Arvuteooria

Kevad 2020

13. praktikumi näidislahendused

1. ülesanne (Markus Rene Pae ja Erki Kuus)

Kuna 23 on algarv, siis

$$U(\mathbb{Z}_{23}) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}, \overline{15}, \overline{16}, \overline{17}, \overline{18}, \overline{19}, \overline{20}, \overline{21}, \overline{22}\}$$

Tõstan selle hulga elemente järjest ruutu:

$\overline{1}^2 = \overline{1}$; $\overline{2}^2 = \overline{4}$; $\overline{3}^2 = \overline{9}$; $\overline{4}^2 = \overline{16}$;
$\overline{5}^2 = \overline{2}$; $\overline{6}^2 = \overline{13}$; $\overline{7}^2 = \overline{3}$; $\overline{8}^2 = \overline{18}$;
$\overline{9}^2 = \overline{12}$; $\overline{10}^2 = \overline{8}$; $\overline{11}^2 = \overline{6}$; $\overline{12}^2 = \overline{6}$;
$\overline{13}^2 = \overline{8}$; $\overline{14}^2 = \overline{12}$; $\overline{15}^2 = \overline{18}$; $\overline{16}^2 = \overline{3}$;
$\overline{17}^2 = \overline{13}$; $\overline{18}^2 = \overline{2}$; $\overline{19}^2 = \overline{16}$; $\overline{20}^2 = \overline{9}$;
$\overline{21}^2 = \overline{4}$; $\overline{22}^2 = \overline{1}$;

Selle põhjal on mooduli 23 järgi kõikvõimalikeks ruutjääkideks $\{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{6}, \overline{8}, \overline{9}, \overline{12}, \overline{13}, \overline{16}, \overline{18}\}$. See on kooskõlas ka loengukonspekti järeldusega 8.6, mis ütleb, et (algarvulise) mooduli 23 järgi leidub $\frac{23-1}{2} = 11$ ruutjääki.

2. ülesanne (Markus Rene Pae ja Erki Kuus)

Vastavalt Euleri kriteeriumile leiame järjest

$$\left(\frac{x}{19}\right) \equiv x^{\frac{19-1}{2}} = x^9 \pmod{19},$$

kus $x \in \{1, \cdots 18\}$. Saame, et

$\overline{1}^9 = \overline{1}$; $\overline{2}^9 = \overline{-1}$; $\overline{3}^9 = \overline{-1}$; $\overline{4}^9 = \overline{2}^9 \cdot \overline{2}^9 = \overline{1}$;
$\overline{5}^9 = \overline{1}$; $\overline{6}^9 = \overline{2}^9 \cdot \overline{3}^9 = \overline{1}$; $\overline{7}^9 = \overline{1}$; $\overline{8}^9 = \overline{4}^9 \cdot \overline{2}^9 = \overline{-1}$;
$\overline{9}^9 = \overline{3}^9 \cdot \overline{3}^9 = \overline{1}$; $\overline{10}^9 = \overline{2}^9 \cdot \overline{5}^9 = \overline{-1}$; $\overline{11}^9 = \overline{1}$; $\overline{12}^9 = \overline{3}^9 \cdot \overline{4}^9 = \overline{-1}$;
$\overline{13}^9 = \overline{-1}$; $\overline{14}^9 = \overline{7}^9 \cdot \overline{2}^9 = \overline{-1}$; $\overline{15}^9 = \overline{5}^9 \cdot \overline{3}^9 = \overline{-1}$; $\overline{16}^9 = \overline{8}^9 \cdot \overline{2}^9 = \overline{1}$;
$\overline{17}^9 = \overline{1}$; $\overline{18}^9 = \overline{9}^9 \cdot \overline{2}^9 = \overline{-1}$; (mod 19)

Seega ruutjäägid on $\{\overline{1}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{9}, \overline{11}, \overline{16}, \overline{17}\}$.See on kooskõlas ka loengukonspekti järeldusega 8.6, mis ütleb, et (algarvulise) mooduli 19 järgi leidub $\frac{19-1}{2} = 9$ ruutjääki.

