Kodutöö nr. 6

Joosep Näks ja Uku Hannes Arismaa

1. Millega on võrdne summa

$$S = \varphi(2) + \varphi(3) + \varphi(4) + \varphi(5) + \varphi(6) + \varphi(7) + \varphi(8) + \varphi(10) + \varphi(20) + \varphi(25) + \varphi(40) + \varphi(50) + \varphi(100)?$$

$$S = \sum_{d|200} \varphi(d) - \varphi(1) - \varphi(200) + \varphi(3) + \varphi(6) + \varphi(7) =$$

$$200 - 1 - 2^{3-1}(2-1)5^{2-1}(5-1) + 2 + 2 + 6 = 129$$

2. Kui palju on selliseid naturaalarve, mis ei ole suuremad kui 2121 ja mille suurim ühistegur arvuga 2020 ei ületa arvu 20?

Võtan suvalise arvu $a = p_1^{k_1} \cdot p_2^{k_2} \cdot ... \cdot p_n^{k_n}$ ning $2020 = p_1^{l_1} \cdot p_2^{l_2} \cdot ... \cdot p_n^{l_n}$, nii et $p_1, ..., p_n$ on erinevad algarvud. Siis $(a, 2020) = p_1^{\min(p_1,l_1)} \cdot p_2^{\min(p_2,l_2)} \cdot ... \cdot p_n^{\min(p_n,l_n)}$. Kuna arvu 2020 standardkuju on $2^2 \cdot 5^1 \cdot 101^1$, on kõik muudele algarvudele vastavad l_i väärtused 0 ning suurima ühisteguri saab taandada arvuks $(a, 2020) = 2^{\min(2,l_1)} \cdot 5^{\min(1,l_2)} \cdot 101^{\min(1,l_n)}$ ehk kõik erinevad võimalikud suurimad ühistegurid on $1, 2, 4, 5, 10, 20$ ja lisaks kõik loetletud arvud läbi korrutatud arvuga 101. Märkan, et kõik loetletud arvud on mitte suuremad kui 20, kuid kui neid arvuga 101 läbi korrutada, on nad suuremad kui 20. Sellest järeldub, et arvu a suurim ühistegur arvuga 2020 on suurem kui 20 parajasti siis, kui $101|a$. Seega on arvude kogus, mille suurim ühistegur arvuga 2020 ei ületa arvu 20, kõigi arvude kogus miinus 101 kordsed arvud. 101 kordseid arve, mis ei ole suuremad kui 2121 on $\left\lfloor \frac{2121}{101} \right\rfloor = 21$ ning seega otsitav kogus on 2121-21=2100.

3. Leida arvu

$$2022^{(2021^{(2020^{\cdots^{2^1}})})}$$

neli viimast kümnendnumbrit.

