Kevad 2015

Märkusi arvuteooria 4. praktikumi kohta:

A. Neljanda praktikumi ülesanded olid tegelikult väga hästi tehtud. Kuigi keskmine oli veidi madalam, kui teises praktikumis, saavutati see ilma tärnülesannete punktideta ja valdav enamus sai vähemalt kuus punkti. Hästi tehtud!

B. Kommentaare ülesannete kaupa:

1. Lihtsaim ja efektiivseim lahendus oli kasutada vähima ühiskordse definitsiooni. Aga sai kasutada ka keerulisemat mõttekäiku, mis demonstreerib mitmesuguseid kasulikke võtteid, mida võib edaspidi vaja minna, näiteks fakti, et

$$[n_1, n_2] = d \cdot n_1' \cdot n_2',$$

kus $d = (n_1, n_2)$, $n_1 = d \cdot n_1'$ ja $n_2 = d \cdot n_2'$. Niisugust lahendust kasutasid Andre Ostrak ja Agnes Lepikult, kes said selle eest mõlemad ühe lisapunkti. Agnese lahendus oli järgmine (sealt on puudu, et $d \neq 0$, sest juht $n = n_1 = n_2 = 0$ on ilmselt tõene):

Lahendus: Peame näitama, et leidub selline $k \in \mathbb{Z}$, et $b - a = kn$ (kongruentsuse definitsioon). Kuna $a \equiv b \pmod{n_1}$ ja $a \equiv b \pmod{n_2}$, siis leiduvad kongruentsuse definitsiooni kohaselt sellised m_1, m_2, et $b - a = n_1 m_1$ ja $b - a = n_2 m_2$. Siis $n_1 m_1 = n_2 m_2$. Olgu $d = (n_1, n_2)$, siis leiduvad n_1', n_2', et $n_1 = dn_1'$ ja $n_2 = dn_2'$ ning $(n_1', n_2') = 1$. Teeme asenduse ja saame, et $m_1 dn_1' = m_2 dn_2'$ ehk $m_1 n_1' = m_2 n_2'$. Kuna $n_2' \mid m_1 n_1'$ ja $(n_1', n_2') = 1$, siis Eukleidese lemma põhjal $n_2' \mid m_1$. Jaguvuse definitsiooni põhjal leidub selline $k \in \mathbb{Z}$, et $m_1 = kn_2'$.

$$b - a = m_1 n_1 = kn_2' n_1 = kn_1 \frac{n_2}{d} = k \frac{n_1 n_2}{(n_1, n_2)}.$$

Lause 1.21 põhjal $n = [n_1, n_2] = \frac{n_1 n_2}{(n_1, n_2)}$. Seega $b - a = kn$ ehk $a \equiv b \pmod{n}$.

2. Üldiselt oli ülesanne kenasti lahendatud paarsuste kontrolli abil. Alternatiivselt võis siin kasutada kongruentse modulo 4. Kuna $0^2 = 0 \equiv 2^2 \pmod 4$ ja $1^2 = 1 \equiv 3^2 \pmod 4$, siis iga $a \in \mathbb{Z}$ korral $a^2 \equiv 0, 1 \pmod 4$. Seega

$a^2+b^2 \equiv c \pmod 4$, kus $c \in \{0+0=0, 0+1=1+0=1, 1+1=2\}$ ja me ei saa kunagi ruutude summat kongruentseks arvuga 3, ehk neljaga jagades jääki 3.

3. Seegi ülesanne oli hästi lahendatud. Ainus asi, mis puudu võis jääda, oli viide Eukleidese lemma järeldusele 1.10, kust

$$(p \in \mathbb{P} \wedge p \mid (a-b)(a+b)) \Longrightarrow (p \mid (a-b) \vee p \mid (a+b)).$$

4. Siin peaaegu keegi ei öelnud otse välja, et arv saab olla ruut ja neljas aste parajasti siis, kui ta on neljas aste. Kõik lahendajad leidsid seejärel lihtsalt kõikvõimalikud neljandad astmed modulo 20, tehes mõnikord liiga palju tööd ja arvutades eraldi välja näiteks $9^4 = 81^2 \equiv 1^2 = 1 \pmod{20}$ ja $11^4 = 121^2 \equiv 1^2 = 1 \pmod{20}$. Tegelikult $11^4 \equiv (-9)^4 = 9^4 \equiv 1 \pmod{20}$ ja me oleks kohe võinud leida $(\pm 9)^4 \pmod{20}$.

