Kodutöö nr. 8

Joosep Näks ja Uku Hannes Arismaa

1. Lahendada kongruents

$$3x^4 + 5x^3 - x^2 - x + 1 \equiv 0 \pmod 7.$$

Kasutame Horneri skeemi ja proovimis meetodit.

	$\overline{3}$	$\overline{-2}$	$\overline{-1}$	$\overline{-1}$	$\overline{1}$
$\overline{0}$	$\overline{3}$	$\overline{-2}$	$\overline{-1}$	$\overline{-1}$	$\overline{1}$
$\overline{1}$	$\overline{3}$	$\overline{1}$	$\overline{0}$	$\overline{-1}$	$\overline{0}$
$\overline{2}$	$\overline{3}$	$\overline{-3}$	$\overline{0}$	$\overline{-1}$	$\overline{-1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{-1}$	$\overline{3}$	$\overline{3}$
$\overline{-3}$	$\overline{3}$	$\overline{3}$	$\overline{-3}$	$\overline{1}$	$\overline{-2}$
$\overline{-2}$	$\overline{3}$	$\overline{-1}$	$\overline{1}$	$\overline{-3}$	$\overline{2}$
$\overline{-1}$	$\overline{3}$	$\overline{2}$	$\overline{-3}$	$\overline{2}$	$\overline{-1}$

Seega leidsime, et ainuke lahend on $\overline{1}$.

2. Tegurdada polünoom

$$f(x) = 2x^5 + 6x^4 + 5x^3 - 3x^2 - 3x + 3$$

mooduli 5 järgi, s.t. üle korpuse $\mathbb{Z}_5$.

Kasutame Horneri skeemi ja proovimis meetodit.

	$\overline{2}$	$\overline{1}$	$\overline{0}$	$\overline{2}$	$\overline{2}$	$\overline{-2}$
$\overline{0}$	$\overline{2}$	$\overline{1}$	$\overline{0}$	$\overline{2}$	$\overline{2}$	$\overline{-2}$
$\overline{1}$	$\overline{2}$	$\overline{-2}$	$\overline{-2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$

Leidsime esimese teguri $(x - \overline{1})$

	$\overline{2}$	$\overline{-2}$	$\overline{-2}$	$\overline{0}$	$\overline{2}$
$\overline{1}$	$\overline{2}$	$\overline{0}$	$\overline{-2}$	$\overline{-2}$	$\overline{0}$

Seega on $(x - \overline{1})$ kahekordne tegur.

	$\overline{2}$	$\overline{0}$	$\overline{-2}$	$\overline{-2}$
$\overline{1}$	$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{-2}$
$\overline{2}$	$\overline{2}$	$\overline{-1}$	$\overline{1}$	$\overline{0}$

	$\overline{2}$	$\overline{-1}$	$\overline{1}$
$\overline{2}$	$\overline{2}$	$\overline{-2}$	$\overline{2}$
$\overline{-2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$
$\overline{-1}$	$\overline{2}$	$\overline{2}$	$\overline{-1}$

Seega saime, et $f(x) \equiv (x-1)^2(x-2)(2x^2 - x + 1) \pmod 5$

3. Milliste x täisarvuliste väärtuste korral on arvu $2x^4 + x^3 - 2x^2 + x - 2$ mõlemad viimased kümnendnumbrid 2?

Ülesanne taandub kongruentsi $2x^4 + x^3 - 2x^2 + x - 2 \equiv 22 \pmod{100}$ lahendamisele. Selleks peame lahendama kongruentsid $2x^4 + x^3 - 2x^2 + x - 2 \equiv 22 \pmod 4$, $2x^4 + x^3 - 2x^2 + x - 2 \equiv 22 \pmod{25} \Leftrightarrow 2x^4 + x^3 - 2x^2 + x - 24 \equiv 0 \pmod{25}$. Esimese lahendiks on ainult $x \equiv 0 \pmod 4$. Mooduli 5 järgi on teise lahenditeks 2 ja 3.

