

## Kodutöö nr. 4

Joosep Näks ja Uku Hannes Arismaa

**1.** Tõestada, et kui  $a \equiv b \pmod{n}$ , siis ka  $a^n \equiv b^n \pmod{n^2}$ . Kas astendajat 2 on võimalik veel suurendada? Põhjendada.

Võttes  $a = q_1n + r_1$  ning  $b = q_2n + r_2$  nii, et  $r_1, r_2 < n$ , saame, et  $a^n$  ja  $b^n$  on kujul  $(qn + r)^n$ . Iga liige lõplikus summas on saadud mingi arvu  $qn$  ja mingi arvu  $r$  korrutamisel. Kui korrutatud on 2 või rohkem liiget  $qn$ , siis liidetav on kongruentne 0 (mod  $n^2$ ). Kui korrutatud on üks liige  $qn$ , siis selliste liidetavate summeerimisel saame, kuna neid on  $n$  tükki (1 iga korra kohta, kui on võimalik  $r$  asemel  $qn$  valida),  $nqn$ , mis on samuti kongruentne 0 (mod  $n^2$ ). Jääb ainult liige  $r^n(qn)^0$  ning see liige  $a$  ja  $b$  korral sama, kuna  $r_1 = r_2$ , kuna  $a$  ja  $b$  on kongruentsed. Kui võtta  $n = 3$  ning  $a = 1$  ja  $b = 4$ , siis saame  $a^n = 1, b^n = 64$  ning kui astendaja on 3, siis saame  $1 \equiv 27 \cdot 2 + 10 \pmod{27}$ , mis ei kehti.

**2.** Leida jääk, mis tekib arvu  $(2019^{64} + 2021^7)^{33}$  jagamisel arvuga 21.

Jagan 21 algteguriteks:  $21 = 3 \cdot 7$ . Kontrollin antud arvu jääki eraldi jagamisel mõlema teguriga. Kasutan järgnevas arutluses omadust, et kui  $a \equiv b \pmod{m}$ , siis  $a^n \equiv b^n \pmod{m}$ , mis järeldub otseselt konsekti lausest 3.7 korrutamise kohta.

2019 jagub arvuga 3 ehk ka  $2019^{64}$  annab jäägiks 0. 2021 annab jäägiks 2, võttes selle seitsmendasse astmesse, saan 128, mis annab arvuga 3 jagades jäägiks 2. Seega on  $2019^{64} + 2021^7$  jääk kolmega jagades 2. Fermat' väikese teoreemi põhjal  $2^{3-1} \equiv 1 \pmod{3}$  ehk  $2^{32} = (2^2)^{16} \equiv 1^{16} \pmod{3}$  ning  $2^{33} = 2^{32} \cdot 2 \equiv 1 \cdot 2 \pmod{3}$  ehk kokku on antud arvu jääk arvuga kolm jagades 2.

2019 annab arvuga 7 jagades jäägi 3. Kasutades Fermat' väikest teoreemi saan  $3^{60} = (3^{7-1})^{10} \equiv 1^{10} \pmod{7}$ . Siit edasi  $3^{64} = 3^4 \cdot 3^{60} \equiv 3^4 \pmod{7} \equiv 4 \pmod{7}$ . 2021 annab jäägiks 5 ning  $5^7 \equiv 5 \pmod{7}$ . Seega on  $2019^{64} + 2021^7$  jääk seitsmega jagades  $4 + 5 = 9 \equiv 2 \pmod{7}$ .  $2^{30} = (2^6)^5 \equiv 1 \pmod{7}$  ja  $2^{33} = 2^{30} \cdot 2^3 \equiv 2^3 \pmod{7} \equiv 1 \pmod{7}$ .

Kuna  $(3, 7) = 1$  ja  $3 \cdot 7 = 21$ , on teoreemi 4.5 põhjal kujutus  $f : \mathbb{Z}_{21} \rightarrow \mathbb{Z}_3 \times \mathbb{Z}_7$ ,  $f(\bar{a}) = (\bar{a}_1, \bar{a}_2)$  bijektiivne. Seega kuna  $f((2019^{64} + 2021^7)^{33}) = f((2019^{64} + 2021^7)^{33}, (2019^{64} + 2021^7)^{33}) = (\bar{2}, \bar{1}) = f(\bar{8})$  ja  $8 < 21$ , siis  $(2019^{64} + 2021^7)^{33}$  jääk arvuga 21 jagades on 8.

