Kevad 2016

Märkusi arvuteooria 4. praktikumi kohta:

A. Esmalt kolmanda praktikumi ülesannetest:

7. ülesanne muutus *-ülesandeks, sest selle lahendasid ära vaid kaks üliõpilast. Seetõttu toon siinkohal ära täieliku lahenduse:

On lihtne kontrollida, et arvud $1, 2, \ldots, 15$ on alati võimalik algarvu liites muuta täisruuduks:

$$1 + 3 = 2^2, 2 + 2 = 2^2, 3 + 13 = 4^2, 4 + 5 = 3^2 \text{ jne.}$$

Arvuga 16 seda aga teha ei õnnestu, seega tekib hüpotees, et otsitavaks arvuks on 16. Järelikult piisab, kui me tõestame, et $16 + p$ ei ole ühegi $p \in \mathbb{P}$ korral täisruut.

Viimase näitamiseks oletame vastuväiteliselt, et leiduvad sellised $a \in \mathbb{N}$ ja $p \in \mathbb{P}$, et $16 + p = a^2$. Kuid siis

$$p = a^2 - 4^2 = (a - 4)(a + 4).$$

Algarvu p jagajateks on vaid ± 1 ja $\pm p$, järelikult kas $a - 4 = 1$, $a - 4 = -1$, $a + 4 = 1$ või $a + 4 = -1$. Neile võimalustele vastavad p väärtused on

$$(\pm 3)^2 - 16 = -7 \quad \text{ja} \quad (\pm 5)^2 - 16 = 9,$$

mis ei ole algarvud. Seega niisuguseid arve a ja p leiduda ei saa ja järelikult on 16 vähim ülesande tingimustele vastav arv.

8. ülesande lahendustes oli pisemaid ebakõlasid (nt. jäeti mõnikord põhjendamata, miks $p_{n+1} \leq p_1 \cdot \ldots \cdot p_n$), aga üldiselt suuri probleeme ei olnud. Lahenduse võtmeks oligi eelmainitud tähelepanek, mis pärineb Eukelidese tõestusest algarvude hulga lõpmatuse kohta.

Alternatiivina võis kasutada Bertrand'i postulaati, millest järeldub, et $p_{n+1} < 2p_n$.

B. Kommentaare ja tüüpvigu ülesannete kaupa:

1. Selle ülesandega raskusi ei olnud, ainsad pisivead võisid olla järeldusele 3.12 või mõnele analoogile (nt. Eukleidese lemma) viitamata jätmine ja natuke lakoonilised mõttekäigud (loe: kui ma arutlust paberil ei näe, siis ma selle

eest punkte ka ei anna; eksamil saab ülesannete eest rohkem kui ühe punkti ja nii võib paar tükki neist kaotsi minna).

2. Lihtsaim lahendus oli kirja panna jäägid mooduli 12 järgi (st. $0, 1, \ldots, 11$) ning järgemööda parameetrite väärtusi valides püüda neist võimalikult paljusid katta. Näiteks valime $a = 1$, siis paaritud arvud rahuldavad kongruentsi $x \equiv 1 \pmod 2$ ja meil tuleb edaspidi tegeleda vaid paarisarvudega. Võtame $c = 2$, siis saavad haaratud $\overline{2}, \overline{6}$ ja $\overline{10}$, jne. Seda tehti mitmel mõnikord kaunis pikal ja segasel viisil (praktikumis maatriksina, kirjalikes lahendustes järjepanu abstraktselt jääke analüüsides). Vastus ei ole ühene ja valikuvabadus on seejuures suhteliselt suur.

3. Üldiselt väga hästi lahendatud ülesanne. Siin oli kaks põhilist lähenemist:

- leida, millega on kongruentsed ruudud mooduli 4 järgi ja millega saab seetõttu olla kongruentne ruutude summa;
- kasutada asjaolu, et arvud m ja n on eri paarsusega.

Tegelikult on see väide nii piisav kui tarvilik ja on tuntud kui Fermat' teoreem kahe täisruudu summadest.

4. Peamiseks puuduseks oli kas abitulemuste (nt. $\binom{p}{k} = \binom{p-1}{k} + \binom{p-1}{k-1}$, või $p \mid \binom{p}{k}$, kui $1 \leq k < p$, viimane on loengukonspektis kirjas lemmana 7.14) või $k!$-ga jagamise (modulo p) lubatavuse põhjendamata jätmine. Kui te kasutate mingit fakti, mis ei sisaldu kas keskkoolikursuses või matemaatika eriala kohustuslikes ainetes, siis on parem seda põhjendada või vähemalt mult küsida, kas seda peab põhjendama. Samuti oli märgata, et mitmed lahendajad olid oma lahenduskäigu suhteliselt mitteoptimaalselt kirja pannud (loe: kui te kasutate kellegi teise lahendusideed – mida ei ole keelatud teha – siis vähemalt jätke selline mulje, et olete ise selle peale tulnud).

