Kontrolltöö 2

Joosep Näks

1. (14 p) Teha kindlaks, kas mooduli n järgi leidub algjuuri ning kui leidub, siis leida nende arv ja üks algjuur, kui

a) $n = 4801$, b) $n = 4802$, c) $n = 4803$, d) $n = 4804$.

a) 4801 on algarv ehk selle järgi leidub algjuuri. Tegurdades ühe võrra väiksemat arvu saan $4801 - 1 = 2^6 \cdot 3 \cdot 5^2$ ehk selleks et kontrollida, kas a on algjuur, tuleb kontrollida et $a^{\frac{4800}{2}}$, $a^{\frac{4800}{3}}$ ja $a^{\frac{4800}{5}}$ ükski ei oleks kongruentsed 1ga mooduli 4801 järgi:

a	a^{960}	a^{1600}	a^{2400}
2	-450	2460	1
3	1		
5	858	2340	1
7	-450	2340	-1

Ehk 7 on algjuur mooduli 4801 järgi.

b) Tegurdan: $4802 = 2 \cdot 7^4$ ehk selle järgi leidub algjuuri. Leian kõigepealt algujuure mooduli 7 järgi, kuna $7 - 1 = 6 = 2 \cdot 3$, kontrollin selleks, et a^2 ja a^3 kumbgi ei oleks kongruentsed 1ga mooduli 7 järgi:

a	a^2	a^3
2	4	1
3	2	2

Ehk 3 on algjuur mooduli 7 järgi. Järgmiseks leian algjuure mooduli 7^2 järgi, selleks on kas 3 või 3+7 ning algjuur astmel 7−1 ei tohi olla kongruentne 1ga mooduli 7^2 järgi. $3^6 \equiv 81 \cdot 9 \equiv 32 \cdot 9 = 288 \equiv -6 \pmod{49}$ ehk 3 on algjuur ka mooduli 7^2 järgi. Seega on ta ka algjuur suvalise mooduli kujul 7^k järgi ehk ka 7^4 järgi. Lõpuks algjuur mooduli $4802 = 2 \cdot 7^4$ järgi on paaritu arv arvudest 3 ja $3 + 7^4$ ehk kuna 3 on paaritu arv, on see mooduli 4802 järgi algjuur.

c) Tegurdan: $4803 = 3 \cdot 1601$ ehk selle mooduli järgi algjuuri ei leidu kuna tegu on kahe erineva kahest suurema algarvu korrutisega.

d) Tegurdan: $4804 = 2^2 \cdot 1201$ ehk selle mooduli järgi algjuuri ei leidu kuna tegu on algarvu ja kõrgema kui esimese astme kahe korrutisega.

2. (14 p) Leida vähim naturaalarv, mille numbrite summa ja korrutis on mõlemad võrdsed arvuga 8100.

Tegurdades saan $8100 = 2^2 \cdot 3^4 \cdot 5^2$ ehk ühekohalised numbrid, millest korrutis koosneda saab on 2, 3, 5 ning 2 ja 3 saavad olla asendatud arvudega 4, 6 või 9. Lisaks saab korrutises olla vabalt valitud kogus numbrit 1. Et lõpuks tulemus arv võimalikult väike oleks, peab ta võimalikult väiksekohaline olema. Vaatlen valikuid läbi, kui tulemusse ainult algtegurid panna ja sinna juurde rida ühtesid, siis algtegurite summa on $2 \cdot 2 + 3 \cdot 4 + 5 \cdot 2 = 26$ ehk juurde tuleb lisada $8100 - 26 = 8074$ ühte, ning kokku tuleb arv $8 + 8074 = 8082$ kohaline, kuna 8 algtegurit (kordustega) on kokku.

Kui kaks kahte asendada ühe neljaga, jääb tegurite summa samaks ehk ühtesid juurde ei tule aga tegurite kogus jääb ühe võrra väiksemaks ehk tulemus jääks 1 võrra lühemaks.

Kui kaks kolme asendada ühe üheksaga, suureneb tegurite summa $9 - 6 = 3$ võrra ehk tulemusarvust jääb 3 ühte vähemaks ning tegurite kogus jääb 1 võrra väiksemaks ehk kokku jääb arv 4 võrra väiksemaks.

Kui üks kaks ja üks kolma asendada kuuega, suureneb tegurite summa $6 - (2 + 3) = 1$ võrra ehk tulemusarvust jääb üks üks vähemaks ning tegurite kogus jääb 1 võrra väiksemaks ehk kokku jääb arv 2 võrra väiksemaks.

