Kodutöö nr. 7

Joosep Näks ja Uku Hannes Arismaa

1. Lahendada lineaarkongruents $2021x + 6590 \equiv 2022 \pmod{2020}$.

$2021x + 6590 \equiv 2022 \pmod{2020} \Leftrightarrow x \equiv 1492 \pmod{2020}$

2. Lahendada lineaarkongruentside süsteem

$$\begin{cases} 3x \equiv 7 & \pmod{25} \\ 7x \equiv 8 & \pmod{20} \\ 11x \equiv 10 & \pmod{15}. \end{cases}$$

Et kasutada Hiina jäägiteoreemi, tahan viia süsteemi kujule, kus võrrandite moodulite vähim ühistegur oleks paarikaupa 1. Et lahendini jõuda, tahan ka, et moodulitesse jääksid alles kõik algtegurid, mis seal on, nende maksimaalsetes astmetes. Seega kuna $25 = 5^2$, $20 = 2^2 \cdot 5$ ja $15 = 3 \cdot 5$, muudan teise mooduli 4ks ja kolmanda mooduli 3ks. Mooduleid saab muuta kuna kui $20|8 - 7x$ ja $4|20$ siis transitiivsuse tõttu ka $4|8 - 7x$ ehk $7x \equiv 8 \pmod 4$ ning analoogselt saab näidata et kolmas võrrand kehtib mooduli 3 järgi.

Eemaldan nüüd tundmatute eest kordajad. On näha, et $25 \cdot 2 + 1 = 51$ jagub kolmega, täpsemalt $51 = 3 \cdot 17$ ehk ringis $\mathbb{Z}_{25}$ on $\overline{3}^{-1} = \overline{17} = \overline{-8}$ ehk esimeses võrrandis saab mõlemad pooled arvuga -8 läbi korrutada ja saab $-8 \cdot 3x \equiv -8 \cdot 7 \pmod{25}$ ehk $x \equiv -6 \pmod{25}$. Teises võrrandis kõigepealt saab uue mooduli tõttu teisendada võrrandi uuele kujule $-x \equiv 0 \pmod 4$ ehk $x \equiv 0 \pmod 4$. Kolmandas võrrandis teisendan võrrandi jällegi uue mooduli järgi ning saan $2x \equiv 1 \pmod 3$, võtan pöördelemendi: $\overline{2}^{-1} = \overline{2}$ ehk $x \equiv 2 \pmod 3$. Seega olen jõudnud uue võrrandisüsteemini:

$$\begin{cases} x \equiv -6 & \pmod{25} \\ x \equiv 0 & \pmod{4} \\ x \equiv 2 & \pmod{3}. \end{cases}$$

Ning selle peal saab rakendada Hiina jäägiteoreemi. Leian esiteks vajalikud moodulite korrutiste pöördelemendid.
$m_1 = 4 \cdot 3 = 12$ ehk kuna $-2 \cdot 12 = -24 \equiv 1 \pmod{25}$, saan $\overline{k_1} = \overline{m_1^{-1}} = \overline{-2}$
Teise võrrandi kordajaid pole mõtet leida kuna a_2 on 0.
$m_3 = 25 \cdot 4 = 100$ ehk $\overline{k_3} = \overline{m_3}^{-1} = \overline{1}^{-1} = \overline{1}$
Ning seega on lahend $x = -6 \cdot (-2) \cdot 12 + 0 + 2 \cdot 100 \cdot 1 = 344$ kõigi moodulite korrutise mooduli järgi ehk kokkuvõttes on süsteemi lahend $x \equiv 344 \equiv 44 \pmod{300}$

3. Lahendada lineaarkongruentside süsteem

$$\begin{cases} 3x \equiv 7 & \pmod{25} \\ 7x \equiv 8 & \pmod{20} \\ 11x \equiv 9 & \pmod{15}. \end{cases}$$

Selle jaoks on eelmises ülesandes juba eeltöö tehtud, ainus asi mis muutus on kolmanda võrrandi vabaliige, seega kui kolmas võrrand uue vabaliikmega teisendada mooduli kolm järgi saab $2x \equiv 0 \pmod 3$ ehk $x \equiv 0 \pmod 3$. Ning olengi saavutanud võrrandi, mille peal Hiina jäägiteoreemi kasutada:

$$\begin{cases} x \equiv -6 & \pmod{25} \\ x \equiv 0 & \pmod{4} \\ x \equiv 0 & \pmod{3}. \end{cases}$$

Erinevus eelmisest ülesandest on vaid see, et nüüd on ka lahendi summa kolmas liige 0 ehk lahendiks on $x = 144 + 0 + 0$ ehk $x \equiv 144 \pmod{300}$.

