Arvuteooria

Kevad 2020

14. praktikumi näidislahendused

1. ülesanne (Mikael Raihhelgauz ja Maret Sõmer)

Ülesandes on vaja leida Jacobi sümboli väärtused.

a) $\left(\frac{667}{941}\right)$

Kuna 667 ja 941 on mõlemad paaritud arvud, ning $941 \equiv 1 \pmod 4$, siis $\left(\frac{667}{941}\right) = \left(\frac{941}{667}\right)$.

Kuna $941 \equiv 274 \pmod{667}$, siis $\left(\frac{941}{667}\right) = \left(\frac{274}{667}\right)$. $\left(\frac{274}{667}\right) = \left(\frac{2\cdot 137}{667}\right)$.

Kuna 667 on paaritu arv , siis $\left(\frac{2\cdot 137}{667}\right) = \left(\frac{2}{667}\right)\left(\frac{137}{667}\right)$.

Kuna $667 \equiv 3 \pmod 8$, siis $\left(\frac{2}{667}\right) = -1$.

Kuna 137 ja 667 on mõlemad paaritud arvud, ning $137 \equiv 1 \pmod 4$, siis $\left(\frac{137}{667}\right) = \left(\frac{667}{137}\right)$.

Kuna $667 \equiv 119 \pmod{137}$, siis $\left(\frac{667}{137}\right) = \left(\frac{119}{137}\right)$.

Kuna 119 ja 137 on mõlemad paaritud arvud, ning $137 \equiv 1 \pmod 4$, siis $\left(\frac{119}{137}\right) = \left(\frac{137}{119}\right)$.

Kuna $137 \equiv 18 \pmod{119}$, siis $\left(\frac{137}{119}\right) = \left(\frac{18}{119}\right)$. $\left(\frac{18}{119}\right) = \left(\frac{2\cdot 9}{119}\right) = \left(\frac{2\cdot 3^2}{119}\right)$

Kuna 119 on paaritu arv ning (3,119)=1, siis $\left(\frac{2\cdot 3^2}{119}\right) = \left(\frac{2}{119}\right)$.

Kuna $119 \equiv -1 \pmod 8$, siis $\left(\frac{2}{119}\right) = 1$.

Seega $\left(\frac{667}{941}\right) = \left(\frac{2}{667}\right)\left(\frac{137}{667}\right) = -1 \cdot 1 = -1$

b) $\left(\frac{451}{691}\right)$

Kuna 451 ja 691 on mõlemad paaritud arvud, ning $451 \equiv 691 \equiv 3 \pmod 4$, siis $\left(\frac{451}{691}\right) =$
$= -\left(\frac{691}{451}\right)$.

Kuna $691 \equiv 240 \pmod{451}$, siis $-\left(\frac{691}{451}\right) = -\left(\frac{240}{451}\right)$.

$-\left(\frac{240}{451}\right) = -\left(\frac{2^4\cdot 15}{451}\right) = -\left(\frac{15\cdot (2^2)^2}{451}\right)$.

Kuna 451 on paaritu arv ning (2,451)=1, siis $-\left(\frac{15\cdot (2^2)^2}{451}\right) = -\left(\frac{15}{451}\right)$.

Kuna 15 ja 451 on mõlemad paaritud arvud, ning $15 \equiv 451 \equiv 3 \pmod 4$, siis $-\left(\frac{15}{451}\right) =$
$= -\Big(-\left(\frac{451}{15}\right)\Big) = \left(\frac{451}{15}\right)$.

Kuna $451 \equiv 1 \pmod{15}$, siis $\left(\frac{451}{15}\right) = \left(\frac{1}{15}\right)$.

Jacobi sümboli definitsioonist $\left(\frac{1}{15}\right) = \left(\frac{1}{3}\right)\left(\frac{1}{5}\right)$ ning lause 8.8 omadusest 3) $\left(\frac{1}{3}\right)\left(\frac{1}{5}\right) = = 1 \cdot 1 = 1$.

