Kodutöö nr. 13

Joosep Näks ja Uku Hannes Arismaa

1. Leida otse, pööratavate elementide ruute järjest välja arvutades, kõik ruutjäägid mooduli 29 järgi.

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14
x^2	1	4	9	16	25	7	20	6	23	13	5	28	24	22

Ülejäänud tabelis oleks samad ruutjäägid, kuna $(-x)^2 = x^2$.

2. Leida kõik ruutjäägid mooduli 31 järgi Euleri kriteeriumi abil.

Euleri kriteeriumi põhjal on Legendre'i sümbol $\left(\frac{a}{31}\right)$ kongruentne arvuga a^{15} mooduli 31 järgi ning arv a on ruutjääk parajasti siis kui $\left(\frac{a}{31}\right) = 1$. Kui aga $a^{15} \equiv -1$, siis kuna $31 \equiv 3 \pmod 4$, saab lause 8.8 põhjal et $(-a)^{15} \equiv 1$ ehk on vaja leida vaid esimesed pooled a^{15} väärtused ning kui $\left(\frac{a}{31}\right) = -1$, siis on $-a$ ruutjääk. Seega leian $a^{15} \pmod{31}$ väärtused:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a^{15}	1	1	-1	1	1	-1	1	1	1	1	-1	-1	-1	1	-1

Ehk ruutjäägid on $1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28$.

3. Leida kõik ruutjäägid mooduli 37 järgi Legendre'i sümboli omaduste abil.

Teame, et 1 on ruutjääk, seega saame seda läbi korrutades täisruutudega teisi ruutjääke. Nii saame veel 4, 9, 16, 25 ning $36 = -1$. Kuna -1 on täisruut, saame sellega täisruudu läbi korrutades uue täisruudu. Nii saame $-25 = 12 = 3 \cdot 2^2$, seega on täisruut ka $3 \cdot 3^2 = 27$. Analoogselt $-16 = 21 = 7 \cdot 3$, seega on täisruut ka $7 \cdot 2^2 = 28$. Saame veel $-3 = 34$, $-7 = 30$, $-4 = 33$ ning $-27 = 10$. Kusjuures $33 = 3 \cdot 11$, seega on algjuur ka 11 ning $-11 = 26$. Kokku saimegi vajalikud 18 algjuurt.

4. Millised järgmistest kongruentsidest on lahenduvad ja mitu lahendit neil on (kui üldse on):

a) $x^2 \equiv -1 \pmod{103}$; b) $x^2 \equiv 8 \pmod{101}$;
c) $x^2 \equiv -8 \pmod{1999}$; d) $x^2 \equiv 8 \pmod{2021}$;
e) $x^2 \equiv 2 \pmod{2020}$; f) $x^2 \equiv 25 \pmod{2024}$.

Antud kongruentsidel leidub lahendeid, kui vastavad Legendre'i sümbolite väärtused on 1. Leian sümbolite väärtused:

a) 103 on algarv ja $103 \equiv 3 \pmod 4$ ehk lause 8.8 põhjal $\left(\frac{-1}{103}\right) = -1$ ning lahendeid ei leidu.

b) 101 on algarv ja $101 \equiv -3 \pmod 8$ ehk teoreemi 8.11 põhjal $\left(\frac{2}{101}\right) = -1$ ning teoreemi 8.8 põhjal $\left(\frac{8}{101}\right) = \left(\frac{2 \cdot 2^2}{101}\right) = \left(\frac{2}{101}\right) = -1$ ehk lahendeid ei leidu.

c) 1999 on algarv, $1999 \equiv -1 \pmod 4$ ja $1999 \equiv -1 \pmod 8$ ehk $\left(\frac{-1}{1999}\right) = -1$ ja $\left(\frac{2}{1999}\right) = 1$ ning kokku pannes $\left(\frac{-8}{1999}\right) = \left(\frac{-1}{1999}\right)\left(\frac{2 \cdot 2^2}{1999}\right) = -1$ ehk lahendeid ei leidu.

d) $2021 = 43 \cdot 47$ ehk võrrandi saab teha kahest võrrandist koosnevaks süsteemiks, üks mooduli 43 ja teine mooduli 47 järgi. Vaatlen kõigepealt võrrandit mooduli 43 järgi. $43 \equiv 3 \pmod 8$ ehk $\left(\frac{8}{43}\right) = \left(\frac{2}{43}\right) = -1$ ehk sellel võrrandil lahendid puuduvad ning seega ka kogu võrrandi süsteemil ja algselt võrrandil lahendid puuduvad.

e) $2020 = 2^2 \cdot 5 \cdot 101$ ehk võrrandi saab jagada kolmest võrrandist koosnevaks süsteemiks, üks mooduli 4, teine mooduli 5 ja kolmas mooduli 101 järgi. Vaatlen esiteks võrrandit mooduli 5 järgi. $5 \equiv -3 \pmod 8$ ehk $\left(\frac{2}{5}\right) = -1$ ehk võrrandil puuduvad lahendid ning ka algsel võrrandil puuduvad lahendid.