Kõige lihtsam lahendusviis on umbes selline (Alvin):

Kehtib

$$\binom{p-1}{k} = \frac{(p-1)!}{k!(p-k-1)!} = \frac{(p-1)(p-2)\ldots(p-k)}{k!}$$

Et $p \mid 0 = k - k$, siis:

$$p-1 \equiv -1 \pmod p, p-2 \equiv -2 \pmod p, \ldots, p-k \equiv -k \pmod p.$$

Lause 3.7 põhjal:

$$(p-1)(p-2)\ldots(p-k) \equiv (-1)^k k! \pmod p$$

Vaatleme järgmist olukorda:

$$\binom{p-1}{k} k! = (p-1)(p-2)\dots(p-k) \equiv (-1)^k k! \pmod{p}$$

Et $k < p$, siis $(k!, p) = 1$ ning lause 3.11 põhjal:

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}$$

nagu tarvis.

5. Jääb järgmisesse praktikumi.

6. Samuti hästi lahendatud ülesanne. Arvutusi saab veidi optimeerida umbes nii:

$2015^{16} \equiv (14^2)^8 = 196^8 \equiv 11^8 = 121^4 \equiv 6^4 = 36^2 \equiv (-10)^2 = 100 \equiv 8 \pmod{23}$,
$2017^{32} \equiv 16^{32} = (-7)^{32} = 49^{16} \equiv 3^{16} = (81)^4 \equiv (-11)^4 = 121^2 \equiv 6^2 = 36 \equiv 13 \pmod{23}$,
$(8+13)^7 = (-2)^7 = -2^7 = -128 \equiv 10 \pmod{23}$.

Selliste ülesannete jaoks kasulikud arvutusvõtted on astmete järjest arvutamine, näiteks $(-2)^5 = (-2)^4 \cdot (-2)$, absoluutväärtuselt väiksema jäägi kasutamine, teadaolevate mooduli kordsetele lähedaste vahetulemuste soosimine. Näiteks leides $10^7 \pmod{11}$, võib kasutada $1001 = 7 \cdot 11 \cdot 13$ ja arvutada

$$10^7 = 10^3 \cdot 10^3 \cdot 10 \equiv (-1)^3 = -1 \equiv 10 \pmod{11}.$$

7. Veel üks ilusasti lahendatud ülesanne. Kontrolli mõttes märgin, et kui kasutada lause 3.14 kriteeriumit 3., siis "vahelduvate märkidega ristsumma" tuleb ± 825.

8. Seda ülesannet lahendati mitmel *ad hoc* viisil, mis kas suurendasid tehtavat tööd või tekitasid kahtlusi vastuse korrektsuses. Seega toon siin ära ühe töötava ja kergelt üldistatava lahendusmeetodi:

Ülesande tingimuste kohaselt

$$99 \mid 1000x + 680 + y - 8.$$

Järelduse 4.3 kohaselt jagub arv 99-ga parajasti siis, kui ta jagub arvudega 9 ja 11. Sõltuvalt sellest, kas $y \geq 8$ või $y < 8$, tekib meil lause 3.14 abil kaks võimalust:

$$\begin{cases} y \in \{8, 9\} \\ 9 \mid x + 6 + 8 + (y - 8) \\ 11 \mid x - 6 + 8 - (y - 8) \end{cases} \iff \begin{cases} y \in \{8, 9\} \\ 9 \mid x + y + 6 \\ 11 \mid x - y - 1 \end{cases}$$

või

$$\begin{cases} 0 \le y \le 7 \\ 9 \mid x+6+7+(2+y) \\ 11 \mid x-6+7-(2+y) \end{cases} \iff \begin{cases} 0 \le y \le 7 \\ 9 \mid x+y+6 \\ 11 \mid x-y-1 \end{cases}.$$

Kokkuvõttes alati

$$\begin{cases} 9 \mid x+y+6 \\ 11 \mid x-y-1 \end{cases}.$$

Kuna $1 \le x \le 9$ ja $0 \le y \le 9$, siis $x+y+6 \in [7,24]$ ning $x-y-1 \in [-9,8]$. Nendes vahemikes on vastavalt 9 või 11 kordseteks vaid 9 ja 18 ning 0, seega saame, et tuleb lahendada võrrandisüsteemid

$$\begin{cases} x+y+6=18 \\ x-y-1=0 \end{cases} \iff \begin{cases} y=12-x \\ 2x+5=18 \end{cases} \iff \begin{cases} x=6\frac{1}{2} \\ y=5\frac{1}{2} \end{cases}$$

ja

$$\begin{cases} x+y+6=9 \\ x-y-1=0 \end{cases} \iff \begin{cases} y=3-x \\ 2x+5=9 \end{cases} \iff \begin{cases} x=2 \\ y=1 \end{cases}.$$

Ainukesed täisarvulised lahendid on järelikult $x=2$ ja $y=1$, ehk arve oli kokku 2681 reaali. Kuna $2681-8=2673=99\cdot 27$, siis kulutas iga piraat rummile 27 reaali, mis kapteni arvestuste tõttu tähendab kas üheksat pudelit à 3 reaali või 27 pudelit à 1 reaal. Hoolimata piraatide kuulsusest rummihävitajatena oletan ma, et esimene variant on tõenäolisem.