Kodutöö nr. 12

Joosep Näks ja Uku Hannes Arismaa

1. Leida arvu 9 indeks *kõigil* võimalikel alustel mooduli 22 järgi.

2. Koostada indeksite tabel alusel 3 mooduli 25 järgi.

Kontrollin esiteks, et 3 on algjuur. Kuna $\varphi(25) = 20 = 2^2 \cdot 5$, on vaja kontrollida, et 3^4 ja 3^10 ei oleks kongruentsed ühega mooduli 25 järgi ning esimene on kongruentne arvuga 6 ja teine arvuga -1 ehk tõepoolest on tegu algjuurega. Tabeli moodustamiseks leian väärtused 3^1 kuni 3^{20}:

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\overline{3^k}$	3	9	2	6	18	4	12	11	8	24	22	16	23	19	7	21	13	14	17	1

Ning selle põhjal saab indeksite tabeli:

	0	1	2	3	4	5	6	7	8	9
0		20	3	1	6		4	15	9	2
1		8	7	17	18		12	19	5	14
2		16	11	13	10					

3. Leida $\mathrm{ind}_2 3$ mooduli 25 järgi. Kasutades saadud indeksit, koostada indeksite tabel alusel 2 mooduli 25 järgi.

4. Leida kõigi rühma $U(\mathbb{Z}_{37})$ elementide järgud ja kõik algjuured mooduli 37 järgi indeksite tabeli abil. Kontrollida vastust ilma astendamist kasutamata.

Leian kõigepealt algjuure mooduli 37 järgi. Kuna $\varphi(37) = 36 = 6^2$, peab vaid kontrollima, kas a^6 on kongruentne arvuga 1, et teada saada, kas a on algjuur. Proovin $a = 2$, sel juhul $a^6 \equiv -10 \not\equiv 1 \pmod{37}$ ehk 2 on algjuur. Et saada indeksid, leian väärtused 2^1 kuni 2^{18} (teine pool astmetest on samade arvude vastandarvud ehk neid pole vaja välja kirjutada):

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\overline{2^k}$	2	4	8	16	32	27	17	34	31	25	13	26	15	30	23	9	18	36

Arvestades, et teoreemi 7.36 põhjal on elemendi b järk $\dfrac{36}{(\mathrm{ind}_2 b, 36)}$ ehk saan moodustada leitud astmete põhjal indeksite ja järkude tabeli:

ind / järk	0	1	2	3	4	5	6	7	8	9
0		36 / 1	1 / 36	26 / 18	2 / 1	23 / 36	27 / 4	32 / 9	3 / 12	16 / 9
1	24 / 3	30 / 6	28 / 9	11 / 36	33 / 12	13 / 36	4 / 9	7 / 36	17 / 36	35 / 36
2	25 / 36	22 / 18	31 / 36	15 / 12	29 / 36	10 / 18	12 / 3	6 / 6	34 / 18	21 / 12
3	14 / 18	9 / 4	5 / 36	20 / 9	8 / 9	19 / 36	18 / 2			

Algjuured on arvud, mille järk on 36 ehk 2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32 ja 35.

5. Lahendada kongruents $2020 \cdot x^{2022} \equiv 2033 \pmod{37}$ indeksite tabeli abil.

6. Milline kongruentsidest $12^{x^3} \equiv 3^2 \pmod{25}$ ja $13^{x^2} \equiv 2^4 \pmod{25}$ on lahenduv? Leida selle üldlahend.

Vaatlen esimest võrrandit. Teisest ülesandest näen, et 3 on algjuur mooduli 25 järgi. Seega lause 7.30 järgi saan võrrandi mõlemast poolest võtta indeksi aluse 3 järgi ning tulemuseks on samaväärne võrrand mooduli $\varphi(25) = 20$ järgi: $\mathrm{ind}_3 12^{x^3} \equiv \mathrm{ind}_3 3^2 \pmod{20}$. Indeksi omaduste järgi saab astme indeksi ette tuua: $x^3 \cdot \mathrm{ind}_3 12 \equiv 2 \cdot \mathrm{ind}_3 3 \pmod{20}$. Teise ülesande tabelist näen, et arvu 12 indeks on 7 ja arvu 3 indeks

on 1 ehk võrrandist jääb alles $7x^3 \equiv 2 \pmod{20}$. Kuna $4 \mid 20$, on kõik lahendid ka lahendid mooduli 4 järgi, kuid proovides läbi kõik x väärtused mooduli 4 järgi on näha, et ükski lahend ei sobi, ehk ka algsel võrrandil puuduvad lahendid.

