Kevad 2014

Märkusi arvuteooria 10. praktikumi kohta:

A. Praktikumi keskmine tõusis jälle normaalsele tasemele tagasi. Loodetavasti tähendab see, et lihtsalt semestri keskel olnud kontrolltööd jmt. võtsid hoo korraks maha ja nüüdseks on kõik kuulajad algjuurtega ikkagi enamvähem tuttavad.

B. Tulevikku vaadates võib ennustada, et eksamile pääsemise piir saab olema umbes 32 punkti ja lisapunktide omad vastavalt 63, 95, 126, 189 ja 252.

C. Üks terminoloogiline märkus: õige on öelda "algjuur mooduli n järgi", MITTE "arvu n algjuur".

D. Kommentaare ülesannete kaupa:

1. Algjuureks oleku kontroll mingi konkreetse (alg)arvu korral käib järelduse 7.21 abil. Seega algjuure kandidaadi a korral tuleb kontrollida, kas $a^{\frac{\varphi(n)}{q}} \equiv 1 \pmod{n}$ kõigi $\varphi(n)$ ALGTEGURITE q korral. Näiteks 37 jaoks on $\varphi(37) = 36 = 2^2 \cdot 3^2$ ja tuleb uurida arve $a^{\frac{36}{2}} = a^{18}$ ja $a^{\frac{36}{3}} = a^{12}$. Aga ka 4. ülesandes esineva mooduli 81 korral saab teha sama: $\varphi(81) = 54 = 2 \cdot 3^3$ ja tuleb uurida arve $a^{\frac{54}{2}} = a^{27}$ ja $a^{\frac{54}{3}} = a^{18}$. Viimasel juhul on lihtsalt efektiivsem leida algjuur mooduli 3 järgi, sealt mooduli 3^2 järgi, ja viimane on alati algjuur mooduli $3^4 = 81$ järgi. EI OLE VAJA uurida kõiki $\varphi(n)$ jagajaid, 37 korral siis astendajaid $1, 2, 3, 4, 6, 9, 12, 18, 36$, piisab maksimaalsetest $\varphi(n)$-st väiksematest astendajatest, ehk arvudest 12 ja 18. Muuseas, kordan veel kord üle, et iga $\overline{a} \in U(\mathbb{Z}_n)$ korral $a^{\varphi(n)} \equiv 1 \pmod{n}$ (Euleri teoreem). Lisaks, ei ole tarvis iga potentsiaalse algjuure korral rakendada järeldust 7.21. See on lihtsalt liialt arvutusmahukas. Piisab, kui leida üks algjuur a, näiteks mooduli 37 korral sobib 2, sest $2^{18} \equiv 36 \not\equiv 1 \pmod{37}$ ja $2^{12} \equiv 26 \not\equiv 1 \pmod{37}$. Siis kõik algjuured avalduvad kujul a^k, $1 \leq k \leq \varphi(n), (k, \varphi(n)) = 1$ (loengus olnud variant järeldusest 7.10). Mooduli 37 korral on sobivad astendajad k järgmised: 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35 ja seega algjuurteks on $2^1 \equiv 2$, $2^5 \equiv 32$, $2^7 \equiv 17$, $2^{11} \equiv 13$, $2^{13} \equiv 15$, $2^{17} \equiv 18$, $2^{19} \equiv 35$, $2^{23} \equiv 5$, $2^{25} \equiv 20$, $2^{29} \equiv 24$, $2^{31} \equiv 22$ ja $2^{35} \equiv 19 \pmod{37}$.

2. See ülesanne on väga hea näide üldise algjuurte leidmise algoritmi kohta. Esiteks, leiame ühe algjuure mooduli 17 järgi. Kuna üldiselt on suhe $\varphi(n) : n$ "suur", siis võime lihtsalt järgemööda proovida arve $a = 2, 3, 4, \ldots$ ja tõenäosus igal sammul algjuurt leida on küllaltki hea. Selleks rakendame järeldust 7.21. Kuna $\varphi(17) = 16 = 2^4$, siis peame kontrollima, kas $a^{\frac{16}{2}} = a^8 \equiv 1 \pmod{17}$. Kui see ei ole nii, siis olemegi leidnud algjuure. Vaatame: $2^8 = 4^4 = 16^2 \equiv (-1)^2 = 1 \pmod{17}$. Seega 2 ei ole algjuur. Aga $3^8 = 9^4 = 81^2 \equiv (-4)^2 = 16 \not\equiv 1 \pmod{17}$ ja 3 on algjuur. Nüüd saame mooduli 17^2 jaoks kasutada järeldust 7.12. Meil tuleb võtta $b \in \{3, 3 + 17 = 20\}$ ning uurida, kas $b^{17-1} \equiv 1 \pmod{17^2 = 289}$. Kuna $3^{16} \equiv 171 \not\equiv 1 \pmod{289}$, on 3 algjuur ka mooduli 17^2 järgi. Teoreemi 7.15 tõttu on 3 algjuur iga mooduli 17^k, $k > 2$, järgi. Kokkuvõttes on 3 seega algjuur kõigi moodulite 17^k, $k \in \mathbb{N}$, järgi. Lõpuks saame kasutada teoreemi 7.16. Kuna arvudest 3 ja $3 + 17^k$ on paaritu arv 3, siis 3 on algjuur iga mooduli $2 \cdot 17^k$, $k \in \mathbb{N}$, järgi.