f) $2024 = 2^3 \cdot 11 \cdot 23$ ehk võrrandi saab jällegi jagada võrrandisüsteemiks.
Uurin esiteks võrrandit mooduli $2^3 = 8$ järgi. Saan teisendada võrrandi kujule $x^2 \equiv 1 \pmod 8$ ning 8. nädala 8. ülesande tulemuse põhjal on sellel võrrandil 4 lahendit.
Järgmiseks uurin võrrandit mooduli 11 järgi. Teisendan võrrandi kujule $x^2 \equiv 3 \pmod{11}$ ning kuna $11 \equiv -1 \pmod{12}$, on $\left(\frac{3}{11}\right) = 1$ ehk lahendeid leidub. Kui mingi lahend b leidub, on ka $-b$ lahend kuna $(-b)^2 = b^2$ ning lause 2.9 põhjal on lahendeid ülimalt 2 ehk sellel võrrandil on 2 lahendit.
Viimaks uurin võrrandit mooduli 23 järgi. Teisendan võrrandi kujule $x^2 \equiv 2 \pmod{23}$ ning kuna $23 \equiv -1 \pmod 8$, siis $\left(\frac{2}{23}\right) = 1$ ehk lahendeid leidub ning eelmise võrrandiga samadel põhjustel on lahendeid 2 tükki.
Kokkuvõttes on võrrandisüsteemis esimesel võrrandil 4 lahendit ning teisel ja kolmandal 2 ehk HJT põhjal on süsteemil kokku $4 \cdot 2 \cdot 2 = 16$ lahendit.

5. Leida kõik algarvud p, mille korral $-p$ on ruutjääk mooduli 11 järgi.

Mooduli 11 järgi on ruutjäägid 1, 4, 9, 5 ning 3. Lemma 8.4 põhjal on ka kõik ruutjääkidega kongruentsed arvud mooduli 11 järgi ruutjäägid ehk $-p$ peab olema kongruentne ühega neist. Seega peab p olema kongruentne $-1 = 10$, $-4 = 7$, $-9 = 2$, $-5 = 6$ või $-3 = 8$ mooduli 11 järgi. Nendest arvudest saab moodustada teoreem 2.6 põhjal 5 aritmeetilist jada, mis igaüks sisaldavad lõpmatu arvu algarve.

6. Olgu $p > 2$ algarv. Tõestada, et iga algjuur mooduli p järgi on mitteruutjääk mooduli p järgi. Kas kehtib ka vastupidine väide? Miks?

Lemma 8.5 põhjal kui c on algjuur mooduli $p > 2$ järgi siis $\left(\frac{c^k}{p}\right) = (-1)^k$ ehk $\left(\frac{c}{p}\right) = -1$ ehk c ei ole ruutjääk.

Järelduse 8.6 põhjal mooduli $p > 2$ järgi leidub $\frac{p-1}{2}$ mitteruutjääki. Algjuuri leidub $\varphi(\varphi(p)) = \varphi(p-1)$ tükki. Arvutusvalemi põhjal saab lahti teha

$$\varphi(n) = \varphi(p_1^{k_1} \cdot ... \cdot p_s^{k_s}) = p_1^{k_1-1} \cdot ... \cdot p_s^{k_s-1}(p_1 - 1)...(p_s - 1) = n \cdot \frac{p_1 - 1}{p_1} \cdot ... \cdot \frac{p_s - 1}{p_s}$$

Kuna p on paaritu algarv, on $p-1$ tegurite hulgas 2 ehk $\varphi(p-1) = (p-1) \cdot \frac{1}{2} \cdot \frac{p_2 - 1}{p_2} \cdot ... \cdot \frac{p_s - 1}{p_s}$ mis tähendab et kui 2 on $p-1$ ainus tegur, on $\varphi(\varphi(p)) = \frac{p-1}{2}$ ehk kuna kõik algjuured on mitteruutjäägid ja algjuuri ning mitteruutjääke on sama palju, siis ka kõik mitteruutjäägid on algjuured. Kuid üldjuhul on arvul $p-1$ ka muid tegureid peale 2, ning sel juhul on algjuuri vähem kui mitteruutjääke ehk iga mitteruutjääk ei pruugi algjuur olla.

7. Olgu $p > 2$ algarv. Tõestada, et 6 on ruutjääk mooduli p järgi parajasti siis, kui $p \equiv \pm 1, \pm 5 \pmod{24}$.

Legendre'i sümboli omadustest saame, et 6 on ruutjääk parajasti siis, kui 2 ja 3 Legendre'i sümbolid on samamärgilised.

Selleks, et 2 ja 3 Legendre'i sümbolid oleks mõlemad 1, peab $p \equiv \pm 1 \pmod{12}$ ning $p \equiv \pm 1 \pmod{8}$. Mooduli 4 järgi saab see olla ainult siis, kui p on mõlema mooduli järgi kongruentne sama arvuga. HJT järgi vastavad meil mõlemale olukorrale üks jäägiklass mooduli 24 järgi, milleks sobivad $\overline{1}$ ning $\overline{-1}$.

