Kevad 2016

Märkusi arvuteooria 15. praktikumi kohta:

A. Kommentaare ja tüüpvigu ülesannete kaupa:

1. Arv 2 on Fermat' tunnistaja arvu $2813 = 29 \cdot 97$ jaoks. Arv 2819 on tegelikult algarv, seega tal ei ole ühtegi Fermat' tunnistajat. Arv $2821 = 7 \cdot 13 \cdot 31$ on Carmichaeli arv, mistõttu tema Fermat' tunnistajad peavad jaguma kas 7, 13 või 31-ga. Viimaste peale võis juhuslike arvudega testides mitte sattuda, aga tavaliselt leiti mõni neist ikkagi üles, sest need on niivõrd väikesed.
Kui üks Fermat' tunnistaja on juba leitud, ei ole mõtet tabeli sama rida edasi täita (ehkki loengukonspektis seda illustratiivsuse mõttes tehtud on).

2. Arv 2 on Miller-Rabini tunnistaja mõlema kordarvu 2813 ja 2821 jaoks. Algarvul 2819 ei ole Miller-Rabini tunnistajaid ja iga testitud arv korrutab tõenäosuse, et tegu on siiski kordarvuga, läbi $0,25$-ga. Näiteks kümne arvuga proovides on tõenäosus, et tegu on algarvuga, vähemalt $99,9999\%$. Muuseas, ei pea tingimata testima arvuga 2, aga see on arvutuslikult kõige lihtasam valik.
Miller-Rabini testi korral tuleb vaadata, et veerus, mis vastab a^t-le, ei oleks arve ± 1 modulo n ja ülejäänud veergudes, mis vastavad $a^{2^r \cdot t}$-dele, ei oleks arvu -1 modulo n. Mõnikord arvati, et teistes veergudes ei tohi olla arvu 1 vmt.

3. Kontrollvastus: TAAVIROIVAS. Üldiselt tähendab see, et digiallkiri on võltsitud, aga seda kas huumorisoonega salajase võtme omaniku poolt (mis teeb allkirja peaaegu vastuvõetavaks) või mõne võltsija poolt, kes on kogemata sattunud TAAVIROIVASeks dekodeeruva sõnumi peale. Viimane tähendab, et ta saab saata autentsena tunduvaid sõnumeid TAAVIROIVAS, aga ainult neid (näiteks vastuseks küsimustele SALASONA, KELLEPOOLKOHTUME, KELLEKONTOTH2KIME jne.)

4. Kontrollvastus: MARTLAAR.

5. Kontrollvastus: EDGARSAVISAAR. Dekodeerimine taandus igale neljakohalisele blokile arvu 206 liitmisele (või arvu 3123 lahutamisele) modulo 3329.

6. Ülesanne põhines tähelepanekul

$$(-1)^{n-1} \equiv 1 \pmod{n},$$

mis kehtib vaid juhul, kui n on paaritu arv.

7. Selle ülesande lahendasid ära ainult kaks kuulajat, seega muutus see *-ülesandeks. Esitan siinkohal ühe võimaliku lahenduse.

Kuna ülesandes on öeldud, et Carmichaeli arv on ruuduvaba, siis peab ta olema erinevate algtegurite korrutis. Carmichaeli arvud on definitsiooni kohaselt kordarvud, mistõttu neid algtegureid on vähemalt kaks tükki. Kui meil õnnestub näidata, et ühelgi Carmichaeli arvul ei ole täpselt kahte algtegurit, siis ongi ülesanne lahendatud.