3 ja 4. Esiteks. alati on hea viia moodul standardkujule. Kui te lihtsalt kirjutate "...ei ole kujul 2,4,p^k ega $2p^k$", siis te võite eksida, ja isegi kui te ei eksi, siis ei ole mul mingit võimalust kontrollida, kas te tõesti mõtlesite ise selle peale, kuulasite kellegi nõuannet või lihtsalt kirjutasite selle lause lootuses, et ükskord peab see ikka õige olema. Lisaks esimese kahe ülesande kohta käivatele märkustele tuleb esile tuua seda, et järeldus 7.21 ei kehti otseselt mitte-algarvuliste moodulite korral. Kehtib selle modifitseeritud variant, kus $p-1$ asemel on $\varphi(n)$. Aga seda varianti kordarvulise mooduli korral rakendades tuleb üldiselt teha rohkem arvutustööd, kui 2. ülesandes toodud skeemi järgides.

5. Osutus väga raskeks, kahetärniülesandeks. Tegelikult on see ülesanne erijuht järgmise peatüki teoreemist 8.18.

6 ja 7. Siin sai kasutada ülesannet 2 (3 on algjuur mooduli 17 järgi) ja ülesannet 5. Seda ülesannet lahendati mõnikord kõiki variante läbi proovides, aga efektiivne lahendusviis on võtta $\overline{13} = \overline{3}^4$, $\overline{x} = \overline{3}^k$ ja kasutada lemmat 7.3 või E. Redi õpiku alajaotuse 7.2 omadust 3, mille kohaselt taanduvad esialgsed kongruentsid kongruentsideks $20k \equiv 4 \pmod{17-1}$ ja $24k \equiv 4 \pmod{17-1}$. Lause 6.2. kohaselt on esimesel neist $\frac{16}{(16,20)} = 4$ lahendit, milleks on $k = 1, 5, 9, 13$, ja teisel ei ole lahendeid, sest $(16, 24) = 8 \not| 4$. Seega on esimese kongruentsi lahenditeks $x \equiv 3^k \pmod{17}$, $k = 1, 5, 9, 13$, ehk jäägiklassid $\overline{3}, \overline{5}, \overline{12}$ ja $\overline{14}$.

8. Tuli välja, et ka see ülesanne sai ühe tärni juurde, sest õigeid lahendusi oli ainult kolm tükki. Seda ülesannet sai ohutult, aga arvutusmahukalt lahendada Horneri skeemiga. Samas on olemas ka parem lahendus: kuna $1+x+x^2+2^3+2^4+2^5+2^6=\frac{x^7-1}{x-1}$, ja ilmselt 1 ei ole selle kongruentsi lahend, siis võime samaväärselt lahendada kongruentsi $x^7 \equiv 1 \pmod{43}$ ning välja jätta lahendi 1. Seda kongruentsi lahendasime me me 9. praktikumi 5. ülesandes ja ühest erinevad lahendid, ehk käesoleva ülesande lahendid, on seega $\overline{4}, \overline{11}, \overline{16}, \overline{21}, \overline{35}$ ja $\overline{41}$.

9. Üldiselt saadi järgu mõistest juba hästi aru ja ülesanne suuri probleeme ei valmistanud. Aga väga sageli jäeti põhjendamata (3. RA viga), miks kongruentsil $x^2 = 1 \pmod{p}$ on vaid kaks lahendit, 1 ja -1. See väide ei kehti suvalise mooduli korral, näiteks $1^2 \equiv 1, (-1)^2 \equiv 1, 5^2 \equiv 1$ ja $(-5)^2 \equiv 1 \pmod{24}$.