3. ülesanne (Johanna Maria Kirss ja Rainer Bõkov)

Kuna $29 \equiv 1 \pmod 4$, siis lause 8.8 omaduse 3 põhjal $\left(\frac{-1}{29}\right) = 1$ ja seega $\left(\frac{a}{29}\right) = \left(\frac{p-a}{29}\right)$. Järelikult piisab leida pooled Legendre'i sümboli väärtustest. Kuna $29 \equiv -3 \pmod 8$, siis teoreemi 8.11 põhjal $\left(\frac{2}{29}\right) = -1$. Kasutame täisarvu 3 puhul Euleri kriteeriumi ja ülejäänute jaoks omadusi lausest 8.8.

Lauri Tart: Arvu 3 puhul saab siin samuti läbi ilma arvutusmahukat Euleri kriteeriumit kasutamata:

$$\left(\frac{3}{29}\right) = \left(\frac{3+29}{29}\right) = \left(\frac{2^5}{29}\right) = \left(\frac{2}{29}\right) = -1.$$

Niisiis

$$\left(\frac{1}{29}\right) = 1,\ \left(\frac{2}{29}\right) = -1,\ \left(\frac{3}{29}\right) \equiv 3^{14} \equiv -1 \pmod{29},\ \left(\frac{4}{29}\right) = \left(\frac{2^2}{29}\right) = (-1)^2 = 1,$$

$$\left(\frac{5}{29}\right) = \left(\frac{24}{29}\right) = \left(\frac{2^3}{29}\right) \cdot \left(\frac{3}{29}\right) = (-1)^3 \cdot (-1) = 1,$$

$$\left(\frac{6}{29}\right) = \left(\frac{2}{29}\right) \cdot \left(\frac{3}{29}\right) = -1 \cdot (-1) = 1,\ \left(\frac{7}{29}\right) = \left(\frac{36}{29}\right) = \left(\frac{6^2}{29}\right) = 1^2 = 1,$$

$$\left(\frac{8}{29}\right) = \left(\frac{2^3}{29}\right) = (-1)^3 = -1,\ \left(\frac{9}{29}\right) = \left(\frac{3^2}{29}\right) = (-1)^2 = 1,$$

$$\left(\frac{10}{29}\right) = \left(\frac{2}{29}\right) \cdot \left(\frac{5}{29}\right) = -1 \cdot 1 = -1,\ \left(\frac{11}{29}\right) = \left(\frac{18}{29}\right) = \left(\frac{2}{29}\right) \cdot \left(\frac{9}{29}\right) = -1 \cdot 1 = -1,$$

$$\left(\frac{12}{29}\right) = \left(\frac{3}{29}\right) \cdot \left(\frac{4}{29}\right) = -1 \cdot 1 = -1,\ \left(\frac{13}{29}\right) = \left(\frac{16}{29}\right) = \left(\frac{2^4}{29}\right) = (-1)^4 = 1,$$

$$\left(\frac{14}{29}\right) = \left(\frac{2}{29}\right) \cdot \left(\frac{7}{29}\right) = -1 \cdot 1 = -1.$$

Saame, et ruutjäägid mooduli 29 järgi on 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28.

4. ülesanne (Mikael Raihhelgauz ja Maret Sõmer)

a) $x^2 \equiv -1 \pmod{17}$
Kõigepealt panen tähele, et 17 on algarv.
Definitsiooni 8.1 kohaselt on -1 ruutjääk mooduli 17 järgi, kui kongruents $x^2 \equiv -1 \pmod{17}$ on lahenduv. Kontrollin, kas -1 on ruutjääk mooduli 17 järgi. Selleks peab Legendre'i sümbol $\left(\frac{-1}{17}\right) = 1$. Lause 8.8 omadusest 3) saan, et $\left(\frac{-1}{17}\right) = 1$, kuna $17 \equiv 1 \pmod 4$. Seega -1 on ruutjääk mooduli 17 järgi, ning kongruents $x^2 \equiv -1 \pmod{17}$ **on lahenduv**.
Teoreemist 7.33 saan, et kui kongruents $x^2 \equiv -1 \pmod{17}$ on lahenduv, siis sellel on täpselt $d = (2,\varphi(17))$ erinevat lahendit. Kuna $\varphi(17) = 16$ ning $(2,16) = 2$, siis kongruentsil $x^2 \equiv -1 \pmod{17}$ on **2 erinevat lahendit**.