4. Lahendada kongruents $2022^{\left(2021^{2020}\right)} \pmod{1995}$.

Vaatame arvu $x := 2022^{\left(2021^{2020}\right)}$ moodulite 3,5,7,19 järgi. Saame järgmised tulemused:
$x \equiv 0 \pmod 3$
$2^4 \equiv 1 \pmod 5 \Rightarrow x \equiv 2^{1^{2020}} \equiv 2 \pmod 5$
$x \equiv -1^{2021^{2020}} \equiv -1 \pmod 7$
$8^6 \equiv 1 \pmod{19} \Rightarrow x \equiv 8^{-1^{2020}} \equiv 8 \pmod{19}$
Siit saame HJT järgi, et $x \equiv 2 \cdot 399 \cdot (-1) - 285 \cdot 3 + 8 \cdot 105 \cdot 2 = 27$

5. Leida suuruselt 2019-s selline naturaalarv n, mille korral nii n kui n^2 annavad arvuga 891 jagades ühe ja sama jäägi.

Märkame, et lahendada $n^2 \equiv n \pmod{891}$ on ekvivalentne ülesandele

$$\begin{cases} n(n-1) \equiv 0 & \pmod{81} \\ n(n-1) \equiv 0 & \pmod{11} \end{cases}$$

Mõlema võrrandi puhul on ainsad lahendid 1 ja 0, kuna kõrvuti olevad arvud ei saa mõlemad jagada sama algarvu. Märkame, et $11 \cdot -22 \equiv 1 \pmod{81}$ ning $81 \cdot 3 \equiv 1 \pmod{11}$, seega saame HJTst võimalikeks lahenditeks $x \equiv 0, x \equiv 649, x \equiv 243$ ning $x \equiv 1 \pmod{891}$. Iga suuruselt 4. selline naturaalarv on 891 kordne, seega 2020. arv oleks $891 \cdot 505$, seega 2019. on $891 \cdot 504 + 649 = 449713$.

6. Tõestada, et kahe järjestikuse ruuduvaba arvu vahe võib olla kuitahes suur.

Kui tahta leida sellist arvu x, millest järgmised n tükki kõik sisaldavad oma tegurite hulgas ruute, saab koostada võrrandisüsteemi kujul $x + i \equiv 0 \pmod{p_i^2}$ ehk i ümber tõstes $x \equiv -i \pmod{p_i^2}$ kus $i = 1, .., n$ ja $p_1, .., p_n$ on vabalt valitud erinevad algarvud. Kuna p_i on kõik erinevad algarvud, pole neil paarikaupa ühistegurit ehk Hiina jäägiteoreemi põhjal leidub süsteemil lahend. Seega saab valida kuitahes suure arvu n ning leidub selline arv x, millest järgmine ruuduvaba arv on vähemalt n arvu kaugusel.

7. Leida vähim *naturaal*arv, mis on korraga kahekordne täisruut, kolmekordne täiskuup ja 1999-kordne 1999-s aste.

Arv, mis me valime peab olema 2 3 ja 1999 kordne, seega kujul $2^i 3^j 1999^k x$. Selleks, et arv oleks täisaste, peavad kõik algtegurid eraldi olema selles astmes, seega kui $x > 1$, siis see ei mõjuta arvu esimest poole täisaste olemist, seega kui leida vähimad i, j, k nii, et arvu esimene pool vastab tingimustele, pole mõtet seda enam $x > 1$ läbi korrutada, kuna see teeks arvu asjatult suuremaks.

Et arv n oleks kahekordne kuup, peab kehtima $n = 2w^2 = 2 \cdot 2^{i-1} 3^j 1999^k$ ehk j ja k peavad kahega jaguma ning i peab jäägiks andma 1. Sama saab arvugeda 3 ja 1999 teha ning saame tingimused $i \equiv 1, j \equiv 0, k \equiv 0 \pmod 2$, $i \equiv 0, j \equiv 1, k \equiv 0 \pmod 3$, $i \equiv 0, j \equiv 0, k \equiv 1 \pmod{1999}$. HJTst saame $i \equiv 1 \cdot 3 \cdot 1999 \cdot 1 = 5997$, $j \equiv 1 \cdot 2 \cdot 1999 \cdot 2 = 7996$, $k \equiv 2 \cdot 3 \cdot 1000 \cdot 1333 \equiv 9996 \pmod{2 \cdot 3 \cdot 1999}$. Asendades need algsesse kujusse saamegi vähima sellise arvu: $2^{5997} \cdot 3^{7996} \cdot 1999^{9996}$.

