

Ülesanded: mooduliga tehted ja nihkeregistrid

märts 2006

1 Ülesanded

Ülesanne 1. Arvuta:

$$(1) \text{süt}(204, 68) \quad (2) \frac{1}{5} \bmod 17 \quad (3) x^4 + 1 \bmod x^2 + 1 .$$

Ülesanne 2. Šifreerimine toimub valemi

$$y = E(x) = 6x + 15 \bmod 49$$

järgi. Leia vastav dešifreerimisteisendus $x = D(y)$ ja tõesta, et leitud teisendus on korrektne, s.t. $D(E(x)) = x$ iga $x \in \{0, \dots, 48\}$ korral.

Ülesanne 2A. Šifreerimine toimub valemi

$$y = E(x) = ax + b \bmod 55$$

järgi. On teada, et $E(2) = 18$ ja $E(6) = 24$. Leia a ja b .

Ülesanne 3. Lahenda kongruentside süsteemid:

$$(a) \begin{cases} 5a + b \equiv 12 \pmod{36} \\ 8a + b \equiv 13 \pmod{36} \end{cases} \quad (b) \begin{cases} 2a + b \equiv 5 \pmod{31} \\ 7a + b \equiv 9 \pmod{31} \end{cases}$$

Ülesanne 4. Leia neljendat järku I-liiki nihkeregistrid (ja vastavad algolekud), mille väljundjadad (nullise sisendjada korral) sisaldavad lõike:

a) 1 0 0 1 1 0 1 0

b) 1 0 0 0 0 1 0 1.

Ülesanne 4A. On teada järgmine neljandat järku nihkeregistri (liik teadmata!) poolt moodustatud väljundjada (nullise sisendi korral), milles üks bitt on kustunud (asendatud tärniga):

$$0 \ 1 \ 1 \ * \ 1 \ 1 \ 0 \ 1$$

Taasta kustunud bitt ja põhjenda vastust!

Ülesanne 5. Kas leiduvad polünoomid $\alpha(x)$ ja $\beta(x)$ (üle \mathbb{Z}_2), nii et kehtiks (polünoomide) võrdus

$$\alpha(x) \cdot (x^2 + 1) + \beta(x) \cdot (x^5 + 1) = 1.$$

Ülesanne 6. Leia polünoom $a(x)$ (üle \mathbb{Z}_2), nii et

$$a(x) \cdot (x^2 + 1) \equiv 1 \pmod{x^4 + x + 1}.$$

Ülesanne 7. Leia neljanda astme polünoom $f(x)$ (üle \mathbb{Z}_2), millel puuduvad juured hulgas \mathbb{Z}_2 ja mis on taanduv, s.t. leiduvad madalama astme mittekonstantsed polünoomid $f_1(x), f_2(x) \in \mathbb{Z}_2[x]$, nii et $f(x) = f_1(x) \cdot f_2(x)$.

Ülesanne 8. Olgu $\vartheta \in \mathbb{R}$ polünoomi $f(x) = x^3 + x + 1 \in \mathbb{R}[x]$ üks juurtest. Avalda kaks ülejäänud (kompleksarvulist) juurt ϑ kaudu.

2 Lahendused

Ülesanne 1. Esimeses alamülesandes kasutame Eukleidese algoritmi:

$$\begin{aligned}(1) \text{ s\"ut}(204, 68) &= \text{ s\"ut}(204 - 2 \cdot 68, 68) = \text{ s\"ut}(68, 68) \\ &= \mathbf{68} .\end{aligned}$$

(2) Teises alamülesandes tähistame esmalt $A = 5$, $B = 17$ ja arvutame suurima ühisteguri, säilitades samal ajal vastust lineaaravaldisena muutujaist A ja B :

$$\begin{aligned}\text{ s\"ut}(A, B) &= \text{ s\"ut}(5, 17) \\ \text{ s\"ut}(A, B - 3A) &= \text{ s\"ut}(5, 2) \\ \text{ s\"ut}(A - 2(B - 3A), B - 3A) &= \text{ s\"ut}(7A - 2B, B - 3A) = \text{ s\"ut}(1, 2) .\end{aligned}$$

Järelikult $7A - 2B = 1$, millest tuleneb, et $7 \cdot 5 \equiv 1 \pmod{17}$, ja seega $\frac{1}{5} \pmod{17} = 7$.