b) $x^2 \equiv 8 \pmod{19}$
Kõigepealt panen tähele, et 19 on algarv.
Definitsiooni 8.1 kohaselt on 8 ruutjääk mooduli 19 järgi, kui kongruents $x^2 \equiv 8 \pmod{17}$ on lahenduv. Kontrollin, kas 8 on ruutjääk mooduli 19 järgi. Selleks peab Legendre'i sümbol $\left(\frac{8}{19}\right) = 1$. Lause 8.8 omadusest 2), kuna $19 \nmid 2$, saan et $\left(\frac{8}{19}\right) = \left(\frac{2\cdot 2^2}{19}\right) = \left(\frac{2}{19}\right)$ ning teoreemist 8.11 saan, et $\left(\frac{2}{19}\right) = -1$, kuna $19 \equiv 3 \pmod 8$. Seega 8 ei ole ruutjääk mooduli 19 järgi, mis tähendab, et kongruents $x^2 \equiv 8 \pmod{19}$ **ei ole lahenduv**.

c) $x^2 \equiv -2 \pmod{2017}$
Kõigepealt panen tähele, et 2017 on algarv.
Definitsiooni 8.1 kohaselt on -2 ruutjääk mooduli 2017 järgi, kui kongruents $x^2 \equiv -2 \pmod{2017}$ on lahenduv. Kontrollin, kas -2 on ruutjääk mooduli 2017 järgi. Selleks peab Legendre'i sümbol $\left(\frac{-2}{2017}\right) = 1$. Lause 8.8 omadusest 1) saan, et $\left(\frac{-2}{2017}\right) = \left(\frac{-1}{2017}\right)\left(\frac{2}{2017}\right)$. Lause 8.8 omadusest 3) saan, et $\left(\frac{-1}{2017}\right) = 1$, kuna $2017 \equiv 1 \pmod 4$. Teoreemist 8.11 saan, et $\left(\frac{2}{2017}\right) = 1$, kuna $2017 \equiv 1 \pmod 8$. Seega $\left(\frac{-2}{2017}\right) = 1 \cdot 1 = 1$. Järelikult -2 on ruutjääk mooduli 2017 järgi, ning kongruents $x^2 \equiv -2 \pmod{2017}$ **on lahenduv**.
Teoreemist 7.33 saan, et kui kongruents $x^2 \equiv -2 \pmod{2017}$ on lahenduv, siis sellel on täpselt $d = (2,\varphi(2017))$ erinevat lahendit. Kuna $\varphi(2017) = 2016$ ning $(2,2016) = 2$, siis kongruentsil $x^2 \equiv -2 \pmod{2017}$ on **2 erinevat lahendit**.

d) $x^2 \equiv -8 \pmod{2019}$
Kõigepealt panen tähele, et arvu 2019 standardkuju on $2019 = 3 \cdot 673$. Seega kongruents $x^2 \equiv -8 \pmod{2019}$ on lause 6.10 põhjal samaväärne kongurentside süsteemiga
$$\begin{cases} x^2 \equiv -8 \pmod 3 \\ x^2 \equiv -8 \pmod{673} \end{cases} \Rightarrow \begin{cases} x^2 \equiv 1 \pmod 3 \\ x^2 \equiv -8 \pmod{673} \end{cases}$$
Järelikult selleks, et kongruents $x^2 \equiv -8 \pmod{2019}$ oleks lahenduv, peavad mõlemad kongruentsid $x^2 \equiv 1 \pmod 3$ ja $x^2 \equiv -8 \pmod{673}$ olema lahenduvad.