$(2x^4 + x^3 - 2x^2 + x - 24)' = 8x^3 + 3x^2 - 4x + 1$

$(8x^3 + 3x^2 - 4x + 1)(2) = 69 \equiv -1 \pmod 5$

$(2x^4 + x^3 - 2x^2 + x - 24)(2) = 10$

Seega peame näite põhjal nüüd leidma lahenduse kongruentsile $-y + 2 \equiv 0 \pmod 5$, saame $y \equiv 2$ ehk üks lahend on $2 + 2 \cdot 5 = 12$.

$(8x^3 + 3x^2 - 4x + 1)(3) = 232 \equiv 2 \pmod 5$

$(2x^4 + x^3 - 2x^2 + x - 24)(3) = 150$

Seega peame näite põhjal nüüd leidma lahenduse kongruentsile $2y + 0 \equiv 0 \pmod 5$, saame $y \equiv 0$ ehk teine lahend on $3 + 0 + \cdot 5 = 3$.

HJT järgi peaks leiduma 2 lahendit. Terava silmaga näeb ära, et need on 12 ja 28.

4. Lahendada kongruents

$$x^4 + 4x^3 + 2x^2 + 2x - 38 \equiv 0 \pmod{125}.$$

Mooduli 5 järgi saame, et ainus lahend on $x \equiv 3$.

$f'(x) \equiv -x^3 + 2x^2 + -x + 2 \pmod 5$ $f'(3) \equiv 3 + 3 - 3 + 2 \equiv 0 \pmod 5$

$f(3) = 175$, $\dfrac{175}{5} = 35 \equiv 0 \pmod 5$

Seega saame, et lahendis kujul $x = 3 + 5y$ oleva y puhul peab kehtima, et $0y + 0 \equiv 0 \pmod 5$, mis kehtib iga $y \in \{0, 1, 2, 3, 4\}$ korral, seega ülesande lahendamiseks, peame uurima x kujul $a + 25b$, $a \in \{3, 8, 13, 18, 23\}$. Iga sellise kuju korral peaksime leidma b valemist $f'(a)b + \dfrac{f(a)}{5^2} \equiv 0 \pmod 5$. Kuna $f'(a) \equiv f'(3) = 0 \pmod 5$, siis lahenduvus ei sõltu b-st ning peame kontrollima, kas mõne a puhul $\dfrac{f(a)}{5^2} \equiv 0 \pmod 5$ ehk teisisõnu, kas $125 \mid f(a)$. $f(3) = 175$, $f(8) = 6250$, $f(13) = 37673$, $f(18) = 128950$, $f(23) = 329575$ Neist jagub 125-ga ainult 6250, seega on lahenditeks $8, 8 + 25, 8 + 50, 8 + 75, 8 + 100$.

5. Lahendada kongruents

$$x^4 + 4x^3 + 2x^2 + 2x + 12 \equiv 0 \pmod{1925}.$$

Kuna 1925=25·7·11, saame polünoomi lahendada igaühe nende järgi eraldi. Kuna $-38 \equiv 12 \pmod{25}$, teame eelmisest ülesandest, et lahendid on 3, 8, 13, -7, -2 (tähistame a). Proovides 7 järgi, saame, et lahenditeks on 1 ja 5 (tähistame b). 11 järgi on ainult 9.

HJT-st saame, et kõik vastused saame kujul $77 \cdot 13a + 275 \cdot 4b + 175 \cdot -1 \cdot 9$, seega need on 218, 383, 603, 768, 988, 1153, 1373, 1538, 1758, 1923.

6. Lahendada mõistatus $\ddot{U}KS \times \ddot{U}KS = 2 * * 2\,1$. (Iga täht tähistab ühte konkreetset numbrit ja $*$ tähistab suvalist, võib-olla erinevat numbrit.)

