Arvuteooria 16. praktikumi ülesanded:

Kordamine II.

1. Tõestada, et mistahes $a, b \in \mathbb{Z}$ korral $(a, b)^2 = (a^2, b^2)$.

2. Röövelparuni jõuk pidas järjekordse söömapeo, kus vardasse aeti nii härgi, sigu kui hanesid. Hinnad olid vahepeal muutunud: 21 krossi härja, endiselt 3 krossi sea ja 7 penni hane eest. Kui kokku kulus seekord 20 naela ja 2 penni, iga härja kohta tuli vähemalt 6 siga, iga sea kohta vähemalt 10 hane, aga kokku mitte rohkem kui 42 tosinat lindu-looma, siis mitu elukat ära söödi?

3. Tõestada, et iga Mersenne'i algarvu $2^n - 1$ astendaja n on samuti algarv. Kas kehtib ka vastupidine väide, st $2^p - 1$ on iga $p \in \mathbb{P}$ korral algarv?

4. Tuua näide kahest isomorfsest ja kahest mitteisomorfsest 666-elemendilisest (jäägiklassi)ringist. Põhjendada oma valikut.

5. Olgu p ja q erinevad paaritud algarvud ning $(p-1, q) = 1 = (p, q-1)$. Tõestada, et $(p-1)^{q-1} \equiv (q-1)^{p-1} \pmod{pq}$.

6. Tõestada, et $\tau(n) \leq 2\sqrt{n}$.

7. Lahendada kongruents

$$3x^5 + 2x^3 - 4x + 4 \equiv 0 \pmod{500}.$$

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

a) $n = 622$, b) $n = 623$, c) $n = 624$, d) $n = 625$.

9. Lahendada kongruents $1 - x + x^2 - x^3 + x^4 - \ldots + x^{2018} \equiv 0 \pmod{147}$.

10. Tõestada, et kui täisruudu a^2 kümnendesituses on paarisarv numbreid, mida tagurpidi kirjutades on ka tulemuseks täisruut b^2, siis $121 \mid a^2$.

11. Olgu $p > 2$ algarv ja r vähim positiivne mitteruutjääk mooduli p järgi. Tõestada, et r on algarv.

12. Salasõnum s kodeeriti kahe avaliku võtmega

$(1322186048072531620674934919183311714221393197982 7, 5555)$ ja

$(1322186048072531620674934919183311714221393197982 7, 747)$

ning saadi krüptogrammid

$$9885416640895527569712520096506650339440913118318 \text{ ja}$$

$$8259135772668463783680656482433692097314524847405.$$

Leida sõnumi esialgne tekst s.