Kevad 2016

Märkusi arvuteooria 13. praktikumi kohta:

A. Kommentaare ja tüüpvigu ülesannete kaupa:

1. Vastus: $1, 2, 4, 8, 9, 13, 15, 16$.
Piisab, kui leida ruudud $1^2, 2^2, \ldots, 8^2$, mida ongi vajalik $\frac{17-1}{2} = 8$ tükki.

2. Vastus: $1, 4, 5, 6, 7, 9, 11, 16, 17$.
Ei ole vaja kõiki astmeid a^9 välja arvutada, näiteks

$$6^9 = 2^9 \cdot 3^9, \quad 7^9 \equiv (-12)^9 = -(2^9)^2 \cdot 3^9 \text{ jne.}$$

3. Vastus: $1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28$.
Kuna $29 \equiv 1 \pmod 4$, siis $\left(\frac{-1}{29}\right) = 1$ ja

$$\left(\frac{a}{29}\right) = \left(\frac{p-a}{29}\right).$$

Seega piisab ainult poolte Legendre'i sümboli väärtuste leidmisest. Ülejäänud juhtudel saab samuti arvutusi optimeerida näiteks nii:

$$\left(\frac{6}{29}\right) = \left(\frac{2}{29}\right) \cdot \left(\frac{3}{29}\right) = 1,$$

$$\left(\frac{7}{29}\right) = \left(\frac{36}{29}\right) = \left(\frac{6^2}{29}\right) = 1,$$

$$\left(\frac{11}{29}\right) = \left(\frac{18}{29}\right) = \left(\frac{2}{29}\right) \cdot \left(\frac{3^2}{29}\right) = \left(\frac{2}{29}\right) = 1.$$

4. Lahenduvad kongruentsid on alamülesannetes a), d) ja f) ning neil kõigil on kaks lahendit. Viimasel juhul on lahendite arv kongruentside süsteemi

$$\begin{cases} x^2 \equiv -2 & \pmod{67} \\ x^2 \equiv -2 & \pmod 2 \end{cases}$$

lahendite arvude korrutis $2 \cdot 1$.
Mõned suuremad vead: Legendre'i sümbol $\left(\frac{1}{2}\right)$ ei ole defineeritud, täisarvude korral tuleb muutujavahetuse $y = \frac{x}{2}$ lubatavust eraldi põhjendada.

5. Siin oli lihtne leida, et $\left(\frac{p}{7}\right) = -1$ ehk p on mitteruutjääk modulo 7. Vahetu kontroll näitab, et mitteruutjäägid on $3, 5$ ja 6, seega $p \equiv 3, 5, 6 \pmod 7$.

6. Kõige lihtsam oli kasutada kas Euleri kriteeriumit ($a^{\frac{p-1}{2}} \equiv 1 \pmod p$, mis on vastuolus algjuureks olekuga) või lemmat 8.5 (ruutjäägid on algjuure paarisarvulised astmed ja järelduse 7.10 tõttu ei ole ükski neist algjuur, sest $2 \mid (2k, p-1)$).

7. Antud juhul jälle

$$\left(\frac{a}{p}\right) = \left(\frac{p-a}{p}\right),$$

mistõttu

$$S := \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 2 \cdot \sum_{a=1}^{(p-1)/2} \left(\frac{a}{p}\right).$$

Kuna ruutjääke ja mitteruutjääke on sama palju, siis $S = 0$, millest kahega taandades järeldubki ülesande väide.
Levinumad vigadest: väitest $S = 0$ üksi ei piisa, sest siis kehtiks seesama väide ka $p \equiv 3 \pmod 4$ korral, mis ei ole tõsi.

8. Antud ülesanne oli mõnevõrra keerulisem. Täielik lahendus:
Eelduse kohaselt $\left(\frac{2}{p}\right) = -1$. Oletame vastuväiteliselt, et antud diofantiline võrrand on lahenduv ja selle lahenditeks on x_0 ja y_0. Siis

$$x_0 \equiv 2y_0 \pmod p$$

ja meil on kaks erijuhtu:

1. $p \mid x_0$, millest $(2, p) = 1$ tõttu ka $p \mid y_0$,
2. $p \nmid x_0$, ja samamoodi $p \nmid y_0$.

Esimesel juhul $x_0 = kp$ ja $y_0 = lp$ mingite $k, l \in \mathbb{Z}$ korral, kust

$$p = p^2(k^2 - 2l^2) \quad \text{ehk} \quad 1 = p(k^2 - 2l^2).$$

See ei ole võimalik, sest $p > 1$.
Teisel juhul on nii x_0 kui y_0 pööratavad modulo p, mistõttu ka $x_0 y_0^{-1}$ on pööratav ja

$$\left(x_0 y_0^{-1}\right)^2 \equiv 2 \pmod p.$$

See on vastuolus alguses leitud faktiga $\left(\frac{2}{p}\right) = -1$. Kokkuvõttes oleme kummalgi juhul jõudnud vastuoluni, seega meie vastuväiteline oletus oli väär ja see diofantiline võrrand ei ole lahenduv.