(3) Kasutame polünoomide jagamist:

$$\begin{array}{r}x^4 + 1 \quad \div \quad x^2 + 1 = x^2 + 1 \\ \underline{x^4 + x^2} \\ x^2 + 1 \\ \underline{x^2 + 1} \\ 0 .\end{array}$$

Et jagamisel tekki jääk tuleb 0, siis järelikult $x^4 + 1 \pmod{x^2 + 1} = 0$.

Ülesanne 2. Dešifreerimisfunktsioon on kujul $D(y) = \frac{1}{6}(y - 15) \pmod{49}$, mille ilmutatud kujul kirjanepuudeks tuleb leida $\frac{1}{6} \pmod{49}$. Selleks kasutame Eukleidese algoritmi, tähistades $A = 6$ ja $B = 49$:

$$\begin{aligned}\text{ s\"ut}(A, B) &= \text{ s\"ut}(6, 49) \\ \text{ s\"ut}(A, B - 8A) &= \text{ s\"ut}(6, 1) .\end{aligned}$$

Seega, $B - 8A = 1$ ja $(-8) \cdot 6 \equiv 1 \pmod{49}$, millest järeldub $\frac{1}{6} \pmod{49} \equiv -8 \equiv 41 \pmod{49}$ ja

$$x = D(y) = 41(y - 15) \pmod{49} = 41y + 22 \pmod{49}.$$

Näitame, et D on korrektne dešifreerimisteisendus. Võtame suvalise $x \in \{0, \dots, 48\}$ ja arvutame:

$$\begin{aligned} D(E(x)) &= D(6x + 15 \bmod 49) = D(6x + 15 + 49m) \\ &= 41(6x + 15 + 49m - 15) \bmod 49 \\ &= 246x + 41 \cdot 49m \bmod 49 = x + 49 \cdot (5x + 41m) \bmod 49 \\ &= x . \end{aligned}$$

Ülesanne 2A. Seostest $E(2) = 18$ ja $E(6) = 24$ saame võrrandisüsteemi:

$$\begin{cases} 2a + b \equiv 18 \pmod{55} \\ 6a + b \equiv 24 \pmod{55} \end{cases}$$

Lahutades alumisest võrrandist ülemise, saame $4a \equiv 6 \pmod{55}$, mille lahendamiseks tuleb esmalt arvutada $\frac{1}{4} \bmod 55$. Tähistades $A = 4$, $B = 55$ ja rakendades Eukleidese algoritmi, saame:

$$\begin{aligned} \text{süt}(A, B) &= \text{süt}(4, 55) \\ \text{süt}(A, B - 13A) &= \text{süt}(4, 3) \\ \text{süt}(A - (B - 13A), B - 13A) &= \text{süt}(14A - B, B - 13A) = \text{süt}(1, 3) . \end{aligned}$$

Seega, $14A - B = 1$ ja $14 \cdot 4 \equiv 1 \pmod{55}$, mistõttu $\frac{1}{4} \bmod 55 \equiv 14$. Nüüd avaldame a ja saame $a \equiv 6 \cdot 14 \equiv \mathbf{29} \pmod{55}$ ja $b = 18 - 2 \cdot 29 \equiv \mathbf{15} \pmod{55}$.

Lahendus 3. Esimesel süsteemil lahend puudub. Lahutades teisest võrrandist esimese, saame $3a \equiv 1 \pmod{36}$, mis on võimatu, sest 36 jagub 3-ga ja seetõttu puudub jäägil 3 pöördelement arvuvallas \mathbb{Z}_{36} .