Arvu viimase nelja kümnendnumbri leidmine on samaväärne arvu esindaja leidmisega jäägiklassis $\mathbb{Z}_{10000}$. Teoreemi 4.5 põhjal kuna $(16, 625) = 1$ ja $16 \cdot 625 = 10000$ siis $\mathbb{Z}_{10000}$ ja $\mathbb{Z}_{16} \times \mathbb{Z}_{625}$ on isomorfsed, seega leian arvu esindaja ringis $\mathbb{Z}_{16} \times \mathbb{Z}_{625}$. Märkan et $2022 \equiv 6 \pmod{16}$ ja $6^4 \equiv 0 \pmod{16}$ ehk kuna antud arvus on 2022 astendaja suurem kui 4, on jäägiklassis $\mathbb{Z}_{16}$ selle esindaja $\overline{0}$.
Jäägiklassi $\mathbb{Z}_{625}$ jaoks leian, et $\varphi(625) = 500$, ning kuna $(625, 2022) = 1$, saan ma Euleri teoreemi põhjal, et $2022^{500} \equiv 1 \pmod{625}$ ehk kui jagada jäägiga $2021^{(2020^{\cdots^{2^1}})} = 500q + r$, siis $2022^{(2021^{(2020^{\cdots^{2^1}})})} \equiv 2022^{500q} \cdot 2022^r \equiv 2022^r \pmod{625}$. Arvu r leidmiseks saab jällegi kasutada Euleri teoreemi, kuna $(2021, 500) = 1$ ja $\varphi(500) = 200$, ehk $2021^{200} \equiv 1 \pmod{500}$. Arvu 2021 astendajat algses arvus vaadates saab aga märgata, et $2020 \equiv 20 \pmod{200}$ ning $20^2 = 400 \equiv 0 \pmod{200}$ ehk kuna algses arvus on 2020 astendaja suurem kui 2, saab võtta $2020^{(2019...^{(2^1)})} = 2020^2 \cdot 2020^{(2019...^{(2^1)})-2} \equiv 0 \pmod{200}$. See tähendab, et algses arvus arvu 2021 astendaja jagub arvuga 200 ning $2021^{(2020^{\cdots^{2^1}})} = (2020^{200})^k \equiv 1 \pmod{500}$ ehk $r = 1$.
Ning lõpuks $2022^{(2021^{(2020^{\cdots^{2^1}})})} \equiv 2022^1 \pmod{625} = 147$.
Seega on antud arvu esindaja ringis $\mathbb{Z}_{16} \times \mathbb{Z}_{625}$ element $(\overline{0}, \overline{147})$. Leian jäägid $625 \equiv 1 \pmod{16}$ ja $147 \equiv 3 \pmod{16}$ ehk otsitav esindaja jäägiklassis Z_{10000} on $625 \cdot 13 + 147 = 8272$.

4. Tõestada, et $a^{37} \equiv a \pmod{1995}$ iga $a \in \mathbb{Z}$ korral.

Samaväärne oleks tõestada $a^{37} = a, a \in \mathbb{Z}_{1995}$, mis omakorda on samaväärne $a^{37} = a, a \in \mathbb{Z}_{19} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$. Vaadates a osi eraldi, saame Fermat' väikese teoreemipõhjal, et näiteks $a_1 \in \mathbb{Z}_{19}$ puhul $a_1^{19-1} = a_1^{18} = \overline{1} \Rightarrow a_1^{2 \cdot 18} = \overline{1}^2 = \overline{1} \Rightarrow a_1^{37} = \overline{1}a_1 = a_1$. Sarnase tulemuseni jõuame ka teistes jäägiklassiringides, kuna $37 \equiv 1 \pmod{3-1}$, $37 \equiv 1 \pmod{5-1}$ ning $37 \equiv 1 \pmod{7-1}$. Kui mõni $a_n = 0$, siis Fermat' väike teoreem ei kehti, aga $\overline{0}^{37} = \overline{0}$ igas jäägiklassiringis, seega ikkagi $a_n^{37} = a_n$ ning seega ka $a^{37} = a$.

5. Leida kõik naturaalarvud n, mille korral $\varphi(n) = 6$.

$6 = 2 \cdot 3$

φ arvutamisel saavad need tegurid tulla kahest kohast: tegur $(p-1)$ või tegur p^{k-1}. Kui 2 tuleb $(p-1)$st, siis saame $p = 3$. Kui siis 3 tuleb p^{k-1}st, saame, et arv on $3^2 = 9$. 3 ei saa tulla $(p-1)$st, sest 4 ei ole algarv. Kui 2 tuleb 2^{2-1} st, siis peaks 3 tulema 3^{2-1}st, aga siis peaks tulemus veel olema korrutatud $(3-1)$ga, seega nii ei saa. On ka võimalus, et $(p-1) = 6$ ehk sobib arv 7. Lisaks 7 ja 9le sobivad ka 14 ja 18, kuna 2ga läbi korrutamisel korrutame me φ läbi $2^{1-1} = 1$ ning $(2-1) = 1$ga.

