

## **Tárgytematika / Course Description** **Számítástudomány**

**GKNB\_MSTM010**

**Tárgyfelelős neve /**

**Teacher's name:** dr. Kallós Gábor

**Félév / Semester:** 2025/26/2

**Beszámolási forma /**

**Assesment:** Vizsga

**Tárgy heti óraszám /**

**Teaching hours(week):** 2/0/0

**Tárgy féléves óraszám /**

**Teaching hours(sem.):** 0/0/0

### **OKTATÁS CÉLJA / AIM OF THE COURSE**

A tantárgy oktatásának célja az, hogy megismertessük a hallgatóságot a Számítástudomány alapjaival. Az elméleti ismeretek mellett jelentős hangsúlyt helyezünk a gyakorlati alkalmazhatóságra; korszerű numerikus és szimbolikus szoftverek támogatásával szemléltetjük a fő eredményeket.

### **TANTÁRGY TARTALMA / DESCRIPTION**

#### **Témakör név: Numerikus és szimbolikus számítások**

Témakör leírása: Motiváció, szoftvereszközök. Numerikus és szimbolikus számítások, közelítések, hibák. Gépi egyszerűsítés, egyenletek megoldhatósága.

Témakör kulcsszavai: Numerikus és szimbolikus számítások

#### **Témakör név: Euklideszi-algoritmus**

Témakör leírása: Prímek és felbonthatatlanok. Euklideszi-algoritmus (Inko számítás), Fibonacci-sorozat. Lánc törtek. Algoritmusok hatékonysága.

Témakör kulcsszavai: Euklideszi-algoritmus, Fibonacci-sorozat. Algoritmusok hatékonysága.

#### **Témakör név: Eratoszthenészi szita és próbaosztásos algoritmus**

Témakör leírása: Eratoszthenészi szita és próbaosztásos algoritmus. Nevezetes matematikai konstansok.

Témakör kulcsszavai: Eratoszthenészi szita és próbaosztásos algoritmus

#### **Témakör név: Fermat-teszt. Euler-tétele.**

Témakör leírása: Tökéletes számok, Mersenne-prímek, Fermat-teszt. Euler-tétele.

Témakör kulcsszavai: Tökéletes számok, Fermat-teszt, Euler-tétele.

#### **Témakör név: Titkosítások, RSA**

Témakör leírása: Titkosítások. RSA, alkalmazások, hibalehetőségek.

Témakör kulcsszavai: Titkosítások, RSA

#### **Témakör név: Fejlettebb prímfelbontó eljárások és prímtesztek**

Témakör leírása: Fejlettebb prímfelbontó eljárások: Fermat módszere, Pollard ró és p-1 algoritmus. Egyéb prímtesztek és felbontó eljárások.

Témakör kulcsszavai: Pollard ró és p-1 algoritmus

### **Témakör név: A gyors szorzás algoritmusai**

Témakör leírása: Mester tétel. A gyors szorzás algoritmusai: hagyományos rekurzív eljárás, Karacuba és Strassen módszere.

Témakör kulcsszavai: Karacuba és Strassen módszere

### **Tevékenység típusok**

#### **Kontakt gyakorlat**

Mérték: 28 tanóra (hour)

Leírás: Géptermi gyakorlat

Kötelező: Nem

Becsült Idő: 28 óra

#### **Otthon megtekintendő videó (új anyag)**

Mérték: 5 db (PCS)

Leírás: Oktató videók

Kötelező: Nem

Becsült Idő: 10 óra

#### **Otthoni gyakorlás**

Mérték: 10 db (PCS)

Leírás: Maple programok írása

Kötelező: Nem

Becsült Idő: 10 óra

---

## **SZÁMONKÉRÉSI ÉS ÉRTÉKELÉSI RENDSZERE / ASSESMENT'S METHOD**

### **Számonkérési forma:**

Vizsga (Exam)

#### **Vizsga számítógép által kiértékelt része**

Mérték: 1 db (PCS)

Leírás: Impera teszt

Kötelező: Igen

Becsült Idő: 40 óra

### **Aláírás kialakításának módja:**

Az aláírás két feltételhez kötött: 1. A hallgató az ellenőrzött órák / alkalmak közül (nem számít az első óra és a katalógusmentes időszak) legalább 4 alkalommal részt kell, hogy vegyen az órán. 2. A félév utolsó negyedében (megállapodás szerint, pl. 10-13. hét) otthonról meg kell írni az előre kiadott elektronikus Impera mintázathoz legalább 40%-os eredménnyel. (Pótlás: élőben az utolsó tanórán.)

### **Érdemjegy kialakításának módja:**

Kötelező elektronikus (Impera teszt) és fakultatív szóbeli vizsga (témakörök a tantárgyi lapon). Beadós feladattal (program, Maple munkalap) jutalompontok érhetők el. (A szorgalmas bejárás és az órai munka is plusz pontokat ér.) [Tanácsok a sikeres vizsgához: A slide-ok sokszor csak vázlatosak, önmagukban nem mindig alkalmasak az önálló tanulásra. A beszámoló sikeres teljesítéséhez nagy segítség, ha valaki figyel az

órán, jegyzetel, átérzi az órán megfogalmazott kérdések fontosságát és megjegyzi a levont tanulságokat, megírja az órai példaprogramokat. Ez a tárgy nem elsősorban "otthon tanuló", hanem inkább "órán megértő". Érdemes gyűjteni a plusz pontokat a bejárásra és az órai munkára, ezek sokat segíthetnek a végén.]

---

### **KÖTELEZŐ IRODALOM / OBLIGATORY MATERIAL**

Katona-Recski-Szabó: A számítástudomány alapjai. Typotex, Budapest, 2003.

Bressoud: Factorization and Primality Testing. Springer, New York. 1989.

Komputer algebrai témájú szakkönyvek, Maple és Matlab könyvek.

---

### **AJÁNLOTT IRODALOM / RECOMMENDED MATERIAL**

Bressoud, D. M.: Factorization and Primality Testing (2011), Springer ISBN: 1461288711

Kallós G.: Órai pdf-ek, segédletek, Impera minták (2023), SZE [Moode-SzeLearning oldalon](#)

O'Connor, J.: Symbolic Computation Maple booklet (2009), St. Andrews University [Moodle-SzElearning oldalon](#)

Katona-Recski-Szabó: A számítástudomány alapjai (2007), Typotex ISBN: 978-963-9326-24-8