Kevad 2020

Arvuteooria 16. praktikumi ülesanded:

Kordamine II.

1. Tõestada, et kui $n \in \mathbb{N}$, siis $[1, 2, \ldots, 2n] = [n+1, n+2, \ldots, 2n]$.

2. Tõestada, et iga $n \in \mathbb{N}$ korral $2^n \mid (n+1)(n+2)\ldots(n+n)$.

3. Leida diofantilise võrrandi $4x + 6y + 10z = 146$ positiivsete lahendite arv.

4. Leida kõik algarvud p, mille korral $p \mid 6^p(p-4)! + 10^{3p}$.

5. Leida ringi $\mathbb{Z}_{691488}$ kõigi selliste elementide $\overline{x}$ arv, mille korral $x^2 \equiv x \pmod{691488}$.

6. Tõestada, et diofantiline võrrand $x^2 + 5 = y^3$ ei ole lahenduv.

7. Leida kõik naturaalarvud n, mille korral $\prod_{d|n} d = n^3$.

8. Lahendada kongruents

$$3x^4 + 3x^3 + 4x^2 + x + 64 \equiv 0 \pmod{875}.$$

9. Teha kindlaks, kas mooduli n järgi leidub algjuuri ning kui leidub, siis leida nende arv ja üks algjuur, kui

a) $n = 509$, b) $n = 512$, c) $n = 515$, d) $n = 686$.

10. Lahendada kongruents $1 - x + x^2 - x^3 + x^4 - \ldots + x^{2030} \equiv 0 \pmod{162}$

11. Olgu p ja q erinevad paaritud algarvud ja $a \in \mathbb{Z}$ ruutjääk mooduli pq järgi. Tõestada, et võrrandil $x^2 \equiv a \pmod{pq}$ on täpselt neli lahendit. Kas see väide jääb kehtima ka siis, kui p ja q on võrdsed?

12. Kasutades loengukonspekti näites 9.8 toodud skeemi neljatäheliste (st. kaheksanumbriliste) blokkide jaoks ja mooduli väiksust, dekodeerida avaliku võtmega $(89942987, 677)$ kodeeritud RSA sõnum

$$19103293485244600190575259093791.$$