Kodutöö nr. 7

Joosep Näks ja Uku Hannes Arismaa

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

2. Tegurdada polünoom
$$f(x) = 2x^5 + 6x^4 + 5x^3 - 3x^2 - 3x + 3$$
mooduli 5 järgi, s.t. üle korpuse $\mathbb{Z}_5$.

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

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

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

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 $2y + \frac{-20}{5} \equiv 2y + 1 \equiv 0 \pmod 5$, 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 $3y + \frac{-5}{5}$, 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 $\left\lfloor \frac{18}{9} \right\rfloor = 2$ võimalust. Kui a on 6 kordne, milleks on $\left\lfloor \frac{17}{6} \right\rfloor = 2$ võimalust, peab ka b olema 6 kordne, milleks on $\left\lfloor \frac{18}{6} \right\rfloor = 3$ võimalust. Kui a on 3 kordne, kuid mitte 6 ega 9

kordne, on selleks võimalusi $\left\lfloor \frac{17}{3} \right\rfloor - 1 - 2 = 2$ ning b peab olema 3 kordne, selleks on $\left\lfloor \frac{18}{3} \right\rfloor = 6$ võimalust. Kui a on 2 kordne kuid mitte 6, on selleks $\left\lfloor \frac{17}{2} \right\rfloor - 2 = 6$ võimalust, ning b peab siis olema 2 kordne, milleks on $\left\lfloor \frac{18}{2} \right\rfloor = 9$ 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 $\frac{1}{17}\frac{2}{18} + \frac{2}{17}\frac{3}{18} + \frac{2}{17}\frac{6}{18} + \frac{6}{17}\frac{9}{18} + \frac{6}{17} = \frac{182}{17 \cdot 18} = \frac{91}{153}$.
Et lahendeid oleks täpselt 1, peab kehtima $(a, n) = 1$. Selle jaoks on 6 a väärtust ehk tõenäosus on $\frac{6}{17}$.

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