- $x^2 \equiv 1 \pmod 3$
  On ilmne, et see kongruents on lahenduv, ning sellel on 2 erinevat lahendit: $x \equiv 1$ ja $x \equiv 2 \pmod 3$.
- $x^2 \equiv -8 \pmod{673}$
  Definitsiooni 8.1 kohaselt on -8 ruutjääk mooduli 673 järgi, kui kongruents $x^2 \equiv -8$

(mod 673) on lahenduv. Kontrollin, kas -8 on ruutjääk mooduli 673 järgi. Selleks peab Legendre'i sümbol $\left(\frac{-8}{673}\right) = 1$. Lause 8.8 omadusest 1) saan, et $\left(\frac{-8}{673}\right) = \left(\frac{-1}{673}\right)\left(\frac{8}{673}\right)$. Lause 8.8 omadusest 3) saan, et $\left(\frac{-1}{673}\right) = 1$, kuna $673 \equiv 1 \pmod 4$. Lause 8.8 omadusest 2), kuna $673 \nmid 2$, saan et $\left(\frac{8}{673}\right) = \left(\frac{2\cdot 2^2}{673}\right) = \left(\frac{2}{673}\right)$. Teoreemist 8.11 saan, et $\left(\frac{2}{673}\right) = 1$, kuna $673 \equiv 1 \pmod 8$. Seega $\left(\frac{-8}{673}\right) = 1 \cdot 1 = 1$. Järelikult -8 on ruutjääk mooduli 673 järgi, ning kongruents $x^2 \equiv -8 \pmod{673}$ on lahenduv.
Teoreemist 7.33 saan, et kui kongruents $x^2 \equiv -8 \pmod{673}$ on lahenduv, siis sellel on täpselt $d = (2,\varphi(673))$ erinevat lahendit. Kuna $\varphi(673) = 672$ ning $(2,672) = 2$, siis kongruentsil $x^2 \equiv -8 \pmod{673}$ on 2 erinevat lahendit.

Kuna kongruentside süsteemi mõlemad kongruentsid on lahenduvad, siis järelikult ka kongurentside süsteem, ehk ka algne kongruents $x^2 \equiv -8 \pmod{2019}$ **on lahenduv**.
Kui kongruentside süsteemi kongruentsidel on vastavalt 2 ja 2 erinevat lahendit, siis on süsteemil kokku $2 \cdot 2 = 4$ erinevat lahendit. Seega algsel kongruentsil on **4 erinevat lahendit**.

e) $x^2 \equiv -2 \pmod{2018}$
Kõigepealt panen tähele, et arvu 2018 standardkuju on $2018 = 2 \cdot 1009$. Seega kongruents $x^2 \equiv -2 \pmod{2018}$ on lause 6.10 põhjal samaväärne kongurentside süsteemiga
$$\begin{cases} x^2 \equiv -2 \pmod 2 \\ x^2 \equiv -2 \pmod{1009} \end{cases} \Rightarrow \begin{cases} x^2 \equiv 0 \pmod 2 \\ x^2 \equiv -2 \pmod{1009} \end{cases}$$
Järelikult selleks, et kongruents $x^2 \equiv -2 \pmod{2018}$ oleks lahenduv, peavad mõlemad kongruentsid $x^2 \equiv 0 \pmod 2$ ja $x^2 \equiv -2 \pmod{1009}$ olema lahenduvad.

- $x^2 \equiv 0 \pmod 2$
  On ilmne, et see kongruents on lahenduv, ning sellel on 1 lahend: $x \equiv 0 \pmod 2$.
- $x^2 \equiv -2 \pmod{1009}$
  Definitsiooni 8.1 kohaselt on -2 ruutjääk mooduli 1009 järgi, kui kongruents $x^2 \equiv -2 \pmod{1009}$ on lahenduv. Kontrollin, kas -2 on ruutjääk mooduli 1009 järgi. Selleks peab Legendre'i sümbol $\left(\frac{-2}{1009}\right) = 1$. Lause 8.8 omadusest 1) saan, et $\left(\frac{-2}{1009}\right) = \left(\frac{-1}{1009}\right)\left(\frac{2}{1009}\right)$. Lause 8.8 omadusest 3) saan, et $\left(\frac{-1}{1009}\right) = 1$, kuna $1009 \equiv 1 \pmod 4$. Teoreemist 8.11 saan, et $\left(\frac{2}{1009}\right) = 1$, kuna $1009 \equiv 1 \pmod 8$. Seega $\left(\frac{-2}{1009}\right) = 1 \cdot 1 = 1$. Järelikult -2 on ruutjääk mooduli 1009 järgi, ning kongruents $x^2 \equiv -2 \pmod{1009}$ on lahenduv.
  Teoreemist 7.33 saan, et kui kongruents $x^2 \equiv -2 \pmod{1009}$ on lahenduv, siis sellel on täpselt $d = (2,\varphi(1009))$ erinevat lahendit. Kuna $\varphi(1009) = 1008$ ning $(2,1008) = 2$, siis kongruentsil $x^2 \equiv -2 \pmod{1009}$ on 2 erinevat lahendit.

