

Neljas harjutustund

21. aprill, 2009

1 Ülesanded

Ülesanne 1. Leia võrrandisüsteemi kõik lahendid vahemikus $[0\dots 21]$:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 6 \pmod{7}. \end{cases}$$

Ülesanne 2. Leia võrrandisüsteemi kõik lahendid vahemikus $[0\dots 293]$:

$$\begin{cases} x \equiv 11 \pmod{6} \\ x \equiv 41 \pmod{49}. \end{cases}$$

Ülesanne 3. Leia ruutjuure $\sqrt{1}$ kõik neli väärtust ringis \mathbb{Z}_{391} .

Ülesanne 4. Mitu kuupjuurt on elemendil $a \neq 0$ ringis \mathbb{Z}_{60829} ?

Ülesanne 5. RSA moodul on $n = 1199021$. On teada, et $598963^2 \equiv 1 \pmod{n}$. Tegurda selle teadmise abil moodul n .

Ülesanne 6. Ühise mooduliga RSA süsteemis kasutatakse avalikku moodulit $n = 391$. Kasutaja A avalik astendaja on $e_1 = 7$ ja kasutaja B avalik astendaja on $e_2 = 5$. Kasutajatele saadetakse ühe ja sama sõnumi $m \in \{0, \dots, 390\}$ krüptogrammide: $E_A(m) = 127$ ja $E_B(m) = 223$. Leia sõnum m .

Ülesanne 7. Miks ei sa RSA krüptosüsteemis kasutada kahe algarvu korrutise $p \cdot q$ asemel vaid ühte algarvu p ja defineerida krüpteerimisfunktsioon valemiga $E(x) = x^e \pmod{p}$?

Ülesanne 8. Ühise mooduliga RSA krüptosüsteemis kasutatakse avalikku moodulit $n = 29329$. Kasutaja A avalik astendaja on $e_1 = 13$. Kasutaja B avalik astendaja on $e_2 = 11$ ja salajane astendaja $d_2 = 23711$. Kuidas saab kasutaja B leida kasutaja A salajase astendaja? Leia see astendaja d_1 .

2 Lahendused

Ülesanne 1. Et $(-2) \cdot 3 + 1 \cdot 7 = 1$, siis saame Hiina jäägiteoreemist, et $x \equiv 1 \cdot 7 \cdot 2 + (-2) \cdot 3 \cdot 6 \equiv 20 \pmod{21}$, millest järeldub, et $x = 20$ on ainus lahend vahemikus $[0 \dots 21]$.

Ülesanne 2. Et $(-8) \cdot 6 + 1 \cdot 49 = 1$, siis saame Hiina jäägiteoreemist, st $x \equiv 1 \cdot 49 \cdot 11 + (-8) \cdot 6 \cdot 41 \equiv 41 \pmod{294}$, millest järeldub, st $x = 41$ on ainus lahend vahemikus $[0 \dots 293]$.

Ülesanne 3. Et $391 = 17 \cdot 23$ ja nii 17 kui ka 23 on algarvud, siis saame kasutada Hiina jäägiteoreemi, mille kohaselt $\mathbb{Z}_{391} \cong \mathbb{Z}_{17} \times \mathbb{Z}_{23}$ ja igale elemendile $x \in \mathbb{Z}_{391}$ vastab üheselt elementide paar $(x_1, x_2) = (x \bmod p, x \bmod q) \in \mathbb{Z}_{17} \times \mathbb{Z}_{23}$. Seosest $x^2 \equiv 1 \pmod{391}$ tulenevad seosed $x_1^2 \equiv 1 \pmod{17}$ ja $x_2^2 \equiv 1 \pmod{23}$. Seega (algarvulise mooduli p järgi on olemas parajasti kaks ühejuurt: 1 ja $-1 \equiv p-1$) $x_1 \in \{1, 16\}$ ja $x_2 \in \{1, 22\}$, mistõttu nelja võimalikku ühejuurt esitavad paarid $\{(1, 1), (1, 22), (16, 1), (16, 22)\}$. Et $3 \cdot 23 + (-4) \cdot 17 = 1$, siis saame Hiina jäägiteoreemist, et

$$x \equiv 3 \cdot 23 \cdot x_1 + (-4) \cdot 17 \cdot x_2 \pmod{391}.$$

Pannes viimases kongruentsis (x_1, x_2) asemele järjest kõik neli paari, saame ühejuurte hulgaks $\{1, 137, 254, 390\}$.

