

Arvuteooria 16. praktikumi ülesanded:

Kordamine II.

1. Leida, milliste astendajate $k \in \mathbb{N}$ korral jagub *mistahes* seitsme järjestikuse täisarvu k . astmete summa (nt $3^k + 4^k + 5^k + 6^k + 7^k + 8^k + 9^k$) alati arvuga 7.

2. Leida kõik arvud $a, b, c \in \mathbb{N}_0$, mille korral

$$[a + c, a] = [b + c, b].$$

3. Eikunagimaa relvajõududes on igas patareis 146 suurtükiväelast, igas eskadronis 204 ratsanikku ja igas pataljonis 595 jalaväelast. Manöövritel osales kokku 35 802 sõdurit. Õppusi juhtinud kindral pani tähele, et (vähemalt) ühe relvaliigi allüksuseid oli algarv tükki. Leida, mitu patareid saadeti manöövritele.

4. Leida kõik algarvud $p, q \in \mathbb{P}$, mille korral $pq \mid 2^p + 2^q$.

5. Leida ringi $\mathbb{Z}_{202420272024}$ kõigi selliste elementide $\bar{x}$ arv, mille korral $\bar{x}^4 = \bar{x}^2$.

6. Leida võrrandi $x^{2024} + y^{2024} = 2^{2025}$ kõik täisarvulised lahendid.

7. Lahendada kongruents

$$x^5 + 6x^4 + x^3 + 2x^2 + 4x - 26 \equiv 0 \pmod{8232}.$$

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

$$\text{a) } n = 9823, \quad \text{b) } n = 9826, \quad \text{c) } n = 9829, \quad \text{d) } n = 9832.$$

9. Leida kõigi rühma $U(\mathbb{Z}_{54})$ elementide järgud ja kõik algjuured mooduli 54 järgi indeksite tabeli abil. Kontrollida *kogu* vastust ilma astendamist kasutamata.

10. Tõestada, et leidub lõpmata palju *paarisarve*, mis *ei* ole Euleri φ -funktsiooni väärtusteks.

11. Tõestada, et iga täisarv $a \in \mathbb{Z}$, mis ei ole täisruut, on mitteruutjäak lõpmata paljude algarvuliste moodulite p järgi.

12. Kasutades loengukonspekti näites 9.8 toodud skeemi 16-täheliste (st. 32-numbriliste) blokkide jaoks ja mooduli väiksust, dekodeerida avaliku võtmega (82380576522004562730052333409507, 65537) kodeeritud RSA sõnum

16530755374160243332104062412854407334866469857147826879008182042043029492999353959032613996740.