Arvuteooria

Näidislahendused

Praktikum 6

1 Markus Rene Pae

Teame, et arvu 120 jagajad on 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60 ja 120. Seega vastavalt Gaussi teoreemile

$$\sum_{d|120} \varphi(d) = 120$$

Summas S on Euleri funktsiooni argumentides kõik peale 7 arvu 120 jagajad. Arvu 120 jagajatest on argumentidena puudu 1, 60 ja 120. Seega summa S on avaldatav kujul:

$$S = \sum_{d|120} \varphi(d) + \varphi(7) - \varphi(1) - \varphi(60) - \varphi(120).$$

On ilmne, et $\varphi(1) = 1$. Nüüd on meil vaja leida $\varphi(7)$, $\varphi(60)$ ja $\varphi(120)$ väärtused, kasutades selleks loengukonspekti teoreemi 5.8:

$$\varphi(7) = 7 - 1 = 6$$

$$\varphi(60) = \varphi\left(2^2 \cdot 3^1 \cdot 5^1\right) = 2^1 \cdot (3-1) \cdot (5-1) = 16$$
$$\varphi(120) = \varphi\left(2^3 \cdot 3^1 \cdot 5^1\right) = 2^2 \cdot (3-1) \cdot (5-1) = 32$$

Sellest lähtuvalt

$$S = \sum_{d|120} \varphi(d) + \varphi(7) - \varphi(1) - \varphi(60) - \varphi(120) = 120 + 6 - 1 - 16 - 32 = 77.$$

2 Johanna Maria Kirss

Kõigepealt märkame, et $2233 = 7 \cdot 11 \cdot 29$. Tekstis antud tingimustele vastavad kõik arvud $n \leq 2345$, mille korral $(2233, n) \in \{1, 7, 11, 29, 7 \cdot 11\}$. Otsime kõigepealt kõik sobivad arvud 1 ja 2233 vahepeal ja defineerime

$$S_1 = |\{1 \leq x \leq 2233, (x, 2233) \in \{1, 7, 11, 29, 77\}\}|.$$

Leidmaks S_1, saame kasutada loengukonspekti lauset 5.10, mille järgi

$$\begin{aligned} S_1 &= \varphi(2233) + \varphi(319) + \varphi(203) + \varphi(77) + \varphi(29) \\ &= \varphi(7)\varphi(11)\varphi(29) + \varphi(11)\varphi(29) + \varphi(7)\varphi(29) + \varphi(7)\varphi(11) + \varphi(29) \\ &= 6 \cdot 10 \cdot 28 + 10 \cdot 28 + 6 \cdot 28 + 6 \cdot 10 + 28 \\ &= 1680 + 280 + 168 + 60 + 28 \\ &= 2216. \end{aligned}$$

Seega arve, mille ühistegur 2233-ga on väiksem kui 123, on lõigus $[1, 2233]$ 2216 tükki.

Vaatleme nüüd arve poollõigult (2233,2345], mille SÜT 2233-ga on sobiv. Antud poollõigus on 112 arvu. Meile sobimatud SÜT-id on $7 \cdot 29 = 203$, $11 \cdot 29 = 319$ ja 2233. Pärast arvu 2233 saab järgmine 203-ga jaguv arv olla loomulikult alles 203 arvu pärast, mis on juba poollõigust väljas. Analoogselt teiste sobimatute SÜT-idega. See tähendab, et kõigist võimalikest SÜT-idest, mis saavad tekkida arvuga 2233, on meile sobimatute esinemine antud poollõigus võimatu. Sellest et mitte sobivad SÜT-d ei saa esineda juba järeldub et kõgil teistel liikmetel on sobivad SÜT-d. Seega tähendab see, et kõigi arvude $2233 < x \leq 2345$ korral $(x, 2233) \in \{1, 7, 11, 29, 77\}$.

Järelikult kokku on selliseid naturaalarve, mis pole suuremad kui 2345 ja mille suurim ühistegur arvuga 2233 on väiksem kui 123, on $2216 + 112 = 2328$.

3 Markus Rene Pae

Selles ülesandes on vaja lahendada kongruents $2022^{\left(2021^{2020}\right)} \equiv x \pmod{1000}$, kus x esindab antud arvu kolme viimast kümnendnumbrit. Kuna $1000 = 8 \cdot 125$ ja $(8, 125) = 1$, siis saame jagada selle kongruentsi kaheks osaks:

1. $2022^{\left(2021^{2020}\right)} \equiv a \pmod 8$. Kuna $2 \mid 2022$ ning silmnähtavalt $2021^{2020} \geqslant 3$, siis $2^3 \mid 2022^{\left(2021^{2020}\right)}$ ehk $2022^{\left(2021^{2020}\right)} \equiv 0 \pmod 8$.

