Kevad 2015

Märkusi arvuteooria 7. praktikumi kohta:

A. Kommentaare ülesannete kaupa:

1. Siin tuli lihtsalt rakendada lineaarkongruentside lahendamise teooriat natuke suurematele arvudele. Alternatiivina võis mooduli lahutada algteguriteks, lahendada lineaarkongruentsid iga osamooduli järgi ja panna vastus jälle HJT abil kokku, aga see on tavaliselt palju arvutusmahukam.

Veidi raskusi tekitasid pöördelemendi leidmine (ÄRGE kasutage valemit $\overline{a}^{-1} = \overline{a^{\varphi(n)-1}}$) ja kongruentsi võimalikult minimaalsele kujule viimine:

$$1218x \equiv 940 \pmod{2015}$$

on samaväärne kongruentsiga

$$609x \equiv 470 \pmod{2015}.$$

2. Hiina jäägiteoreemi abil kongruentside süsteemi lahendades on mugav kasutada tähistust

$$\overline{k_i} = (\overline{m_i}_{n_i})^{-1}.$$

3. Siin püüdsid mitmed minna järk-järgulise astendamise teed. Palju lihtsam on proovida mõne mooduli jaoks midagi võimatut järeldada, antud juhul näiteks

$$x \equiv 3 \pmod{8} \Longrightarrow x \equiv 3 \pmod{4}$$

ja

$$x \equiv 9 \pmod{28} \Longrightarrow x \equiv 9 \equiv 1 \pmod{4}.$$

4. ja 5. olid hästi tehtud.

6. Üldiselt ka kenasti lahendatud. Vastus ei olnud ühene, sest piisas lahendada süsteem

$$\begin{cases} x \equiv 0 & \pmod{p_1^2} \\ x+1 \equiv 0 & \pmod{p_2^2} \\ x+2 \equiv 0 & \pmod{p_3^2}, \end{cases}$$

kus p_1, p_2, p_3 on erinevad algarvud. Kui valida nendeks 2, 3 ja 5, siis saame vastuseks 548, 549, 550, aga järjekorda muutes võib saada ka $124, 125, 126$ (need jaguvad vastavalt arvudega 4, 25 ja 9).

7. Muutus *-ülesandeks, sest oli vaid kaks lahendajat. Iseenesest piisas lahenduseks vaid HJT rakendamisest süsteemile

$$\begin{cases} x \equiv 0 & (\mathrm{mod}\ p_1^n) \\ x+1 \equiv 0 & (\mathrm{mod}\ p_2^n) \\ \dots & \\ x+(n-1) \equiv 0 & (\mathrm{mod}\ p_n^n), \end{cases},$$

kus p_i on näiteks i-s algarv.

8. Põhimõtteliselt järgmise praktikumi ülesanne, mida sai lahendada ka otse järk-järgulist lahendamist (loengukonspekti näide 6.8) kasutades.

9. Paremate ülesannetega paistsid silma Rasmus (eriti raske, aga HJT-ga nõrgalt seotud ülesanne) ja Taisi (huvitavate lisaparameetritega humoorikas ülesanne).