A mérnök–informatikus szakos hallgatók
Bevezetés a Számításelméletbe I. tárgyának vizsgatételei
(2015/2016. tanév első félév)

1. Térbeli koordinátageometria: sík egyenlete, egyenes egyenletrendszere (paraméteres és nem paraméteres alakban is). Skaláris szorzat fogalma és kiszámítása (biz. nélkül); vektoriális szorzat fogalma és kiszámítása (biz. nélkül). Adott térbeli vektorok lineáris függetlenségének, $\mathbb{R}^3$-beli generátorrendszer voltának, illetve bázis voltának geometriai feltétele.

2. $\mathbb{R}^n$ és $\mathbb{R}^n$ alterének fogalma. Lineáris kombináció, generált altér (és ennek altér volta), generátorrendszer. Lineáris függetlenség (ennek kétféle definíciója és ezek ekvivalenciája). Az „újonnan érkező vektor lemmája”. F-G egyenlőtlenség.

3. Bázis és dimenzió fogalma, a dimenzió egyértelműsége. Standard bázis, $\mathbb{R}^n$ dimenziója. Koordinátavektor fogalma és annak egyértelműsége. Bázis létezése $\mathbb{R}^n$ tetszőleges alterében.

4. Lineáris egyenletrendszer megoldása Gauss-eliminációval. Megoldhatóság, a megoldás egyértelműségének feltétele. Lépcsős alak és redukált lépcsős alak fogalma. Kapcsolat az egyenletek és ismeretlenek száma, illetve a megoldás egyértelműsége között.

5. Determináns definíciója, alaptulajdonságai, kiszámítása. A transzponált determinánsa.

6. A determinánsok kifejtési tétele. Műveletek mátrixokkal (összeadás, skalárral szorzás, szorzás, transzponálás), ezek tulajdonságai. Determinánsok szorzástétele (biz. nélkül).

7. $n \times n$-es lineáris egyenletrendszer egyértelmű megoldhatóságának jellemzése a determináns segítségével. Kapcsolat a lineáris egyenletrendszerek, az $\mathbb{R}^n$-beli generált altérhez tartozás kérdése, illetve a mátrixszorzáson alapuló mátrixegyenletek között. Kapcsolat négyzetes mátrix determinánsa, illetve a sorok és az oszlopok lineáris függetlensége között.

8. Mátrix inverze, létezésének szükséges és elégséges feltétele, az inverz kiszámítása. Mátrix rangja, a rangfogalmak egyenlősége, a rang kiszámítása.

9. Lineáris leképezés fogalma, mátrixa. Szükséges és elégséges feltétel egy függvény lineáris leképezés voltára. Lineáris leképezések szorzata, szorzat mátrixa. Következmény: addíciós tételek a $\sin$ és $\cos$ függvényekre.

10. Lineáris transzformáció invertálhatósága. Lineáris leképezések magtere, képtere, ezek altér volta. Dimenziótétel.

11. Bázistranszformáció fogalma, lineáris transzformáció mátrixa adott bázis szerint, annak kiszámítása.

12. Négyzetes mátrixok sajátértékei és sajátvektorai, ezek meghatározása. Karakterisztikus polinom.

13. Oszthatóság, prímszámok, a számelmélet alaptétele (csak a felbonthatóság bizonyításával). Prímek számossága, $\pi(n)$ nagyságrendje (biz. nélkül). Kongruencia fogalma, alapműveletek kongruenciákkal.

14. Lineáris kongruenciák: a megoldhatóság feltétele, a megoldások száma. Euklideszi algoritmus, annak lépésszáma, alkalmazása lineáris kongruenciák megoldására is (konkrét példán).

15. Euler-féle φ-függvény, képlet a meghatározására (csak prímhatvány esetre bizonyítva). Redukált maradékrendszer, Euler-Fermat-tétel, kis Fermat-tétel. Kétismeretlenes, lineáris diofantikus egyenlet megoldása (konkrét példán). Két kongruenciából álló kongruenciarendszer megoldása (konkrét példán).

16. Polinomiális futásidejű algoritmus (vázlatos) fogalma. Számelmélet és algoritmusok: alapműveletek, hatványozás az egészek körében és modulo m. Prímtesztelés, Carmichael számok. Nyilvános kulcsú titkosítás, RSA-kód

17. Halmazok számossága: egyenlő, kisebb-egyenlő, illetve kisebb számosságú halmaz definíciója, Cantor-Bernstein-tétel (biz. nélkül). Példák: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, a $(0, 1)$ nyílt intervallum számossága, ezek viszonya. Megszámlálhatóan végtelen és kontinuum számosságú halmaz fogalma. Hatványhalmaz számossága, Cantor-tétel. $\mathbb{N}$ hatványhalmazának számossága.