Kevad 2015

Vihjeid 5. praktikumiks

1. Tabelist on tegelikult vaja täita ainult veidi üle poole.

2. Teoreem 4.10.

3. Teoreem 4.10 ja Eukleidese algoritm.

4. Teoreem 4.10, Järeldus 4.9 sellisel kujul, nagu ta oli loengus, fakt, et kõik jäägiklassiringi elemendid peale $\overline{0}$ on kas pööratavad või nullitegurid, Teoreem 4.5.

5. Teoreem 4.10, Järeldus 4.9 sellisel kujul, nagu ta oli loengus, Lause 4.8.

6. Eukleidese lemma.

7. Fakti, et kõik jäägiklassiringi elemendid peale $\overline{0}$ on kas pööratavad või nullitegurid, tõestus (tuleb neljapäevases loengus). See ülesanne on olemas ka Ellen Redi arvuteooria õpikus, aga niivõrd erineval kujul, et viimase ülesleidmine on arvatavasti keerulisem, kui ise lahendamine.

8. Teoreem 5.13 (Fermat' väike teoreem: kui $p \in \mathbb{P}$ ja $(a, p) = 1$, siis $a^{p-1} \equiv 1 \pmod{p}$, millest järeldub Järeldus 5.14: $b^p \equiv b \pmod{p}$ iga b korral). See ülesanne on tegelikult erijuht sellisest teemast, nagu kuupvastavus ("cubic reciprocity"), mida me tegelikult käesolevas arvuteooria kursuses ei käsitle.