Kodutöö nr. 11

Joosep Näks ja Uku Hannes Arismaa

1. Leida kõik algjuured mooduli 58 järgi.

Teeme indeksite tabeli eelmisest korrast teada oleva algjuure 19 järgi.

	1	3	5	7	9
0	28	13	18	20	26
1	9	2	3	21	1
2	5	24	8	11	
3	25	22	10	19	15
4	7	17	16	23	12
5	6	4	27	14	

Nenedest on algjuured need, mille indeksid on rühma järguga 28 ühistegurita ehk 3, 11, 15, 19, 21, 27, 21, 37, 39, 43, 47, 55.

2. Teha kindlaks, kas mooduli n järgi leidub algjuuri ja kui leidub, siis leida nende arv ja üks algjuur, kui *a*) $n = 166$, *b*) $n = 167$, *c*) $n = 168$.

Teoreemi 7.21 põhjal on teada, et mooduli n järgi leidub algjuuri, kui n esitub kujul 2, 4, p^k või $2p^k$, kus $p > 2$ on algarv. Tegurdades saab $166 = 2 \cdot 83$ ja $168 = 2^3 \cdot 3 \cdot 7$ ning 167 on ise algarv. Seega mooduli 168 järgi algjuuri ei leidu, 166 ja 167 järgi leidub. Teoreemi 7.27 põhjal kui mooduli n järgi leidub algjuuri, on neid $\varphi(\varphi(n))$ tükki ehk mooduli 166 järgi on $\varphi(\varphi(166)) = 40$ algjuurt ning mooduli 167 järgi on $\varphi(\varphi(167)) = 82$ algjuurt.
Mooduli 166 järgi algjuure leidmiseks leian kõigepealt algjuure mooduli 83 järgi. Kuna $83 - 1 = 2 \cdot 41$, on järelduse 7.24 põhjal arv a algjuur parajasti siis, kui $a^{41} \not\equiv 1 \pmod{83}$ ja $a^2 \not\equiv 1 \pmod{83}$. Proovin $a = 2$: $2^{41} \equiv -1 \pmod{83}$ ja $2^2 \equiv 4 \pmod{83}$ ehk 2 sobib algjuureks. Teoreemi 7.18 järgi kui 2 on algjuur mooduli 83 järgi siis mooduli $2 \cdot 83 = 166$ järgi on algjuur paaritu arv arvudest 2 ja $2 + 83 = 85$ ehk 85 on algjuur mooduli 166 järgi.
Mooduli 167 järgi kuna $167-1 = 83 \cdot 2$, on a algjuur parajasti siis, kui $a^{83} \not\equiv 1 \pmod{167}$ ja $a^2 \not\equiv 1 \pmod{167}$. Proovin $a = 2$: $2^{83} \equiv 1 \pmod{167}$ ehk 2 ei sobi algjuureks, proovin $a = 3$: $3^{83} \equiv 1 \pmod{167}$ ehk 3 samuti ei sobi algjuureks, proovin $a = 4$: $4^{83} \equiv 1 \pmod{167}$, proovin $a = 5$: $5^{83} \equiv -1 \pmod{167}$ ja $5^5 \equiv 25 \pmod{167}$ ehk 5 on algjuur mooduli 167 järgi.

3. Teha kindlaks, kas mooduli n järgi leidub algjuuri ja kui leidub, siis leida nende arv ja üks algjuur, kui *a*) $n = 337$, *b*) $n = 338$, *c*) $n = 339$.