Teise süsteemi korrektne lahend on $a = 7$ ja $b = 22$. Lahutame teisest võrrandist esimese ja saame $5a \equiv 4 \pmod{31}$. Et 31 on algarv, siis leidub jäägil 5 ka pöördelement, milleks on $-6 \equiv 25$, sest $31 - 6 \cdot 5 = 1$. Seega $a \equiv 4 \cdot (-6) \equiv -24 \equiv 7 \pmod{31}$. Asendades $a = 7$ esimesse võrrandisse, saame $b \equiv 5 - 2 \cdot 7 \equiv -9 \equiv 22 \pmod{31}$.

Ülesanne 4. Analüüsides tundmatu registri käitumist esimese nelja takti jooksul, saame juhul a), et algolek $S^0 = S_3^0 S_2^0 S_1^0 S_0^0$ oli 1 0 0 1. Ülejäänud kolm olekut S^1 , S^2 ja S^3 avalduvad järgmiselt:

$$S^1 = 0011, \quad S^2 = 0110, \quad S^3 = 1101.$$

Jada viimane bitt 0 vastab olekubitile S_0^4 . Kasutades esimest liiki nihkereg-
istrit iseloomustavat rekurrentset seost

$$S_0^{i+1} = r_0 S_3^i + r_1 S_2^i + r_2 S_1^i + r_3 S_0^i,$$

saame olemasolevate andmete põhjal ($i = 0 \dots 3$) järgmise võrrandisüsteemi:

$$\begin{aligned} 1r_0 + 0r_1 + 0r_2 + 1r_3 &= 1 \\ 0r_0 + 0r_1 + 1r_2 + 1r_3 &= 0 \\ 0r_0 + 1r_1 + 1r_2 + 0r_3 &= 1 \\ 1r_0 + 1r_1 + 0r_2 + 1r_3 &= 0, \end{aligned}$$

mida lehendades saame, et $r_0 = r_1 = 1$ ja $r_2 = r_3 = 0$.

Talitledes analoogiliselt juhul b), saame teiseks võrrandiks

$$0r_0 + 0r_1 + 0r_2 + 0r_3 = 1,$$

mis ei ole muidugi lahenduv. Seetõttu ei leidu ka vastava väljundjada lõiguga
I-liiki nihkeregistrit.

Lahendus 4A. Kustunud bitt oli 0. Vastasel korral oleks väljundjadas
järjest 5 ühte. Et aga registri järk on 4 ja sisendis on nullid, siis peaksid
väljundjadas viiele ühele järgnema kõik ühed. Allesjäänud bittidest selgub,
et nii see pole.

Ülesanne 5. Nimetatud omadustega polünoome ei leidu, sest siis peaks
polünoom $f(x) = \alpha(x) \cdot (x^2 + 1) + \beta(x) \cdot (x^5 + 1)$ võrduma konstantse
polünoomiga 1, mistõttu peaks olema $f(0) = f(1) = 1$. Kontroll näitab
aga, et

$$f(1) = \alpha(1) \cdot (1^2 + 1) + \beta(1) \cdot (1^5 + 1) = \alpha(1) \cdot 0 + \beta(1) \cdot 0 = 0 \neq 1.$$

Ülesanne 6. Et mooduli võtmine (antud juhul polünoomi $x^4 + x + 1$ järgi)
säilitab polünoomide korrutamise, siis juhul kui kongruents

$$a(x) \cdot (x^2 + 1) \equiv 1 \pmod{x^4 + x + 1}.$$

on üldse lahenduv, peab leiduma ka lahend $a(x)$, mille aste ei ületa kolme, s.t.
kui $A(x)$ on suvaline lahend, siis on lahend ka $a(x) = A(x) \pmod{x^4 + x + 1}$.
Seega otsime lahendit kujul

$$a(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0.$$

Arvutame kõigepealt $a(x) \cdot (x^2 + 1) \bmod(x^4 + x + 1)$. Kõigepealt leiame, et