Leian alustuseks lahendid võrrandile $x^2 \equiv 21 \pmod{100}$ ehk $x^2 - 21 \equiv 0 \pmod{100}$ ning leian hiljem nende hulgast arvud, mis sobivad ülejäänud tingimustega kokku.
Mooduli saab lahti tegurdada $100 = 2^2 \cdot 5^2$, seega leian 4 ja 5 järgi lahendid: $x^2 - 21 \equiv x^2 - 1 \equiv 0 \pmod 4$, mille lahenditeks saab läbiproovimisel $x = 1$ ja $x = 3$, ning $x^2 - 21 \equiv x^2 - 1 \equiv 0 \pmod 5$, mille lahenditeks saab $x = 1$ ja $x = 4$.
Leian nüüd mooduli 25 järgi lahendeid kujul $x = 1 + 5y$. Arvestades et $(x^2 - 21)' = 2x$, saame $x = 1$ korral $f(1) = -20$ ja $f'(1) = 2$. Nendest saab võrrandi $2y + \dfrac{-20}{5} \equiv 2y + 1 \equiv 0 \pmod 5$, mille ainsaks lahendiks on $y = 2$. Seega mooduli 25 järgi on lahendid $y = 2 + 5z$, kus $z \in \mathbb{Z}$ ehk algse kongruentsi lahenditeks saab $1 + 5(2 + 5x) = 1 + 10 + 25x \equiv 11 \pmod{25}$ ehk $x \equiv 11 \pmod{25}$.
Teiseks leian lahendid kujul $x = 4 + 5y$. Saan $f(4) = -5$ ja $f'(4) = 8 \equiv 3 \pmod 5$, millest tuleb võrrand $3y + \dfrac{-5}{5}$, mille ainsaks lahendiks on $y = 2$. Seega mooduli 25 järgi on lahendid $y = 2 + 5z$ ehk algse kongruentsi lahenditeks saab $4 + 5(2 + 5z) = 4 + 10 + 25z \equiv -11 \pmod{25}$ ehk $x \equiv -11 \pmod{25}$.
Kokkuvõttes on olemas neli süsteemi,

$$\begin{cases} x \equiv a_1 \pmod 4 \\ x \equiv a_2 \pmod{25} \end{cases}$$

Kus $a_1 \in \{1, 3\}$ ja $a_2 \in \{11, -11\}$. On lihtne näha, et nendega saab lahendid $x_1 \equiv 61 \pmod{100}$, $x_2 \equiv 89 \pmod{100}$, $x_3 \equiv 11 \pmod{100}$ ja $x_4 \equiv 39 \pmod{100}$. Seega $\ddot{U}KS = 100z + x_i$, kusjuures $\ddot{U} = z$ ehk $0 < z < 10$. Esimeste z väärtustega saab $\ddot{U}KS \times \ddot{U}KS$ tulemuseks

	x_1	x_2	x_3	x_4
$z = 1$	25921	35721	12321	19321
$z = 2$	68121	83521	44521	57121

Nendest ainult variant $\ddot{U}KS = 161$ on numbriga 2 algav viiekohaline arv, kusjuures $z = 2$ puhul on kõik tulemused suuremad kui võimalik tulemus olla saaks ning kui z suurendada, muutuvad korrutised suuremaks ehk rohkem lahendeid ei saa leiduda. Seega on ainus lahend $\ddot{U}KS = 161$.

7. Olgu a juhuslik täisarv vahemikust $[1, 17]$ ja b samuti juhuslik täisarv vahemikust $[1, 18]$. Milline on tõenäosus, et kongruentsil $ax \equiv b \pmod{18}$ on vähemalt üks lahend? Täpselt üks lahend?

