

# Valik ülesandeid aines “Sissejuhatus andmeturbesse”

29.aprill, 2004

## 1 Ülesanded

**Ülesanne 1.** Tõesta, et  $p$  on algarv parajasti siis, kui

$$x^{p-1} \equiv 1 \pmod{p}$$

iga  $x \in \{1, \dots, p-1\}$  korral.

**Ülesanne 2.** Arvuta (võimalikult lihtsal viisil)  $7^{183} \pmod{13}$  ja  $5^{122} \pmod{21}$ .

**Ülesanne 3.** RSA algoritmis kasutatavad algarvud on  $p = 11$  ja  $q = 23$ . Avalik astendaja on  $e = 3$ . Leia salajane astendaja  $d$ .

**Ülesanne 4.** Tõesta, et iga algarvu  $p$  korral  $(p-1)! \equiv -1 \pmod{p}$ .

**Ülesanne 5.** Tõesta, et  $n^5 - n$  jagub alati (iga  $n \in \mathbb{Z}$  korral) 30-ga.

**Ülesanne 6.** Kuidas veenduda 20 inimeselise grupiga 15 minuti jooksul, et  $2^{16} + 1$  on algarv, kasutamata igasugust arvutustehnikat (vaid paber ja pliiats on lubatud).

## 2 Lahendused

**Ülesanne 1.** Kui  $p$  on algarv, siis seos  $x^{p-1} \equiv 1 \pmod{p}$  (iga  $x \in \{1, \dots, p-1\}$  korral) jäeldub Fermat' teoreemist. Kui  $p$  ei ole algarv ja ütleme  $p = p_1 \cdot p_2$ , kus  $p_1 \neq 1 \neq p_2$ , siis elemendil  $p_1 \in \{1, \dots, p-1\}$  puudub pöördelement mooduli  $p$  järgi. Seega ei saa kehtida seos  $p_1^{p-1} \equiv 1 \pmod{p}$ , sest muidu oleks  $p_1^{p-2}$  elemendi pöördelement:  $p_1 \cdot p_1^{p-2} = p_1^{p-1} \equiv 1 \pmod{p}$ .

**Ülesanne 2.** Avaldise  $7^{183} \pmod{13}$  arvutamisel esitame astendaja järgmiselt  $183 = 15 \cdot 12 + 3$  kasutame Fermat' teoreemi algarvu  $p = 13$  korral:

$$7^{183} \pmod{13} = 7^{15 \cdot 12 + 3} \pmod{13} = \underbrace{(7^{15})^{12}}_{\equiv 1 \pmod{13}} \cdot 7^3 \pmod{13} = 7^3 \pmod{13} = 5.$$

Avaldise  $5^{122} \pmod{21}$  arvutamiseks Fermat' teoreemist ei piisa, kuid siin saab kasutada Euleri teoreemi. Leides kõigepealt arvu 21 Euleri funktsiooni  $\phi(21) = \phi(3 \cdot 7) = (3-1) \cdot (7-1) = 12$  ja seejärel avaldades astendaja  $122 = 10 \cdot 12 + 2$ , saame:

$$5^{122} \pmod{21} = 5^{10 \cdot 12 + 2} \pmod{21} = \underbrace{(5^{10})^{12}}_{\equiv 1 \pmod{21}} \cdot 5^2 \pmod{21} = 5^2 \pmod{21} = 4.$$

**Ülesanne 3.** Leiame Euleri funktsiooni  $\phi(n) = \phi(11 \cdot 23) = 10 \cdot 22 = 220$  ja arvutame  $e = 3$  pöördelemendi  $d$  mooduli  $\phi(n)$  järgi, kasutades Euleri algoritmi. Saame:

$$220 - 73 \cdot 3 = 1,$$

millest järelduvalt  $d \equiv -73 \equiv 220 - 73 \equiv 147$ .

**Ülesanne 4.** Fermat' teoreemist tulenevalt on arvud  $\{1, \dots, p-1\}$  polünoomi  $x^{p-1} - 1$  juured korpuses  $\mathbb{Z}_p$ . Seega on arvud  $\{0, 1, \dots, p-1\}$  polünoomi  $x^p - x$  juurteks. Et aga korpuses ei saa  $p$ -astme polünoomil olla rohkem kui  $p$  erinevat juurt, saame

$$x^p - x \equiv (x-0) \cdot (x-1) \cdot (x-2) \cdot \dots \cdot (x-(p-1)) \pmod{p}.$$

Avades sulud ja võrreldes vastavates polünoomides (üle  $\mathbb{Z}_p$ ) liikme  $x^1 = x$  kordajaid, saame

$$-1 \equiv \cdot(-1) \cdot (-2) \cdot \dots \cdot (-(p-1)) \pmod{p}.$$

Et kõik kahest suuremad algarvud on paaritud, siis on paremal pool alati paarisarv  $(p-1)$  liikmeid, mistõttu miinusmärgid tegurite eest võib ära jätta. Juhul  $p = 2$  veendume väite kehtivuses vahetu arvutuse teel.

**Ülesanne 5.** Piisab kui näitame, et  $n^5 - n$  jagub alati algarvudega 2, 3 ja 5. Selleks kasutame teguriteks lahutust:

$$n^5 - n = (n - 1) \cdot n \cdot (n + 1) \cdot (n^2 + 1).$$

Kahega ja kolmega jaguvus on ilmne, sest  $n^5 - n$  teguriteks lahutus sisaldab alati (iga  $n$  korral) kolme järjestikust tegurit  $n - 1$ ,  $n$  ja  $n + 1$ . Üks neist kolmest peab jaguma alati kolmega ja üks kahega.

Viiega jaguvuse analüüs toimub analoogilise võttega. Arvestades, et  $n \bmod 5 \in \{0, \dots, 4\}$ , analüüsime kõiki viite võimalust. Kui  $n \bmod 5 = 0$ , siis tegur  $n$  jagub 5-ga. Kui  $n \bmod 5 = 1$ , siis tegur  $n - 1$  jagub 5-ga. Kui  $n \bmod 5 \in \{2, 3\}$ , siis tegur  $n^2 + 1$  jagub 5-ga. Kui aga  $n \bmod 5 = 4$ , siis jagub 5-ga tegur  $(n + 1)$ .

**Ülesanne 6.** Definiitsiooni järgi on mingi arv  $p$  algarv parajasti siis kui ta ei jagu ühegi arvuga vahemikust  $\{2, \dots, p - 1\}$ . Tõestamiseks, et  $p = 2^{16} + 1$  on algarv kasutame tähelepanekut, et piisab kui kontrollida arvu  $p$  jagumatus arvudega vahemikust  $\{2, \dots, \lfloor \sqrt{p} \rfloor\}$ , sest mittetriviaalse teguriteks lahutuse  $p = p_1 \cdot p_2$  olemasolu korral peab üks teguritest langema nimetatud vahemikku, sest eeldus  $p_1, p_2 > \sqrt{p}$  viiks vastuolule:  $p = \sqrt{p} \cdot \sqrt{p} < p_1 \cdot p_2 = p$ .

Vahemikus  $\{2, \dots, \lfloor \sqrt{p} \rfloor\}$  on antud juhul  $2^8 = 256$  arvu, millest pooled on paarisarvud, millega jaguvust ilmselt ei ole vaja kontrollida. Seega ei ole vaja teostada rohkem kui 128 proovijagamist, mis ilmselt on jõukohane 20-le inimesele veerand tunni jooksul. Loomulikult on võimalik proovijagamiste arvu veelgi vähendada, kuid esitatud lahendus on ülesande kontekstis piisav.