Kevad 2016

Märkusi arvuteooria 9. praktikumi kohta:

A. Vaheeksamiks soovitan kõigil ka need kordavad ülesanded läbi lahendada, mida praktikumiks teha ei jõudnud.

B. Kommentaare ja tüüpvigu ülesannete kaupa:

1. Otsitav jääk on 11. Siin võis lihtsalt avaldise

$$S := (2k-1)^2 + (2k+1)^2 + (2k+3)^2$$

lahti kirjutada. Alternatiivina saab leida, et

$$S \equiv 0 \pmod 3 \quad \text{ja} \quad S \equiv 3 \pmod 4$$

ning kasutada Hiina jäägiteoreemi. Kui võtta $2k-1, 2k+1, 2k+3$ asemele $x-2, x, x+2$, siis tuli rohkem vaeva näha, seega muutujate valik on mõnikord kasulik läbi mõelda.

2. Kõik otsitavad täisarvude kolmikud on

$$(144, 144, 2016), (144, 288, 1008), (144, 288, 2016), (144, 1008, 2016),$$

$$(144, 2016, 2016), (288, 288, 1008), (288, 1008, 1008), (288, 1008, 2016).$$

ning eelnevate kõikvõimalikud ümberjärjestused ja märgiga varustamised, nt. $(-2016, -144, 2016)$. Viimased kaks lisavõimalust võisid jääda kahe silma vahele, samuti asjaolu, et arvud võivad korduda. Lisaks oli peaaegu kõigil probleeme põhjendamisega, miks just täpselt kolmikud sobivad (st. miks ükski teine kolmik ei rahulda ülesande tingimusi). Lihtsaim viis seda teha on järjestada need arvud suuruse järjekorras ära ja kasutada lauset 1.20 SÜT ning VÜK uurimiseks. Siis on lihtne näha, et esimene arv peab olema kas 144 või 288 ja viimane kas 1008 või 2016. Edasine on juba läbiproovimise küsimus.

3. See ülesanne taandus peale loomade koguarvu arvestamist diofantilisele võrrandile $409x + 229y = 15720$, millel on ühene positiivne lahend $x = 11$ ja $y = 49$. Seega šeik ostis 11 elevanti, 49 hobust ja $800 - 60 = 740$ kaam**e**lit.

4. Õiged vastused on 5 ja 13: $9 \cdot 5 + 4 = 7^2$ ja $9 \cdot 13 + 4 = 11^2$. Idee on siin sama, mis 3. praktikumi 7. ülesandes. Ainuke ohtlik koht on see, et kui

$9p = (a+2)(a-2)$, siis ei pea tingimata kehtima, et $p = a+2$ või $p = a-2$, põhimõtteliselt võib juhtuda ka, et $3p = a+2$ või $3p = a-2$ (tegelikult küll ei juhtu).

5. Siin sai (arvutusvahenditest mööda minnes) kasutada jaguvustunnuseid kas 9 või 11 jaoks:

$$52817 \equiv 5-2+8-1+7 \equiv 6 \pmod{11},$$

$$3212146 \equiv 3-2+1-2+1-4+6 \equiv 3 \pmod{11},$$

$$52817 \cdot 3212146 \equiv 6 \cdot 3 \equiv 7 \pmod{11}.$$

Seega

$$11 \mid 169655{\times}15282 - 7 = 169655{\times}15275$$

ja

$$0 \equiv 1-6+9-6+5-5+x-1+5-2+7-5 \equiv x+2 \pmod{11}.$$

Kuna $0 \leq x \leq 9$, siis $x = 9$. Üheksaga jaguvus annab kaks lahendit, mida tuleb edasi analüüsida, aga kuna 11>10, siis 11-ga jaguvuse jaoks on vastus kümnendkuju jaoks alati ühene.

6. Kordan üle, et isomorfismi on mugav kasutada suunas $\mathbb{Z}_2 \times \mathbb{Z}_9 \to \mathbb{Z}_{18}$. Kui 18 asemel oleks suurem arv, näiteks $360 = 5 \cdot 8 \cdot 9$, siis on lihtne leida

$$U(\mathbb{Z}_5) \times U(\mathbb{Z}_8) \times U(\mathbb{Z}_9) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\} \times \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\} \times \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}.$$

Hiina jäägiteoreem annab meile nüüd kongruentside süsteemide

$$\begin{cases} x \equiv 1,2,3,4 & \pmod 5 \\ x \equiv 1,3,5,7 & \pmod 8 \\ x \equiv 1,2,4,5,7,8 & \pmod 9 \end{cases}$$

lahendid

$$x = a_1 \cdot 72 \cdot 3 + a_2 \cdot 45 \cdot 5 + a_3 \cdot 40 \cdot 7 = 216 \cdot a_1 + 225 \cdot a_2 + 280 \cdot a_3,$$

$a_1 \in \{1,2,3,4\}$, $a_1 \in \{1,3,5,7\}$, $a_3 \in \{1,2,4,5,7,8\}$.