Vaatlen teist võrrandit. Võtan jällegi mõlemast poolest indeksi alusel 3: $\operatorname{ind}_3 13^{x^2} \equiv \operatorname{ind}_3 2^4 \pmod{20}$ ehk kasutades indeksi omadusi ja teise ülesande tabelit saab $x^2 \cdot 17 \equiv 4 \cdot 3 \pmod{20}$. Korrutan mõlemad pooled läbi arvuga -7: $x^2 \equiv -4 \pmod{20}$. Tegurdades saan $20 = 2^2 \cdot 5$ ehk saan võrrandi jagada võrrandisüsteemiks

$$\begin{cases} x^2 \equiv -4 \pmod 4 \\ x^2 \equiv -4 \pmod 5 \end{cases}$$

Läbi proovides saan esimese võrrandi lahenditeks $x \equiv 0 \pmod 4$ ja $x \equiv 2 \pmod 4$ ehk $x \equiv 0 \pmod 2$ ning teise võrrandi lahenditeks $x \equiv 1 \pmod 5$ ja $x \equiv -1 \pmod 5$. Seega on HJT põhjal esialgse võrrandi lahendid $x \equiv 6 \pmod{10}$ ja $x \equiv 4 \pmod{10}$.

7. Leida, milliste arvude $1 \leq a \leq 27$ korral on kongruents $x^{15} \equiv a \pmod p$ lahenduv korraga *kõigi* moodulite $p = 7, 13, 27$ järgi.

8. Olgu $p > 2$ algarv ja $a \in \mathbb{Z}$. Leida kongruentsi $x^{12} = a \pmod p$ kõik võimalikud lahendite arvud ja tuua iga juhu kohta näide, mis seda realiseerib.

Juhul, kui $a = 0$, on alati 1 lahend, milleks on $x = 0$, kuna $\mathbb{Z}_p$ kõik elemendid peale $\overline{0}$ on pööratavad ning pööratavate elementide korrutamisel saab tulemuseks alati pööratava elemendi. Muudel juhtudel pole $x = 0$ kunagi lahend, kuna see annab iga mooduli järgi tulemuseks 0, seega saame edasi vaadata vaid pööratavaid x ja a väärtuseid.

Kui x_0 on mingi $x^{12} \equiv a \pmod p$ lahend, on x_0^{-1} võrrandi $x^{12} \equiv a^{-1} \pmod p$ lahend. Kui võrrandil $x^{12} \equiv a \pmod p$ leidub veel lahendeid, saab iga sellise lahendi x' kohta ühe võrrandi $x^{12} \equiv 1 \pmod p$ lahendi kuna kui vastavatesse võrranditesse lahendid x' ja x_0^{-1} sisse panna ning võrrandite pooled kokku korrutada saab $(x')^{12} \cdot (x_0^{-1})^{12} \equiv a \cdot a^{-1} \pmod p$ ehk $(x' \cdot x_0^{-1})^{12} \equiv 1 \pmod p$. Seega on iga lahendi x' kohta $a = 1$ võrrandi lahend $x' \cdot x_0^{-1}$ (x' saab ka olla sama mis x_0, mis puhul tuleb lahend $x_0 \cdot x_0^{-1} = 1$). Sellised saadud lahendid on kõik erinevad kuna kui leidub kaks x' väärtust x_1' ja x_2', mis annavad sama $a = 1$ võrrandi lahendi, siis kehtib $x_1' \cdot x_0^{-1} = x_2' \cdot x_0^{-1}$ ning kui mõlemad pooled arvuga x_0 läbi korrutada, saab $x_1' = x_2'$ ehk need on samad arvud. Seega on võrrandi $x^{12} \equiv 1 \pmod p$ lahendite hulk vähemalt samasuur nagu ühegi võrrandi $x^{12} \equiv a \pmod p$ lahendite hulk.

