A mérnök–informatikus szakos hallgatók
Bevezetés a Számításelméletbe I. tárgyának vizsgatételei
(2018/2019. tanév első félév)

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

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

3. **Euler-féle φ-függvény**, képlet a meghatározására (csak prímhatvány esetre bizonyítva). Redukált maradékrendszer, **Euler-Fermat-tétel**, kis Fermat-tétel. Két kongruenciából álló kongruenciarendszer megoldása (konkrét, megadott példán).

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

5. Térbeli koordinátageometria: **sík egyenlete**, **egyenes egyenletrendszerei (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.

6. **$\mathbb{R}^n$ 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**.

7. **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.

8. **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.

9. **Determináns definíciója, alaptulajdonságai, kiszámítása**.

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

11. **$n \times n$-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.

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

13. **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.

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

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

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