A mérnök–informatikus szakos hallgatók
Bevezetés a Számításelméletbe I. tárgyának vizsgatételei
(2016/2017. tanév első félév)

1. Térbeli koordinátageometria: **sík egyenlete**, **egyenes egyenletrendszerei**.Skaláris szorzat fogalma és kiszámítása (biz. nélkül); vektoriális szorzat fogalma és kiszámítása (biz. nélkül).

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

6. $n \times n$**-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.

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

8. **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. Lineáris transzformáció invertálhatósága.

9. **Lineáris leképezések magtere, képtere**, ezek altér volta. Dimenziótétel.

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

11. **Négyzetes mátrixok sajátértékei és sajátvektorai, ezek meghatározása**. Karakterisztikus polinom. A sajátértékek és sajátvektorok kapcsolata lineáris transzformáció valamely bázis szerinti mátrixának diagonalitásával.

12. **Oszthatóság, prímszámok, a számelmélet alaptétele** (csak a felbonthatóság bizonyításával). Prímek számossága, hézag a szomszédos prímek között, $\pi(n)$ nagyságrendje (biz. nélkül). **Kongruencia fogalma, alapműveletek kongruenciákkal**.

13. **Lineáris kongruenciák: a megoldhatóság szükséges és elégséges feltétele, a megoldások száma**. **Euklideszi algoritmus**, annak lépésszáma, alkalmazása lineáris kongruenciák megoldására is (konkrét, megadott példán).

14. **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, megadott példán). Két kongruenciából álló kongruenciarendszer megoldása (konkrét, megadott példán).

15. Polinomiális futásidejű algoritmus (vázlatos) fogalma. Számelmélet és algoritmusok: alapműveletek, hatványozás az egészek körében és modulo m (ez utóbbi konkrét, megadott példán). Prímtesztelés, Carmichael számok. Nyilvános kulcsú titkosírás, megvalósítása RSA-kóddal.

16. 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.

17. Hatványhalmaz számossága, Cantor-tétel. $\mathbb{N}$ hatványhalmazának számossága.