Seega $\left(\frac{451}{691}\right) = 1$.

c) $\left(\frac{8439}{6661}\right)$

Kuna $8439 \equiv 1778 \pmod{667}$, siis $\left(\frac{8439}{6661}\right) = \left(\frac{1778}{6661}\right)$. $\left(\frac{1778}{6661}\right) = \left(\frac{2 \cdot 889}{6661}\right)$.

Kuna 6661 on paaritu arv , siis $\left(\frac{2 \cdot 889}{6661}\right) = \left(\frac{2}{6661}\right)\left(\frac{889}{6661}\right)$.

Kuna $6661 \equiv -3 \pmod{8}$, siis $\left(\frac{2}{6661}\right) = -1$.

Kuna 889 ja 6661 on mõlemad paaritud arvud, ning $889 \equiv 1 \pmod{4}$, siis $\left(\frac{889}{6661}\right) = = \left(\frac{6661}{889}\right)$.

Kuna $6661 \equiv 438 \pmod{889}$, siis $\left(\frac{6661}{889}\right) = \left(\frac{438}{889}\right)$. $\left(\frac{438}{889}\right) = \left(\frac{2 \cdot 219}{889}\right)$.

Kuna 889 on paaritu arv , siis $\left(\frac{2 \cdot 219}{889}\right) = \left(\frac{2}{889}\right)\left(\frac{219}{889}\right)$.

Kuna $889 \equiv 1 \pmod{8}$, siis $\left(\frac{2}{889}\right) = 1$.

Kuna 219 ja 889 on mõlemad paaritud arvud, ning $889 \equiv 1 \pmod{4}$, siis $\left(\frac{219}{889}\right) = \left(\frac{889}{219}\right)$.

Kuna $889 \equiv 13 \pmod{219}$, siis $\left(\frac{889}{219}\right) = \left(\frac{13}{219}\right)$.

Kuna 13 ja 219 on mõlemad paaritud arvud, ning $13 \equiv 1 \pmod{4}$, siis $\left(\frac{13}{219}\right) = \left(\frac{219}{13}\right)$.

Kuna $219 \equiv 11 \pmod{13}$, siis $\left(\frac{219}{13}\right) = \left(\frac{11}{13}\right)$.

Kuna 11 ja 13 on mõlemad paaritud arvud, ning $13 \equiv 1 \pmod{4}$, siis $\left(\frac{11}{13}\right) = \left(\frac{13}{11}\right)$.

Kuna $13 \equiv 2 \pmod{11}$, siis $\left(\frac{13}{11}\right) = \left(\frac{2}{11}\right)$.

Kuna $11 \equiv 3 \pmod{4}$, siis $\left(\frac{2}{11}\right) = -1$.

Seega $\left(\frac{8439}{6661}\right) = \left(\frac{2}{6661}\right)\left(\frac{889}{6661}\right) = -1 \cdot \left(\frac{2}{889}\right)\left(\frac{219}{889}\right) = -1 \cdot 1 \cdot (-1) = 1$

2. ülesanne (Erki Külaots ja Marcus Lõo)

Leiame, milliste algarvuliste moodulite p järgi on 3 ruutjääk, ehk uurime, millal kehtib

$$\left(\frac{3}{p}\right) = 1, \quad p \in \mathbb{P}.$$

Esiteks, kui $p = 2$, siis peaks olema kongruents $x^2 \equiv 3 \equiv 1 \pmod 2$ lahenduv. Seda ta ka on, lahendiks on $x_0 \equiv 1$. Teiseks, kui $p = 3$, siis pole 3 ruutjääk, sest $\left(\frac{3}{3}\right) = 0$.
Jääb vaadata juhud, kui $p \neq 3 \wedge p \neq 2$. Siis saame kasutada ruutvastavusseadust:

$$\left(\frac{3}{p}\right) = (-1)^{\frac{2(p-1)}{4}} \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right).$$

Siin on kaks juhtu. Kui $p \equiv 1 \pmod 4$, siis on $\frac{p-1}{2}$ paarisarv ja

