Kevad 2015

Märkusi arvuteooria 13. praktikumi kohta:

A. Kommentaare ülesannete kaupa:

1. Ülesanne oli puhtalt arvutamise peale, aga siin sai oma tegevust veidi optimeerida. Kuna $(-x)^2 = x^2$, siis ei ole mõtet leida rohkem ruute, kui

$$\begin{aligned} 1^2 &= 1 = (-1)^2 = 10^2, \\ 2^2 &= 4 = (-2)^2 = 9^2, \\ 3^2 &= 9 = (-3)^2 = 8^2, \\ 4^2 &\equiv 5 = (-4)^2 = 7^2 \pmod{11}, \\ 5^2 &\equiv 3 = (-5)^2 = 6^2 \pmod{11}. \end{aligned}$$

Vastust saab kontrollida, teades, et kokku peab olema $\frac{11-1}{2} = 5$ ruutjääki ja sama palju mitteruutjääke. Need 5 ruutjääki on seega $1, 3, 4, 5$ ja 9.

2. Euleri kriteeriumi kohaselt tuleb siin järjest leida

$$\left(\frac{x}{17}\right) \equiv x^{\frac{17-1}{2}} = x^8 \pmod{17},$$

$x = 1, 2, \ldots, 16$. Selline astendamine ei ole arvutuslikult väga efektiivne, mistõttu tasub otsida võimalusi arvutuste lihtsustamiseks. Parim tähelepanek on jälle, et $x^8 = (-x)^8$ ja me peame leidma vaid astmed, kus $x = 1, 2, \ldots, 8$. Ka konkreetsete astmete jaoks on omaette võtteid:

- kordarvu korral saame minna üle juba leitud algteguritele, näiteks $\left(\frac{6}{17}\right) \equiv 6^8 = 2^8 \cdot 3^8 \pmod{17}$,
- mõned algarvud on võimalik viia sobivale kordarvulisele kujule, näiteks $\left(\frac{5}{17}\right) = \left(\frac{-12}{17}\right) = (-1)^8 \cdot (2^8)^2 \cdot 3^8$.

Kontrollmehhanisme on seekord kaks: peab tulema $\frac{17-1}{2} = 8$ ruutjääki ja kõik astendamised peavad andma lõpuks kas 1 või -1.

Kontrollvastus: ruutjäägid mooduli 17 järgi on $1, 2, 4, 8, 9, 13, 15$ ja 16.

3. Siin oli kaks varianti: kasutada lemmat 8.5 ja leida mõne algjuure kõik paarisarvulised astmed (mitte eriti efektiivne ilma indeksite tabelita) või

rakendada mitmesuguseid Legendre'i sümboli omadusi (lemma 8.4, Euleri kriteerium, lause 8.8, teoreem 8.11, Gaussi ruutvastavusseadus). Viimane lähenemine on tõhusam.

Esiteks on otstarbekas leida $\left(\frac{-1}{23}\right) = -1$, sest $23 \equiv 3 \pmod 4$. Seetõttu

$$\left(\frac{23-x}{23}\right) = \left(\frac{-x}{23}\right) = \left(\frac{-1}{23}\right) \cdot \left(\frac{x}{23}\right) = -\left(\frac{x}{23}\right)$$

ja meil on jälle vaja arvutada vaid pooled väärtused. Muuseas, ei ole eriti hea kasutada kriteeriume kujul $\left(\frac{2}{17}\right) = 2^{\frac{23^2-1}{8}}$, sest astendamine võtab aega. Vastav neljaga või kaheksaga jaguvuse kriteerium (siin $23 \equiv -1 \pmod 8$) on üldiselt lihtsam ja kiirem. Samuti tasub kõik sellised põhjendused kirja panna, sest kirjutades eksami ajal lihtsalt $\left(\frac{2}{17}\right) = 1$, ei tea ma, kuidas te selle tulemuseni jõudsite (võib-olla huupi pakkudes, õigeid vastuseid on ca. 50%) ja võtan mõne punkti maha. Kui te kasutate Gaussi ruutvastavusseadust, siis on vajalik kirja panna, kuidas te "pööramisel" tekkiva märgi leidsite ja et mõlemad sümbolis esinevad arvud on algarvud.

Näitevõtteid:

$$\left(\frac{1}{23}\right) = -\left(\frac{22}{23}\right) = 1,$$

$$\left(\frac{2}{23}\right) = -\left(\frac{21}{23}\right) = 1, \text{ sest } 23 \equiv -1 \pmod 8,$$

$$\left(\frac{3}{23}\right) = -\left(\frac{20}{23}\right) \equiv 3^{\frac{23-1}{2}} = 3^{11} = 9 \cdot 27^3 \equiv 9 \cdot (4)^3$$
$$= 16 \cdot 36 \equiv -7 \cdot 13 = -91 \equiv 1 \pmod{23},$$

$$\left(\frac{4}{23}\right) = -\left(\frac{19}{23}\right) = \left(\frac{2^2}{23}\right) = 1,$$

$$\left(\frac{5}{23}\right) = -\left(\frac{18}{23}\right) = -\left(\frac{2}{23}\right) \cdot \left(\frac{3^2}{23}\right) = -1^2 = -1,$$

$$\left(\frac{6}{23}\right) = -\left(\frac{17}{23}\right) = \left(\frac{2}{23}\right) \cdot \left(\frac{3}{23}\right) = 1^2 = 1,$$