2. $2022^{\left(2021^{2020}\right)} \equiv b \pmod{125}$. Kuna $(2022, 125) = 1$ ning $\varphi(125) = \varphi\left(5^3\right) = 5^{3-2} \cdot (5-1) = 100$, siis $2022^{100} \equiv 1 \pmod{125}$ vastavalt Euleri teoreemile.

Leiame nüüd jäägi, mille 2021^{2020} annab 100-ga jagamisel. Kuna $(2021, 100) = 1$ ning $\varphi(100) = \varphi\left(2^2 \cdot 5^2\right) == 40$, siis vastavalt Euleri teoreemile $2021^{40} \equiv 1 \pmod{100}$. Kuna $2021^{2020} = 2021^{40 \cdot 50 + 20}$, siis $2021^{2020} \equiv 2021^{20} \equiv 21^{20} \equiv 441^{10} \equiv 41^{10} \equiv 1681^5 \equiv 81^5 \equiv 1 \pmod{100}$.
Sellest tulenevalt on arv 2021^{2020} avaldatav kujul $100k + 1$, kus k on mingi täisarv. Seega kuna $2022^{100} \equiv 1 \pmod{125}$, siis $2022^{\left(2021^{2020}\right)} = 2022^{100k+1} \equiv 2022^1 \equiv 22 \pmod{125}$.
Nüüdseks oleme kindlaks teinud, et $2022^{\left(2021^{2020}\right)} \equiv 0 \pmod 8$ ning $2022^{\left(2021^{2020}\right)} \equiv 22 \pmod{125}$. Viimast kongruentsi rahuldavad 22, 147, 272, 397, 522, 647, 772 ja 897. Nendest ainus, mis on kongruentne 0-ga mooduli 8 järgi on 272.

4 Lahenduse autor on toimetusele teada

Paneme tähele, et $2015 = 5 \cdot 13 \cdot 31$.
Näitame, et iga $a \in \mathbb{Z}$ korral $a^{61} \equiv a \pmod{5}$, $a^{61} \equiv a \pmod{13}$ ja $a^{61} \equiv a \pmod{31}$:

- Kui $5 \mid a$, siis $a^{61} \equiv 0 \equiv a \pmod{5}$.

  Kui $5 \nmid a$ ja kuna $5 \in \mathbb{P}$, siis Fermat' väikese teoreemi põhjal $a^4 \equiv 1 \pmod{5}$. Seega $a^{61} \equiv \left(a^4\right)^{15} \cdot a \equiv 1^{15} \cdot a \equiv 1 \cdot a \equiv a \pmod{5}$.

- Kui $13 \mid a$, siis $a^{61} \equiv 0 \equiv a \pmod{13}$.

  Kui $13 \nmid a$ ja kuna $13 \in \mathbb{P}$, siis Fermat' väikese teoreemi põhjal $a^{12} \equiv 1 \pmod{13}$. Seega $a^{61} \equiv \left(a^{12}\right)^5 \cdot a \equiv 1^5 \cdot a \equiv 1 \cdot a \equiv a \pmod{13}$.

- Kui $31 \mid a$, siis $a^{61} \equiv 0 \equiv a \pmod{31}$.

  Kui $31 \nmid a$ ja kuna $31 \in \mathbb{P}$, siis Fermat' väikese teoreemi põhjal $a^{31} \equiv 1 \pmod{31}$. Seega $a^{61} \equiv \left(a^{30}\right)^2 \cdot a \equiv 1^2 \cdot a \equiv 1 \cdot a \equiv a \pmod{31}$.

Niisiis $a^{61} \equiv a \pmod{5}$, $a^{61} \equiv a \pmod{13}$ ja $a^{61} \equiv a \pmod{31}$ iga $a \in \mathbb{Z}$ korral ehk $5 \mid a^{61} - a$, $13 \mid a^{61} - a$ ja $31 \mid a^{61} - a$. Kuna 5, 13 ja 31 on paarikaupa ühistegurita, siis ka $2015 \mid a^{61} - a$, seega $a^{61} \equiv a \pmod{2015}$.

5 Erki Külaots

Vaatame, kuna $\varphi(m) = 1$.
Kui $m = 1$, siis $\varphi(1) = 1$
Kui $m > 1$, siis m-i standardkuju on $m = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ ning

$$\varphi(m) = (p_1 - 1)(p_1^{k_1 - 1}) \cdot \ldots \cdot (p_s - 1)(p_s^{k_s - 1})$$

See on võrdne ühega, kui kõik tegurid on ühed. Kui $p_i \geq 3$, siis $p_i - 1 \geq 2$ ja seega ainuke algtegur saab olla 2 ning kui selle kahe aste on suurem kui üks, siis 2^{k-1} on ka suurem kui üks, seega ainuke sobiv m on sellisel juhul 2

Kuna ainukesed võimalused $\varphi(m) = 1$ jaoks on $m = 1$ ja $m = 2$, siis peame nüüd lahendama võrrandid $\varphi(n) = 1$ ja $\varphi(n) = 2$.

