Kevad 2018

Vihjeid 14. praktikumiks

1. Näide 8.22. Vt. ka `http://kodu.ut.ee/~ltart/Arvuteooria_k2014/AT_Ptk9_n2ited.pdf`

2. Lause 1.6, lemma 8.4, teoreem 8.14, lause 8.8. Algarv ei lõpe paarisnumbriga.

3. Märkus peale definitsiooni 8.1, märkus 8.17. Lause 8.8 ja teoreem 8.11. Alapeatükk 6.5.

4. Definitsioon 8.1, märkus 8.17, lause 8.21, näide 8.22.

5. $\left(\frac{-1}{2017}\right) = \left(\frac{2}{2017}\right) = 1$. Kongruents saab kuju $x^2 \equiv (y'+z')(y'-z') = uv \pmod{2017}$. See on lahenduv kolmel juhul: $2017 \mid uv$, $\left(\frac{u}{2017}\right) = \left(\frac{v}{2017}\right) = 1$ ja $\left(\frac{u}{2017}\right) = \left(\frac{v}{2017}\right) = -1$. Järeldus 8.6.

6. Teoreemi 2.2 tõestus polünoomiga $x^4 - x^2 + 1$. Teoreem 6.6 juhul $p \equiv 1 \pmod 4$ (lause 8.8) ja $p \equiv 1 \pmod 3$ (sest $\left(\frac{3}{p}\right) = 1$ parajasti siis, kui $p \equiv 1 \pmod 3$, miks?)

7. Olgu p otsitav algtegur ja $q = 2^{16} + 1$. Näidata, et $\mathrm{ord}_{U(\mathbb{Z}_p)}(12) = 2^{16}$, $p \geq q \in \mathbb{P}$, $\left(\frac{3}{q}\right) = -1$ ja $q \mid 12^{(2^{15})} + 1$ (teoreem 5.13, lause 8.7.)

8. Lemma 10.26. Teoreem 8.12. Olgu $x \equiv r \pmod p$, $ax \equiv s \pmod p$ ja $0 < r, s < p$. Permutatsioon $x \mapsto y$, kus

$$y = \begin{cases} n - s, & \text{kui } r < \frac{p}{2} < s \text{ või } r > \frac{p}{2} > s, \\ s, & \text{muudel juhutudel} \end{cases},$$

on paaris, miks?

On ka teisi tõestusi (vt Zolotarjovi lemma).