Alternatiivina võib arvutada neljandaid astmeid modulo 4 ja 5, sest $20 = 4 \cdot 5$. Sel juhul $0^4 = 0, (\pm 1)^4 = 1, (\pm 2)^4 = 16$ ja kuna $16 \equiv 1 \pmod 5$ ning $16 \equiv 0 \pmod 4$, siis on neljandad astmed modulo 20 alati kongruentsed kas nulli või ühega nii mooduli 4 kui mooduli 5 järgi. Üks variant siit jätkata oleks lahendada Hiina jäägiteoreemi abil kongruentside süsteemid

$$\begin{cases} x \equiv 0 \pmod 4 \\ x \equiv 0 \pmod 5 \end{cases}, \begin{cases} x \equiv 0 \pmod 4 \\ x \equiv 1 \pmod 5 \end{cases}, \begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 0 \pmod 5 \end{cases}$$

ja

$$\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 1 \pmod 5 \end{cases}.$$

Kuna meil ei ole veel Hiina jäägiteoreemi olnud ja moodul on väike, siis toimime niiviisi: kõik arvud modulo 20, mis on kongruentsed ühe või nulliga modulo 5, on 0,5,10,15,1,6,11,16. Kuna $10 \equiv 6 \equiv 2 \pmod 4$ ja $11 \equiv 15 \equiv 3 \pmod 4$, siis vastuseks sobivad vaid $0, 5, 1$ ja 16, nagu soovitud.

5. Ülesanne lahendati enamjaolt kenasti ära, aga seejuures tehti tihti ebavajalikke arvutusi liiga suurte arvudega. Mooduli järgi arvutamise eelis ongi see, et me saame alati minna vähimale jäägile ja teha tehteid ainult moodulist väiksemate arvudega. Ja ruute on arvutuslikult lihtsam leida, kui kuupe, mille abil paljud lahendajad leidsid 7^9.

Üks optimaalne arvutuskäik: kuna $2014 = 87 \cdot 23 + 13 \equiv 13 \pmod{23}$, siis $2016 = 2014 + 2 \equiv 13 + 2 = 15 \pmod{23}$. Järelikult

$$2014^{16} \equiv 13^{16} = 169^8 \equiv 8^8 = 64^4 \equiv 18^4 \equiv (-5)^4 = 25^2 \equiv 2^2 = 4 \pmod{23},$$

$$2016^{32} \equiv 15^{32} = 225^{16} \equiv (-5)^{16} = 2^8 = 4^4 = 16^2 \equiv (-7)^2 = 49 \equiv 3 \pmod{23}$$

ja

$$\begin{aligned}(2014^{16} + 2016^{32})^9 &\equiv 7^{8+1} = 7 \cdot 7^8 = 7 \cdot 49^4 \equiv 7 \cdot 3^4 = 7 \cdot 9^2 \\ &= 7 \cdot 81 \equiv 7 \cdot 12 = 84 \equiv \mathbf{15} \pmod{23}.\end{aligned}$$

Märkus TEX-is tasub astendamisel alati kasutada loogelisi sulge, muidu tekivad kirjutised `2014^16`↦ 2014^16 korrektse `2014^{16}`↦ 2014^{16} asemel.