6. Olgu $n \in \mathbb{N}$. Leida $\sum_{d|n} \mu(d)\sigma(\frac{n}{d})$.

Hakkame algusest pihta. Näitame, et μ ning σ on nõrgalt multiplikatiivsed (mõlemad funktsioonid kohal 1 on 1, seda me ei näita). Kui arvude suurim ühistegur on 1, siis ei tohi nende algtegurdustes olla ühiseid algarve, vastasel juhul oleks selle mingi aste nende suurimaks ühisteguriks. Kui võtta ühe arvu algteguriteks $p_1 ... p_s$ ning teisel $p_{s+1} ... p_{s+t}$, saame

$$\sigma(p_1^{k_1} \cdot ... \cdot p_s^{k_s})\sigma(p_{s+1}^{k_{s+1}} \cdot ... \cdot p_{s+t}^{k_{s+t}}) = \frac{p_1^{k_1+1}-1}{p_1-1} \cdot ... \cdot \frac{p_{s+t}^{k_{s+t}+1}-1}{p_{s+t}-1} = \sigma(p_1^{k_1} \cdot ... \cdot p_{s+t}^{k_{s+t}})$$

μ puhul, kui üks argumentidest on mingi täisruudu kordne, on ka korrutis, seega 0ga korrutades saame vastuseks 0. Kui üks arvudest on paarisarvu algteguritega, siis see ei muuda korrutise tegurite arvu paarsust ning seega ka μ väärtust, seega 1ga korrutamine ei muuda väärtust. Kui korrutame paarituarvulise algteguritega arvuga, siis tegurite arvu paarsus muutub, seega vastus korrutub -1ga. Seega on μ ka nõrgalt multiplikatiivne.

Nüüd näitame, et funktsioon, mida uurime (edaspidi f) on multiplikatiivne. Kuni n ja x on ühistegurita, on ühe jagajad teise jagajatega ühistegurita, vastasel juhul saame vastuolu. n ja x suvalised jagajad korrutades saame nx jagaja. See korrutamine on bijektsioon x ja n jagajate hulkade otsekorrutise ning nx jagajate hulga vahel. Iga nx jagaja puhul, saab selle algtegurduse jagada algarvudeks, mis jagavd x, ning, mis jagavad n, kusjuures x jagavate algarvude korrutis jagab x, kuna neist ükski ei jaga n, muidu poleks x ja n ühistegurita, seega kui nende korrutis ei jagaks x ei jagaks need ka nx, mis on vastuolu. Sarnase arutelu saame läbi teha ka n-le vastavate algteguritega. Nii x ja n algteguriteks jagamine näitab ka injektiivsust, kuna nx tegurist saadavad x-le ja n-le vastavad tegurid on üheselt määratud. Neid teadmisi kasutades saame, et

$$\begin{aligned} f(n)f(x) &= \sum_{d_n|n} \sum_{d_x|x} \mu(d_n)\mu(d_x)\sigma(\frac{n}{d_n})\sigma(\frac{x}{d_x}) \\ &= \sum_{d_n|n} \sum_{d_x|x} \mu(d_n d_x)\sigma(\frac{nx}{d_n d_x}) \\ &= \sum_{d|nx} \mu(d)\sigma(\frac{nx}{d}) \end{aligned}$$

Funktsioon f kohal 1 on samuti 1. Mingi p^n korral on $f(p^n) = \mu(1)\sigma(p^n) + \mu(p)\sigma(p^{n-1}) = \frac{p^{n+1}-1}{p-1} - \frac{p^n-1}{p-1} = \frac{p^n(p-1)}{p-1} = p^n$, kuna p^n jagajad on kõik kujul $p^x, 0 \le x \le n$ ning jagajad, kus $x \ge 2$, on $\mu(p^x) = 0$, seega summa väärtuse arvutamiseks piisab arvutada korrutised jagajate 1 ning p jaoks. Kuna f on multiplikatiivne saame,

