Kevad 2014

Märkusi arvuteooria 14. praktikumi kohta:

A. Ülesandeid lahendati üllatuslikult vähe, ehkki nad ei olnud eelmise nädala omadest raskemad. Tõenäoliselt on tegu semestri lõpu, kontrolltööde jmt. kõrvalmõjuga.

B. Üks läbiv probleem oli see, et (eriti Legendre'i ja Jacobi sümbolite arvutamisel) ei põhjendatud iga mittetriviaalset sammu, nagu näiteks märgi muutumine ruutvastavusseaduse rakendamisel. Vaadake 14. praktikumi näitefailist järgi, kuidas seda teha.

B. Kommentaare ülesannete kaupa:

1. Üldiselt oli ülesanne hästi lahendatud, ehkki ma soovitan veelkord vaadata näitefaili, vältida kordarvude tegurdamist ja Euleri kriteeriumi ning kasutada Gaussi ruutvastavusseadust ja Jacobi sümbolit (st kontrollima peab ainult paarituks olemist). Paljudel lahendajatel jäid ka tähelepanuta omaduse $\left(\frac{ab^2}{n}\right) = \left(\frac{a}{n}\right)$, kui $(b, n) = 1$, kasutuskohad.

2. Ülesanne taandub kongruentside süsteemidele

$$\begin{cases} p \equiv 1 \pmod 4 \\ p \equiv \pm 1 \pmod 5 \end{cases}$$

ja

$$\begin{cases} p \equiv 3 \pmod 4 \\ p \equiv \pm 3 \pmod 5 \end{cases},$$

mis vastavad juhtudele $\left(\frac{-1}{p}\right) = 1$ ja $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1$ ning $\left(\frac{-1}{p}\right) = -1$ ja $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = -1$. Mitmel lahendajal jäi teine võimalus vaatluse alt välja. Hiina jäägiteoreem annab meile seetõttu neli lahendit: 1,3,7 ja 9 (mod 20).

3. Peale b) osa teisendamist kujule $y^2 \equiv 31 \pmod{97}$ taandub ülesanne Legendre'i sümbolite $\left(\frac{123}{197}\right) = -1$ ja $\left(\frac{31}{97}\right) = 1$ leidmisele, sest (NB!) 197 ning 97 on algarvud. Tänu märkusele 9.17 ei piisa kordarvulise mooduli n korral

kongruentsi $x^2 \equiv a \pmod{n}$ lahenduvuseks faktist $\left(\frac{a}{n}\right) = 1$. Samas siiski juhul $\left(\frac{a}{n}\right) = -1$ ei leidu lahendeid ka kordarvulise n korral.

4. Siin tekib jälle kaks võimalust: kas $\left(\frac{-1}{n}\right) = 1$ ja $\left(\frac{2}{n}\right) = -1$ või $\left(\frac{-1}{n}\right) = -1$ ja $\left(\frac{2}{n}\right) = 1$, kust saame kongruentside süsteemid

$$\begin{cases} p \equiv 3 \pmod 4 \\ p \equiv \pm 1 \pmod 8 \end{cases}$$

ja

$$\begin{cases} p \equiv 1 \pmod 4 \\ p \equiv \pm 3 \pmod 8 \end{cases}.$$

(Seda ei ole loengukonspektis küll otseselt kirjas, aga ka Jacobi sümboli korral kehtivad teoreemi 9.10 ja lause 9.7 3) kongruentsusel põhinevad variandid.) Alternatiivne ja veidi raskem viis oli uurida -1 astendaja paarsust vastavalt lausele 9.21. Neid kongruentse saab (ja peab!) lahendada ilma Hiina jäägiteoreemita ning vastuseks on 5 ja 7 $\pmod 8$.

5. Kui $n \equiv 1 \pmod 8$, siis ka $n \equiv 1 \pmod 4$, $\left(\frac{2}{n}\right) = 1 = \left(\frac{-1}{n}\right)$ ja

$$\left(\frac{-2a}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{2}{n}\right)\left(\frac{a}{n}\right) = \left(\frac{a}{n}\right) = -1.$$

Seda üldjuhul ka näidati, ehkki jällegi mõnikord keerulisemalt, analüüsides -1 astmeid, mis tekivad lause 9.21 tõttu. Aga "vastupidise väite" kehtivus jäi valdaval enamusel kontrollimata, ja see oli ülesande isegi olulisem osa. Vastupidine väide (kui kongruents $x^2 + 2a \equiv 0 \pmod n$ ei ole lahenduv, siis $\left(\frac{a}{n}\right) = -1$) EI KEHTI. Näiteks $x^2 + 2 \cdot (-1) \equiv 0 \pmod{25}$ ei ole lahenduv, sest muidu lahenduks ka kongruents $x^2+2\cdot(-1) \equiv 0 \pmod 5$, aga $\left(\frac{2}{5}\right) = -1$. Samas $\left(\frac{-1}{25}\right) = \left(\frac{-1}{5}\right)^2 = 1$.

6. Lahendusidee oli selline: kui $m \mid n^2-2$, siis $2 \equiv n^2 \pmod m$, ehk $\left(\frac{2}{m}\right) = 1$ (märkuse 9.17 tõttu ei saa kehtida $\left(\frac{2}{m}\right) = -1$), mis kehtib parajasti siis, kui $m \equiv \pm 1 \pmod 8$. Mitu lahendajat suutsid aga teha sellise lükke, et tõestasid, et arvud kujul $m = 8k \pm 1$ rahuldavad seost $\left(\frac{2}{m}\right) = 1$. Sellest ei piisa isegi väitmaks, et $2 \equiv n^2 \pmod m$ on lahenduv, kui m juhtub olema kordarv. Ja KÕIGI jagajate kohta ei saa me sellest väitest eriti midagi teada.