Oletame vastuväiteliselt, et $n = pq$ on Carmichaeli arv, kus p ja q on erinevad algarvud. Kuna p on algarv, siis leidub ruutjääk a modulo p. Hiina jäägiteoreemi kohaselt on kongruentside süsteem

$$\begin{cases} x \equiv a & \pmod{p}, \\ x \equiv 1 & \pmod{q} \end{cases}$$

lahenduv. Olgu x_0 üks selle süsteemi lahend. Siis $(x_0, p) = 1$ (muidu $p \mid a$, mis on vastuolus a algjuureks olekuga) ja $(x_0, q) = (1, q) = 1$. Lemma 4.1 kohaselt ka $(x_0, n) = 1$ ja Carmichaeli arvu definitsioonist saame, et

$$x_0^{n-1} \equiv 1 \pmod{n}.$$

Ilmselt siis ka $a^{n-1} \equiv x_0^{n-1} \equiv 1 \pmod{p}$. Lemma 7.3 põhjal

$$\varphi(p) = p - 1 \mid n - 1.$$

Kui vahetada eelnevas arutelus p ja q rollid, siis samamoodi saab näidata, et $q - 1 \mid n - 1$. Nüüd

$$p - 1 \mid n - 1 = pq - 1 = (p - 1)q + (q - 1),$$

seega ka $p - 1 \mid q - 1$. Analoogiliselt $q - 1 \mid p - 1$ ja kuna $p, q > 1$, siis $p - 1 = q - 1$ ehk $p = q$. See on vastuolus meie eeldusega $p \neq q$. Oleme jõudnud vastuoluni, järelikult meie oletus, et Carmichaeli arvul võib olla täpselt kaks erinevat algtegurit, ei pea paika ja kõigil Carmichaeli arvudel on vähemalt kolm erinevat algtegurit.

Koht, mis võis kahe silma vahele jääda, on näitamine, et $(x_0, n) = 1$. Samuti võis kasutada kahte algjuurt, ühte modulo p ja teist modulo q (ühe algjuure ja arvu 1 asemel). Lahendus sellest märkimisväärselt ei muutu.

8. Antud ülesannet ei lahendanud keegi ära. Seetõttu esitan siinkohal täieliku lahenduse.

Esiteks, kongruentsi $x^2 \equiv b^2 \pmod{n}$ lahendid on samad, mis kongruentside süsteemi

$$\begin{cases} x^2 \equiv b^2 & (\text{mod } p), \\ x^2 \equiv b^2 & (\text{mod } q) \end{cases}$$

lahendid. Kuna b^2 on ilmselt ruutjääk mõlema mooduli p ja q järgi (kui $p \mid b$, siis ka $p \mid a$, aga $(a, pq) = 1$; sama kehtib arvu q korral), siis kummalgi kongruentsil on täpselt kaks erinevat lahendit ja Hiina jäägiteoreemi tõttu on tervel süsteemil neli erinevat lahendit.

Oletame, et meil on olemas mingi arvutuslikult efektiivne meetod nende nelja ruutjuure leidmiseks. Kasutame seda meetodit, et leida mittetriviaalne ruutjuur arvust 1, st. leiame $c \in \mathbb{Z}$ nii, et

$$c^2 \equiv 1 \pmod{n}$$

ja $c \not\equiv \pm 1 \pmod{n}$. Siis

$$(c+1)(c-1) \equiv 0 \pmod{n}$$

ja $n \nmid c \pm 1$, sest vastasel korral $c \equiv \pm 1 \pmod{n}$. Järelikult

$$n \mid (c+1)(c-1)$$

ja kas $(n, c+1) > 1$ või $(n, c+1) = 1$ ja Eukleidese lemmast $n \mid c-1$. Viimane võimalus on meil eelnevalt välistatud ja kui $(n, c+1) = n$, siis $n \mid c+1$, mis samuti ei kehti. Kokkuvõttes oleme seega saanud, et

$$1 < (n, c+1) < n.$$

Kuna arvul n on ainult kaks endast väiksemat ja ühest suuremat jagajat, nimelt p ja q, siis $(n, c+1) \in \{p, q\}$. Järelikult ühe algteguri leidmiseks piisab suurima ühisteguri $(n, c+1)$ leidmisest, mida saab Eukleidese algoritmi abil efektiivselt teha.