Kevad 2015

Märkusi arvuteooria 15. praktikumi kohta:

A. Kuna seekord olid ülesanded suhteliselt lihtsad, siis vähemalt arvutusliku osaga said enam-vähem kõik kenasti hakkama. Loodetavasti jätkub see trend viimases praktikumis ja eksamil.

B. Kommentaare ülesannete kaupa:

1. Ainus probleem, mis siin tekkis, oli peale mingi a korral $a^{n-1} \not\equiv 1 \pmod{n}$ saamist edasi testimine. Selleks hetkeks on meil arv n Fermat' testist läbi kukkunud ja rohkem ei ole mõtet arvutada.
Kontrollvastus: $1729 = 7 \cdot 13 \cdot 19$ on kordarv (tegelikult Carmichaeli arv), $1731 = 3 \cdot 577$ samuti, 1733 on algarv.

2. Meenutan, et Miller-Rabini testis on astendades vaja leida vaid a^{t_i} ja seda siis järjest ruutu tõsta.

3. Kuna AUTENTNE tekst allkirjastati VOLTSINGuna, siis digiallkiri ei olnud õige. Aga teatud mööndustega oli tegu õige allkirjaga valel dokumendil, seega isikusamasuse tuvastamiseks sellest piisaks (kui arvestamata jätta nö. naiivse RSA kõik teised puudused).

4. Salajane sõnum on SALAJANE. Kogu tegevus oli siin sama, mis 3. ülesandes, ainult avalik ja salajane võti vahetasid oma rollid ära.

5. Meenutame natuke mooduli järgi astendamist:

$$\begin{aligned} 21^{21} \equiv (-2)^{21} &= -(2^6)^3 \cdot 2^3 = -64^3 \cdot 8 \equiv -(-5)^3 \cdot 8 \\ &= 25 \cdot 40 \equiv 2 \cdot (-6) = -12 \equiv 11 \pmod{23}. \end{aligned}$$

Järelikult ühissaladuseks on arv 11.

6. Siin tuli kasutada Fermat' väikest teoreemi arvu $561 = 3 \cdot 11 \cdot 17$ kõigile algteguritele ja tulemus kas loengukonspekti järelduse 4.3 või Hiina jäägiteoreemi abil kokku panna. Ainus tüüpviga oli fakti

$$(a, 561) = 1 \iff (a, 3) = (a, 11) = (a, 17) = 1$$

põhjendamata jätmine (selleks piisas viitest järeldusele 4.3 või Hiina jäägiteoreemile).

7. Muutus lahendajate vähesuse tõttu *-ülesandeks. Näidislahendus: oletame vastuväiteliselt, et $n = p^l \cdot m$ on Carmichaeli arv, kus $p \in \mathbb{P}$, $m, l \in \mathbb{N}$, $l \geq 2$ ja $(m, p) = 1$, st. eraldame ruutu sisaldavas Carmichaeli arvust n välja selle ruudu mõne algteguri kõrgeima astme p^l. Võtame $a := 1 + pm$.

Esiteks $(a, n) = 1$, sest vastasel juhul leidub mingi suurima ühisteguri $(a, n) > 1$ algtegur $q \in \mathbb{P}$ selliselt, et $q \mid a$ ja $q \mid n = p^l m$. Järelduse 1.11 tõttu kas $q \mid m$ või $q \mid p^l$. Kuna q on algarv, siis viimasel juhul $q = p$ ja $p \mid a = 1 + pm$, mis ei ole võimalik. Kui aga $q \mid m$, siis $q \mid a$ tõttu $q \mid a - pm = 1$, samuti vastuolu. Järelikult meie vastuväiteline oletus, et $(a, n) > 1$ on väär ja $(a, n) = 1$.

Nüüd piisab vaid tähele panna, et binoomvalemist

$$\begin{aligned} a^{n-1} = (1 + pm)^{n-1} &= 1 + (n-1) \cdot pm + \binom{n-1}{2} p^2 m^2 + \dots \\ &\equiv 1 + (n-1) \cdot pm = 1 + p^{l+1} m^2 - pm \equiv 1 - pm \pmod{p^2}. \end{aligned}$$

Seega kui kehtiks $1 - pm \equiv 1 \pmod{p^2}$, siis $p^2 \mid pm$ ehk $p \mid m$, aga $(p, m) = 1$. Järelikult $a^{n-1} \not\equiv 1 \pmod{p^2}$, mistõttu ka $a^{n-1} \not\equiv 1 \pmod{n}$, sest $n = p^2 \cdot p^{l-2} m$ ja kui $a^{n-1} \equiv 1 \pmod{n}$, siis kehtib sama kongruents ka mooduli p^2 järgi. Kokkuvõttes oleme leidnud arvu a nii, et $(a, n) = 1$ ja $a^{n-1} \not\equiv 1 \pmod{n}$, mis on vastuolus Carmichaeli arvu definitsiooniga. Seetõttu ei ole võimalik, et Carmichaeli arv ei oleks ruuduvaba.

8. Ka sellele ülesandele tuli millegipärast tärn juurde. Lahendus on näha RSA võtmete leidmise skeemist: teades moodulit $\varphi(n)$ ja avalikku astendajat e, saab (tagurpidi Eukleidese algoritmi abil) leida $\overline{d} = \overline{e}^{-1} \in \mathbb{Z}_{\varphi(n)}$. Aga see d ongi salajane astendaja, mille abil on võimalik kõiki salakirju dekodeerida ja allkirju võltsida. Tegelikult on $\varphi(n)$ abil võimalik isegi $n = pq$ ära tegurdada:

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

seega $q = n - \varphi(n) - p + 1$ ja $n = pq = (n - \varphi(n) + 1)p - p^2$ ehk

$$p^2 + (\varphi(n) - n - 1)p + n = 0.$$

See on ruutvõrrand p suhtes, mida me oskame lahendada, kuna eelduse kohaselt on mõlemad kordajates esinevad arvud n ja $\varphi(n)$ teada. Sümmeetria tõttu p ja q vahel on antud ruutvõrrandi teine lahend tegelikult q.