Kokku saab kas asendada kaks kahte neljaga ja kaks korda kaks kolme üheksaga või kaks korda 2 ja 3 asendada kuuega ning üks kord kaks kolme asendada üheksaga. Esimesel juhul jääks tulemusarv $1 + 3 + 3 = 7$ võrra lühemaks ning teisel juhul samuti $2 + 2 + 3 = 7$ võrra lühemaks ehk mõlemad asendusvariandid on ekvivalentsed arvu pikkuse koha pealt.

Kui arvud on sama pikad, siis selleks, et suuruselt vähim arv ümberjärjestusega saavutada, tuleb arvus numbrid ära sorteerida väiksemast suuremaks. Algne vaid algtegureid kasutav tulemusarv on seega ...11122333355, esimesest asendusest saadud arv ...11145599 ning teisest asendusest saadud arv ...11155669 ning kuna asendusest saadud arvudel ühtede kogused on samad, on näha et esimene asendus annab väiksema arvu ehk vähim tingimustele vastav arv on 45599, mille ees on $8100 - (4+5+5+9+9) = 8068$ ühte.

3. (14 p) Tõestada, et kui $m \mid n$, siis $\frac{\sigma(m)}{m} \leq \frac{\sigma(n)}{n}$.

Kuna $m \mid n$, leidub selline arv a, et $a \cdot m = n$. Kui arvu m standardkuju on $m = p_1^{k_1} \cdot p_2^{k_2} \cdot ... \cdot p_s^{k_s}$, saab sigma funktsiooni arvutusvalemi järgi lahti kirjutada: $\frac{\sigma(m)}{m} = \frac{p_1^{k_1+1}-1}{p_1^{k_1}(p_1-1)} \cdot \frac{p_2^{k_2+1}-1}{p_2^{k_2}(p_2-1)} \cdot ... \cdot \frac{p_s^{k_s+1}-1}{p_s^{k_s}(p_s-1)}$.

Olgu arvu a standardkuju $a = q_1^{l_1} \cdot q_2^{l_2} \cdot ... \cdot q_s^{l_s}$, siis saab arvu n lahti kirjutada $n = m \cdot q_1 \cdot q_1 ... \cdot q_1 \cdot q_2 \cdot ... \cdot q_s$ ning otsitava võrratuse kehtivuseks piisab kui näidata, et kehtib

$$\frac{\sigma(m)}{m} \leq \frac{\sigma(m \cdot q_1)}{m \cdot q_1} \leq \frac{\sigma(m \cdot q_1 \cdot q_1)}{m \cdot q_1 \cdot q_1} \leq ... \leq \frac{\sigma(n)}{n}$$

ehk on vaja näidata, et kehtib $\frac{\sigma(m)}{m} \leq \frac{\sigma(m \cdot q)}{m \cdot q}$, kus q on algarv.

Kui q leidub juba arvu m algtegurite hulgas on ainus $\frac{\sigma(m)}{m}$ liige, mis muutub $\frac{q^{k+1}-1}{q^k(q-1)}$, nimelt k suureneb ühe võrra. Näitan et see kehtib:

$$\begin{aligned} p \geq 1 &\Leftrightarrow -p \leq -1 \\ &\Leftrightarrow p^{k+2} - p \leq p^{k+2} - 1 \\ &\Leftrightarrow (p^{k+1}-1)(p-1)p \leq (p^{k+2}-1)(p-1) \\ &\Leftrightarrow (p^{k+1}-1)(p-1)p^{k+1} \leq (p^{k+2}-1)(p-1)p^k \\ &\Leftrightarrow \frac{p^{k+1}-1}{(p-1)p^k} \leq \frac{p^{k+2}-1}{(p-1)p^{k+1}} \end{aligned}$$

Kui q ei leidu arvu m algtegurite hulgas, siis ainus asi mis kujus $\frac{\sigma(m)}{m}$ muutub, arvuga q korrutamisel, on see et tekib lisa liige $\frac{q^{1+1}-1}{q^1(q-1)}$. Et algne võrratus kehtiks, peab see uus liige olema suurem või võrdne ühega. Näitan et see kehtib:

$$\begin{aligned} \frac{q^{1+1}-1}{q(q-1)} \geq 1 &\Leftrightarrow q^2 - 1 \geq q(q-1) \\ &\Leftrightarrow (q-1)(q+1) \geq q(q-1) \\ &\Leftrightarrow q+1 \geq q \end{aligned}$$

4. (12 p) Sõnastada ja tõestada teoreem algjuurte leidmisest mooduli $2p^k$ järgi.

Teoreem: kui a on algjuur mooduli p^k järgi, on paaritu arv arvudest a ja $a + p^k$ algjuur mooduli $2p^k$ järgi.