6. Selle ülesande juures jäid põhjendused tihti poolikuks. Üks võimalik terviklik lahendus on selline: kuna meil on vaja leida paarisarvud $\underline{abc}$, mis jaguvad arvuga 18, siis $a, b, c \in 0, 2, 4, 6, 8$, $a \neq 0$ ja üheksaga jaguvuse tunnuse põhjal $9 \mid a + b + c$, sest $18 = 2 \cdot 9$, $(2, 9) = 1$ ja $\underline{abc}$ jagub c paarisarvuks oleku tõttu alati kahega. Piirangu $a, b, c \in 0, 2, 4, 6, 8$, $a \neq 0$ tõttu $2 = 2 + 0 + 0 \leq a + b + c \leq 8 + 8 + 8 = 24$. Selles vahemikus on vaid kaks üheksaga jaguvat arvu, nimelt 9 ja 18, aga esimene neist ei saa olla kolme paarisarvu summa. Seega oleme taandanud esialgse ülesande sellise kolme arvu $a, b, c \in 0, 2, 4, 6, 8$, $a \neq 0$ leidmisele, mille summa oleks 18. Võttes järjest $a = 8, 6, 4, 2$, $b = 8, 6, 4, 2, 0$ ja peame silmas, et $c < 10$ saame, et

$$\begin{aligned}18 &= 8 + 8 + 2 = 8 + 6 + 4 = 8 + 4 + 6 = 8 + 2 + 8 = 6 + 8 + 4 \\ &= 6 + 6 + 6 = 6 + 4 + 8 = 4 + 8 + 6 = 4 + 6 + 8 = 2 + 8 + 8.\end{aligned}$$

Seega otsitavad arvud on 288, 468, 486, 648, 666, 684, 828, 846, 864 ja 882.

7. Samamoodi olid põhjendused veidi lünklikud. Väga ilusa lahenduse esitas jälle Agnes, mille eest ta sai lisapunkti ja mille ma siinkohal ära toon:

Lahendus: Arv jagub 11-ga, kui tema vahelduvate märkidega numbrite summa jagub 11-ga. Suurim võimalik arv, mille saab antud numbritest moodustada (juhul kui pooled neist on negatiivsed), on $6-3+5-2+4-1 = 9$, ning vähim -9. Seega ainus võimalus, et neist moodustatud arv jaguks 11-ga, on see, kui nende vahelduvate märkidega summa on 0 (neist numbritest moodustatud arv jaguks 11-ga ka siis, kui nende numbrite summa oleks 11, 22.., aga selliseid summasid antud numbritega saada võimalik pole). Numbrite hulgas on 3 paarisarvu ja 3 paaritut. Paarisarvu ja paaritu arvu summa on paaritu arv. Seega antud hulgas igale paarisarvule paaritu arvu liitmisel saame 3 paaritut arvu. Kahe paaritu arvu summa on paarisarv ning sellele paarisarvule veel viimase paaritu arvu liites saame taas paaritu arvu. 0 on aga paarisarv. See tähendab, et neid numbreid kokku liites pole võimalik saada summaks 0. Järelikult neist numbritest moodustatud kuuekohaline arv arvuga 11 ei jagu.

8. Üldiselt õnnestus kõigil jaguvustunnuste vmt. abil leida, et kulu ühe seltsiliikme kohta oli € 51.10. Ülesande tingimuste kohaselt oli ühe pudeli hinnaks x kümnesendist. Edasi ei analüüsitud aga kõiki juhte läbi. Teen seda siinkohal ise:

Tähistades sümboliga y tellitud pudelite arvu seltsiliikme kohta, tekib meil võrdus $x \cdot y = 511 = 7 \cdot 73$. Seega aritmeetika põhiteoreemi abil kas $x = 1, y = 511$, $x = 7, y = 73$, $x = 73, y = 7$ või $x = 511, y = 1$. Esimesed kaks juhtu annavad pudeli hinnaks € 0.10 või € 0.70, mis ei ole reaalne. Seega kas telliti 72 pudelit (üks igale liikmele) hinnaga € 51.10 pudel, või $72 \cdot 7 = 504$ pudelit (seitse igale liikmele) hinnaga € 7.30 pudel. Mingite mööndustega on mõlemad võimalused realistlikud, aga arvestades koguseid ja üliõpilaste mitte eriti rasket rahakotti, siis tõenäoliselt oli pudeli hinnaks € 7.30 ja iga seltsiliige võttis kaasa mõned sõbrad, kes aitasid tal need 7 pudelit ära juua ja tegid muidu peo lõbusamaks.