Lause 6.2 põhjal on antud kongruents lahenduv parajasti siis, kui $(a, 18) \mid b$. Seega kui $a = 9$, peab b olema 9 kordne, milleks on $\left\lfloor \dfrac{18}{9} \right\rfloor = 2$ võimalust. Kui a on 6 kordne, milleks on $\left\lfloor \dfrac{17}{6} \right\rfloor = 2$ võimalust, peab ka b olema 6 kordne, milleks on $\left\lfloor \dfrac{18}{6} \right\rfloor = 3$ võimalust. Kui a on 3 kordne, kuid mitte 6 ega 9 kordne, on selleks võimalusi $\left\lfloor \dfrac{17}{3} \right\rfloor - 1 - 2 = 2$ ning b peab olema 3 kordne, selleks on $\left\lfloor \dfrac{18}{3} \right\rfloor = 6$ võimalust. Kui a on 2 kordne kuid mitte 6, on selleks $\left\lfloor \dfrac{17}{2} \right\rfloor - 2 = 6$ võimalust, ning b peab siis olema 2 kordne, milleks on $\left\lfloor \dfrac{18}{2} \right\rfloor = 9$ võimalust. Ülejäänud a väärtuste puhul $(a, 18) = 1$ ehk sobivad kõik b väärtused, neid a väärtuseid on $17 - 1 - 2 - 2 - 6 = 6$. Seega on kokku tõenäosus et lahendeid leidub $\dfrac{1}{17}\dfrac{2}{18} + \dfrac{2}{17}\dfrac{3}{18} + \dfrac{2}{17}\dfrac{6}{18} + \dfrac{6}{17}\dfrac{9}{18} + \dfrac{6}{17} = \dfrac{182}{17 \cdot 18} = \dfrac{91}{153}$.
Et lahendeid oleks täpselt 1, peab kehtima $(a, n) = 1$. Selle jaoks on 6 a väärtust ehk tõenäosus on $\dfrac{6}{17}$.

8. Tõestada, et kongruentsil $x^2 \equiv 1 \pmod{2^k}$ on üks lahend, kui $k = 1$, kaks lahendit, kui $k = 2$, ning neli lahendit, kui $k \geq 3$.

Lihtsal läbivaatlusel on näha, et $k = 1$ puhul on ainus lahend 1, $k = 2$ puhul lahendid 1 ja 3 ning $k = 3$ puhul 1, 3, 5 ja 7. Pakun nüüd, et iga $k \geq 3$ puhul on 4 lahendit $1, 2^{k-1} - 1, 2^{k-1} + 1, -1$ ning tõestan seda induktsiooniga. Baas on üleeelmises lauses antud. Sammuks eeldan, et k puhul leiduvad lahendid $L = \{1, 2^{k-1} - 1, 2^{k-1} + 1, -1\}$ ning leian lahendid $k + 1$ jaoks.
Arvutades välja tuletise $(x^2 - 1)' = 2x \equiv 0 \pmod{2}$ on näha, et kui leida lahendit võttes aluseks ühe võrra väiksema mooduli astmega lahend $a \in L$, siis uueks lahendiks on $x = a + 2^k y$, kus y on järgneva võrrandi lahend: $f'(a)y + \dfrac{f(a)}{2^k} \equiv 0 \pmod{2}$, kuid kuna $f'(a) \equiv 0 \pmod{2}$, jääb sellest võrrandist alles $\dfrac{f(a)}{2^k} \equiv 0 \pmod{2}$ ehk $\dfrac{a^2 - 1}{2^k} \equiv 0 \pmod{2}$. Kontrollin selle kõigi L liikmete puhul läbi.
Kui $a = 1$, siis $\dfrac{1 - 1}{2^k} \equiv 0 \pmod{2}$ kehtib ehk saame lahendid mõlema võimaliku y väärtuse jaoks: $x_1 = 1 + 0 \cdot 2^k$ ja $x_2 = 1 + 1 \cdot 2^k$.
Kui $a = 2^{k-1} - 1$, siis $\dfrac{(2^{k-1} - 1)^2 - 1}{2^k} \equiv \dfrac{2^{2k-2} - 2^k}{2^k} \equiv -1 \not\equiv 0 \pmod{2}$ ehk siit lahendeid ei tule.
Kui $a = 2^{k-1} + 1$, siis $\dfrac{(2^{k-1} + 1)^2 - 1}{2^k} \equiv \dfrac{2^{2k-2} + 2^k}{2^k} \equiv 1 \not\equiv 0 \pmod{2}$ ehk siit lahendeid ei tule.
Kui $a = -1$, siis $\dfrac{(-1)^2 - 1}{2^k} \equiv 0 \pmod{2}$ kehtib ehk saame lahendid mõlema võimaliku y väärtuse jaoks: $x_3 = -1 + 0 \cdot 2^k$ ja $x_4 = -1 + 1 \cdot 2^k$.
Seega on saadud lahendite hulk $1, 2^k - 1, 2^k + 1, -1$, mida oligi vaja näidata.