8. Tõestada, et iga paarisarvu $m = 2k \in \mathbb{Z}$ ja naturaalarvu n korral leiduvad $a, b \in \mathbb{Z}$ nii, et $m = a - b$ ja $(a, n) = (b, n) = 1$.

Tegurdan m ja n algteguriteks nii, et p_i on tegurid, mis jagavad nii n kui ka m, q_i jagavad vaid arvu m ning r_i vaid arvu n. Saan $m = \prod_i p_i^{u_i} \cdot \prod_i q_i^{v_i}$ ja $n = \prod_i p_i^{u_i} \cdot \prod_i r_i^{z_i}$.

Leian iga i jaoks saab leida sellise a_i väärtuse, et $a_i \not\equiv 0 \pmod{r_i}$ ja $a_i \not\equiv -\prod_i p_i^{u_i} \pmod{r_i}$. Sellised a_i väärtused leiduvad, kuna r_i on alati suurem kui 2 ehk jäägiklassiringis $\mathbb{Z}_{r_i}$ on vähemalt 3 liiget (kui n jagub 2ga, on 2 p_i väärtuste hulgas, kuna on teada et m on paarisarv). Koostan võrrandisüsteemi võrranditega $x \equiv a_i \pmod{r_i}$ ja $x \equiv 1 \pmod{p_i}$. Hiina jäägiteoreemi põhjal leidub sellel lahend kuna r_i ja p_i on paarikaupa ühistegurita.

Võtan nüüd $b = x \cdot \prod_i q_i^{v_i}$ ja $a = m + b$. Arv x ei oma arvuga n ühistegurit, kuna võrrandid, mille järgi x leitud sai, ütlevad et ükski arvu n tegur ei jaga arvu x ning ükski q_i ei jaga arvu n seega n ja b ei oma ühistegurit. Arv a ei jagu ühegi algarvuga p_i, kuna $a = m + x \cdot \prod_i q_i^{v_i} \equiv 0 + a_i \cdot \prod_i q_i^{v_i} \not\equiv 0 \pmod{p_i}$. Viimane kehtib seepärast, et q_i ja p_i on alati erinevad algarvud ehk nende suurim ühistegur on 1. Ta ei jagu ka ühegi algarvuga r_i, kuna $a = \prod_i p_i^{u_i} \cdot \prod_i q_i^{v_i} + x \cdot \prod_i q_i^{v_i} = \prod_i q_i^{v_i} (\prod_i p_i^{u_i} + x)$ ning on teada et arvud q_i korrutis ei jagu arvudega r_i ning eelduste kohaselt $\prod_i p_i^{u_i} + x \not\equiv \prod_i p_i^{u_i} - \prod_i p_i^{u_i} = 0 \pmod{r_i}$ ehk ka korrutise teine pool ei saa jaguda ühegi arvuga r_i.

9. Koostada tekstülesanne, mida saab lahendada Hiina jäägiteoreemi abil.
(Ülesande tekst ja selle **lahendus** tuleb esitada kirjalikult. Põhimõtteliselt vale lahendusega ülesanne annab 0 punkti. Kõige originaalsema ülesande ja kõige raskema ülesande koostajad saavad kumbki 3-5 punkti sõltuvalt ülesande tasemest. Kloonitud ülesannete esitajad saavad 0 punkti.)

Ülesanne: Rabamatkal märkad, et teepeale jäävad jõhvikad on 10m vahedega ning murakad 19m vahedega. Olles kõndinud 87m viimasest kohast, kus murakas ja jõhvikas olid kõrvuti, märkad, et nüüd, kus raba hakkab otsa lõppema, on iga jõhvikas 12m kaugusel eelmisest ning iga murakas 23m kaugusel eelmisest. Kui mitme meetri pärast sa jälle murakat ja jõhvikat lähestikku näed?

Lahendus: Leian kõigepealt viimaste jõhvika ja muraka asukohad enne rabast väljumist, $87 \equiv 7 \pmod{10}$ ja $87 \equiv 11 \pmod{19}$ ehk viimasest jõhvikast on möödas 7m ja viimasest murakast 11m. Nüüd uute vahedega saan võrrandid $x \equiv -7 \pmod{12}$ ja $x \equiv -11 \pmod{23}$, kus x on läbitud tee alates tihedama raba lõpust. Süsteemi lahendades saan $x = 23 \cdot (-1) \cdot (-7) + 12 \cdot (-11) \cdot 2 = -103 \equiv 173 \pmod{12 \cdot 23}$. Ehk järgmine kord oli murakat ja jõhvikat korraga näha 173m peale raba kõrgsoo lõppu.