Väide töötab ka vastupidi, kui võrrandil $x^{12} \equiv a \pmod p$ leidub mingi lahend x_0, saab iga võrrandi $x^{12} \equiv 1 \pmod p$ lahendi x' kohta ühe $x^{12} \equiv a \pmod p$ lahendi kujul $x' \cdot x_0$ kuna lahendid sisse pannes ja võrrandite pooled kokku korrutades saab $(x')^{12} \cdot (x_0)^{12} \equiv 1 \cdot a \pmod p$ ehk $(x' \cdot x_0)^{12} \equiv a \pmod p$. Seega kui võrrandil $x^{12} \equiv a \pmod p$ leidub lahendeid, on neid täpselt samapalju nagu võrrandil $x^{12} \equiv 1 \pmod p$.

On ka võimalus et võrrandil $x^{12} \equiv a \pmod p$ ei ole lahendeid, näiteks võrrandil $x^{12} \equiv 2 \pmod 3$ saab väärtuseid läbi proovides et lahendid puuduvad.

Uurin võrrandi $x^{12} \equiv 1 \pmod p$ lahendite kogust. Teoreemi 7.6 põhjal on selle võrrandi lahendid arvud, mille järk on arvu 12 tegur ehk 1, 2, 3, 4, 6 või 12. Kui mingi tegur d ei jaga arvu $p - 1$, ei leidu Lagrange'i teoreemi tõttu ühtegi seda järku elementi. Kui aga leidub, seda järku elemendid teoreemis 7.12 tõestatud võrduse 25 põhjal $\{c^k \mid 1 \leq k \leq d, (k, d) = 1\}$, kus c on mingi algjuur, ning selliste elementide kogus on $\varphi(d)$.

Seega suurim võimalik lahendite kogus on võrrandil $x^{12} \equiv 1 \pmod p$, kus $12 \mid p-1$ ehk näiteks $p = 13$ ning lahendite kogus sel juhul on teoreemis 7.12 tõestatud võrduse 24 põhjal $\sum_{d \mid 12} \varphi(d) = 12$.

Teised võimalikud lahendite kogused sellisel kujul võrrandite puhul on kõigepealt moodulid p, mille puhul $p-1$ jagub arvuga 6 kuid mitte 12 ehk näiteks $p = 7$, mille korral on lahendite kogus $\sum_{d \mid 6} \varphi(d) = 6$.

Veel on sellised moodulid, mille korral $p - 1$ jagub arvuga 4 kuid mitte arvuga 12 ehk näiteks $p = 5$, mille korral on lahendite kogus 4.

Oleksid võimalikud ka sellised moodulid, mille korral $p - 1$ jagub arvuga 3 kuid mitte arvuga 6, kuid sel juhul peaks $p = 3k + 1$, kus k on paaritu arv, kuid kuna 3 ja k on paaritud, on ka nende korrutis paaritu ehk sellele 1 liites saab paarisarvu ning ainus paaris algarv on 2, mis ei sobi p väärtuseks.

On ka sellised moodulid, mille korral $p - 1$ jagub arvuga 2 kuid mitte arvuga 4 ega 3 ehk näiteks $p = 11$, mis puhul on lahendite kogus 2.

Viimaks oleksid ka moodulid, mille korral $p-1$ ei jagu ei 2 ega 3ga, kuid selleks jällegi p olema paarisarv.

Kokkuvõttes on võimalikud lahendite kogused 0, 1, 2, 4, 6 ja 12.

9^*. Olgu $p > 2$ algarv ja A rühma $\mathbb{Z}_p^*$ alamrühm, kusjuures $6 \mid |A|$. Tõestada, et leiduvad $a, b, c \in A$ nii, et $a + b = c$.

10^*. Olgu $n \in \mathbb{N}$. Tõestada, et leidub lõpmata palju selliseid algarve p, et mooduli p järgi vähim positiivne algjuur $a > n$.