Kevad 2016

Märkusi arvuteooria 14. praktikumi kohta:

A. Kaks üldist märkust:

- kõiki oma lahenduse samme tuleb põhjendada; kui te ei ole endas kindlad, siis küsige abi kas kaaskuulajatelt või minult (peale loengut/praktikumi, e-kirja teel jne.);
- kui teie lahendus on identne mõne teise esitatud lahendusega, siis lähevad punktid lahendajate vahel jagamisele.

B. Kommentaare ja tüüpvigu ülesannete kaupa:

1. Siin oli paljudel puudu põhjendustest, näiteks miks $\left(\frac{389}{6667}\right) = \left(\frac{6667}{389}\right)$ või $\left(\frac{2}{389}\right) = -1$. Piisab, kui mainida, et $389 \equiv 1 \pmod 4$ või $389 \equiv 5 \pmod 8$.

Arvu 6667 tegurdamine kujule $6667 = 59 \cdot 113$ EI OLE optimaalne viis Jacobi sümboli väärtuse leidmiseks. Proovige seda ilma arvuti abita teha!

Kontrollvastus: $\left(\frac{9779}{6667}\right) = -1$.

2. Siin tuli kindlaks teha, et p peab olema mitteruutjääk modulo 13 ja leida mitteruutjäägid modulo 13. Selleks võis kasutada nii Jacobi sümbolit (asjaolu $\left(\frac{-1}{13}\right) = 1$ võimaldab poole tööst kokku hoida), leida lihtsalt $1^2, 2^2, \ldots, 6^2$ modulo 13 või kasutada teoreemi 7.33 ja indeksite tabelit modulo 13.

Vastuseks on $p \equiv 2, 5, 6, 7, 8, 11 \pmod{13}$ JA $p > 2$, sest algarvu 2 korral on 13 ruutjääk.

3. Faktist $\left(\frac{162}{209}\right) = 1$ ei piisa kongruentsi $x^2 \equiv 162 \pmod{209}$ lahenduvuseks, sest $209 = 11 \cdot 19$ ei ole algarv. Tegelikult ei ole kumbki kongruentsidest lahenduv.

4. Tarvilikkuse tõestus tugines otse Jacobi sümboli väärtuse arvutamisele. Vastupidine väide kehtib, kui n on algarv. Minimaalne kordarv, mis sobib näitamaks, et üldiselt piisavus ei kehti, on 35, sest $11, 19, 27$ on kas algarvud või paaritu arvu algarvude korrutised. Ja tõepoolest, $a = 1$ ning $n = 35$ korral kongruents ei ole lahenduv, aga $\left(\frac{1}{35}\right) = 1 \neq -1$.

5. Siin võis kasutada otse lause 8.21 osa 1., aga tõestada sai ka lause 8.8 osa 3. abil algtegurite kaudu. Nimelt on iga paarituarvuline jagaja paaritute algtegurite korrutis.

6. See oli veidi keerukam ülesanne. Suhteliselt lihtne tõestus on alljärgnev.

Esiteks, ruutjääk ei ole algjuur (eelmise praktikumi ülesanne), seega algjuured moodustavad osa mitteruutjääkidest. Mitteruutjääke on $\frac{p-1}{2}$ tükki ja algjuuri on

$$\varphi(\varphi(p)) = \varphi(2^{2^k} + 1 - 1) = 2^{2^k - 1} = \frac{p-1}{2}$$

tükki. Järelikult peavad kõik mitteruutjäägid olema algjuured. Arv 3 on aga mitteruutjääk, sest

$$\left(\frac{3}{2^{2^k}+1}\right) = \left(\frac{2^{2^k}+1}{3}\right) = \left(\frac{(-1)^{2^k}+1}{3}\right) = \left(\frac{2}{3}\right) = -1$$

tänu faktile $2^{2^k} + 1 \equiv 1 \pmod 4$, kui $k \geq 1$.

7. Õige vastus: kõigi algarvude $p \equiv 1 \pmod 4$ korral.

Täielik lahendus: kui sellised täisarvud x ja y õnnestub leida, siis y on pööratav modulo p. Olgu $yz \equiv 1 \pmod p$. Sel juhul tänu asjaolule $p \mid p^k$ kehtib

$$(xz)^2 \equiv -1 \pmod y$$

ehk $\left(\frac{-1}{p}\right) = 1$. Viimane kehtib aga parajasti siis, kui $p \equiv 1 \pmod 4$.

Vastupidi, kui $p \equiv 1 \pmod 4$, siis $z^2 \equiv -1 \pmod p$ mingi täisarvu z korral, järelikult võttes $x = 1$ ja $y = z$ saame, et

$$x^2 + y^2 = 1^2 + z^2 \equiv 1 - 1 = 0 \pmod p.$$

Ilmselt ka $(1, p) = 1 = (z, p)$. Kokkuvõttes $p \equiv 1 \pmod 4$ parajasti siis, kui kongruents $x^2 + y^2 = 0 \pmod p$ on lahenduv rühmas $\mathbb{Z}_p^*$.

Kongruentsi $x^2 + y^2 = 0 \pmod{p^k}$ lahenduvusest $\mathbb{Z}_p^*$-s järeldub ilmselt sama kongruentsi lahenduvus modulo p. Teisipidi, kui kongruents $x^2 + y^2 = 0 \pmod p$ on lahenduv $\mathbb{Z}_p^*$-s, siis fikseerides lahendi $y = y_0$, on lahenduv kongruents

$$x^2 \equiv -y_0^2 \pmod p.$$

Kaheksanda praktikumi 8. ülesande kohaselt on siis lahenduv ka kongruents $x^2 \equiv -y_0^2 \pmod{p^k}$, mistõttu on lahenduv ka $x^2 + y^2 = 0 \pmod{p^k}$ (võtame $y = y_0$ ja $x = x_0$, kus $x_0^2 \equiv -y_0^2 \pmod{p^k}$).

Kokku oleme saanud, et

$$\begin{aligned} p \equiv 1 \pmod 4 &\iff x^2 + y^2 = 0 \pmod p \text{ on lahenduv rühmas } \mathbb{Z}_p^* \\ &\iff x^2 + y^2 = 0 \pmod{p^k} \text{ on lahenduv rühmas } \mathbb{Z}_p^*. \end{aligned}$$

Seda oligi vaja näidata. Paneme siin tähele, et tingimus "rühmas $\mathbb{Z}_p^*$" on oluline, sest muidu võiks võtta $x = y = 0$, mis on iga p korral lahendiks. Seetõttu on oluline kontrollida, et x ja y oleks arvuga p ühistegurita.

8. Tõestuse idee on sarnane Eukleidese tõestusega algarvude lõpmatusest. Vastuväitelise tõestuse läbiviimiseks saab konstrueerida arvu

$$a = (2 \cdot p_1 \cdot \ldots \cdot p_n)^2 + 3,$$

kus $p_1, \ldots, p_n$ on kõik algarvud kujul $6k + 1$. Arvul a on algtegur $p > 3$ (miks?). Eraldi juhte $p \equiv \pm 1 \pmod 4$ analüüsides tuleb välja, et

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) \text{ ja ilmselt } \left(\frac{-3}{p}\right) = 1.$$

Kuid $\left(\frac{p}{3}\right) = 1$ vaid siis, kui $p \equiv 1 \pmod 3$ ehk $p \equiv 1 \pmod 6$ (juht $p \equiv 4 \pmod 6$ ei anna algarvu).