Kevad 2014

Märkusi arvuteooria 9. praktikumi kohta:

A. Praktikumi keskmine oli tänu kesisele osavõtule ja abstraktsetele ülesannetele veidi üle 2! See on tõsine ohumärk. Mina ei saa teie eest ülesannete lahendamise oskust omandada, aga ma saan anda konsultatsioone, kui selleks vajadus tekib. Kui te tunnetate seda vajadust, siis tehke mulle vastav ettepanek (soovitatavalt koos teiste sama meelt kuulajatega).

B. Seekord siis sellised kommentaarid ülesannete kaupa:

1. Elemendil $\overline{8}$ ei ole järku rühmas $U(\mathbb{Z}_{26})$, sest ta ei kuulu sellesse rühma (kuna $(8, 26) \neq 1$). Elemendi $\overline{a}$ astmete leidmisel on lihtsam kasutada vastavat absoluutväärtuselt vähimat arvu (nt. $\overline{21} = \overline{-5}$ mooduli 26 järgi). Kui te olete jõudnud faktini, et ükski astmetest $\overline{a}^k$, $k = 1, 2, \ldots, \frac{\varphi(n)}{2}$ ei ole $\overline{1}$, siis edasi ei tasu astendada, sest elemendi järk saab olla vaid $\varphi(n)$ jagaja ning vastav jagatis q ei saa olla vahemikus $2 > q > 1$. Ning alati $\overline{a}^{\varphi(n)} = \overline{1}$.

2. Lihtne viis seda ülesannet lahendada on panna tähele (ja tõestada ära), et

- 2 on algjuur mooduli 53 järgi;
- kaardi nr. x järjekorranumber peale segamist on $2x \pmod{53}$.

Seega on meil vaja leida vähim arv m, mille korral $\underbrace{2 \cdot 2 \cdot \ldots \cdot 2}_{\text{m}} x \equiv x \pmod{53}$, iga $x = 1, 2, \ldots, 52$ puhul. Tänu sellele, et $x = 1, 2, \ldots, 52$ on kõik pööratavad mooduli 53 järgi, on samaväärne sellise vähima naturaalarvu m leidmine, mille korral $2^m \equiv 1 \pmod{53}$. Kuna 2 on algjuur, peab kehtima $m = \varphi(53) = 52$.

3. IGA pööratava elemendi korral tuli ARVULISELT välja leida tema astmed (nt. $5^1 = 5, 5^2 \equiv 7, 5^3 \equiv 8, 5^4 \equiv 4, 5^5 \equiv 2, 5^6 \equiv 1$ mooduli 9 järgi), või ainult järelduse 7.21 kohaselt vajalikud astmed (nt. $5^2 \equiv 7, 5^3 \equiv 8$ mooduli 9 järgi). Ei tohtinud kasutada teoreemi 7.18. Sellest ei piisa, et te kirjutate, et $U(\mathbb{Z}_9) = \{\overline{5}, \overline{5}^2, \overline{5}^3, \overline{5}^4, \overline{5}^5, \overline{5}^6\}$, astmeid välja ei arvuta ja ülejäänud mitte-algjuurtega ei tee mitte midagi. Kontrolli jaoks on väga kasulik järeldus 7.24, st. algjuurte olemasolul on neid $\varphi(\varphi(n))$ tükki.

4. Ülesanne oli mõeldud nii, et te leiate KÕIGI ringi $\mathbb{Z}_{12}$ elementide astmed (nt. $2, 2^2 = 4, 2^3 = 8, 2^4 \equiv 4, \ldots$, seega 2 ei saa järku omada ega algjuur olla, $5, 5^2 \equiv 1$, seega 5 on 2. järku element, aga $|U(\mathbb{Z}_{12})| = 4$, jne).

5. Siin sai kas välja arvutada kõik 3 astmed esimesest 42-ni, või kasutada järeldust 7.21 (vajalikud astmed on $3^6 \equiv 41, 3^{14} \equiv 36$ ja $3^{21} \equiv 42$). Siis tuli teha asendus $x = \overline{3}^k$ (sest 3 on algjuur ja 0 ilmselt ei sobi lahendiks ning kuna 43 on algarv, on muud elemendid pööratavad ja järelikult algjuure 3 astmed). Kui nüüd rakendada lemmat 4.3 juhule $(3^k)^7 \equiv 1 \pmod{43}$, siis saame, et $42 \mid 7k$ ehk $6|k$. Kuna $k \in \{1, 2, \ldots, 42\}$, siis $k = 6, 12, 18, 24, 30, 36, 42$ ja

$$x \in \{\overline{3}^6 = \overline{41}, \overline{3}^{12} = \overline{4}, \overline{3}^{18} = \overline{35}, \overline{3}^{24} = \overline{16}, \overline{3}^{30} = \overline{11}, \overline{3}^{36} = \overline{21}, \overline{3}^{42} = \overline{1}\}.$$

Ilmselt need kõik ka rahuldavad antud võrrandit. Muuseas on siit näha, et korpuses $\mathbb{Z}_{43}$ on 7. astme polünoomvõrrandil $x^7 = 1$ tõepoolest 7 lahendit.

6. Esitati Ellen Redi arvuteooria õpiku lahendust, mida aga ei suudetud alati korrektselt juhule $k = 2$ tagasi viia. Rõhutan siin veel kord, et elemendi a aste on m siis, kui $a^m = 1$ JA kõigi $n < m$ korral $a^n \neq 1$. Võrdus $a^m = 1$ ütleb lihtsalt seda, et elemendi a järk on arvu m jagaja (vt. lemma 7.3). Lahenduste vähesuse tõttu on see ülesanne tärnülesanne.

7. Sama probleem, aga lisaks on E. Redi tõestus vigane. Lahendajaid oli ülimalt üks, seega on tegu kahetärniülesandega. Selle juurde tuleme järgmises praktikumis veel tagasi.

8. Kuidagi oli vaja näidata, et kui algarvulise mooduli p korral $-1 \equiv \pmod{p}$, siis $p \equiv 1 \pmod 4$ ehk $p = 4k + 1$ mingi täisarvu k korral. Seda saab teha algjuurte kaudu, ruutjääkide teooria abil või ka vähemalt ühel elementaarsemal viisil. Edasine on väga sarnane juhu $4k - 1$ tõestusele. Kuna õigeid lahendusi oli vaid üks, siis on see kahetärniülesanne.

9. Esiteks oli ülesande sõnastuses nõutud algjuurte kasutamist. Seda ülesannet saab lahendada ka ilma algjuurteta, aga selle eest punkte ei saanud. Ja algjuuri sisaldavates lahendustes jäeti üldiselt vahele põhjendus, miks algjuure a korral $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ (sest $b = a^{\frac{p-1}{2}}$ korral $b \neq 1$, muidu a ei oleks algjuur; $b^2 = 1$ ja võrrandil $x^2 - 1 = 0$ on vaid kaks lahendit, 1 ja -1, kuna $\mathbb{Z}_p$ on korpus, vt. lause 2.9).