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right).$$

Uurime millal $\left(\frac{p}{3}\right) = 1$, s.t. kongruents

$$x^2 \equiv p \pmod 3$$

on lahenduv. Ka siin on erinevad juhud. Kui $p \equiv 1 \pmod 3$, siis on ta lahenduv. Kongruents $x^2 \equiv 2 \pmod 3$ aga pole lahenduv. Kokkuvõttes saame siit, et kui $p \equiv 1 \pmod 4 \wedge p \equiv 1 \pmod 3$, siis on 3 ruutjääk mod p. Kasutame selle süsteemi leidmiseks Hiina jäägiteoreemi:

$$\begin{aligned} m_1 = 4, k_1 = 1; \quad m_2 = 3, k_2 = 3 \\ p = 4 + 3 \cdot 3 = 13 \equiv 1 \pmod{12}. \end{aligned}$$

Seega $p \equiv 1 \pmod{12}$.
Teine juht on, kui $p \equiv 3 \pmod 4$. Kuna ka $3 \equiv 3 \pmod 4$, siis

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right).$$

Järelikult on arvu 3 ruutjäägiks olemiseks tarvilik, et $\left(\frac{p}{3}\right) = -1$ ehk kongruents

$$x^2 \equiv p \pmod 3$$

pole lahenduv. Eelnevast teame, et on võimalik siis, kui $p \equiv 2 \pmod 3$, sest juhul $p \equiv 1 \pmod 3$ on see lahenduv. Seega, kui $p \equiv 2 \pmod 3 \wedge p \equiv 3 \pmod 4$, siis on 3 ruutjääk mooduli p järgi. Taas HJT-d rakendades saame, et $p \equiv 11 \pmod{12}$.

Teiseks kontrollime, millise $p \in \mathbb{P}$ korral on 5 ruutjääk mod p.
Kui $p = 2$, siis peab kehtima

$$\left(\frac{5}{2}\right) = 1.$$

See kehtib sarnastel kaalutustel ülesande esimese poolega.
Kui $p = 3$, siis peab lahenduma kongruents

$$x^2 \equiv 5 \equiv 2 \pmod 3.$$

See pole lahenduv, seega sellisel juhul pole 5 ruutjääk.
$p = 5$, siis pole 5 ruutjääk triviaalselt.
Nüüd vaatleme juhte, kui $p > 5$. Kasutame taas ruutvastavusseadust.

$$\left(\frac{5}{p}\right) = (-1)^{\frac{4(p-1)}{4}} \left(\frac{p}{5}\right) = (-1)^{p-1} \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right)$$

Seega vaatleme juhte.
$x^2 \equiv 1 \pmod 5$ on lahenduv.
$x^2 \equiv 2 \pmod 5$ pole lahenduv.
$x^2 \equiv 3 \pmod 5$ pole lahenduv.
$x^2 \equiv 4 \pmod 5$ on lahenduv.
v. Seega oleme saanud, et 5 on ruutjääk siis, kui kas $p = 2$ või $p \equiv \pm 1 \pmod 5$ ja 3 on ruutjääk siis, kui $p \equiv \pm 1 \pmod 3$.

3. ülesanne (Johanna Maria Kirss ja Rainer Bõkov)

Teisendame antud kongruentsi

$$\begin{aligned} x^2 + 4a(x+2) + 4a^2 &\equiv 0 \pmod n, \\ x^2 + 4ax + 4a^2 + 8a &\equiv 0 \pmod n, \\ (x+2a)^2 &\equiv -8a \pmod n. \end{aligned}$$

Tähistades $y = x + 2a$ saame uue muutuja suhtes ruutkongruentsi $y^2 \equiv -8a \pmod n$. Kui $n \equiv 3 \pmod 8$, siis ka $n \equiv 3 \pmod 4$ ja $\left(\frac{2}{n}\right) = -1 = \left(\frac{-1}{n}\right)$. Leiame Legendre'i sümboli väärtuse

$$\left(\frac{-8a}{n}\right) = \left(\frac{2^3}{n}\right)\left(\frac{-1}{n}\right)\left(\frac{a}{n}\right) = (-1)^5 = -1.$$

Märkuse 8.17 põhjal tähendab see kongruentsi mittelahenduvust.

