Kodutöö nr. 14

Joosep Näks ja Uku Hannes Arismaa

1. Leida Jacobi sümboli väärtus: a) $\left(\frac{455}{667}\right)$, b) $\left(\frac{1473}{881}\right)$, c) $\left(\frac{9271}{8009}\right)$.

a) $\left(\frac{455}{667}\right) = \left(\frac{212}{455}\right) = \left(\frac{53}{455}\right) = -\left(\frac{31}{53}\right) = \left(\frac{22}{31}\right) = -\left(\frac{11}{31}\right) = \left(\frac{9}{11}\right) = \left(\frac{2}{9}\right) = 1$

b) $\left(\frac{1473}{881}\right) = \left(\frac{592}{881}\right) = \left(\frac{37}{881}\right) = \left(\frac{30}{37}\right) = -\left(\frac{15}{37}\right) = -\left(\frac{7}{15}\right) = \left(\frac{1}{7}\right) = 1$

c) $\left(\frac{9271}{8009}\right) = \left(\frac{1262}{8009}\right) = \left(\frac{631}{8009}\right) = \left(\frac{437}{631}\right) = \left(\frac{194}{437}\right) = -\left(\frac{97}{437}\right) = \left(\frac{49}{97}\right) = 1$

2. Leida, milliste algarvuliste moodulite p järgi on arv -13 mitteruutjääk.

Uurin Legendre'i sümbolit $\left(\frac{-13}{p}\right)$. Legendre'i sümboli omaduste järgi saab selle lahti teha korrutiseks $\left(\frac{-1}{p}\right)\left(\frac{13}{p}\right)$. Esimene tegur on 1, kui $p \equiv 1 \pmod 4$ ning -1 kui $p \equiv -1 \pmod 4$. Ruutvastavusseaduse põhjal saab teise teguri ümber pöörata, kuna $13 \equiv 1 \pmod 4$: $\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right)$. Selliste Legendre'i sümbolite väärtused on aga samaväärsed vastavate $a \equiv p \pmod{13}$ esindajate Legendre'i sümboli väärtustega kus $0 \leq a \leq 13$.

Vaatlen need läbi. Kui $a = 13$, on p 13 kordne ehk ainus võimalik selline algarv on 13 ning see ei ole mitteruutjääk.

Kui $a = 1$, siis on Legendre'i sümboli väärtus 1.

Kui $a = 2$, on sümboli väärtus -1 kuna $13 \equiv -3 \pmod 8$.

Kui $a = 3$, on sümboli väärtus 1 kuna $13 \equiv 1 \pmod{12}$.

Kui $a = 4$, saab teisendada $\left(\frac{2^2}{13}\right) = \left(\frac{1}{13}\right) = 1$.

Kui $a = 5$, saab teisendada $\left(\frac{5}{13}\right) = \left(\frac{-2^3}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{2}{13}\right) = 1 \cdot (-1) = -1$.

Kui $a = 6$, saab $\left(\frac{6}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = -1 \cdot 1 = -1$.

Kuna $13 \equiv 1 \pmod 4$ ehk $\left(\frac{-1}{13}\right) = 1$, on teine pool a väärtuseid teistpidi järjekorras. Vaadates nüüd algset sümbolit $\left(\frac{-13}{p}\right)$, on selle väärtus -1 parajasti siis, kui kas $p \equiv 1 \pmod 4$ ja p on kongruentne mõnega arvudest $2, 5, 6, 7, 8, 11$ mooduli 13 järgi või kui $p \equiv 3 \pmod 4$ ja p on kongruentne mõnega arvudest $1, 3, 4, 9, 10, 12$ mooduli 13 järgi.

3. Olgu a täisarv ja n naturaalarv, kusjuures $n \equiv 5 \pmod{24}$. Tõestada, et kui $\left(\frac{a}{n}\right) = -1$, siis kongruents $x^2 + 6a(x+1) + 9a^2 \equiv 0 \pmod n$ ei ole lahenduv. Kas kehtib ka vastupidine väide?

Lausest 8.21 saame tõsiasjad $\left(\frac{-1}{n}\right) = 1$, $\left(\frac{2}{n}\right) = -1$, $\left(\frac{3}{n}\right) = \left(\frac{n}{3}\right) = -1$. Nüüd vaadates kongruentsi saame $x^2+6a(x+1)+9a^2 = (x+3a)^2+6a \equiv 0 \pmod n$, seega kui see on lahenduv, siis on $(x+3a)^2 \equiv -6a \pmod n$, seega $\left(\frac{(x+3a)^2}{n}\right) = \left(\frac{-6a}{n}\right) = 1 \cdot (-1)^3 = -1$, mis on vastuolu, kuna $(x+3a)^2$ on ruutjääk, seega peaks selle Jacobi sümbol olema 1.

Kui võtta n=77 ning $a = 6$, siis $x^2 + 6a(x+1) + 9a^2 \equiv x^2 + x + 3 \equiv 0 \pmod 7$, millel puuduvad lahendid, seega pole neid ka mooduli 77 järgi. Samas $\left(\frac{6}{77}\right) = -\left(\frac{3}{77}\right) = -\left(\frac{77}{3}\right) = 1$.