$\varphi(n) = 1$ lahendeid me juba teame, need on $n = 1$ ja $n = 2$.

$\varphi(n) = 2$ korral peavad ennist mainitud valemis olema teguriteks ühed ja täpselt üks 2. Kui $p_i \geq 5$, siis $p_i - 1 \geq 4$. Seega sobivad algtegurid on 2 ja 3. Kui arvu n teguriks on 3^2, siis me saame juba $(3 - 1) \cdot 3 = 6$ seega kolme aste peab olema väiksem kui 2.

Kui arvu n teguriks on 2^3, siis me saame funktsiooni väärtuseks suurema arvu kui neli, seega algteguri 2 aste on maksimaalselt 2. Need jätavad meile kontrollida: $n = 3$, $n = 6$, $n = 4$ ja $n = 12$.

$$\begin{aligned}\varphi(3) &= 2\\ \varphi(4) &= 2\\ \varphi(6) &= 2\\ \varphi(12) &= 4\end{aligned}$$

Seega on sobivad lahenditeks $\{1, 2, 3, 4, 6\}$

6 Lahenduse autor on toimetusele teada

Teame, et $\varphi(n)$ on naturaalarvude arv, mis on n-ga ühistegurita ning $\tau(n)$ on n-i positiivsete jagajate arv. Seejuures kõik need arvud on väiksemad või võrdsed arvuga n.

Ainus arv mis on n-ga ühistegurita ja jagab seda, on üks (Kui $a \geq 2$ ja $a \mid n$, siis $(a, n) \geq a \geq 2$, mistõttu a pole n-ga ühistegurita.). Seega kõik teised arvud kas jagavad n-i, on temaga ühistegurita või siis ei jaga n-i aga pole ka temaga ühistegurita.

Selleks, et $\varphi(n) + \tau(n) > n$, peab iga arv $a \leq n$, olema kas n jagaja või temaga ühistegurita.

Vaatame kolme juhtu:

- Kui $n = 1$, siis $\varphi(1) + \tau(1) = 1 + 1 = 2 > 1$.
- Kui $n = p \in \mathbb{P}$ on algarv, siis $\varphi(p) + \tau(p) = (p - 1) + 2 = p + 1 > p$. (Vastavalt algaarvu definitsioonile, on algarvul p kaks positiivet jagajat: 1 ja p, seega $\tau(p) = 2$),
- Kui n on kordarv, siis $n = ab$, kus $a, b \geq 2$, üldistust kitsendamata eeldame, et $a \leq b$.

  Kuna selleks, et $\varphi(n) + \tau(n) > n$, peab iga n-st väiksem naturaalarv olema kas n jagaja või sellega ühistegurita. Vaatame arvu $x = n - a = ab - a = a(b - 1)$.

  Kuna $a \mid x = a(b - 1)$ ja $a \mid n = ab$, siis $a \mid (x, n)$, mistõttu $(x, n) \geq a \geq 2$. Kuna x-l on n-ga ühest suurem ühistegur, siis peab meie võrduse kehtimiseks x olema n jagaja. Seega $x \mid n$ ehk $a(b - 1) \mid ab$. Siit saame, et $b - 1 \mid b$ ja seega $b - 1 = 1$ ehk $b = 2$. Kuna eelduse kohaselt $a \leq b$, siis ka $a = 2$.

  Seega ainus sobiv kordarv on $n = ab = 2 \cdot 2 = 4$.

Järelikult sobivad n väärtused on 1, 4 ja kõik algarvud.

7 Lahenduse autor on toimetusele teada

Vaatame 2 juhtu:

- Kui n on paarisarv, siis Euleri teoreemi kohaselt on täiuslik arv n kujul $2^k(2^k-1), k \in \mathbb{N}$, kus 2^k-1 on algarv. Seega on sel juhul arvul n täpselt üks paaritu algtegur (2^k-1). Edasi ei ole enam mõtet vaadata, sest kõik paarisarvulised täiuslikud arvud on sellisel kujul.
- Kui n on paaritu arv ehk siis oletame vastuväiteliselt, et täiuslikul arvul n on täpselt kaks erinevat algtegurit ehk $n = p^j \cdot q^k$, kus $j, k \in \mathbb{N}$ ja $p \neq q$ on erinevad paaritud arvud.

