



Tantárgy kód

BMETE929302

Tantárgy azonosító adatok

1.	A tárgy címe	Számítógépes számelmélet 2									
2.	A tárgy angol címe	Computation number theory 2									
3.	A tárgy rövid címe	Szám gépSzámelm2	Követelmény	2	+	0	+	0	v	Kredit	3
4.	Ajánlott/kötelező tanulmányi rend										
	vagy	Tantárgy kód 1	Rövid cím 1	Tantárgy kód 2	Rövid cím 2	Tantárgy kód 3	Rövid cím 3				
	4.1	TE929201	Szám gépszámelm								
	4.2										
	4.3										
5.	Kizáró tantárgyak										
6.	A tantárgy felelős tanszéke	Analízis Tanszék									
7.	A tantárgy felelős oktatója	Dr. Járai Antal	beosztása	egyetemi tanár							

Akkreditációs adatok

8.	Akkreditációra benyújtás időpontja	2004.09.30.	Akkreditációs bizottsági döntés időpontja	2004.10.26.
----	------------------------------------	--------------------	---	-------------

Megjegyzések

Csak az űrlap fehéren hagyott mezőibe írjunk és a mezők között a **tabulátor** billentyűvel haladjunk! Ha egy kitöltött mezőből tabulátor billentyűvel lépünk ki, több más mező értéke automatikusan megváltozhat. Egy adott mezőre lépve, az állapotsorban megjelenő rövid, ill. az F1 gomb megnyomásakor kapható hosszabb leírás ad segítséget a kitöltéshez. A *tantárgy kódot* a dékáni hivatal adja.

1-2. sorok: A tárgy címének (max. 60 karakter) legalább egy karakterben különböznie kell minden más, Neptunban regisztrált tárgy címétől.

3. sor: A rövid cím jellegzetes, legfeljebb 16 karakter hosszúságú rövidítés. A követelmény eladás+gyakorlat+labor formátumú, az utolsó mező a félév végi számonkérés típusa (v,f,a vagy s, részletes információ az F1 gombra). A kredit megadásánál ügyelni kell arra, hogy az alább részletezett, a tantárgy elvégzéséhez átlagosan szükséges tanulmányi munka mennyiségével összhangban legyen (összes óraszám = kredit*30 óra).

4. sor: Legfeljebb 3, már korábban hallgatott tárgy adható meg a 4.1 sorban. A 4.2 és 4.3 sorok *vagyilag* lehetőségek megadására szolgálnak, például abban az esetben, ha az egyik tárgynak korábban oktatott változatai is megfelelnek. **5. sor:** A *kizáró tantárgyaknál* azokat a tárgyakat kell felsorolni, amelyek tematikái a most akkreditálandó tárggyal 75% vagy annál nagyobb átfedést mutatnak.

6-7. sorok: A felelős tanszék és oktató hatáskörét, ill. kijelölésének feltételeit a *Képzési Kódex 2001* c. dokumentum 9.1 fejezete tartalmazza.

Tematika			
7.	A tantárgy az alábbi témakörök ismeretére épít		
	Számelmélet alapjai, informatika alapjai, a tárgy első féléve		
8.	A tantárgy célkitűzése, feladata a szakképzés céljának megvalósításában		
	választható tárgy		
9.	A tantárgy részletes tematikája		
	Gyors aritmetika és polinomaritmetika: Karacuba módszere, FFT, Schönhage-Strassen gyorsorzás és egyéb módszerek. Elliptikus függvények. Elliptikus görbék és paraméterezésük. Faktorizálás elliptikus görbékkel. Prímtesztelés elliptikus görbékkel. Polinomfaktorizálás véges testek felett. Prímtesztelés polinomiális időben. Szitamódszerek: Dixon módszere, lánctörtek alkalmazása, kvadrátikus szita, számtest szita.		
10.	Követelmények, az osztályzat (aláírás) kialakításának módja		
	szorgalmi időszakban	részvétel az előadáson	vizsgaidőszakban vizsga
11.	Pótlási lehetőségek		
	TVSz szerint		
12.	Konzultációs lehetőségek		
	vizsga előtt, megbeszélés szerint		
13.	Jegyzet, tankönyv, felhasználható irodalom		
	jegyzet: http://compalg.inf.elte.hu/~ajarai letölthető .ps file, részletes irodalomjegyzékkel		

14.	A tantárgy elvégzéséhez átlagosan szükséges tanulmányi munka mennyisége órákban (a teljes szemeszterre számítva)		
	14.1	Kontakt óra	28
	14.2	Félévközi felkészülés órákra	20
	14.3	Felkészülés zárthelyire	0
	14.4	Zárthelyik megírása	0
	14.5	Házi feladat elkészítése	12
	14.6	Kijelölt írásos tananyag elsajátítása (beszámoló)	0
	14.7		0
	14.8	Vizsgafelkészülés	30
	14.9	Összesen	90
15.	Ellenrz adat	Kredit * 30	90

A tantárgy tematikáját kidolgozta			
16.	Név	beosztás	Munkahely (tanszék, kutatóintézet stb.)
	Dr. Járai Antal	egyetemi tanár	Analízis Tsz.

A tanszékvezet		
17.	Neve	aláírása
	Dr. Petz Dénes	

Megjegyzések
14.1 sor: Értéke automatikusan kitöltődik az rlap elektronikus változatában, a „Követelmény” címszónál megadott óraszám értékek alapján, az (eladás+gyakorlat+labor) * (14 oktatási hét) formula szerint. **14.4 sor:** Értéke 0, ha a zárthelyik íratása kontakt órákon történik, egyébként pedig a minimálisan szükséges számú zárthelyi megírásához felhasználandó idő (a pót zárthelyik nélkül). **14.7 sor:** Az „Egyéb elfoglaltság” szöveg helyére a tevékenység konkrét megnevezését kell írni.
15. sor: Az itt szereplő értéknek és a **14.9 sorban** automatikusan megjelenő tanulmányi óraszám összegnek hozzávetőlegesen meg kell egyeznie! Tájékoztatásul azt vegyük figyelembe, hogy a hallgatók által egy szemeszterben átlagosan 30 kreditnyi munkamennyiséget kell teljesíteni, azaz a szorgalmi és vizsgaidőszak során elvárt terhelés összesen kb. 900 munkaóra.