamel1n0_m17ea, szamel1n0_m17ga
- **Ajánlott félév**: 1
- **Státusz**: kötelező

Tantárgyfelelős

- Károlyi Gyula, Algebra és Számelmélet Tanszék, Matematikai Intézet.

Előfeltételek

Az előadás előfeltételei:

- *Gyenge*: a gyakorlat

Megjegyzések

- A Számelmélet1 normál és intenzív változata egymás között átjárható.
Ennél a tárgynál a gyakorlaton is legalább 50%-ban az elméleti anyag elmélyítése történik.

A tematikát kidolgozta:

- Sárközy András, Algebra és Számelmélet Tanszék, Matematikai Intézet.

Szükséges előismeretek

A tárgy a középiskolai matematika anyag ismeretét követeli.

A tantárgy célkitűzése

A tárgy célja az alapvető számelméleti ismeretek bemutatása. A normál változat azt jelenti, hogy az akkreditált tematikában szereplő tananyag keretein belül elsősorban az alapvető fogalmakat, tételeket, módszereket tárgyaljuk igen részletesen, figyelmet fordítva a középiskolai hiánypótlásra is. Az intenzív változatot csak azoknak ajánljuk, akik matematikailag érettebbek, azaz a középiskolában az átlagosnál magasabb szintű matematikaoktatásban részesültek, vagy már ott is intenzíven foglalkoztak matematikával.

Irodalom

- **Freud Róbert, Gyarmati Edit**: *Számelmélet*. Nemzeti Tankönyvkiadó, 2006.
- **Sárközy András, Surányi János**: *Számelmélet feladatgyűjtemény*. Egyetemi jegyzet.
- **Szalay Mihály**: *Számelmélet*. TypoTeX Kiadó, 1998.
- **Sárközy András**: *Számelmélet*. Műszaki Könyvkiadó, 1976.

Tematika

- Oszthatóság, legnagyobb közös osztó, euklideszi algoritmus, felbonthatatlan és prímszámok, a számelmélet alaptétele, következmények.

- Nevezetes additív és multiplikatív számelméleti függvények. Összegzési függvény.
- Kongruenciák, teljes és redukált maradékrendszer. $\varphi(n)$ multiplikativitása. Az Euler-Fermat tétel. Lineáris kongruenciák, lineáris diophantikus egyenletek. Az $x^2 - y^2 = n$ egyenlet. Pitagoraszi számhármassok. Lineáris kongruencia-rendszerek. Számítógépes alkalmazások.
- Magasabb fokú kongruenciák. Redukció prímmhatvány, ill. prím modulusra. Megoldásszám, fokszámredukció prím modulus esetén. Wilson tétele. $x^k \equiv 1 \pmod{p}$. k -adik hatványmaradékok. A rend definíciója és tulajdonságai. Hány a van $o(a)=k$ -val (bizonyítás nélkül)? Primitív gyök, index. Kvadratikusan maradékok. A Legendre-szimbólum és alaptulajdonságai.
- Végtelen sok prím létezése.