7. Vastus on $1152 = 2 \cdot \varphi(2016)$, sest lihtmurd võib olla ka negatiivne.

8. Õige vastus on 4 (mod 23). Euleri või Fermat' väikest teoreemi on astendaja vähendamiseks hea kasutada kujul $a^{\varphi(n)} \equiv 1 \pmod n$ või $a^{p-1} \equiv 1 \pmod p$, mitte $a^p \equiv a \pmod p$. Arvust $\varphi(n)$ väiksemaid astmeid on hea arvutada nö. binaarkujul, nt.

$$14^{15} = 14{\cdot}14^2{\cdot}14^4{\cdot}14^8 \equiv 14{\cdot}12{\cdot}12^2{\cdot}12^4 \equiv 14{\cdot}12{\cdot}6{\cdot}6^2 \equiv 14{\cdot}12{\cdot}6{\cdot}13 \equiv 17 \pmod{23}.$$

9. Õige vastus: arvud kujul $p^{11}, p^2 \cdot q^3, p \cdot q^5, p \cdot q \cdot r^2$, kus p, q, r on erinevad algarvud. Vähim selline arv on $2^2 \cdot 3 \cdot 5 = 60$. Tüüpvigu: arvud p, q, r ei pea olema suuruse järjekorras, juht $p \cdot q^5$ ei ole "liiga suur" võrreldes järgmise kahega, seega ka selle puhul tuleb miinimum leida (see on 96, mis on samas suurusjärgus arvuga 60).

10. Ülesanne muutus tärnülesandeks, seega toon ära täieliku lahenduse. Peamiseks abitulemuseks oli 2015. aasta täpselt sama praktikumi sama numbriga ülesanne, mille kohaselt alati

$$x^{325} \equiv x \pmod{247}.$$

Tähistame

$$S := x + x^2 + \ldots + x^{324}$$

ja korrutame selle läbi teguriga $(x-1)$. Siis abitulemusest (mille lahendusidee on sama, kui 6. praktikumi 4. ülesandel, ehk Fermat' väike teoreem)

$$S(x-1) = x^{325} - x \equiv 0 \pmod{247}.$$

Viimane on samaväärne süsteemiga

$$\begin{cases} S(x-1) \equiv 0 & \pmod{13} \\ S(x-1) \equiv 0 & \pmod{19} \end{cases}.$$

Kuna 13 ja 19 on algarvud, siis $\mathbb{Z}_{13}$ ja $\mathbb{Z}_{19}$ on korpused. Korpustes ei ole nullitegureid, järelikult kas $S \equiv 0 \pmod{13}$ või $x - 1 \equiv 0 \pmod{13}$ ning samamoodi $S \equiv 0 \pmod{19}$ või $x - 1 \equiv 0 \pmod{19}$. Seega tekib meil neli süsteemi:

$$\begin{cases} S \equiv 0 & \pmod{13} \\ S \equiv 0 & \pmod{19} \end{cases}; \quad \begin{cases} x \equiv 1 & \pmod{13} \\ S \equiv 0 & \pmod{19} \end{cases};$$

$$\begin{cases} S \equiv 0 & \pmod{13} \\ x \equiv 1 & \pmod{19} \end{cases}; \quad \begin{cases} x \equiv 1 & \pmod{13} \\ x \equiv 1 & \pmod{19} \end{cases}.$$

Kui $S \equiv 0 \pmod{247}$, siis ka $S \equiv 0 \pmod{13}$ ja $S \equiv 0 \pmod{19}$. Kuna

$$1^{324} + \ldots + 1 = 324 \equiv 12 \not\equiv 0 \pmod{13}$$

ja

$$1^{324} + \ldots + 1 = 324 \equiv 1 \not\equiv 0 \pmod{19},$$

siis kolm viimast juhtu meile lahendeid ei anna. Lisaks oleme näidanud, et $S \equiv 0 \pmod{k}$ kehtib parajasti siis, kui $x \not\equiv 1 \pmod{k}$, $k \in \{13, 19\}$. Järelikult kolmele viimasele juhule vastavad süsteemid

$$\begin{cases} x \equiv 1 & \pmod{13} \\ x \equiv 0, 2, 3, \ldots, 18 & \pmod{19} \end{cases};$$

$$\begin{cases} x \equiv 0, 2, 3, \ldots 12 & (\mathrm{mod}\ 13) \\ x \equiv 1 & (\mathrm{mod}\ 19) \end{cases}; \quad \begin{cases} x \equiv 1 & (\mathrm{mod}\ 13) \\ x \equiv 1 & (\mathrm{mod}\ 19) \end{cases}.$$

Lahendades need süsteemid HJT abil saame, et $S \not\equiv 0$, kui

$$x \equiv 1, 14, 20, 27, 39, 40, 53, 58, 66, 77, 79, 92, 96, 105, 115, 118, 131 \pmod{247}$$

või

$$x \equiv 134, 144, 153, 157, 170, 172, 183, 191, 196, 210, 219, 222, 229, 235 \pmod{247}.$$

Esimene süsteem tähendab aga jällegi HJT kohaselt, et tõepoolest $S \equiv 0 \pmod{247}$. Kokkuvõttes on lahendid kõik jäägiklassid peale kahel eeltoodud real esinevate 31, seega kokku on 216 lahendit.

11. Siin tuli lahendada kongruentside süsteem

$$\begin{cases} x \equiv 51 & (\mathrm{mod}\ 57) \\ x \equiv 53 & (\mathrm{mod}\ 56) \\ x \equiv 0 & (\mathrm{mod}\ 55) \end{cases}.$$

Selle lahendiks on $x \equiv 165 \pmod{55 \cdot 56 \cdot 57}$. Järelikult iga piraat sai endale vähemalt $\frac{165}{55} = 3$ soovi. Mõnikord koostati siin vale võrrandisüsteem või piirduti ainult soovide koguarvuga 165 ja õiget vastust (soove piraadi kohta) ei kirjutatudki välja.

12. Õige vastus on kas 7 ja 43 modulo 90. Kontrolliks: vaheetappide vastused on $x \equiv 1 \pmod{2}$, $x \equiv 2, 3 \pmod{5}$, $x \equiv 0, 1 \pmod{3}$ ja $x \equiv 7 \pmod{9}$.