

Vihjeid 10. praktikumiks

1. Definitsioon 7.2. Lagrange'i teoreem.
2. Uurida sobiva elemendi järku rühmas $U(\mathbb{Z}_{97})$. Lagrange'i teoreem. Võib kasutada järeldusi 7.23 või 7.24, aga see ei ole tingimata vajalik.
3. Definitsioonid 7.2 ja 7.4. Astendada tuleb ka mittepööratavaid elemente.
4. Definitsioonid 7.2 ja 7.4. Lause 7.11. Järeldus 7.13. Järeldus 7.17. Teoreem 7.27. Võib kasutada järeldusi 7.23 või 7.24, aga see ei ole tingimata vajalik.
5. Kuuenda praktikumi 8. ülesanne või elemendi a järk rühmas $U(\mathbb{Z}_{a^n-1})$.
6. Teoreem 7.21. Kui $\bar{a}$ on $U(\mathbb{Z}_n)$ moodustaja, on seda ka $\bar{a}^{-1}$ (miks?). V.a. mõned erijuhud, ei ole ükski $U(\mathbb{Z}_n)$ moodustaja iseenda pöördelement (miks?).
7. Teoreem 7.12. Fakt $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, kui a on algjuur mooduli p järgi. Kui p on kordarv, siis uurida tema tegurite esinemist korrutises $(p-1)!$.
8. Vaadelda eraldi juhte, kus $p = q$ ja $p \neq q$. Leida algjuured moodulite p^k ja q^l järgi ning kombineerida need HJT abil elemendiks, mille järk on kas $[p-1, q-1]$ või selle kordne. Igas tsüklilises rühmas on täpselt üks iga selle rühma järgu jagaja järku element (põhjendada!).