4. Leida võrrandi $10x^2 - 12xy + 8y^2 = 2022$ täisarvuliste lahendite arv.

Kõigepealt lihtsustamiseks jagan võrrandi läbi arvuga 2: $5x^2 - 6xy + 4y^2 = 1011$. Vaatlen võrrandit mooduli 11 järgi, siis saan võrrandi ümber kirjutada kui $16x^2 + 16xy + 4y^2 = (4x + 2y)^2 \equiv 1011 \equiv -1 \pmod{11}$. Seega leidub sellel võrrandil lahendeid parajasti siis, kui -1 on mooduli 11 järgi ruutjääk, kuid kuna $11 \equiv 3 \pmod 4$, ei ole tegu ruutjäägiga, ning ühtegi lahendit ei leidu.

5. Tõestada, et arvu $n^2 - 2$ kõik jagajad on kas kujul $8k \pm 1$ või $8k \pm 2$.

Paneme tähele, et $n^2 - 2$ algtegurduses on 2 aste maksimaalselt 1, kuna kui n on paaritu, on tulemus paaritu ning kui n on paaris, on n^2 4 kordne, seega $n^2 - 2$ ei ole 4 kordne, olles samas 2 kordne. Seega, ei saa olla ükski jagaja kujul $8k + 4$ või $8k$, kuna nendes on 2 aste liiga suur.

Paneme tähele, et $n^2 \equiv 2 \pmod{n^2 - 2}$, mis peab kehtima ka siis, kui mooduliks on mõni $n^2 - 2$ algtegur. Seega iga algteguri järgi on 2 ruutjääk, mis välistab selle, et mõni algtegur saaks olla kujul $8k \pm 3$.

Iga jagaja on lihtsalt mingi algtegurite korrutis. Paneme tähele, et korrutades $8k \pm 1$ kujul algtegureid, saame tulemuseks $8k \pm 1$ ning kui seda üks kord 2ga läbi korrutada, millest rohkem ei saa, saame saada tegureid kujul $8k \pm 2$. Rohkem võimalusi ei ole.

6. Tõestada ilma Dirichlet' teoreemi kasutamata, et leidub lõpmata palju algarve kujul $8k + 3$.

Oletan, et algarve kujul $8k + 3$ on lõplik kogus ning need on $p_1, p_2, .., p_n$. Korrutan need kokku ja saan $m = p_1 \cdot p_2 \cdot .. \cdot p_n$. Vaatlen arvu $w = n^2 + 2$. Ükski algarv kujul $8k + 3$ ei saa seda jagada kuna kõik sellised algarvud jagavad arvu n^2 ning et mõni selline tegur ka arvu w jagaks, peaks ta jagama ka arvu 2, kuid 2 ei ole kujul $8k + 3$ ning ükski teine algarv ei jaga arvu 2. Olgu q mingi arvu w tegur. See tähendab, et $w \equiv 0 \pmod q$ ehk $n^2 \equiv -2 \pmod q$ ehk $\left(\frac{-2}{q}\right) = 1$. Legendre'i sümboli omaduste järgi tähendab see, et $q \equiv 1 \pmod 8$ või $q \equiv 3 \pmod 8$. Nagu enne näidatud, ei ole arvul w ühtegi algtegurit kujul $8k+3$, ehk kõik algtegurid peavad olema kujul $8k+1$ ning kui selliseid algtegureid kokku korrutada on ka tulemus kujul $8k + 1$ ehk ka arv $w = n^2 + 2$ on sellisel kujul ning n^2 on seega kujul $8k - 1$. Kui aga algarve kujul $8k + 3$ kokku korrutada saab $(8k + 3)(8t + 3) = 8(8kt + 3k + 3t + 1) + 1$ ehk arvu kujul $8k + 1$ ning kui seda uuesti $8k + 3$ kujul arvuga läbi korrutada saab $(8k + 1)(8t + 3) = 8(8kt + 3k + t) + 3$ ehk n ja ka n^2 saab olla vaid kujul $8k + 1$ või $8k + 3$ kuid mitte $8k - 1$, mis annab vastuolu ehk sellisel kujul algarve peab olema lõputu kogus.

7. Tõestada, et iga algarvu $p \geq 7$ korral leiduvad kolm järjestikust naturaalarvu $n, n + 1, n + 2$ nii, et n ja $n + 2$ on ruutjäägid ja $n + 1$ on mitteruutjääk mooduli p järgi.

Vähim mitteruutjääk q on alati algarv, kuna kui see oleks kordarv, siis iga selle algtegur oleks sellest väiksem algarv Legendre'i sümboliga 1, ning nende korrutisel peaks ka olema Legendre'i sümbol 1.

Kui 2 on ruutjääk, siis esimese algarvu ümber, mis pole ruutjääk on kaks paarisarvu, mille kõik algtegurid on väiksemad või võrdsed nendest poolega, seega väiksemad, kui vähim mitteruutjäägist algarv, seega ruutjäägid, seega on nende Legendre'i sümbolid 1 ning nende korrutise, mis on esiaglne paarisarv, Legendre'i sümbol sammuti 1, seega on need ruutjäägid ning olemegi saanud soovitud mustri.