Teoreemi 7.21 põhjal on teada, et mooduli n järgi leidub algjuuri, kui n esitub kujul 2, 4, p^k või $2p^k$, kus $p > 2$ on algarv. Tegurdades saab $338 = 2 \cdot 13^2$ ja $339 = 3 \cdot 113$ ning 337 on ise algarv. Seega mooduli 339 järgi algjuuri ei leidu, 338 ja 337 järgi leidub. Teoreemi 7.27 põhjal kui mooduli n järgi leidub algjuuri, on neid $\varphi(\varphi(n))$ tükki ehk mooduli 338 järgi on $\varphi(\varphi(338)) = 48$ algjuurt ning mooduli 337 järgi on $\varphi(\varphi(337)) = 96$ algjuurt.
Mooduli 338 järgi algjuure leidmiseks leian kõigepealt algjuure mooduli 13 järgi. Kuna $13 - 1 = 2^2 \cdot 3$, on järelduse 7.24 põhjal arv a algjuur parajasti siis, kui $a^6 \not\equiv 1 \pmod{13}$ ja $a^4 \not\equiv 1 \pmod{13}$. Proovin $a = 2$: $2^6 \equiv -1 \pmod{13}$ ja $2^4 \equiv 3 \pmod{13}$ ehk 2 sobib algjuureks. Järelduse 7.15 järgi kui 2 on algjuur mooduli 13 järgi siis mooduli $13^2 = 169$ järgi on algjuur 2 või 2+13. $2^{13-1} \equiv 40 \pmod{169}$, seega sobib algjuureks 2. Teoreemi 7.18 järgi kui 2 on algjuur mooduli 169 järgi siis mooduli $2 \cdot 169 = 338$ järgi on algjuur paaritu arv arvudest 2 ja $2 + 169 = 171$ ehk 171 on algjuur mooduli 338 järgi.
Mooduli 337 järgi kuna $337-1 = 2^4 \cdot 3 \cdot 7$, on a algjuur parajasti siis, kui $a^{168} \not\equiv 1 \pmod{337}$, $a^{112} \not\equiv 1 \pmod{337}$ ja $a^{48} \not\equiv 1 \pmod{337}$. Proovin $a = 10$: $10^{168} \equiv -1 \pmod{337}$, $10^{112} \equiv 128 \pmod{337}$ ja $10^{48} \equiv 175 \pmod{337}$ ehk 10 on algjuur mooduli 337 järgi.

4. Lahendada kongruents $1 - x + x^2 - x^3 + x^4 + \ldots - x^{2023} \equiv 0 \pmod{58}$.

Korrutan võrrandi mõlemad pooled läbi elemendiga $x+1$. Sellega ei saa samaväärset võrrandit, kuna $x+1$ võib olla nullitegur, kuid kõik esialgse võrrandi lahendid on ka uue võrrandi lahendite hulgas, nii et lõpus kontrollin lahendite sobivust. Paremale poolele jääb ikka 0, aga vasakule poolele tekib summa $(1+x)-(x+x^2)+(x^2+x^3)-\ldots-(x^{2023}+x^{2024})$. Siin on näha, et sulud lahti tehes on igas sulus teine liidetav järgmise sulu esimese liidetava vastandarv ehk kõik peale esimese ja viimase liidetava taanduvad maha ning alles jääb võrrand $1 - x^{2024} \equiv 0 \pmod{58}$ ehk $x^{2024} \equiv 1 \pmod{58}$. Kuna $\varphi(58) = 28$, kehtib FVT järgi $x^{28} \equiv 1 \pmod{58}$ ehk $x^{2024} = x^{28 \cdot 72 + 8} \equiv x^8 \pmod{58}$.

Teoreemi 7.6 põhjal kehtib $x^8 \equiv 1 \pmod{58}$ parajasti siis, kui $m \mid 8$, kus m on elemendi x järk. Seega on lahenditeks elemendid, mille järk on 1, 2, 4 või 8. Lagrange'i teoreemi tõttu aga peab elemendi järk ka rühma järku jagama ehk kuna $8 \nmid 28$, ei leidu elemente, mille järk oleks 8. Ainus esimest järku element on 1. Esimesest ülesandest saan, et üks algjuur mooduli 58 järgi on 19. Teoreemi 7.36 põhjal on m järku elemendid parajasti need elemendid b, mille puhul kehtib $(\mathrm{ind}_{19} b, \varphi(58)) = \dfrac{\varphi(58)}{m}$ ehk $(\mathrm{ind}_{19} b, 28) = \dfrac{28}{m}$.

Seega teist järku elemendid on elemendid, mille indeksi suurim ühistegur arvuga 28 on 14. 14 kordseid indekseid on kaks tükki, 14 ja 28 ning ainult 14 annab suurimaks ühisteguriks arvuga 28 arvu 14 ehk 14 on lahendi indeks. Esimese ülesande tabeli põhjal on selleks lahendiks -1.

Neljandat järku elemendid on elemendid, mille indeksi suurim ühistegur arvuga 28 on 7. Kuna lisaks arvule 7 on 28 ainus algtegur 2, on sobivad indeksid kõik paaritud 7 kordsed arvud ehk 7 ja 21. Esimese ülesande tabeli põhjal on nendele indeksitele vastavad arvud 17 ja 41.