**3.** Tõestada, et kui  $n \in \mathbb{N}$  ja  $(n, 6) = 1$ , siis  $24 \mid n^2 - 1$ .

$n^2 - 1 = (n+1)(n-1)$ . Kuna  $(n, 6) = 1$ , siis ei jagu  $n$  2 ja 3ga. Kuna  $n, n-1$  ja  $n+1$  näol on tegemist kolme järjestikuse arvuga, siis peab üks nendest jaguma kolmega. Kuna  $n$  on paaritu on ülejäänud paaris, kusjuures üks jagub vähemalt 4ga, kuna tegemist on järjestikuste paarisarvudega. Seega  $(n+1)(n-1)$  peab jaguma 3 ning  $4 \cdot 2$ ga ehk kokku 24ga.

4. Tõestada, et kui täisarv  $a$  on korraga täiskuup ja mõne teise täisarvu viies aste, siis  $a \equiv 0, 1, 21, 22, 34, 43, 55, 56, 76 \pmod{77}$ .

Kuna  $a$  on nii mingi arvu kuup kui ka mingi teise arvu viies aste, peavad  $a$  standardkujus kõigi algtegurite astmed jaguma nii 3 kui ka 5ga, ehk need astmed peavad olema 15 kordsed. Kuna  $77 = 7 \cdot 11$ , vaatlen eraldi jääki 7 ja 11ga jagamisel. Arvu  $a$  suvalise teguri  $p^{15k}$  jääk 7ga jagamisel: kõigepealt jagan algtegurit ennast  $p = 7q + r$ , seejärel  $(7q + r)^{15k} \equiv ((r^6)^2 \cdot r^3)^k \equiv (r^3)^k \pmod{7}$ . Vaatlen kõiki võimalikke  $r^3 \pmod{7}$  väärtuseid:

0	1	2	3	4	5	6
0	1	1	-1	1	-1	-1

Vaatlen samamoodi suvalise teguri  $p^{15k}$  arvuga 11 jagamisel tekkivad jääki. Kõigepealt jagan algtegurit ennast:  $p = 11q + r$ , seejärel astendatuna:  $(11q + r)^{15k} \equiv (r^{10} \cdot r^5)^k \equiv (r^5)^k \pmod{11}$ . Kõik võimalikud  $r^5 \pmod{11}$  väärtused:

0	1	2	3	4	5	6	7	8	9	10
0	1	-1	1	1	1	-1	-1	-1	1	-1

Seega on kõigi sobilike arvude puhul iga teguri jääk nii 7 kui ka 11ga jagamisel -1, 0 või 1 ning kui neid omavahel korrutada, jääb tulemus ikkagi nende 3 valiku hulka. Kui vaadata antud jääkide, mis peaksid tekkima 77ga jagamisel, jääke 7 ja 11 järgi, siis need on vastavalt  $0 \rightarrow (0, 0), 1 \rightarrow (1, 1), 21 \rightarrow (0, -1), 22 \rightarrow (1, 0), 34 \rightarrow (-1, 1), 43 \rightarrow (1, -1), 55 \rightarrow (-1, 0), 56 \rightarrow (0, 1), 76 \rightarrow (-1, -1)$ , ehk kõik võimalikud kombinatsioonid -1, 0 ja 1st. Seega kuna  $(7, 11) = 1$  ja  $7 \cdot 11 = 77$ , on  $\mathbb{Z}_7 \times \mathbb{Z}_{11} \rightarrow \mathbb{Z}_{77}$  kujutis bijektsioon ning kuna kõik sobilikud arvud annavad 7 ja 11ga jagamisel jäägi -1, 0 või 1, annavad nad ka arvuga 77 jagamisel sobiva jäägi.

5. Kas võrrandil  $x^3 + y^4 = 2022$  leidub naturaalarvulisi lahendipaare  $x, y$ ?

Naturaalarvude kuubid, mis on väiksemad kui 2022 ehk mida veel saaks kasutada summas on 1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, 1331 ning 1728. Sobivad neljandada astmed on 1, 16, 81, 256, 625, 1296. 1728ga ei saa sellist summat moodustada, kuna pole sobivat 4. astet, mis lõppeks 4ga. 1331 puhul sobiks viimase numbri puhul 81 ja 1, mis on liiga väikesed. 1000 puhul pole ühtegi 2ga lõppevat 4. astet. Läbivaatluse põhjal 729 ja 1296 ei sobi ning väiksemate  $x$  ja  $y$  valikute korral on summa 2022st väiksem.