$$x^2 a(x) \bmod(x^4 + x + 1) = a_1 x^3 + (a_0 + a_3)x^2 + (a_2 + a_3)x + a_2.$$

Seega taandub ülesanne järgmise polünoomide võrduse lahendamisele:

$$(a_1 + a_3)x^3 + (a_0 + a_2 + a_3)x^2 + (a_1 + a_2 + a_3)x + a_0 + a_2 = 1,$$

mis omakorda taandub võrrandisüsteemile (üle \mathbb{Z}_2):

$$\begin{aligned} 0 &= a_1 + a_3 \\ 0 &= a_0 + a_2 + a_3 \\ 0 &= a_1 + a_2 + a_3 \\ 1 &= a_0 + a_2. \end{aligned}$$

Lahendades saame, et $a_0 = a_1 = a_3 = 1$ ja $a_2 = 0$. Seega on otsitav polünoom $a(x) = x^3 + x + 1$, mille sobivust lahendina kinnitab ka otsene kontroll.

Ülesanne 7. Et igal lineaarpolünoomil $g(x) \in \mathbb{Z}_2[x]$ on juur korpuses $\mathbb{Z}_2 = \{0, 1\}$, siis lineaarpolünoomid teguriteks $f_1(x)$ ja $f_2(x)$ ei sobi. Jääb seega üle, et mõlemad $f(x)$ tegurid $f_1(x)$ ja $f_2(x)$ on ruutpolünoomid. Et polünoomil $f(x)$ ei tohtinud olla juurt hulgas \mathbb{Z}_2 , siis sellest järeldub, et mõlema teguri vabaliikmed on võrdsed 1-ga, kuna vastasel korral jaguks $f(x)$ lineaarpolünoomiga x ja omaks juurt $0 \in \mathbb{Z}_2$. Seega sobiksid teguriteks ainult polünoomid kujul:

$$x^2 + \varphi x + 1,$$

kus $\varphi \in \{0, 1\}$. Et aga $\varphi = 0$ ei sobi teguriteks lahutuse $x^2 + 1 = (x+1)(x+1)$ tõttu, siis ainus võimalus tegurina on polünoom $f_1(x) = f_2(x) = x^2 + x + 1$. Tõepoolest, sellel polünoomil puuduvad juured hulgas $\mathbb{Z}_2 = \{0, 1\}$, sest $f_1(1) = f_1(0) = 1$. Seega on sobilik neljanda astme polünoom

$$f(x) = (x^2 + x + 1)^2 = x^4 + x^2 + 1.$$

Ülesanne 8. Kui ϑ on polünoomi $f(x) = x^3 + x + 1$ juur, siis järelikult $f(x)$ jagub lineaarpolünoomiga $(x - \vartheta)$. Teostades otsese jagamistehte (arvestades seost $\vartheta^3 + \vartheta + 1 = 0$), saame et

$$x^3 + x + 1 = (x - \vartheta) \cdot (x^2 + \vartheta x + \vartheta^2 + 1) .$$

Tõepoolest, selleni jõuame teostades polünoomide jagamistehte:

$$\begin{array}{r} x^3 + x + 1 \div x - \vartheta \\ \underline{x^3 - \vartheta x^2} \\ \vartheta x^2 + x + 1 \\ \underline{\vartheta x^2 - \vartheta^2 x} \\ (1 + \vartheta^2)x + 1 \\ \underline{(1 + \vartheta^2) - \vartheta(1 + \vartheta^2)} \\ \vartheta^3 + \vartheta + 1 = 0 . \end{array}$$

Ülejäänud juured ϑ_1, ϑ_2 annab seega ruutvõrrandi

$$x^2 + \vartheta x + \vartheta^2 + 1 = 0$$

lahendamine, millest saame, et

$$\vartheta_{1,2} = -\frac{\vartheta}{2} \pm \sqrt{\frac{\vartheta^2}{4} - \vartheta^2 - 1} .$$