Kevad 2018

Vihjeid 10. praktikumiks

1. Definitsioon 7.2. Lagrange'i teoreem.

2. Uurida sobiva elemendi järku rühmas $U(\mathbb{Z}_{49})$.

3. Definitsioonid 7.2 ja 7.4.

4. Definitsioonid 7.2 ja 7.4. Järeldus 7.12. Võib kasutada järeldust 7.23, aga see ei ole tingimata vajalik.

5. Näidata, et $\frac{p-1}{2}$ ja -2 järgud mooduli p järgi on samad. Vaadelda nüüd eraldi juhte, kus $\frac{p-1}{2}$ on paaris või paaritu. Tõestada, et $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, kui a on algjuur mooduli p järgi (lause 2.9 ja lemma 7.6).

6. Tõestada, et $\varphi(n)$ ei saa kunagi olla 118, 218 või 318. Teoreem 7.27.

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. Teoreem 7.12. Geomeetrilise jada summa valem (mis tingimustel seda rakendada tohib?). Lemma 7.6.