Kevad 2022

Vihjeid 14. praktikumiks

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

2. Lemma 8.4, lause 8.8, teoreem 8.14 (ruutvastavusseadus), teoreem 6.6 (HJT).

3. Laused 8.18 ja 8.21. Märkus 8.17.

4. Eraldada täisruut, korrutades/jagades kongruentsi sobiva arvuga läbi. Vaadelda tulemust sobivalt valitud algarvulise mooduli järgi. Märkus 8.17.

5. Tõestada ja kasutada fakti, et iga algjuur on mitteruutjääk. Leida mitteruutjääkide ja algjuurte arvud mooduli p järgi.

6. Vaadelda polünoomi $f(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$ väärtust kohal $x = 2 * q_1 \cdot \ldots \cdot q_s$.

7. Vastuväitelisel eeldusel on vahemikes $[0, \frac{p-1}{4}]$, $(\frac{p-1}{4}, \frac{p-1}{2}]$, $(\frac{p-1}{2}, \frac{3(p-1)}{4}]$ ja $(\frac{3(p-1)}{4}, p-1]$ liiga palju ruutjääke (kõik, iga teine, kolmas, neljas, või 1 vähem kui vahemik täpselt ei jagu), v.a. väikesed p väärtused, mida saab käsitsi kontrollida. Alternatiivselt, 2019. a. sarnane ülesanne.

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).