Vastupidine väide üldiselt ei kehti. Näiteks $a = 1$ ja $n = 35$ korral kongruents $y^2 \equiv 27 \pmod{35}$ ei ole lahenduv, aga $\left(\frac{1}{35}\right) = 1 \neq -1$.

4. ülesanne (Erki Külaots ja Marcus Lõo)

Lihtsustame avaldist.

$$\begin{aligned} 6x^2 - 8xy + 10y^2 &= 2018 \\ 3x^2 - 4xy + 5y^2 &= 1009 \end{aligned}$$

Vaatame seda võrdust mooduli 11 järgi.

$$\begin{aligned} 3x^2 - 4xy + 5y^2 &\equiv 1009 \equiv 8 \pmod{11} \\ 3 \cdot (3x^2 - 4xy + 5y^2) &\equiv 3 \cdot 8 \pmod{11} \\ 9x^2 - 12xy + 15y^2 &\equiv 24 \pmod{11} \\ 9x^2 - 12xy + 4y^2 &\equiv 2 \pmod{11} \\ (3x - 2y)^2 &\equiv 2 \pmod{11} \end{aligned}$$

$$\left(\frac{2}{11}\right) = -1$$

Seega sellel võrrandil pole mooduli 11 järgi lahendeid ja järelikult pole ka üldiselt võrdusel $6x^2 - 8xy + 10y^2 = 2018$ täisarvulisi lahendeid.

5. ülesanne (Mikael Raihhelgauz ja Maret Sõmer)

Olgu $p > 7$ suvaline algarv. Oletame vastuväiteliselt, et mooduli p järgi ei leidu kahte järjestikust ruutjääki. Et 1 on kindlasti ruutjääk, siis 2 peab olema mitteruutjääk. Järelikult 4 on ruutjääk, sest lause 8.8 põhjal

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

Eelduse kohaselt 3 ja 5 on mitteruutjäägid. Ühtlasi

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

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

$$\left(\frac{9}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{3}{p}\right) = -1 \cdot (-1) = 1.$$

7 peab olema mitteruutjääk, sest järgneb ruutjäägile. Kokkuvõttes peab kindlasti kehtima järjestus:

1,	2, 3,	4, 5,	6, 7,	8, 9
R,	M, M,	R, M,	M, R,	M, R.

Järelduse 8.6 kohaselt ruutjääke ja mitteruutjääke peab olema ringis $\mathbb{Z}_p$ võrdselt. Oleme "kasutanud ära"4 ruutjääki ja 5 mitteruutjääki ehk jäänud on veel $\frac{p-1}{2} - 4$ ruutjääki ja $\frac{p-1}{2} - 5$ mitteruutjääki. Samas eelduse kohaselt peab igale järgmisele ruutjäägile vahetult eelnema vähemalt üks mitteruutjääk. Et aga "kasutamata"ruutjääke on ühe võrra rohkem, ei ole niisugune järjestus võimalik.

6. ülesanne (lahenduse autorid on toimetusele teada)

Oletame vastuväiteliselt, et leidub lõplik arv selliseid algarve, olgu need $p_1, p_2, \dots p_n$.

Vaatame arvu $a = (p_1 p_2 \dots p_n)^2 + 4$. Paneme tähele, et kuna $p_i \equiv 5 \pmod 8$ ja $5^2 \equiv 1 \pmod 8$, siis $p_1 p_2 \dots p_n \equiv 1,5 \pmod 8$, millest saame, et $(p_1 p_2 \dots p_n)^2 \equiv 1 \pmod 8$.

Lauri Tart: Lihtsamini:

$$p_i \equiv 1{,}5 \pmod 8 \Longrightarrow p_i^2 \equiv 1^2 = 1 = 5^2 \pmod 8 \Longrightarrow (p_1 p_2 \dots p_n)^2 = p_1^2 p_2^2 \dots p_n^2 = 1 \pmod 7.$$

Järelikult $a \equiv 5 \pmod 8$. a on paaritu arv, seega on ka kõik selle algtegurid paaritud. Olgu p arvu a algtegur, et $p \mid a$ ehk $(p_1 p_2 \dots p_n)^2 \equiv -4 \pmod p$, seega -4 on ruutjääk ehk $1 = \left(\frac{-4}{p}\right) = \left(\frac{-1 \cdot 2^2}{p}\right) = \left(\frac{-1}{p}\right)$.

