Kevad 2014

Märkusi arvuteooria 6. praktikumi kohta:

A. Esimene uue kirjalike tööde hindamissüsteemi praktikum oli täiesti rahuldav, kedagi ei hinnatud veel rohkem kui 2. rangusastme järgi ja kuigi esines 3. rangusastme vigu, siis hetkel ei ole keegi veel 3. rangusastmele jõudnud. Tuletan meelde, et kuni 3. raskusastme vead ON eksamil eristatavad ja karistatavad (ühe-kahe punkti mahus).

Ja lõpuks õnnestus isegi üks kohalolev kirjalike lahenduste esitaja tahvli juurde meelitada...

B. Ülesannete kaupa esines seekord selliseid tüüpvigu:

1. Jäeti vaatlemata juht, kui arvul n ei ole standardkuju, st $n = 1$. See on 3. rangusastme (edaspidi RA) viga.

2. Enamasti tehti ülesannet efektiivselt, loengukonspekti lause 5.10 abil. Esines ka alternatiivseid variante, mis olid raskemini teostatavad ja jälgitavad. Üks esilekerkinud 3. RA viga oli see, et jäeti põhjendamata, kuidas leiti kõik need võimalikud kolmeteistkümnest väiksemad ühistegurid. Ja lahenduses ei ole muuseas vajalik leida arve $\frac{n}{d}$, sest meil on vaja ainult $\varphi(\frac{n}{d})$-d, mille me leiame standardkuju abil. Standardkuju tuleb aga n standardkujust vastava teguri ärajätmisel.

3. Paljud arvutasid lihtsalt kõik φ väärtused välja. Nii saab, aga lihtsam on kasutada Gaussi teoreemi (5.11) ja leida, et $S = 80 - \varphi(2) - \varphi(20) = 80 - 1 - 8 = 71$. Ja $\varphi(1) = 1$ definitsiooni põhjal, sest arvul 1 ei ole standardkuju.

4. Osutus kaunis raskeks ja seega *-ülesandeks. Kõigi juhtude ammendamine oli tõepoolest teatud kontsentreerumist nõudev töö ja selle kirjapanek ei rahuldanud alati 4. RA-d. Tärnülesannete korral muidugi enam rangusastmed ei loe ja oluline on vaid lahendus.

5. Vaja oli leida viimane kümnendnumber (see oli 7), mitte sajandnumber (mis oli 07 ehk samamoodi 7) ega kümneliste number (vastavalt 0). Järelikult piisas arvutamisest mooduli 10 järgi ja ei olnud vaja moodulit 100. Sellisel juhul lihtsustub tunduvalt lahenduse viimane samm, 3^{15} leidmine, sest $3^4 \equiv 1 \pmod{10}$. Samuti esines mitmes lahenduses üks 3. RA viga, milleks oli Euleri teoreemi eelduste (antud juhul $(3, 10) = 1$) kontrollimata jätmine.

6. Jälle 3. RA viga on mainimata jätmine, et $(7, 13) = 1$ (just seetõttu saame me järeldada, et kui $a^{12} \equiv b^{12} \pmod 7$ ja $a^{12} \equiv b^{12} \pmod{13}$, siis $a^{12} \equiv b^{12} \pmod{91}$). Samuti proovisid mitmed lahendajad lihtsalt juurida, st leiti, et $a^{72} = (a^{12})^6 \equiv (b^{12})^6 = b^{72} \pmod{91}$ ja seetõttu $a^{12} \equiv b^{12} \pmod{91}$. Isegi reaalarvude korral ei ole juured üheselt määratud ja jäägiklassides on juurimine väga keeruline teema. Puhtformaalselt näiteks $13^{72} \equiv 1 = 1^{72} \pmod{91}$, aga $13^{12} \not\equiv 1 = 1^{12} \pmod{91}$, kuigi meie ülesanne selle juhu välistab.

8. Jälle oli vaatlemata juht $n = 1$ ja tõestati vaid pool ülesannet, st kas piisavus või tarvilikkus. Väljend "parajasti siis" tähendab piisavust JA tarvilikkust. Esimene neist on 3., teine juba 1. RA viga.