$$\left(\frac{7}{23}\right) = -\left(\frac{16}{23}\right) = -\left(\frac{23}{7}\right) = -\left(\frac{2}{7}\right) = -1,$$
sest $7, 23 \in \mathbb{P}, 7 \equiv 23 \equiv 3 \pmod 4$ ja $7 \equiv -1 \pmod 8$,

$$\left(\frac{8}{23}\right) = -\left(\frac{15}{23}\right) = \left(\frac{2^3}{23}\right) = \left(\frac{2}{23}\right) = 1,$$

$$\left(\frac{9}{23}\right) = -\left(\frac{14}{23}\right) = \left(\frac{3^2}{23}\right) = 1,$$
$$\left(\frac{10}{23}\right) = -\left(\frac{13}{23}\right) = \left(\frac{2}{23}\right)\cdot\left(\frac{5}{23}\right) = 1\cdot(-1) = -1,$$
$$\left(\frac{11}{23}\right) = -\left(\frac{12}{23}\right) = -\left(\frac{2^2}{23}\right)\cdot\left(\frac{3}{23}\right) = -1^3 = -1.$$

Seega ruutjäägid on $1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18$, mis sobib meie teadmisega, et kokku peab olema $\frac{23-1}{2} = 11$ ruutjääki.
Lõppmärkus: sümbolit $\left(\frac{11}{23}\right)$ loetakse "üksteist kahekümne kolme suhtes", mitte "üksteist jagatud kahekümne kolmega" vmt.

4. Ülesande lahendamisel võis kasutada nii teoreemi 7.30 kui Legendre'i sümbolit. Viimane on jälle efektiivsem. Lahenduste tüüpilised kitsaskohad olid:

- oma tegevuse väga vähene selgitamine (eksamil ei saa te punkte peamiselt mitte õige vastuse, vaid õige lahendusmeetodi eest),
- kust tuleb lahendite arv, kui vastav Legendre'i sümboli väärtus on 1, ja mis on sellel pistmist algarvulise mooduliga (vihje: lause 2.9),
- arvutused stiilis $\left(\frac{2}{59}\right) = (-1)^{\frac{59^2-1}{8}}$, mille parem variant on: $\left(\frac{2}{59}\right) = -1$, sest $59 \equiv 3 \pmod 8$.

5. Kasutades Gaussi ruutvastavusseadust sai üle minna kujule $\left(\frac{p}{5}\right) = -1$ ning seejärel analüüsida p jääke modulo 5. Eelmise ülesande probleemid kandusid osaliselt ka sellesse ülesandesse. Lõpuks, mingi hulga algarvudega läbi proovimine EI OLE tõestus.

6. Vähesed lahendajad panid ilusasti tähele, et sellisel kujul olevate algarvude p korral
$$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) = -1 \pmod p.$$

7. Antud ülesandest sai lahenduste väikese arvu tõttu *-ülesanne. Lahenduseks piisas tähelepanekust, et tänu lemmale 8.5 tuleb liita mingi algjuure paarituarvuliste astmete ruudud, st. geomeetrilise rea summa valemi kohaselt
$$S = \sum_{\substack{i=1 \\ i\equiv 1 \pmod 2}}^{p-1} (a^i)^2 = a^2 + a^6 + \ldots + a^{2(p-2)} = a^2 \cdot \frac{a^{2(p-1)} - 1}{a^4 - 1}.$$

Kuna $a^{p-1} \equiv 1 \pmod{p}$ ja $a^4 \not\equiv 1$, sest a kui algjuur on vähemalt $7 - 1 = 6$ järku element tänu nõudele $p > 5$. Seega nulliga jagamist ei ole ja

$$S \equiv a^2 \cdot \frac{1^2 - 1}{a^4 - 1} = 0 \pmod{p},$$

mida oligi tarvis tõestada.

8. Jälle tuli ülesandele tärn lisada. Lahendamiseks oli siin mitu meetodit. Lihtsamaid nende seast on järgmine: üks arvudest $2, 5$ ja 10 on alati ruutjääk, sest kui $\left(\frac{2}{p}\right) = \left(\frac{5}{p}\right) = -1$, siis $\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{5}{p}\right) = (-1)^2 = 1$. Järelikult sisaldab vähemalt üks paaridest $(1 = 1^2, 2)$, $(4 = 2^2, 5)$ ja $(9 = 3^2, 10)$ kahte ruutjääki. Seega on meil alati vähemalt kaks kõrvutiolevat ruutjääki. Kirjutame kõik arvud $1, 2, \ldots, p - 1$ järjest üles ning värvime ruutjäägid siniseks ja mitteruutjäägid punaseks. Kui ei leiduks kõrvutiolevaid mitteruutjääke, siis peab meil olema $\frac{p-1}{2}$ punast arvu ja siniste arvude rühmad nende vahel. Et selline olukord toimuda saaks, peab niisuguseid eraldavaid siniste arvude rühmi olema minimaalselt sama palju, kui punaseid arve (üldiselt piisab ka ühe võrra vähemast, aga ma teame, et esimene blokk, mis algab arvuga 1, on sinine). Kuna meil on vähemalt kaks kõrvutist ruutjääki, on siniste arvude rühmi ülimalt $\frac{p-1}{2} - 1$, aga punaseid arve on, nagu juba märgitud, $\frac{p-1}{2}$ tükki. See ei ole kooskõlas meie tähelepanekuga, et punaseid arve ei saa olla rohkem, kui neid eraldavaid siniste arvude blokke, mistõttu on meie oletus, et mitteruutjäägid ei satu kunagi kõrvuti, väär.