Kuna kongruentside süsteemi mõlemad kongruentsid on lahenduvad, siis järelikult ka kongurentside süsteem, ehk ka algne kongruents $x^2 \equiv -2 \pmod{2018}$ **on lahenduv**.
Kui kongruentside süsteemi kongruentsidel on vastavalt 1 ja 2 erinevat lahendit, siis on süsteemil kokku $1 \cdot 2 = 2$ erinevat lahendit. Seega algsel kongruentsil on **2 erinevat lahendit**.

f) $x^2 \equiv 19 \pmod{2020}$

Kõigepealt panen tähele, et arvu 2020 standardkuju on $2020 = 2^2 \cdot 5 \cdot 101$. Seega kongruents $x^2 \equiv 19 \pmod{2020}$ on lause 6.10 põhjal samaväärne kongurentside süsteemiga

$$\begin{cases} x^2 \equiv 19 \pmod{2^2} \\ x^2 \equiv 19 \pmod{5} \\ x^2 \equiv 19 \pmod{101} \end{cases} \Rightarrow \begin{cases} x^2 \equiv -1 \pmod{4} \\ x^2 \equiv -1 \pmod{5} \\ x^2 \equiv 19 \pmod{101} \end{cases}$$

Järelikult selleks, et kongruents $x^2 \equiv 19 \pmod{2020}$ oleks lahenduv, peavad kõik kongruentsid $x^2 \equiv -1 \pmod{4}$, $x^2 \equiv -1 \pmod{5}$ ja $x^2 \equiv 19 \pmod{101}$ olema lahenduvad.

- $x^2 \equiv -1 \pmod{4}$
  Proovin läbi kõik võimalikud lahendid:
  - $x \equiv 0 \pmod{4}$: $x^2 \equiv 0 \not\equiv -1 \pmod{4}$
  - $x \equiv 1 \pmod{4}$: $x^2 \equiv 1 \not\equiv -1 \pmod{4}$
  - $x \equiv 2 \pmod{4}$: $x^2 \equiv 4 \equiv 0 \not\equiv -1 \pmod{4}$
  - $x \equiv 3 \pmod{4}$: $x^2 \equiv 9 \equiv 1 \not\equiv -1 \pmod{4}$

  Seega kongruents $x^2 \equiv -1 \pmod{4}$ ei ole lahenduv.

Kuna üks kongruentsi süsteemi kongruentsidest ei ole lahenduv, siis ka kongruentside süsteem, ehk ka algne kongruents $x^2 \equiv 19 \pmod{2020}$ **ei ole lahenduv**.

5. ülesanne (Markus Rene Pae ja Erki Kuus)

Selles ülesandes on vaja leida kõik algarvud p (või tingimus selliste algarvude jaoks), et

$$\left(\frac{-18}{p}\right) = 1.$$

Esiteks, kui $p = 2$ või $p = 3$, siis vastavalt Legendre'i sümboli definitsioonist $2 \mid -18$ või $3 \mid -18$, millest järeldub automaatselt, et $\left(\frac{-18}{p}\right) = 0$. Seega $p > 3$.

Saame rakendada loengukonspekti lause 8.8 nimekirjas olevat 2. omadust:

$$\left(\frac{-18}{p}\right) = \left(\frac{-2 \cdot 3^2}{p}\right) = \left(\frac{-2}{p}\right).$$

Seda lauset saab rakendada ainult seepärast, et $p > 3$, millest järeldub, et $3 \nmid p$. Kui rakendada loengukonspekti lause 8.8 nimekirjas toodud 1. omadust, siis:

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) = 1.$$

Kahe Legendre'i sümboli korrutis on võrdne ühega parajasti siis, kui mõlemad sümbolid on samaaegselt võrdsed 1-ga või samaaegselt võrdsed -1-ga.