Seega olen saanud lahendid 1, 17, 41 ja -1. Kui $x+1 \neq 0$, saab algse võrrandiga samaväärse võrrandi korrutades arvuga $x+1$ läbi võrrandi mõlemad pooled ja ka mooduli, saades uue võrrandi $x^{2024} \equiv 1 \pmod{58(x+1)}$. $x+1=0$ kehtib vaid lahendi $x=-1$ juures, ning kui see algsesse võrrandisse sisse asendada, tekib summa, kus kõigi paaritu astmega liikmete märk vahetub ja kõigi liikmete absoluutväärtus on 1 ehk summas on 2024 korda 1 kokku liidetud ning $2024 \equiv -7 \not\equiv 0 \pmod{58}$ ehk -1 ei sobi lahendiks. Teiste lahendite jaoks proovin uut saadud võrrandit.

$x = 1$ puhul $1^{2024} \equiv 1 \pmod{58 \cdot 2}$ ehk 1 sobib lahendiks.

$x = 17$ puhul $\varphi(58 \cdot (17+1)) = 336$ ning $17^{2024} \equiv 17^{6 \cdot 336 + 8} \equiv 17^8 \equiv 1 \pmod{58(17+1)}$ ehk 17 sobib lahendiks.

$x = 41$ puhul $\varphi(58 \cdot (41+1)) = 672$ ning $41^{2024} \equiv 41^{3 \cdot 672 + 8} \equiv (41)^8 \equiv 1 \pmod{58(41+1)}$ ehk 41 sobib lahendiks.

5. Tõestada, et kui $n \geq 2$, siis iga Fermat' arvu $F_n = 2^{2^n} + 1$ mistahes algtegur on kujul $k2^{n+1} + 1$.

Paneme tähele, et rühamas $U(\mathbb{Z}_{F_n})$ $\overline{2}^x = \overline{2^x}$, kuni $x < 2^n$, seejärel saame, et $\overline{2}^{2^n} = \overline{-1}$, mida omakorda $\overline{2}$ga korrutades fikseerime lõpuks $\overline{2}$ järgu kui 2^{n+1}. Vaadates sama protsessi F_n algtegureile (mis kõik peavad olema paaritud) vastavate jäägiklasside otsekorrutises, saame $(\overline{2} \times \ldots \times \overline{2})^{2^n} = (\overline{-1} \times \ldots \times \overline{-1})$ ning $(\overline{2} \times \ldots \times \overline{2})^{2^{n+1}} = (\overline{1} \times \ldots \times \overline{1})$. Näeme, et igale algtegurile vastavas rühmas, peab $\overline{2}$ järk jagama 2^{n+1} (Lemma 7.6). Kui see on aga väiksem, peaks see samuti jagama 2^n, millisel juhul, poleks $\overline{2}^{2^n}$ selles rühmas $\overline{-1}$, seega on igale algtegurile vastavas rühmas $\overline{2}$ järk täpselt 2^{n+1}. Lagrange'i teoreemi järgi peab 2^{n+1} jagama selle rühma järku, milleks on $\varphi(p^m) = (p-1)p^{m-1}$. Kuna p oli paaritu, siis saame Eukleidese lemmast, et $2^{n+1} \mid p-1 \Leftrightarrow k2^{n+1} + 1 = p$.

6. Leida kõik algarvud p, mille järgi on olemas täpselt 16 erinevat algjuurt.

Teoreemi 7.27 leidub mooduli p järgi täpselt $\varphi(\varphi(p))$ algjuurt. Leian kõigepealt kõik võimalikud $\varphi(x) = 16$ lahendid. Kuna φ funktsiooni arvutusvalem on $\varphi(p_1^{k_1}p_2^{k_2}..p_s^{k_s}) = p_1^{k_1-1}(p_1-1)p_2^{k_2-1}(p_2-1)..p_s^{k_s-1}(p_s-1)$, peavad kõik $\varphi(x)$ algtegurid p_i olema kas ise arvu x algtegurid või peab $p_i - 1$ olema arvu x tegur. Arvu 16 teguriteks on 1, 2, 4, 8 ja 16. Nendest endast on algarv vaid 2 ning nendest 1 võrra suurematest arvudest on algarvud 2, 3, 5 ja 17. Seega saab 2 esineda arvu x algtegurina ükskõik millise astmega ning 3, 5 ja 17 saavad esineda astmega 1.

