Kevad 2015

Märkusi arvuteooria 16. praktikumi kohta:

A. Kuna tegu oli sisuliselt kordamisküsimustega, siis soovitan neil, kes kõiki 12 ülesannet vähemalt osaliselt ära ei lahendanud, tõsiselt kogu praktikumimaterjal üle vaadata. Eelnevate aastate kogemuste kohaselt tulevad eksamiülesanded kahjuks nii mõnelegi eksaminandile täiesti ootamatutena hoolimata kogu semestri jooksul tehtud tööst.

B. Kommentaare ülesannete kaupa:

1. Lahendamiseks oli mitu viisi, sealhulgas avaldise $(x+1)^4 - x^4$ mitmesugustel viisidel teisendamine. Lihtsaim variant on tähele panna, et x ja x^4 on sama paarsusega ning arvud x ja $x+1$ on eri paarsusega.

2. Ülesanne oli väga hästi lahendatud. Ainus asi, mida üldiselt ei tehtud, oli vastuse 4 pullvasikat ja 21 lehmvasikat kontroll:

$$4 \cdot 610 + 21 \cdot 360 = 10000.$$

3. Siin oli raskusi põhjendamisega, et iga ülesandes vaadeldav algarv on kujul $x \equiv 1, 3, 7, 9 \pmod{10}$. See on tegelikult kaunis ilmne, sest paarisarvulisi jääke ei saa x paarituse tõttu tulla ja jääk 5 annaks viiega jaguva arvu või algarvu 5, mis on samuti välistatud. Nüüd on lihtne arvutada $x^2 \equiv \pm 1 \pmod{10}$, mistõttu kas x^2+1 või x^2-1 annab kümnega jagamisel jäägi null ehk lõpeb arvuga null.

4. Antud ülesanne osutus kaunis raskeks. Lihtsaim lahendus on teisendada

$$3^{2n+1} + 2^{n+2} = 3 \cdot 9^n + 4 \cdot 2^n \equiv 3 \cdot 2^n - 3 \cdot 2^n = 0 \pmod{7}.$$

Alternatiivina võis kasutada fakti, et $\varphi(7) = 6$, seega $x^{6k+l} \equiv x^l \pmod{7}$ iga $k, l \in \mathbb{N}$ korral, ja veenduda, et väide kehtib $n = 1, 2, 3, 4, 5, 6$ korral.

5. Lahendamisel jäi tihti puudu põhjendus, miks

$$U(\mathbb{Z}_{40}) \cong U(\mathbb{Z}_5 \times Z_8) = U(\mathbb{Z}_5) \times U(Z_8)$$

(järeldus 4.9 ja lause 5.6, mis loengus olid üheks lauseks kokku võetud). Samuti kasutati viitamata lauset 4.15 (mis eksamil on veel andestatav). Tegelikult on antud ülesande lahendamiseks isegi erinevat meetodit (vt. 5. praktikumi tagasisidet).

Positiivsema poole pealt, mitu lahendajat tulid ise selle peale, et kontrollida oma vastust Euleri φ-funktsiooni abil: kokku pidi tulema $\varphi(4 \cdot 8) = 16$ pööratavat elementi ja $40 - 16 - 1 = 23$ nullitegurit.

6. Enamiku lahenduste probleem oli otse kõigi φ väärtuste leidmine. Gaussi teoreemi (teoreem 5.11) tõttu

$$1 + S = \sum_{d|6561} \varphi(d) = 6561,$$

seega $S = 6560$. Seda, et $6561 = 3^8$ kõik ühest suuremad jagajad ongi summas S esinevad arvud, peab muidugi ka põhjendama.

7. Tuli välja, et ülesande teksti teisendamine kongruentside süsteemiks

$$\begin{cases} x \equiv 5 \pmod 3 \\ x \equiv 8 \pmod 5 \\ x \equiv 3 \pmod 8 \end{cases}$$

oli küllaltki raske. Lahendit (siin $x \equiv 83 \pmod{120}$) tasub muuseas alati kontrollida.

8. Sellise ülesande puhul on hea kasutada Horneri skeemi nii proovimismeetodi jaoks algarvulise mooduli korral kui ka kordajate $f(x_i)$ ja $f'(x_i)$ leidmiseks, kui lahendada kongruentsi mingi algarvu kõrgema astme järgi. Lõppvastuse jaoks on üldine meetod küll Hiina jäägiteoreem, aga mõnikord saab ka lihtsamalt, näiteks $x \equiv 1 \pmod{125}$ ja $x \equiv 0 \pmod 2$ annavad kokku, et $x \equiv 126 \pmod{260}$, sest 126 on paarisarv arvudest 1 ja $1 + 125$.

Kontrollvastus: $x \equiv 1, 32, 94, 126, 157, 219 \pmod{250}$.

9. Soovitan üle vaadata 11. praktikumi ja selle tagasiside. Kui n on kujul p^k või $2 \cdot p^k$, $p \in \mathbb{P}$, siis ei ole otstarbekas kasutada järeldust 7.20. Parem on kasutada teoreeme 7.11, 7.15 ja 7.16.

Meenutan veel, et element $\overline{2} \notin U(\mathbb{Z}_{26})$, seega 2 ei saa olla algjuur mooduli 26 järgi. Lõpuks, järelduse 7.21 kasutamisel on alati hea kontrollivõimalus see, et algjuure a korral $a^{\frac{p-1}{2}} \equiv -1 \pmod p$. Kui see nii ei ole, siis olete midagi valesti teinud.

Kontrollvastus: a) 8 algjuurt, üks neist on 2; b) 4 algjuurt, üks neist on 15; c) 6 algjuurt, üks neist on 2; d) algjuuri ei ole.

10. Indekseerimine ja läbijagamine annavad, et $x \equiv 4 \pmod 6$. Vastuse võib-ki sellisele kujule jätta.

11. Ikka veel ei ole Jacobi sümboliga kõik korras. Kordan veelkord üle, kust abi saab: vastavate praktikumide tagasiside käesoleval ja eelmistel aastatel, 2014. a. näiteülesanne, loengukonspetki näide 8.15. Lahendusmeetodi põhimõtteks on järjest Jacobi sümbolit ruutvastavusseaduse abil pöörata, vahesammudena kahe astmeid eraldades ja mooduli järgi taandades.

Ikka veel ei ole kõigil selge, et meil ei ole sümbolit $\left(\frac{n}{2m}\right)$. Lahendussammude põhjendamine on kahjuks samuti jätkuvalt puudulik.

Kontrollvastus: $\left(\frac{7297}{4457}\right) = 1$.

12. Kuna eksamil arvutit kasutada ei saa, siis käsitsi tehes on üks optimaalne lahendus selline:

$$7^{14} = 49^7 \equiv (-2)^7 = -2^4 \cdot 2^3 = -16 \cdot 8 \equiv 1 \cdot 8 = 8 \pmod{17}.$$

Kandvaks ideeks on siin astendades võimalikult mooduli 17 lähedasi arve saada, eeltoodud näites on selleks $2^4 = 16$.