

Ülesandeid Hiina jäägiteoreemist

12.aprill, 2007

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} ?

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 järelikult on igal arvul $a \in \mathbb{Z}_{60829}$ täpselt üks kuupjuur.