Kevad 2018

Arvuteooria 11. praktikumi ülesanded:

Algjuured II.

1. Leida kõik algjuured mooduli 41 järgi.

2. Teha kindlaks, kas mooduli n järgi leidub algjuuri ning kui leidub, siis leida nende arv ja üks algjuur, kui a) $n = 105$, b) $n = 106$, c) $n = 107$.

3. Teha kindlaks, kas mooduli n järgi leidub algjuuri ning kui leidub, siis leida nende arv ja üks algjuur, kui a) $n = 242$, b) $n = 243$, c) $n = 244$.

4. Lahendada kongruents $1 - x + x^2 - x^3 + x^4 + \ldots + x^{2018} \equiv 0 \pmod{43}$.

5. Olgu p ja q erinevad paaritud algarvud. Tõestada, et neil on ühine algjuur, st $a \in \mathbb{Z}$, mis on algjuur nii mooduli p kui mooduli q järgi.

6. Tõestada, et kui $a > 1$, $n \in \mathbb{N}$ ja $(a, n) = 1$, siis $n \mid \varphi(a^n - 1)$.

7. Tõestada, et mistahes paaritu $p \in \mathbb{P}$ korral leidub $1 < a < p$ nii, et a on korraga algjuur kõigi moodulite jaoks, mis on kujul p^k, $k \in \mathbb{N}$.

8. Olgu q ja $p = 2q + 1$ paaritud algarvud ning $1 < a < p - 1$. Tõestada, et $p - a^2$ on algjuur mooduli p järgi.

9*. Olgu $p > 2$ algarv ja $a \not\equiv 0, 1, -1 \pmod{p}$. Tõestada, et kongruentsil $a^x \equiv 1 \pmod{p^x}$ on ainult lõplik arv lahendeid.

10**. Tõestada, et kui mooduli n järgi ei leidu algjuuri ja $(x, n) = 1$, siis

$$x^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{n}.$$