Tõestus: oletame et a on paaritu. Kuna a on algjuur mooduli p^k järgi, on a ka pööratav element ringis $\mathbb{Z}_{p^k}$ ehk $(a, p^k) = 1$ ning kuna a on paaritu, siis ka $(a, 2) = 1$. Seega ka $(a, 2p^k) = 1$ ehk ta on ka pööratav element ringis $\mathbb{Z}_{2p^k}$.

Kuna a on algjuur mooduli p^k järgi, on tema järk rühmas $U(\mathbb{Z}_{p^k})$ võrdne rühma järguga ehk $m = \varphi(p^k) = p^{k-1}(p-1)$. Olgu n elemendi a järk rühmas $U(\mathbb{Z}_{2p^k})$. Siis ühelt poolt Lagrange'i teoreemi tõttu $n \mid |U(\mathbb{Z}_{2p^k})| = \varphi(2p^k) = p^{k-1}(p-1) = m$ ehk $n \leq m$. Teiselt poolt järgu definitsioonist tuleneb $a^n \equiv 1 \pmod{2p^k}$ ning sellest järeldub et $a^n \equiv 1 \pmod{p^k}$ ehk $m \mid n$ ehk $m \leq n$ ning seega $m = n$ ehk elemendi a järk on sama mis rühma järk ehk a on algjuur mooduli $2p^k$ järgi.

5. (26 p) Sõnastada ja tõestada Gaussi ruutvastavusseadus. Gaussi lemmat ja selle järeldust võib kasutada ilma tõestuseta.

Teoreem: kui $p > 2$ ja $q > 2$ on erinevad paaritud algarvud, kehtib

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

Tõestus:
Koostan reaalarvude tasandile ristküliku nurkadega $(0,0), \left(\frac{p}{2},0\right), \left(0,\frac{q}{2}\right), \left(\frac{p}{2},\frac{q}{2}\right)$ ehk hulga $R = \left\{(x,y) \in \mathbb{R}^2 \mid 0 < x < \frac{p}{2}, 0 < y < \frac{q}{2}\right\}$ ning nimetan selle täisarvuliste koordinaatidega punktid võrepunktideks. Kuna iga võrepunkti (m,n) korral koordinaatid on suuremad kui 0 ehk suuremad või võrdsed 1ga ning väiksemad kui vastavalt $\frac{p}{2}$ või $\frac{q}{2}$ ning p ja q on mõlemad paaritud ehk on koordinaadid väiksemad või võrdsed kui $\frac{p-1}{2}$ või $\frac{q-1}{2}$, seega on võrepunktide kogus $\frac{p-1}{2} \cdot \frac{p-1}{2}$.

Tõmban ristkülikule diagonaali, kuna see läbib punkte $(0,0)$ ja $(\frac{q}{2},\frac{q}{2})$, on selle võrrand $y = \frac{p}{q}x$ ehk $qy = px$. Kuna p ja q on erinevad algarvud, kehtib $(p,q) = 1$ ehk eukleidese lemma tõttu kui leidub diagonaalil võrepunkte, siis nende puhul kehtib $p \mid x$ ja $q \mid y$, kuid kuna $1 \leq x \leq \frac{p-1}{2}$ ja $1 \leq y \leq \frac{q-1}{2}$, ei saa need jaguvused kehtida ehk diagonaalil ei leidu võrepunkte. Tähistame diagonaalist allpool oleva ristküliku osa T_1 ja ülal oleva osa T_2 ning kuna diagonaalil võrepunktid puuduvad, on T_1 ja T_2 võrepunktide ühend kõigi võrepunktide hulk.

Fikseerin mingi $1 \leq x \leq \frac{p-1}{2}$, siis selle x väärtusele vastavaid võrepunkte hulgas T_1 on nii palju, kui vahemikus $1 \leq y \leq \frac{qx}{p}$ väärtuseid ehk $\left\lfloor \frac{qx}{p} \right\rfloor$ tükki. Seega on kokku T_1 võrepunktide kogus $\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{qk}{p} \right\rfloor$ ning analoogselt koordinaadid vahetades saab, et T_2 võrepunktide kogus on $\sum_{l=1}^{\frac{q-1}{2}} \left\lfloor \frac{pl}{q} \right\rfloor$ ehk kogu võrepunktide kogus on

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{qk}{p} \right\rfloor + \sum_{l=1}^{\frac{q-1}{2}} \left\lfloor \frac{pl}{q} \right\rfloor$$

Ehk kasutades Gaussi lemmast järelduvat lauset 8.13 saab Legrende'i sümbolite korrutise lahti kirjutada

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{qk}{p} \right\rfloor} \cdot (-1)^{\sum_{l=1}^{\frac{q-1}{2}} \left\lfloor \frac{pl}{q} \right\rfloor} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Ning lõpuks saab algse otsitava tulemuse kätte:

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