

<b>Tantárgy neve: Diszkrét matematika II</b>	<b>Kreditértéke: 5 kredit</b>
A tantárgy <b>besorolása: kötelező</b>	
A tantárgy <b>elméleti vagy gyakorlati jellegének mértéke: 90-10</b> (kredit%)	
A <b>tanóra típusa</b> : ea. / gyak. / konz. és <b>óraszám</b> a: 2 / 2 / 1 az adott <b>félévben</b> ,	
A <b>számonkérés módja</b> (koll. / gyj. / <b>egyéb</b> ): koll / gyj	
A tantárgy <b>tantervi helye</b> (hányadik félév): <b>3. félév</b>	
Előtanulmányi feltételek ( <i>ha vannak</i> ): <b>Diszkrét matematika I.</b>	

### **Tantárgy-leírás: az elsajátítandó ismeretanyag tömör, ugyanakkor informáló leírása**

**Oszthatóság:** oszthatóság a természetes és egész számok körében. Asszociáltak és egységek, felbonthatatlan elem és prímelem. Legnagyobb közös osztó, legkisebb közös többszörös, relatív prímek. Bővített euklideszi algoritmus egész számokra és következményei. A számelmélet alaptétele. Prímszámok, szita.

**Kongruenciák:** maradékosztályok, teljes és redukált maradékrendszerek,  $\mathbb{Z}/m\mathbb{Z}$  szerkezete. Komplement számábrázolás. Euler-féle függvény, Euler-Fermat-tétel, Fermat-tétel. Lineáris kongruenciarendszer megoldása. Diofantikus problémák, a kínai maradéktétel. Az RSA-eljárás és alkalmazásai. Az Euler-féle függvény számítása.

**Polinomok:** polinomgyűrűk alaptulajdonságai, polinomfüggvények. A maradékos osztás tétele polinomokra és következményei. Polinom algebrai deriváltja, többszörös gyökök. Irreducibilis polinomok és testbővítések, véges testek. Irreducibilis polinomok a komplex, valós, racionális és az egész számok felett, Gauss tétele. Lagrange-interpoláció, titok megoszlás, többhatározatlanú polinomok.

**Forráskódolás:** információ, bit, entrópia, a kódolás alapjai. Betűnkénti kódolás, kódfa, prefix kód, egyenletes kód és vesszős kód. McMillan-egyenlőtlenség, átlagos szóhosszúság, optimális kód és konstrukciója, Shannon tétele zajmentes csatornára. A szótárkódok alap gondolata.

**Hibakorlátozó kódolás:** hibajelző és hibajavító kódok, egyszerű példák, kódok távolsága és súlya. Hamming-korlát, Singleton-korlát. Lineáris kód, generátormátrix, ellenőrző mátrix, szindrómakódolás, példák. Polinom kódok, CRC-kódok, Reed-Solomon-kódok és dekódolásuk.

### **A legfontosabb kötelező, illetve ajánlott irodalom (jegyzet, tankönyv) felsorolása bibliográfiai adatokkal (szerző, cím, kiadás adatai, (esetleg oldalak), ISBN)**

Járai A. (szerk.): Bevezetés a matematikába - informatikai alkalmazásokkal, ELTE Eötvös kiadó, 2012, 444 o.; negyedik, javított és bővített kiadás; ISBN 987 963 284 077 2.

Ajánlott:

Láng Csabáné: Bevezetés a matematikába

Lehman, E.; Leighton, F.T.; Meyer, A.R. (2014). Mathematics for computer science.

Biggs, N.L. (2002). Discrete mathematics. Oxford University Press (Second Edition).

**Azoknak az előírt szakmai kompetenciáknak, kompetencia-elemeknek (*tudás, képesség stb., KKK 8. pont*) a felsorolása, amelyek kialakításához a tantárgy jellemzően, érdemben hozzájárul**

*pl.:*

**a) tudása**

- Ismeri az informatikai szakterület tudásanyagát megalapozó általános és specifikus matematikai, számítástudományi elveket, tényeket, szabályokat, összefüggéseket, és eljárásokat. Az érintett területek: analízis (kalkulus), numerikus analízis, diszkrét matematika, lineáris algebra, operációkutatás, valószínűségszámítás és statisztika, logikai alapok, számításteória, algoritmusok tervezése és elemzése, automaták és formális nyelvek, mesterséges intelligencia alapjai.

-

**b) képességei**

- Képes az általános és specifikus matematikai, számítástudományi elveket, tényeket, szabályokat, összefüggéseket alkalmazni informatikai szakterületen.

- Képes az informatika formális modelljeinek alkalmazására.

**Tantárgy felelőse (*név, beosztás, tud. fokozat*): Burcsi Péter, egyetemi docens, PhD, dr. habil.**