Analoogse aruteluga jõuame olukorrast, kus 2 ja 3 Legendre'i sümbolid peavad mõlemad olema -1, lahenditeni $\overline{5}$ ning $\overline{-5}$ mooduli 24 järgi.

8. Olgu $p > 2$ algarv ja r ruutjääk mooduli p järgi. Tõestada, et leidub teine ruutjääk s sama mooduli järgi nii, et $s - r$ on mitteruutjääk. Näidata, et kui võtta $s = a^2$, $0 \leq a \leq p-1$ arvu a juhuslikult valides, siis tõenäosus eelmainitud ruutjääki saada läheneb mooduli p suurenedes arvule $\frac{1}{2}$.

Oletame vastuväiteliselt et kui r on ruutjääk mooduli p järgi, siis iga teise ruutjäägi s puhul on ka $s-r$ ruutjääk. See aga tähendab et kuna ka $s-r$ on ruutjääk, saab selle võtta s asemele ehk ka $(s-r)-r = s-2r$ on ruutjääk ning seda korrates saab et kõik arvud kujul $s - nr$ on ruutjäägid. Algarvulise mooduli järgi on kõik arvud peale p kordsete pööratavad, ning p kordsed arvud ei ole ruutjäägid ehk r on ka pööratav arv. Seega saab võtta $n = sr^{-1}$ ja saada et $s - sr^{-1}r = 0$ on ruutjääk, kuid 0 ei ole kunagi ruutjääk ehk saime vastuolu.

Tõenäosuse leidmiseks vaatan kõik variandid läbi. Kui arv $a^2 - r$ on mitteruutjääk siis $\frac{1 - \left(\frac{a^2-r}{p}\right)}{2} = 1$ ning vastasel juhul $\frac{1 - \left(\frac{a^2-r}{p}\right)}{2} = 0$ ehk kui kokku summeerida $\frac{1 - \left(\frac{a^2-r}{p}\right)}{2}$ väärtused kõigi a väärtuste puhul, saab mitteruutjääkide koguse. Selle summa saab viia ka järgnevale kujule:

$$\sum_{x=0}^{p-1} \left(\frac{x^2 - r}{p}\right) = \sum_{y=0}^{p-1} \left(\left(\frac{y}{p}\right) + 1\right)\left(\frac{y-r}{p}\right)$$

Seda seetõttu, et kui paremas pooles y on mitteruutjääk, siis $\left(\left(\frac{y}{p}\right) + 1\right) = 0$ ehk kogu liige on 0 kuid kui y on ruutjääk, siis $\left(\left(\frac{y}{p}\right) + 1\right) = 2$ ning kuna y on ruutjääk, saab asendada $y = x^2$ ehk korrutise teise poole saab ümber kirjutada kui $\left(\frac{x^2 - r}{p}\right)$, mis ongi sama, mis võrrandi vasaku poole liige. Seega on paremal poolel summeeritud kokku vasaku poole liige, kus x^2 läbib kõik võimalikud ruutjäägid täpselt ühe korra ning $y = 0$ juhul on liikme väärtus $\left(\frac{-r}{p}\right)$. Vasakul poolel läbitakse samuti ruutjääke, kuid liikmeid on kaks korda rohkem kui erinevaid ruutjääke leidub, kuna ruutjääkide kogus on $\frac{p-1}{2}$. Samas saab märgata, et $x^2 = (-x)^2$ ehk igat väärtust läbitakse kaks korda, ehk läbitakse erinevaid väärtuseid täpselt nii palju, kui on erinevaid ruutjääke ning seega summeeritakse ka sellel poolel liige kokku kõigi ruutjääkidega kaks korda. Erandiks on jällegi $x = 0$, mis puhul on liige $\left(\frac{-r}{p}\right)$, nagu ka paremal pool.

Selles kujus saab veel sulud avada ning saavutada järgmise kuju:

$$\sum_{y=0}^{p-1} \left(\left(\frac{y}{p}\right) + 1\right)\left(\frac{y-r}{p}\right) = \sum_{y=0}^{p-1} \left(\left(\frac{y}{p}\right)\left(\frac{y-r}{p}\right) + \left(\frac{y-r}{p}\right)\right) = \sum_{y=0}^{p-1} \left(\frac{y}{p}\right)\left(\frac{y-r}{p}\right)$$

Teine võrdus kehtib, kuna kui summeerida liige $\left(\frac{y-r}{p}\right)$ nii et y läbib väärtused 0 kuni $p-1$, siis saavutab $y - r$ kõik väärtused mooduli p järgi ühe korra, ning mooduli p järgi on $\frac{p-1}{2}$ ruutjääki ja sama palju mitteruutjääke ehk need taandavad üksteist maha. Paariliseta jääb vaid 0, mille Legendre'i sümbol on 0 ehk see summat ei muuda.

Siit edasi said oskused otsa.