Esiteks kui x on mingi 2 aste, siis $2^{k-1}(2-1) = 16$ ehk $k = 5$ ning $x = 32$. Kuid lõpuks peab kehtima $\varphi(p) = p - 1 = x$, kuid $32 + 1 = 33$ ei ole algarv ehk siit ei saa sobivat vastust.
Kui x tegurite hulgas on 2 ja 3, siis $2^{k-1}(2-1) \cdot 3^{1-1}(3-1) = 16$ kust saab $k = 4$ ehk $x = 48$. Kuid jällegi $48 + 1 = 49$ ei ole algarv ehk see ei ole sobiv vastus. Kui võtta algtegurite hulka ka 5, saab $2^{k-1}3^0(3-2)5^0(5-1) = 16$ kus $k = 2$ ehk $x = 60$, ning 61 on algarv ehk see on üks sobilikest p väärtustest. 17 ei saa kolmega koos algtegurite hulka võtta, kuna $17 - 1$ on juba ise 16.
Kui 3 välja jätta ja ainult 2 ja 5 kasutada x algteguriteks, saab $2^{k-1}5^0(5-1) = 16$, kust saab $k = 3$ ehk $x = 40$ ning kuna 41 on algarv, sobib see p väärtuseks.
Kui võtta 2 ja 17 algteguriteks, saab $2^{k-1} \cdot 17^0(17-1) = 16$, kus $k = 1$ ehk $x = 34$, kuid $34 + 1 = 35$ ei ole jällegi algarv. Siin saaks ka 2 tegurite hulgast välja jätta, kuna $17 - 1$ on ise 16 ehk 17 sobiks ise x väärtuseks kuid $17 + 1 = 18$ ei ole algarv ehk see ei sobi p väärtuseks.

Seega on kokkuvõttes kaks sobivat p väärtust: 61 ja 41.

7. Tõestada, et kui algarvulise mooduli p järgi leidub täpselt $k \geq 2$ algjuurt, siis mistahes $k - 1$ **erineva** algjuure korrutis on samuti algjuur.

Kui mooduli p järgi leidub algjuur a järguga j, siis $a^j = \overline{1}$, seega leidub sellel üheselt määratud pöördelement a^{j-1} (märkus: iga algjuure aste on erinev element, seega tavaliselt meil siin probleeme ei teki, erandiks on juht $j-1 = j$, aga siis tuleb välja, et $p = 3$ ning k on sellisel juhul liiga väike), mis eelmise nädala tulemuste põhjal on samuti algjuur. Seega saab kõikide algjuurte korrutises igale algjuurele läbi seada vastavusse pöördelemendi, saades korrutiseks $\overline{1}$. Sellest mistahes $k - 1$ erineva algjuure korrutise saamiseks peame identifitseerima selle algjuure, mida me korrutisse ei taha ning kõikide algjuurte korrutise $(\overline{1})$ korrutama selle algjuure pöördelemendiga, mis on ka algjuur, saades kokku algjuure.

8. Olgu n naturaalarv. Tõestada, et

$$\prod_{\substack{1\le a\le n\\(a,n)=1}} a \equiv \begin{cases} 0 \pmod 1; \\ 1 \pmod n, \text{ kui mooduli } n>1 \text{ järgi ei leidu algjuuri;} \\ -1 \pmod n, \text{ kui mooduli } n>1 \text{ järgi leidub algjuuri.} \end{cases}$$

Vasakpoolses korrutises on kõik arvud $\mathbb{Z}_n$ pööratavad elemendid, ehk neil leiduvad pöördelemendid, millega saab neid paari panna ja kõigi paaride korrutised on 1. Probleeme tekitavad vaid elemendid, mis on ise enda pöördelemendid, ehk võrrandi $x^2 \equiv 1 \pmod n$ lahendid. Uurin neid lahendeid. Teoreemi 6.10 järgi kui n esitub standardkujul $n = p_1^{k_1}p_2^{k_2}..p_s^{k_s}$, siis võrrand $x^2 \equiv 1 \pmod n$ on samaväärne võrrandite süsteemiga

$$\begin{cases} x^2 \equiv 1 \pmod{p_1^{k_1}} \\ x^2 \equiv 1 \pmod{p_2^{k_2}} \\ \dots \\ x^2 \equiv 1 \pmod{p_s^{k_s}} \end{cases}$$

