Kevad 2018

Vihjeid 11. praktikumiks

1. Järeldused 7.24 ja 7.13. Kontrolliks sobib teoreem 7.27.

2. Teoreemid 7.21 ja 7.27. Teoreem 7.19 ja järeldus 7.24.

3. Teoreemid 7.21 ja 7.27. Järeldused 7.15 ja 7.24, teoreemid 7.18 ja 7.19.

4. Teoreem 7.12. Geomeetrilise rea summa valem. Järeldus 7.24, lemma 7.6. Alternatiivselt järeldus 7.34 ja lemma 7.31.

5. Teoreemid 7.12. Vaadelda sobivaid elemente kujul $a + kp \pmod{q}$, kus $k \in \mathbb{N}$ ja a on algjuur mooduli p järgi. Teoreem 4.10.

6. Vaadelda $\overline{a}$ järku mooduli $a^n - 1$ järgi. Lagrange'i teoreem.

7. Tõestada abiväited:

(a) Kui $1 < a < p$ on algjuur mooduli p järgi, siis ka $1 < b < p$, kus $\overline{b} = (\overline{a})^{-1} \in U(\mathbb{Z}_p)$, on algjuur mooduli p järgi;

(b) Kui kumbki a ja b järkudest ei ole $\varphi(p^2)$, siis $p^2 \mid (ab)^{p-1} - 1$;

(c) Samadel eeldustel ka $p^2 \mid ab - 1$, mis on vastuolu.

8. Järeldus 7.24, lause 2.9, Lagrange'i teoreem. Tõestada abiväide:
$-1 \equiv a^2 \pmod{p}$ mingi $a \in \mathbb{Z}$ korral parajasti siis, kui $p \equiv 1 \pmod{4}$ (vihje: $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, kui a on algjuur mooduli p järgi).