Kevad 2014

Märkusi arvuteooria 13. praktikumi kohta:

A. Tundub, et peale lõplikke korpusi on ülesanded jälle lihtsamaks ja tehtavamaks läinud. Loodetavasti see trend jätkub, kuigi nii mõnigi kuulaja on tulemuste tabeli põhjal otsustades juba alla andnud. Veel ei tasu alla anda, lõpp juba paistab.

B. Kommentaare ülesannete kaupa:

1. ülesanne oli kõigil hästi lahendatud, ainult vastus jäeti mõnikord kirjutamata. See oli esimese kolme ülesande puhul üldse läbiv probleem. Ainus märkus, mida siin teha, on see, et ruute tasub leida kuni $\left(\frac{p-1}{2}\right)^2$-ni, edasi need korduvad.

2. See ülesanne oli samuti ilusasti lahendatud, kuigi eksamit silmas pidades tuleb teil osata leida suuri astmeid jäägiklassiringides ka ilma arvutustehnika abita. Näiteks $7^6 = 49^3 \equiv (-3)^3 = -27 \equiv -1 \pmod{13}$, MITTE $7^6 = 117649 \equiv ? \equiv -1 \pmod{13}$.

3. Siin on arvutuslikult otstarbekas Legendre'i sümboli omadusi kasutada niiviisi:

- Esmalt leida $\left(\frac{-1}{17}\right) = 1$, sest $17 \equiv 1 \pmod 4$ (lause 9.7 osa 3). Seetõttu
$$\left(\frac{p-a}{17}\right) = \left(\frac{-a}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{a}{17}\right) = \left(\frac{a}{17}\right)$$
vastavalt lemmale 9.4 ja lause 9.7 osale 1. Järelikult piisab vaid poolte Legendre'i sümbolite leidmisest, näiteks $\left(\frac{11}{17}\right) = \left(\frac{6}{17}\right)$.
- Leida $\left(\frac{1}{17}\right) = 1$ ja $\left(\frac{2}{17}\right) = 1$ vastavalt lause 9.7 osale 3 ja teoreemile 9.10 ($17 \equiv 1 \pmod 4$ ja $17 \equiv 1 \pmod 8$).
- Algarvude a korral leida $\left(\frac{a}{17}\right)$ vastavalt Euleri kriteeriumile, näiteks $\left(\frac{3}{17}\right) \equiv 3^8 \equiv -1 \pmod{17}$. Mõnikord saab siin osaliselt eelnevaid tulemusi kasutada, näiteks $\left(\frac{5}{17}\right) = \left(\frac{12}{17}\right) = \left(\frac{3\cdot 2^2}{17}\right) = \left(\frac{3}{17}\right) = -1$ tänu lause 9.7 osale 2 ja eeltoodule.

- Kordarvude jaoks kasutada lause 9.7 osa 1 ja eelnevaid tulemusi, näiteks $\left(\frac{6}{17}\right) = \left(\frac{2\cdot 3}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{3}{17}\right) = 1 \cdot (-1) = -1$.

Need võtted koos Gaussi ruutvastavusseadusega ongi aluseks Legendre'i ja Jacobi sümbolite (järgmine praktikum) efektiivseks leidmiseks.

4. Üheksanda peatüki sissejuhatusest on teada, et kongruentsil $x^2 \equiv a \pmod{p}$, $p \nmid a$, on algarvu $p > 2$ korral täpselt 0 (a on mitteruutjääk) või 2 (a on ruutjääk) lahendit. Seega esimesed neli alamülesannet taanduvad Legendre'i sümboli leidmisele. Viimases kahes alamülesandes on vaja kongruents $x^2 \equiv a \pmod{2p}$ viia süsteemiks

$$\begin{cases} x^2 \equiv a \pmod{p} \\ x^2 \equiv a \pmod{2} \end{cases}.$$

Viimane on lahenduv parajasti siis, kui kõik selles sisalduvad kongruentsid on lahenduvad, ja lahendite arv on võrdne kõigi süsteemi kuuluvate kongruentside lahendite arvude korrutisega. Kuna $x^2 = a \pmod{2}$ on alati üheselt lahenduv, taandusid ka viimased alamülesanded Legendre'i sümboli arvutamisele.

5. Siin piisas sellest, kui leida $\left(\frac{0}{7}\right) = 0, \left(\frac{1}{7}\right) = 1, \left(\frac{2}{7}\right) = 1, \left(\frac{3}{7}\right) = -1, \left(\frac{4}{7}\right) = 1, \left(\frac{5}{7}\right) = -1, \left(\frac{6}{7}\right) = -1$. Kuna p on mooduli 7 järgi kongruentne kas 0, 1, 2, 3, 4, 5 või 6-ga, siis ta saab olla ruutjääk parajasti siis, kui ta on kongruentne kas 1, 2 või 4-ga. Ei ole vaja kuidagi eraldi piisavust ja tarvilikkust tõestama hakata.

7. Lahendamisel sai kasutada kas järeldust 7.21 või otse algjuure definitsiooni järgu abil, sest kui $a \equiv b^2 \pmod{p}$, siis $a^{\frac{p-1}{2}} = (b^2)^{\frac{p-1}{2}} = b^{p-1} \equiv 1 \pmod{p}$ vastavalt Fermat' väikesele teoreemile ($p \nmid b$, muidu $a = b^2 \equiv 0$ ei oleks algjuur).

8. Üldiselt esitati kõigi erinevate ruutjääkide summa ilusasti kujul

$$S = \frac{p(p+1)(p-1)}{24}.$$

Sellest järeldati kohe, et kui p "sulgude ette tuua", siis tõepoolest p jagab seda avaldist. Mis jäi tähelepanuta, on see, et jaguvuse jaoks on lisaks vaja, et $S = p \cdot k$, kus $k \in \mathbb{Z}$, ehk on tarvis näidata, et $\frac{(p+1)(p-1)}{24} \in \mathbb{Z}$. Seda oli lihtne teha Eukleidese lemma abil, kui võtta arvesse asjaolu, et p on kolmest suurem algarv ja $24 = 3 \cdot 2^3$.