Kui 2 pole ruutjääk, siis mustri vältimiseks peab ka 3 olema mitteruutjääk. 4 on alati ruutjääk. Samuti Legendre'i sümbolite põhjal, kuna ei 2 ega 3 ole ruutjääk, peab seda olema 6. Nüüd saame, et ka 5 peab olema ruutjääk. 9 on ruutjääk, 8 pole. Seega ei saa 7 olle ruutjääk, muidu saavutaksime jällegi mustri. Nüüd teame eelneva põhjal, et 14 on ruutjääk, 15 pole ning 16 on, seega oleme enamustel juhtudel saavutanud mustri.

14st väiksemate algarvude korral märkame, et 7 puhul on 2 algjuur. 11 ja 13 puhul kuigi 2 pole ruutjääk, siis 1 ja 3 on (vastavalt 5 ja 4 ruut), seega leiame ikkagi soovitud mustri.

8. Olgu $p > 2$ algarv, $a \in \mathbb{Z}$ ja $(a, p) = 1$. Leida $\sum_{i=1}^{p} \left(\frac{i^2 + a}{p} \right)$.

Euleri kriteeriumi põhjal saab summa liikme ümber kirjutada ning seejärel binoomvalemi järgi lahti teha:

$$\left(\frac{i^2 + a}{p} \right) \equiv (i^2 + a)^{\frac{p-1}{2}} = \sum_{k=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{k} i^{2k} a^{\frac{p-1}{2} - k} \pmod{p}$$

Vaadates algset summat, saab selle summa uue summa sisse tõsta:

$$\sum_{i=1}^{p} \sum_{k=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{k} i^{2k} a^{\frac{p-1}{2} - k} = \sum_{k=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{k} \left(\sum_{i=1}^{p} i^{2k} \right) a^{\frac{p-1}{2} - k}$$

Vaatlen lähemalt summat $\sum_{i=1}^{p} i^{2k}$. Summa ülemist piiri saab ühe võrra vähendada, kuna $p^{2k} \equiv 0 \pmod{p}$ ehk jääb alles $\sum_{i=1}^{p-1} i^{2k}$. Kuna liidetakse kokku kõik pööratavad elemendid astmel $2k$, saab võtta mingi algjuure a mooduli p järgi ning kirjutada summa liige ümber algjuure astmeks ja seejärel summa kokku võtta geomeetrilise jada summana:

$$\sum_{i=1}^{p-1} i^{2k} = \sum_{i=0}^{p-2} (a^i)^{2k} = \sum_{i=0}^{p-2} (a^{2k})^i = \frac{(a^{2k})^{(p-1)} - 1}{a^{2k} - 1} = \frac{(a^{p-1})^{(2k)} - 1}{a^{2k} - 1}$$

Nimetajas FVT põhjal $a^{p-1} \equiv 1 \pmod{p}$ ehk terve nimetaja on kongruentne arvuga 0 ning lugejas kuna a järk on $p - 1$, siis niikaua kui kehtib $0 < k < \frac{p-1}{2}$, ei saa $a^{2k} \equiv 1 \pmod{p}$ kehtida ehk lugeja on pööratav. Seega kui $0 < k < \frac{p-1}{2}$, on selle summa väärtus 0 ning algses summas kõik sellised liikmed taanduvad maha, alles jäävad vaid kaks liiget, $k = 0$ ja $k = \frac{p-1}{2}$. Kui $k = 0$, on kõik sisemise summa liikmed väärtusega 1 ehk summa väärtus on $\sum_{i=1}^{p} i^0 = p \equiv 0 \pmod{p}$ ning ka see liige taandub maha. Kui $k = \frac{p-1}{2}$, siis $\sum_{i=1}^{p} i^{p-1} \equiv p^{p-1} + \sum_{i=1}^{p-1} 1 = p^{p-1} + p - 1 \equiv p - 1 \pmod{p}$. Seega tuleb terve liikme väärtuseks $\binom{\frac{p-1}{2}}{\frac{p-1}{2}} \left(\sum_{i=1}^{p} i^{p-1} \right) a^{\frac{p-1}{2} - \frac{p-1}{2}} = p - 1$.

Seega on algne summa $\sum_{i=1}^{p} \left(\frac{i^2 + a}{p} \right)$. kongruentne arvuga $p - 1$. Summas on liikmeid p tükki, millest iga ühe absoluutväärtus on 0 või 1 ehk summa absoluutväärtus saab olla ülimalt p ning vahemikku $-p$ kuni p jääb kaks arvu, mis on kongruentsed arvuga $p - 1$, need on -1 ja $p - 1$. Kuna $p - 1$ on kõige suuremast võimalikust väärtusest vaid 1 võrra väiksem, tähendab see, et kui summa väärtus on $p - 1$, siis on summas $p - 1$ liiget, mille väärtused on 1 ning üks liige, mille väärtus on 0.