Ülesanne 4. Kuupjuure leidmine elemendile $a \neq 0$ ringis \mathbb{Z}_{60829} tähendab võrrandi $x^3 \equiv a \pmod{60829}$ lahendite arvu leidmist. Et võrrand meenutab RSA algoritmiga krüpteerimist (standardse astendajaga 3), siis esimene loomulik hüpotees võiks olla see, et arv $n = 60829$ on kahe algarvu p ja q korrutis. Tõepoolest, proovides jagada arvu n esimeste algarvudega

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59 \dots$$

märkame, et meie hüpotees peab paika: $60829 = 59 \cdot 1031$. Seega $\phi(n) = (p-1)(q-1) = 58 \cdot 1030 = 59740$ ja kuna $(3, 59740) = 1$ siis on 3 pööratav element mooduli $\phi(n)$ järgi. Seega leidub astendaja d , nii et iga $x \in \mathbb{Z}_{60829}$ korral kehtib $(x^3)^d \bmod 60829 = 1$. Seega on kuupfunktsioon antud tingimustel pööratav ja jäerlikult on igal arvul $a \in \mathbb{Z}_{60829}$ täpselt üks kuupjuur.

Ülesanne 5. Mooduli $n = 1199021$ proovimise teel tegurdamine on ilmselt liiga töömahukas. Teisendame kongruentsi $598963^2 \equiv 1 \pmod{n}$ järgmisele kujule:

$$598963^2 - 1 \equiv (598963 - 1) \cdot (598963 + 1) \equiv 598962 \cdot 598964 \equiv 0 \pmod{n}.$$

Eeldades, et $n = pq$, kus p ja q on algarvud, saame et korrutis $598962 \cdot 598964$ jagub n -ga kuid kumbki teguritest n -ga jaguda ei saa sest nad on n -st rangelt väiksemad. Seega jagub üks tegureist arvuga p ja teine neist arvuga q . Seega saame otsitava teguri kätte, kui arvutame suurima ühisteguri:

$$(598962, 1199021) = 1097,$$

mis on algarv. Kontroll näitabki, et $1199021 = 1097 \cdot 1093$.

Ülesanne 6. Esmalt paneme tähele, et $3e_2 - 2e_1 = 1$. Et e_1 kordaja on negatiivne, arvutame

$$\frac{1}{127} \pmod{391} = 117 .$$

Seega,

$$m = 117^2 \cdot 223^3 = 151805082663 \equiv 100 \pmod{391} .$$

Ülesanne 7. Funktsioon $y = E(x) = x^e \pmod{p}$ ei sobi krüpteerimisfunktsiooniks, sest tema pööramiseks piisab, kui leida Eukleidese algoritmi abil d , nii et $e \cdot d \equiv 1 \pmod{p-1}$, ja arvutada $x = y^d \pmod{p}$. RSA krüptosüsteemis aga see meetod ei tööta, sest teades vaid korrutist $n = pq$, ei saa efektiivselt arvutada Euleri funktsiooni $\varphi(n) = (p-1)(q-1)$ väärtust, mis on aga vajalik pöördastendaja d leidmiseks.

Ülesanne 8. Arvutame esmalt:

$$f = (e_1, e_2 d_2 - 1) = (13, 11 \cdot 23711 - 1) = (13, 260820) = 1 ,$$

ja võtame $t = \frac{e_2 d_2 - 1}{f} = 260820$. Siis leiame Eukleidese algoritmi abil:

$$\frac{1}{13} \pmod{260820} = 240757 ,$$

mis sobib salajaseks astendajaks d_1 .