Kevad 2016

Vihjeid 10. praktikumiks

1. Rühma elemendi järgu definitsioon. Lagrange'i teoreem.

2. Vaadelda sobiva elemendi järku rühmas $U(\mathbb{Z}_{79})$.

3. Algjuure ja elemendi järgu definitsioonid.

4. Algjuure ja elemendi järgu definitsioonid. Järeldus 7.10. Võib kasutada järeldust 7.21, aga see ei ole tarvilik.

5. Tõestada järgmised abitulemused:

$$a^2 + a + 1 \equiv 0 \pmod{p},$$
$$(a+1)^2 \equiv a \pmod{p},$$
$$(a+1)^3 \equiv -1 \pmod{p}.$$

Selleks, et $\overline{a+1}$ järk oleks 6, ei piisa vaid kongruentsist $(a+1)^6 \equiv 1 \pmod{p}$.

6. Kongruents $n^4 \equiv -1 \pmod{p}$. Lemma 7.3.

7. Teoreem 7.9. Lemma 7.3. Lause 6.2. Vaadelda eraldi juhte $p \mid a$ ja $p \nmid a$.

8. Teoreem 7.9. Lause 2.9. Lemma 7.3.