

Arvuteooria 16. praktikumi ülesanded

Kordamine

1. Kas aritm. jadas $11, 27, 43, 59, 75, \dots$ esineb 7 järjestikust kordarvu?
2. Geneetiliselt muundatud kuldkalake täidab igal aastal sama arvu soove püüdja kohta, kusjuures lubatud soove on esimesel aastal 3, teisel 5 ja kolmandal 8 ning see arv hakkab siis korduma. Kuna kuldkalakese võime soove täita on igal aastal täpselt sama ja ta on sunnitud selle tervenisti ära kasutama, siis täidab ta iga aasta viimase püüdja jaoks juba järgmise aasta jagu soove. Mitut ulmelist nõudmist kuldkalake aastas täide viima peab?
3. Olgu p ja $2p + 1$ algarvud. Näita, et $\varphi(4p + 2) = \varphi(4p) + 2$.
4. Leia arvu $5^{5^{\dots^5}}$ jagamisel arvuga 100 tekkiv jääk, kui siin konstruktsioonis arv 5 esineb n korda.
5. Too näide ühikelemendiga kommutatiivsest ringist R , milles on 24 elementi (ehk $|R| = 24$) ja pööratavaid elemente on

(a) $|U(R)| = 8$,

(b) $|U(R)| = 4$,

(c) $|U(R)| = 2$.

- ## 6. Lahenda kongruents

$$3x^4 - 8x^3 + 8x^2 - 3x + 3 \equiv 0 \pmod{225}.$$

7. Tee kindlaks, kas mooduli n järgi leidub algjuuri ning kui leidub, siis leia nende arv ja üks algjuur, kui

(a) $n = 384$,

(b) $n = 4374$,

(c) $n = 567$,

(d) $n = 1331$.

- ## 8. Lahenda kongruents

$$9^x \equiv 13 \pmod{166}.$$

- 9.
- Leia kongruentsi*

$$x^2 \equiv 11471 \pmod{20753}$$

lahendite arv, kui on teada, et 11471 ja 20753 on algarvud.

10. Caesar ja Marcus Antonius avastasid, et šifr, mida nad kasutasid omavaheliseks suhtlemiseks oli murdud keltide poolt. Nad otsustavad kasutada Diffie-Hellmani võtmevahetust selleks, et saada uue jagatud saladuse selle šifri jaoks. Keltide špioonid lugesid nii võtmevahetuseks saadetud kirjad: Caesarilt “XXXVII II XXXIIII” ja Marcuselt “XVIII”, kui ka hiljem kodeeritud sõnumid: Caesarilt “GXIXGDNPRA” ja Marcuselt “DGFNORZZIA”. Tee kindlaks, mis oli nende poolt saadud jagatud saladus ja dekodeeri kodeeritud sõnumid. Võib eeldada, et nad kasutavad lihtsat šifri ja ladina tähestiku 23 tähega. Kas Diffie-Hellmani võtmevahetuse murdmine on tarvilik sõnumite dekodeerimiseks või saab ka ilma?