

Vihjeid 12. praktikumiks

1. Järeldus 7.24. Järeldus 7.13. Kontrolliks teoreem 7.27. Näide 7.29. Teoreem 7.32 annab võimaluse arvutusi kokku hoida.
2. Näide 7.29. Kontrollida, et 3 on tõepoolest algjuur. Võib kasutada 3. ülesande ideed ja mõnda kättesaadavat indeksi tabelit.
3. Ülesanne 2. Teoreem 7.32, punkt 6).
4. Teoreem 7.36. Näide 7.37. Vt ka slaide “Indeksi tabel modulo 29” kodulehe viidete alt. Kontrollmeetodit tutvustati loengus.
5. Näide 7.35. Ülesanne 4.
6. Teoreem 7.33. Lemma 7.6. Teoreem 7.36. Indeksi tabelid moodulite 13, 17 ja 25 järgi. Esimesed kaks võib leida nt E. Redi õpikust, viimase või selle vajaliku osa peate ise tegema.
7. Tõestada abitulemus $(a - 1)^{2k+3} \equiv a - 2 \pmod{p}$. 11. praktikumi 6. ülesanne.
8. Vaadata läbi kõik erinevad juhud (sealhulgas tekkivad erijuhud). Wilsoni teoreem ja HJT.