Lause 8.8 põhjal peab $p \equiv 1 \pmod 4$ ehk $p \equiv 1 \pmod 8$ või $p \equiv 5 \pmod 8$.

Kuna a kõik algtegurid p peavad olema kujul $p \equiv 1 \pmod 8$ või $p \equiv 5 \pmod 8$ ning $a \equiv 5 \pmod 8$, siis peab leiduma mingi algtegur q nii et $q \equiv 5 \pmod 8$ (kuna vastasel juhul $a \equiv 1 \pmod 8$).

Kuna eelduse kohaselt on algarve kujul $8k+5$ lõplik arv, siis $q = p_i$. Seega $q \mid a - (p_1 p_2 \dots p_n) = 4$, ainus sobiv algarv on $q = 2$, mis on aga vastuolus eeldusega, et $2 \nmid a$, kuna $a \equiv 5 \pmod 8$.

Saime vastuolu, seega leidub lõpmata palju algarve kujul $8k + 5$.

7. ülesanne (lahenduse autorid on toimetusele teada)

Oletame vastuväiteliselt, a on kordarv ning vähim mitteruutjääk mooduli p järgi, seega $\left(\frac{a}{p}\right) = -1$

Kuna a on kordarv, siis $a = xy$, kus $1 < x, y < a$, seega

$$-1 = \left(\frac{a}{p}\right) = \left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right) \cdot \left(\frac{y}{p}\right)$$

Seega kuna $-1 = \left(\frac{x}{p}\right) \cdot \left(\frac{y}{p}\right)$, üks teguritest peab olema -1, teine 1 (kuna Legendre'i sümboli võimalikud väärtused on 0, 1 ja -1). Üldistust kitsendamata olgu $-1 = \left(\frac{y}{p}\right)$, mis on samaväärne sellega, et y on mitteruutjääk mooduli p järgi, samas aga $1 < y < a$, mis on vastuolus eeldusega, et a on vähim mitteruutjääk.

Leime vähima algarvu q, mille jaoks 7 on vähim positiivne mitteruutjääk. Seega otsime vähimat algarvu q nii, et $\left(\frac{2}{q}\right) = \left(\frac{3}{q}\right) = \left(\frac{5}{q}\right) = 1$ ning $\left(\frac{7}{q}\right) = -1$.

Eeldusest $\left(\frac{2}{q}\right) = 1$, saame $p \equiv \pm 1 \pmod 8$.

Ülesandest 2 põhjal saame, et $\left(\frac{3}{q}\right) = 1$ on samaväärne sellega, et $q \equiv \pm 1 \pmod{12}$ ning $\left(\frac{3}{q}\right) = 1$ järeldub, et $q \equiv \pm 1 \pmod 5$.

Saame kongruentside süsteemi:

$$\begin{cases} q \equiv \pm 1 \pmod 8 \\ q \equiv \pm 1 \pmod{12} \\ q \equiv \pm 1 \pmod 5 \end{cases}$$

Selle süsteemi lahendid on $q \equiv 1, 49, 71, 119 \pmod{120}$. Vähim algarvuline lahend on seega on $q = 71$, mis on sobiv lahend, kuna $\left(\frac{7}{71}\right) = -1$.

8. ülesanne (Erki Külaots ja Marcus Lõo)

Piisab, kui näitame, et iga algarvu $p = p_k \in \mathbb{P}$ korral kehtib

$$\left(\frac{2}{q}\right) = \left(\frac{3}{q}\right) = \left(\frac{5}{q}\right) = \ldots = \left(\frac{p_{k-1}}{q}\right) = 1 \wedge \left(\frac{p_k}{q}\right) = -1$$

Olgu $q \equiv 1 \pmod 8$, siis esiteks $\left(\frac{2}{q}\right) = 1$ ja teiseks Gaussi ruutvastavusseadusest saame, et $\left(\frac{p_i}{q}\right) = \left(\frac{q}{p_i}\right)$, kus $i \in \mathbb{N}$.