  Teoreemi 5.21 b) osa põhjal saame, et

$$\begin{aligned}
\sigma(n) &= 2n \\
\frac{(p^{j+1}-1)(q^{k+1}-1)}{(p-1)(q-1)} &= 2 \cdot p^j \cdot q^k \\
\frac{(p^{j+1}-1)(q^{k+1}-1)}{p^j \cdot q^k \cdot (p-1)(q-1)} &= 2 \\
\frac{\left(p-\frac{1}{p^j}\right) \cdot \left(q-\frac{1}{q^k}\right)}{(p-1)(q-1)} &= 2 \\
\frac{p-\frac{1}{p^j}}{p-1} \cdot \frac{q-\frac{1}{q^k}}{q-1} &= 2
\end{aligned}$$

  Paneme tähele, et $\frac{p-\frac{1}{p^j}}{p-1} < \frac{p}{p-1} = 1 + \frac{1}{p-1} < 1 + \frac{1}{3-1} = 1 + \frac{1}{2} = \frac{3}{2}$, analoogiliselt $\frac{q-\frac{1}{q^k}}{q-1} < 1 + \frac{1}{4} = \frac{5}{4}$. (Kuna p ja q on erinevat paaritud algarvud, siis üks on neist vähemalt 3 ja teine vähemalt 5)

  Seega $\frac{p-\frac{1}{p^j}}{p-1} \cdot \frac{q-\frac{1}{q^k}}{q-1} < \frac{3}{2} \cdot \frac{5}{4} = \frac{15}{8} < \frac{16}{8} = 2$

  Seega võrduse parem pool peab olema 2-st väiksem, mistõttu võrdus ei saa kunagi kehtida ehk jõudsime vastuoluni.

8 Külaots ja Luhaäär

$$\sum_{d|n} \mu(d)^2 \cdot \varphi(d)^2 = \prod_{p|n} (1 + (p-1)^2)$$

Üritame mõista, mida see summa kokku liidab. Kui $\mu(d)$ sihthulk on $\{-1, 0, 1\}$, siis funktsiooni $\mu(d)^2$ sihthulk on $\{0, 1\}$, kus $\mu(d)^2 = 0$ parajasti siis, kui leidub algarv p nii, et $p^2 \mid d$ ja muul ajal on funktsiooni väärtus 1. Seega summas on olulised kõik n-i tegurid, mille algtegurite suurim aste on 1.

Kui n on oma standardkujul ($n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$), siis meile pakuvad huvi ainult n-i tegurid kujul $d = p_{l_1} \cdot \ldots \cdot p_{l_m}$, kus $l_1, ..., l_m \in \{1, .., s\}$ ja $l_1 < ... < l_m$ ning arv 1. Seega meid huvitavad ainult kõik erinevad kombinatsioonid, mida saab moodustada n-i algteguritest. Seejuures teame, et $\varphi(d) = (p_{l_1} - 1) \cdot \ldots \cdot (p_{l_m} - 1)$ ehk korrutise tegurid on kujul $(p_{l_i} - 1)$. Kui leida $\varphi(d)^2$, siis need tegurid on ruudus ($(p_{l_i} - 1)^2$). Seega

$$\varphi(d)^2 = \prod_{i=1}^{m} (p_{l_i} - 1)^2.$$

Lugedes n-i jagaja 1 eraldi, saame me oma summa teisendada kujule

$$\sum_{d|n} \varphi(d)^2 = 1 + \sum_{p_{l_1} \cdot \ldots \cdot p_{l_m} | n} \varphi(p_{l_1} \cdot \ldots \cdot p_{l_m})^2 = 1 + \sum_{p_{l_1} \cdot \ldots \cdot p_{l_m} | n} \prod_{i=1}^{m} (p_{l_i} - 1)^2.$$

Vaatame nüüd algse võrduse paremat poolt

$$\prod_{p|n} (1 + (p-1)^2) = \prod_{i=1}^{s} (1 + (p_i - 1)^2)$$

Kui me selle lahti korrutame (liiget $(p_i - 1)^2$ mitte avades), tekib meile 2^s liidetavat, kus s on arvu n algtegurite arv. Iga selline liidetav koosneb mingist arvust teguritest kujul $(p_i - 1)^2$. Realiseeruvad kõik võimalikud kombinatsioonid, sest iga teguri juures saame läbi korrutades valida, kas korrutame ta liidetavasse või mitte (korrutame ühega). Kuna ka summa

$$1 + \sum_{p_{l_1} \cdot \ldots \cdot p_{l_m} | n} \prod_{i=1}^{m} (p_{l_i} - 1)^2$$

koosneb täpselt nendest samadest liidetavatest, siis võrdus kehtib.