Kevad 2016

Vihjeid 11. praktikumiks

1. Järeldused 7.21 ja 7.10. Kontrolliks sobib teoreem 7.24.

2. Teoreemid 7.18 ja 7.24. Järeldus 7.21, teoreemid 7.11 ja 7.16.

3. Teoreemid 7.18 ja 7.24. Järeldus 7.21, teoreemid 7.11, 7.15 ja 7.16.

4. Geomeetrilise rea summa valem. Ülesanne 1 ja lemma 7.3.

5. Arvu 4 järk rühmas $\mathbb{Z}_p$ ei ületa kunagi arvu $\frac{p-1}{2}$.

6. Tõestada abiväide: kui a ei ole algjuur modulo m, siis ta ei ole seda ka modulo mn.

7. Esimene variant: taandada ülesanne kongruentsile $2x \equiv 0 \pmod{\varphi(n)}$ ja näidata, et viimasel on täpselt kaks lahendit.
Teine variant: teoreem 7.18 ja 5. praktikumi 8. ülesande lahendusidee.

8. Avaldada jäägiklass $\overline{g}$ jäägiklasside $\overline{g-1}$ ja $\overline{g+1}$ kaudu modulo p. Tõestada eelneva abil, et $\overline{g}$ järk ei ületa $\overline{g-1}$ järku.