Kevad 2014

Märkusi arvuteooria 7. praktikumi kohta:

A. Meil on nüüd esimesed kolmanda raskusastme lahendajad.

B. Läbivateks probleemideks olid pöördelementide leidmine ilma põhjendusteta (mis mõnikord ka vigu kaasa tõi), Hiina jäägiteoreemi asemel "järkjärgulise" meetodi kasutamine (mis on pikem ja vigadealtim), kongruentsi mõlema poole läbijagamine ilma moodulit läbi jagamata (vrdl. konspekti Lause 3.11) ja HJT eelduse (paarikaupa ühistegurita moodulid) kontrollimata jätmine.

Edaspidiseks tasub meelde jätta, et kui te näete kongruentsi kujul

$$ax \equiv ab \pmod{n},$$

siis sellest järeldub (juhul $(a, n) = 1$ on samaväärne) kongruents

$$x \equiv b \pmod{\frac{n}{(a, n)}}.$$

St. ei kehti, et kui $2x \equiv 2 \pmod 4$, siis ka $x \equiv 1 \pmod 4$; tõene on vaid $x \equiv 1 \pmod 2$.

Lisaks eelnevale esines ülesannete kaupa järgmisi tüüpvigu:

1. Eukleidese algoritmi asemel võeti teatud arvude suurim ühistegur "laest" või kasutati Euleri teoreemil põhinevat vähemefektiivset valemit. Arvutuslikult parem metoodika on Eukleidese algoritm.

2. Ei olnud põhjendatud, miks on vaja leida $[584, 116]$. See on juba 2. raskusastme viga.

4. "Järkjärguline" meetod ei ole siin kõige otstarbekam. Lihtsam on leida, et esimesest ja kolmandast kongruentsist järelduvad vastavalt, et $x \equiv 2 \equiv 0 \pmod 2$ ja $x \equiv 5 \equiv 1 \pmod 2$, mis ei saa korraga kehtida.

5. Millegipärast ei tahnud paljud Hiina kindralitega seotud ülesande korral Hiina jäägiteoreemi kasutada.

6. Siin võis peale "järkjärgulise" meetodi kasutada ka kongruentside elimineerimist. Näiteks

$$x \equiv 4 \pmod 6 \iff x \equiv 4 \equiv 0 \pmod 2 \quad \text{ja} \quad x \equiv 4 \equiv 1 \pmod 3,$$

mis järelduvad kongruentsidest $3x \equiv 4 \pmod 4$ ja $7x \equiv 16 \pmod 9$. Niiviisi saab lõpuks jõuda olukorrani, kus HJT rakendamine on võimalik, ja tehtav töö ei ole kuidagi suurem "järkjärgulise" meetodi omast.

8. Selle ülesande lahendas ära vaid üks üliõpilane, mistõttu sai sellest kahetärniülesanne. Aga see EI OLNUD mingis mõttes keeruline ülesanne ja põhiidee oli sama, mis eelmisel ülesandel (HJT üle algarvude).

9. Üldiselt oli ülesande püstitusest puudu nõue, et lahend peab olema minimaalne sobiv naturaalarv. Sel põhjusel ei olnud alati selge ülesande seos HJT-ga, mis mõnel puhul tingis ka punktist ilmajäämise.