$$f(p_1^{k_1} \cdot ... \cdot p_s^{k_s}) = p_1^{k_1} \cdot ... \cdot p_s^{k_s}$$

7. Leida kõik täiuslikud paarisarvud, mis ei ole avaldatavad järjestikuste kuupide summana.

Teoreemi 5.21 põhjal $\sigma(a) = \frac{p_1^{k_1+1}-1}{p_1-1} \cdot \frac{p_2^{k_2+1}-1}{p_2-1} \cdot ... \cdot \frac{p_n^{k_n+1}-1}{p_n-1}$, kus $p_1, .., p_n$ on a algtegurid. Kui mingite a ja b puhul $(a, b) = 1$, siis on nende algtegurid ilma kattuvusteta, ehk $a \cdot b$ standardkujus on iga algtegur kas a või b algtegur ning ka sama astmega, nagu a või b standardkujus. Seega on $\sigma(a \cdot b)$ eelnevalt näidatud korrutise kujus iga tegur sama, nagu kas $\sigma(a)$ või $\sigma(b)$ korrutises. Seega kui $(a, b) = 1$ siis $\sigma(a \cdot b) = \sigma(a)\sigma(b)$.

Järgmiseks näitan, et iga täiuslik paarisarv n on esitatav kujul $2^{p-1}(2^p - 1)$. Kuna n on paarisarv, kehtib $n = 2^p b$, kus b on paaritu arv ja p on mingi naturaalarv, ehk kehtib ka $(2^p, b) = 1$. Seega kasutades eelmises lõigus kasutatud omadust $2^{p+1}b = 2 \cdot 2^p \cdot b = 2n = \sigma(n) = \sigma(2^p)\sigma(b) = (2^{p+1} - 1)\sigma(b)$. Arvu 2^{p+1} ainus algtegur on 2 ja $(2^{p+1} - 1)$ on paaritu ehk $(2^{p+1}, 2^{p+1} - 1) = 1$ ning $2^{p+1} - 1$ jagab saadud võrduste paremat otsa ehk ta jagab ka vasakut otsa, seega $2^{p+1}-1$ jagab arvu b. Tähistan $b = (2^{p+1}-1)c$. Seega $2^{p+1}(2^{p+1} - 1)c = (2^{p+1} - 1)\sigma(b) \Leftrightarrow 2^{p+1}c = \sigma(b)$. Kuna b jagab arvu b ja c jagab arvu b, kehtib $2^{p+1}c = \sigma(b) \geq b + c = (2^{p+1} - 1)c + c = 2^{p+1}c$. Kuna vasak ja parem ots on võrdsed, kehtib $\sigma(b) = b + c$. $\sigma(b)$ on kõigi arvu b jagajate summa ja ka arv 1 jagab arvu b ehk 1 peab selle summa liige olema, kuid ka b ja c jagavad arvu b ehk ka nemad peavad summa liikmed olema. Seega kehtib kas $b = 1$ või $c = 1$. Esimesel juhul aga $\sigma(b) = \sigma(1) = 1 = 1 + c$ ehk $c = 0$, kuid sel juhul $b = (2^{p+1} - 1)c = 0$, mis annab vastuolu. Ehk peab kehtima $c = 1$. Asendades selle eelnevatesse kujudesse sisse saab $2n = (2^{p+1} - 1)2^{p+1}$ ehk $n = (2^{p+1} - 1)2^p$. Võttes $p' = p + 1$ saab selle veel teisendada kujule $n = 2^{p'-1}(2^{p'} - 1)$ nagu lõigu alguses soovitud.
Veelgi enam, kui p' on paaris, siis $2^{p'} = 4^k \equiv 1 \pmod 3$, ehk $2^{p'} - 1$ on 3 kordne arv, kuid varem sai näidatud, et $\sigma(2^{p'} - 1) = \sigma(b) = 1 + b$, ehk $2^{p'} - 1$ ainsad kordajad on 1 ja tema ise nii et algarv, ning ainus kolmega jaguv algarv on 3, mis juhul $p' = 2$. Seega on p' paaritu arv või 2.