6. Olgu  $p$  algarv. Leida jääk, mis tekib binoomkordaja  $\binom{2p}{p}$  jagamisel arvuga  $p$ .

Binoomkordaja saab ümber kirjutada kui  $\frac{(2p)!}{p^2(p-1)!(p-1)!}$ . Kuna vaja on leida jääki selle jagamisel arvuga  $p$ , saab tegeleda jäägiklassis  $\mathbb{Z}_p$ , mis on korpus, kuna  $p$  on algarv. Seega on kõik selle elemendid peale nullelemendi pööratavad ehk saab igale  $(p-1)!$  tegurile leida pöördarvu teisest  $(p-1)!$  korrutisest. Kuna jagamine on sama, mis pöördarvuga korrutamine, saab võtta korrutisest  $(p-1)!^2$  arvude ja pöördarvude paarid ning kuna arvu pöördarvu pöördarvu ja arvu pöördarvu korrutis on 1, on ka kõigi tekkivate paaride korrutis 1.

Seega jääb binoomkordajast alles  $\frac{(2p)!}{p^2}$ . Arvuga  $p$  jagamisel saab ülemisest korrutisest maha taandada  $p$

ja  $2p$  ehk alles jääb  $\prod_{i=1}^{p-1} i \cdot \prod_{i=1}^{p-1} (p+i) \cdot 2$ . Kuna  $p+i \equiv i \pmod{p}$ , on korrutis sama, mis  $2(p-1)!^2$ , kuid  $(p-1)!^2$  sisaldab jällegi arvude ja nende pöördarvude paare ehk binoomkordajat arvuga  $p$  jagades on jääk alati 2.

7. 990 perearsti süstisid kõik ära sama koguse vaktsiini. Terviseamet kaotas aga saatedokumendid ära ja kui need üles leiti, olid paberid lumes ära vettinud ja sealt võis vaid välja lugeda, et kokku oli sel päeval perearstidele välja jagatud  $\bullet\bullet 46 \bullet\bullet$  doosi. Aidake Üllar Lannol oma töökohta säilitada ja leidke suurim, vähim ja keskmine (kui võimalusi on paarisarv, siis kaks keskmist) võimalik vaktsiinidooside koguarv.

Tähistan arvu kui  $\overline{ab46cd}$ . Kuna kõik süstisid sama arvu, peab lõplik süstimiste arv olema 990 kordne, seega ka 10 korde, seega  $d = 0$ . Ülejäänud numbrite puhul peame vaatama, et saadav arv jaguks 99ga. Seega peab summa  $\overline{0a} + \overline{b4} + \overline{6c}$  jaguma 99ga, kuna  $100 \equiv 1 \pmod{99}$ . Ainus variant on see, et kogu summa on 99, sest 198 pole saavutatav. Summa saab ümber tõsta nõnda:  $\overline{0a} + \overline{b4} + \overline{6c} = 64 + \overline{ba} + c$ . Selleks peab  $\overline{ba}$  ja  $c$  summa olema  $99 - 64 = 35$ . Arvu  $c$  väärtused saavad olla 0..9, nendele vastavad  $\overline{ba}$  väärtused on 35..26. Kuna esialgse arvu kümnendesitluses on nad järjestuses  $a, b, c$ , saab lõplike vastuste järjekorra määramiseks kasutada  $a$  väärtust ning kui  $a$  on sama, siis  $b$  väärtust. Võimalikud  $\overline{ab}$  väärtused on järjestatuna 13, 23, 33, 43, 53, 62, 72, 82, 92 Seega on suureim võimalik vaktsiinide arv 924660, vähim 134640 ja keskmine 534600.

8. Arvud 202020 kuni 212121 kirjutatakse järjest üles. Kas niiviisi saadav täisarv

$$202020202021 \dots 212120212121$$

jagub arvuga 13?

Arvu saab ümber kirjutada summana

$$\begin{aligned} \sum_{i=0}^{10100010100} (2020202021 + i) \cdot (10^{12})^{10100010100-i} &\equiv \sum_{i=0}^{10100010100} (2020202021 + i) \cdot (1)^{10100010100-i} \pmod{13} \\ &= \sum_{i=0}^{10100010100} (2020202021 + i) \\ &= 2020202021 \cdot (1010010100 + 1) + \sum_{i=0}^{10100010100} i \\ &= 2020202021 \cdot 1010010101 + \frac{10100010100(10100010100 + 1)}{2} \\ &= 1010010101 \cdot (2020202021 + 505005050) \\ &= 1010010101 \cdot 202525207071 \equiv 9 \cdot 5 \equiv 6 \pmod{13} \end{aligned}$$

Ehk antud arv annab arvuga 13 jagades jäägi 6.