Lauri Tart: Ruutvastavusseaduse rakendamiseks on vaja, et $q \neq p_i$ ja mõlemad on paaritud. Seda alljärgnev kongruentside süsteem tõesti garanteerib, aga need tingimused vajavad siiski välja kirjutamist ja üle kontrollimist.

Seega võime kirjutada uue tingimuse

$$\left(\frac{q}{3}\right) = \left(\frac{q}{5}\right) = \ldots = \left(\frac{q}{p_{k-1}}\right) = 1 \wedge \left(\frac{q}{p_k}\right) = -1$$

Teame, et iga p_i korral $\left(\frac{1}{p_i}\right) = 1$ ja lause 8.4 põhjal, kui $q \equiv 1 \pmod{p_i}$, siis ka $\left(\frac{q}{p_i}\right) = = 1$. Olgu α mitteruutjääk mooduli p_k järgi ehk $\left(\frac{\alpha}{p_k}\right) = -1$, siis kui $q \equiv \alpha \pmod{p_k}$, siis $\left(\frac{q}{p_k}\right) = -1$.

Järelikult saame järgneva lineaarkongruentside süsteemi.

$$\begin{cases} q \equiv 1 & \pmod 8 \\ q \equiv 1 & \pmod 3 \\ q \equiv 1 & \pmod 5 \\ \quad \ldots & \\ q \equiv 1 & \pmod{p_{k-1}} \\ q \equiv \alpha & \pmod{p_k} \end{cases}$$

Kuna mooduliteks on paarikaupa erinevad algarvud ja 2^3, siis nad on paarikaupa ühistegurita ning teame tänu Hiina jäägiteoreemile, et sellele leidub ühene lahend c mooduli $8 \cdot 3 \cdot \ldots \cdot p_{k-1} \cdot p_k$ järgi. Ehk q on kujul $q = 8 \cdot 3 \cdot \ldots \cdot p_{k-1} \cdot p_k \cdot m + c$, kus $m \in \mathbb{N}$.

Dirichlet' teoreemist saame, et kui $(c, 8 \cdot 3 \cdot \ldots \cdot p_{k-1} \cdot p_k) = 1$, siis aritmeetilises jadas $8 \cdot 3 \cdot \ldots \cdot p_{k-1} \cdot p_k \cdot m + c$ leidub lõpmatu palju algarve. Kui oleks $(c, 8 \cdot 3 \cdot \ldots \cdot p_{k-1} \cdot p_k) \neq 1$, siis leiduks p_i, et $p_i \mid c \iff \exists s \in \mathbb{Z} \colon p_i \cdot s = c$, aga see ei sobiks kokku lineaarkongruentside süsteemiga, sest siis $q \equiv 8 \cdot 3 \cdot \ldots \cdot p_k \cdot m + p_i \cdot s \equiv 0 \pmod{p_i}$, kuid see pole võimalik. Järelikult $(c, 8 \cdot 3 \cdot \ldots \cdot p_{k-1} \cdot p_k) = 1$ ja leidub algarv q kujul $q = 8 \cdot 3 \cdot \ldots \cdot p_{k-1} \cdot p_k \cdot m + c$.

Lauri Tart: Teine variant on veel: $2 \mid (c, 8 \cdot 3 \cdot \ldots \cdot p_{k-1} \cdot p_k)$, mis viib vastuoluni kongruentsiga $q \equiv 1 \pmod 8$, kuna siis $2 \mid q = 8k + 1$.

See konstruktsioon eeldab, et p_k on paaritu seega näitame, et $p = 2$ on ka mingi algarvu jaoks vähim positiivne mitteruutjääk. Selleks paneme tähele, et $\left(\frac{0}{3}\right) = 0$, $\left(\frac{1}{3}\right) = 1$ ja $\left(\frac{2}{3}\right) = -1$. Seega kui $p = 2$, siis $q = 3$.

Lauri Tart: Kui $p = 2$, siis väide tegelikult ei kehti, sest sel juhul ei ole ühtegi mitteruutjääki üleüldse olemas.