Väidan, et esimese n järjestikuse kuubi summa on $n^2(2n^2-1)$ ehk $\sum_{i=0}^{n-1}(2i+1)^3 = n^2(2n^2-1)$. Tõestan seda induktsiooniga. Baasiks kui $n = 1$ siis $1^3 = 1^2(2 \cdot 1^2-1)$. Sammuks eeldan et $\sum_{i=0}^{k-1}(2i+1)^3 = k^2(2k^2-1)$ kehtib ning kui sellele liita mõlemale poolele juurde $(2k + 1)^3$, saab

$$\sum_{i=0}^{k}(2i+1)^3 = k^2(2k^2-1)+(2k+1)^3 = 2k^4-k^2+8k^3+12k^2+6k+1 = (k+1)^2(2k^2+4k+1) = (k+1)^2(2(k+1)^2-1)$$

ehk summa valem kehtib.

Kui nüüd võtta suvaline täiuslik paarisarv m, on see esitatav kujul $m = 2^{p-1}(2^p - 1)$. Kui $p = 2$, on $m = 6$, ning see ei ole esitatav järjestikuste paaritute kuupidena, kuna ainus paaritu kuup, mis pole suurem kui 6 on 1. Teiste p väärtuste puhul tehes asendus $n = 2^{\frac{p-1}{2}}$ ($p - 1$ jagub kahega kuna p on paaritu), saab $m = n^2(2n^2 - 1)$, mis on esimese n paaritu arv kuupide summa.
Seega ainus täiuslik paarisarv on 6.

8. Tõestada, et igal paaritul täiuslikul arvul on vähemalt kolm erinevat algtegurit.

Vaatlen alustuseks ühe erineva algteguriga täiuslikke arve. Teoreemi 5.21 põhjal saab nad avaldada kujul $2n = 2p^k = \sigma(n) = \frac{p^{k+1}-1}{p-1}$. Korrutan võrrandi $2p^k = \frac{p^{k+1}-1}{p-1}$ mõlemad pooled läbi $p-1$ga, mis pole 0, kuna p on algarv ehk 2 või suurem. Saan $2p^{k+1} - 2p^k = p^{k+1} - 1$ ehk $p^k(2-p) = 1$. Kuid selleks, et võrrandi vasak pool positiivne oleks, peaks p olema väiksem kui 2 ning selliseid algarve ei leidu.
Avaldan sarnaselt kahe erineva algteguriga täiusliku arvu: $2n = 2p^k \cdot q^t = \sigma(n) = \frac{p^{k+1}-1}{p-1} \cdot \frac{q^{t+1}-1}{q-1}$.
Jagan mõlemad pooled läbi arvuga n: $2 = \frac{p-p^{-k}}{p-1} \cdot \frac{q-q^{-t}}{q-1} = \left(\frac{p}{p-1} - \frac{p^{-k}}{p-1}\right) \cdot \left(\frac{q}{q-1} - \frac{q^{-t}}{q-1}\right)$.
Eelduste kohaselt on p ja q algarvud ja k ja t naturaalarvud ehk $0 < p^{-k} < 1 < p$ ehk viimatise korrutise tegurid on positiivsed, ning kui mõlemale tegurile juurde liita positiivne arv, on tulemuseks saadud korrutise väärtus suurem algsest korrutisest ehk

$$\left(\frac{p}{p-1} - \frac{p^{-k}}{p-1}\right) \cdot \left(\frac{q}{q-1} - \frac{q^{-t}}{q-1}\right) < \frac{p}{p-1} \cdot \frac{q}{q-1} = \frac{1}{1-\frac{1}{p}} \cdot \frac{1}{1-\frac{1}{q}}$$

Kui saadud kujus võtta p ja q kõige väiksemateks võimalikeks algarvudeks $p = 3$ ja $q = 5$ (2 ei ole võimalik kuna vaatleme vaid paarituid täiuslikke arve), on selle väärtus $\frac{15}{8} < 2$ ning on näha, et p ja q suurendamisel väheneb väärtus, ehk selle kuju väärtus on alati väiksem kui 2, kuid see annab vastuolu, kuna see peaks olema rangelt suurem kui 2, et n oleks täiuslik arv.