1. Kui $\left(\frac{-1}{p}\right) = 1$ ja $\left(\frac{2}{p}\right) = 1$, siis sellest järeldub

   $$p \equiv 1 \pmod 4 \quad \text{ning} \quad p \equiv \pm 1 \pmod 8.$$

   Kuna $p \equiv 1 \pmod 4$ on samaväärne kongruentsiga $p \equiv 1{,}5 \pmod 8$, siis antud tingimusest saame kätte selle, et $p \equiv 1 \pmod 8$ (muud tingimused viitavad vastuoluni).

2. Kui $\left(\frac{-1}{p}\right) = -1$ ja $\left(\frac{2}{p}\right) = -1$, siis sellest järeldub

   $$p \equiv 3 \pmod 4 \quad \text{ning} \quad p \equiv \pm 3 \pmod 8.$$

   Kuna $p \equiv 1 \pmod 4$ on samaväärne kongruentsiga $p \equiv 3{,}7 \pmod 8$, siis antud tingimusest saame kätte selle, et $p \equiv 3 \pmod 8$ (muud tingimused viitavad vastuoluni).

Järelikult -18 on ruutjääk mooduli p järgi parajasti siis, kui $p > 3$ ning p annab 8-ga jagamisel jäägiks kas 1 või 3. Selliseid algarve, mis on kujul $8k + 1$ või $8k + 3$, on Dirichlet' teoreemile tuginedes lõpmata palju.

6. ülesanne (Johanna Maria Kirss ja Rainer Bõkov)

Näitame, et aritmeetilises jadas leidub lõpmatult täisruute parajasti siis, kui temas leidub vähemalt üks täisruut. On ilmne, et kui jadas leidub lõpmatult palju täisruute, siis temas leidub vähemalt üks täisruut. Näitame teistpidi implikatsiooni. Fikseerime mingid a,$b \in \mathbb{N}$, millega defineerime jada $(a+nb)_{n=1}^{\infty}$. Olgu mingi $k \in \mathbb{N}$ korral $a+kb$ täisruut ehk leidugu mingi $x \in \mathbb{N}$ nii, et $x^2 = a+kb$. Fikseerime nüüd mingi naturaalarvu l. Siis

$$(x+lb)^2 = x^2 + 2xlb + l^2b^2 = (a+kb) + (2xl + l^2b)b = a + (k + 2xl + l^2b)b \in (a+nb).$$

Näeme, et iga $l \in \mathbb{N}$ korral kuulub täisruut $(x+lb)^2$ algsesse jadasse ning seega sisaldab jada $(a+nb)$ lõpmata palju täisruute.

Märkame, et kõik arvud jadas $(a+nb)$ on mooduli b järgi kongruentsed arvuga a. Seega piisab meil leida, kunas on lahenduv kongruents $x^2 \equiv a \pmod{b}$. Kui kongruents pole lahenduv, siis ilmselt pole ühegi täisarvu korral võimalik saada arvu, mis kuuluks sellesse jadasse. Kui aga kongruents on lahenduv, siis on jadas lõpmata palju täisruute.

Seega on piisav ja tarvilik tingimus selleks, et jadas oleks lõpmatult palju täisruute see, et kongruents $x^2 \equiv a \pmod{b}$ omab mingit lahendit.

Lauri Tart: Ehk teisisõnu, arv a on ruutjääk (või 0) mooduli b järgi.

7. ülesanne (lahenduse autorid on toimetusele teada)

Vaatame arvupaare, mille summa on $-1 = p-1$ mooduli p järgi:

0	$p-1$
1	$p-2$
2	$p-3$
$\dots$	$\dots$
$\frac{p-1}{2}$	$\frac{p-1}{2}$

Näeme, et selliseid paare on kokku $\frac{p-1}{2}+1$ tükki, seejuures ükski arv ei esine rohkem kui ühes paaris.