Uurin võrrandit $x^2 \equiv 1 \pmod{p^k}$. Juhul kui $p = 2$, on kahekasanda praktikumi tulemuste põhjal lahenditeks $k = 1$ puhul vaid 1, $k = 2$ puhul 1 ja -1 ning $k > 2$ puhul $1, 2^{k-1}-1, 2^{k-1}+1, -1$. Kui $p > 2$, leidub mooduli p^k järgi algjuuri. Teoreemi 7.6 põhjal on võrrandi lahenditeks elemendid, mille järk jagab arvu 2 ehk järk saab olla kas 1 või 2. Ainus element, mille järk on 1 on 1. Elemendi -1 järk on 2 kuna $(-1)^2 = 1$ ja rohkem teist järku elemente ei leidu kuna teoreemi 7.36 põhjal peab iga teist järku elemendi b jaoks kehtima $(\text{ind}_a b, \varphi(n)) = \dfrac{\varphi(n)}{2}$, kus a on mingi algjuur, ehk nende indeks peab olema $\dfrac{\varphi(n)}{2}$ kordne, kuid elemendi -1 indeks on juba $\dfrac{\varphi(n)}{2}$, elemendi 1 indeks on $\varphi(n)$ ning rohkem sobivaid indekseid vahemikus 1 kuni $\varphi(n)$ ei leidu.

Seega kui 2 ei ole algtegurite hulgas, saab HJT-st 2^s lahendit, mida saab iga astendatud algteguri $p_i^{k_i}$ järgi pooleks teha kaheks hulgaks: 2^{s-1} lahendit, mis on mooduli $p_i^{k_i}$ järgi kongruentsed arvuga -1 ning 2^{s-1} lahendit, mis on kongruentsed arvuga 1. Kuni $s > 1$, on 2^{s-1} paarisarv ehk kui esimeses loetletud hulgas kõik lahendid omavahel kokku korrutada, on korrutise tulemus kongruentne arvuga $(-1)^{2^{s-1}} = 1$ mooduli $p_i^{k_i}$ järgi ning seega ka kõigi lahendite kokku korrutamine on kongruentne arvuga 1 kõigi moodulite $p_i^{k_i}$ järgi ehk ka mooduli n järgi. Kui $s = 1$, koosneb süsteem vaid ühest võrrandist, ning selle kaks lahendit on 1 ja -1, mille kokku korrutamine annab mooduli n järgi tulemuse -1.

Kui eelmises lõigus käsitletud tulemuste hulka lisada sellised n väärtused, kus $p_1 = 2$ ja $k_1 = 1$, siis lisatud võrrandil on vaid 1 lahend ehk süsteemi lahendite kogus ei muutu ning see lahend on kongruentne nii 1 kui ka -1ga mooduli 2 järgi ehk see ei muuda lahendite kongruentsust mooduli n järgi. Kui 2 aste $k_1 = 2$, siis on 2 lahendit, 1 ja -1, ehk sarnaselt teiste algteguritega kui 2 on ainus algtegur, on korrutise tulemus on kongruentne -1ga mooduli 2 järgi ning kui on teisi algtegureid veel, on kokku paarisarv selliseid lahendeid, mis on kongruentsed -1ga ehk korrutis on kongruentne 1ga mooduli 2 järgi. Kui 2 aste on suurem kui 2, on lahendeid 4: $1, 2^{k-1}-1, 2^{k-1}+1, -1$. Need kokku korrutades saab $-((2^{k-1})^2-1) = 1-2^k \cdot 2^{k-2} \equiv 1 \pmod{2^k}$ ehk olenemata teiste algtegurite kogusest on lahendite korrutis mooduli 2^k järgi 1. Samuti on siin paarisarv lahendeid, ehk kui leidub teisi algtegureid, on eelmise lõigu põhjal korrutis ka nende moodulite järgi 1.

Seega olen saanud, et kui n esitub kujul p^k, $2p^k$, 2 või 4, on otsitav korrutis kongruentne arvuga -1 mooduli n järgi ning igal muul juhul kongruentne arvuga 1. Need on ka parajasti need n kujud, milliste moodulite järgi leidub algjuuri, ehk kui mooduli n järgi leidub algjuuri, on korrutise tulemus kongruentne arvuga -1 ning kui ei leidu algjuuri, kongruentne arvuga 1, mida oligi tarvis näidata.