Samas järelduse 8.6 põhjal on täpselt $\frac{p-1}{2}$ mitteruutjääki, seega Dirichlet' printsiibi põhjal leidub vähemalt üks paar, kus kumbki liidetav ei ole mitteruutjääk (ehk on $0 = 0^2$ või ruutjääk), seega saame vastavast reast selle kongruentsi lahendi.

8. ülesanne (Mikael Raihhelgauz ja Maret Sõmer)

Vaatleme kõiki mod p nullist erinevaid jääke kasvavas järjekorras: $\bar{1}, \bar{2}, \ldots, \overline{p-1}$. Oletame vastuväiteliselt, et kunagi ei paikne kaks ruutjääki kõrvuti. Kuna $\bar{1}$ on igal juhul ruutjääk, peab 2 olema mitteruutjääk ning lause 8.8 põhjal

$$\left(\frac{4}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{2}{p}\right) = (-1)\cdot(-1) = 1$$

ehk 4 on ruutjääk. 3 ja 5 peavad seega olema mitteruutjäägid. Kuna ringis $\mathbb{Z}_p$ on võrdne arv ruutjääke ja mitteruutjääke, siis eelduse kohaselt alates neljast peavad need paiknema rangelt vaheldumisi, s.t ülejäänud ruutjäägid on parajasti neljast suuremad paarisarvud.

Lauri Tart: See põhjendus päris ei tööta, sest 6,7,8 võivad meile teadaolevalt siiski kõik olla mitteruutjäägid, kui $p \neq 7$. Dirichlet' printsiipi siin veel rakendada ei saa.

Lahendus: Juhul $p = 7$ on 2 ruutjääk ja meil on ruutjääkide paar (1,2). Kui $p > 7$, st $p \geq 13$, ja 1 ega 4 ei moodusta ruutjääkide paari, siis

$$\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right) = (-1)(-1) = 1 \quad \text{ja alati} \quad \left(\frac{9}{p}\right) = 1.$$

Ehk oleme ikkagi leidnud ruutjääkide paari (9,10).

Kui väga tahta Dirichlet' printsiipi kasutada, siis nii: vaatame teadaolevate ruutjääkide ja mitteruutjääkide asetsemist kuni arvuni 10 ja arvestame, et 9 on samuti ruutjääk, ehk 8 ja 10 ei tohi seda olla:

RMMRM??MRM...

Seejuures ?? tohib sisaldada vaid ühte ruutjääki. Dirichlet' printsiibi kohaselt peab kahte ruutjääki eraldama vähemalt üks mitteruutjääk, seega kümnest suuremate arvude seas peab olema ruutjääkide arv R^+ mitte rohkem kui 1 võrra suurem mitteruutjääkide arvust. Aga siis on kokku ülimalt $R^+ + 4 \leq \lfloor \frac{p-10}{2} \rfloor + 4 = \frac{p-11}{2} + 4 = \frac{p-3}{2}$ ruutjääki, sest p on paaritu. Järelduse 8.6 põhjal peab neid olema aga täpselt $\frac{p-1}{2} > \frac{p-3}{2}$!

Ent

$$\left(\frac{8}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{2}{p}\right) = 1\cdot(-1) = -1.$$

Oleme jõudnud vastuoluni!

Järelikult peab alati leiduma ruutjääkide paar kujul $(\bar{k}, \overline{k+1})$. Vaatleme nüüd seda paari mugavuse mõttes ühe elemendina m (arvestame ta sümboolselt ruutjääkide hulka), mis jääb $\overline{k-1}$ ja $\overline{k+2}$ vahele. Meil on siis $\frac{p-1}{2} - 1$ ruutjääki ja $\frac{p-1}{2}$ mitteruutjääki. Oletame, et igat järjestikuste mitteruutjääkide paari lahutab vähemalt üks ruutjääk. Selliseid paare on kokku $\frac{p-1}{2} - 1$. Ent kogu järjestuse esimene element on kindlasti ruutjääk, seega nn "lahutajaid"saab olla vaid $\frac{p-1}{2} - 2$ tükki. Näeme, et vähemalt ühe järjestikuste mitteruutjääkide paari korral vajalikku lahutajat ei leidu – seega leidub mitteruutjääkide paar $(\bar{l}, \overline{l+1})$.