

Arvuteooria 14. praktikumi ülesanded

1. Arvuta

(a) $\left(\frac{160}{693}\right)$;

(b) $\left(\frac{6738}{2771}\right)$;

(c) $\left(\frac{343}{585}\right)$.

2. Leia Gaussi ruutvastavusseaduse abil kõik algarvud p , mille järgi 17 on ruutjääk.

3. Mitu lahendit on järgmistel kongruentsidel:

(a) $x^2 \equiv 162 \pmod{317}$;

(b) $526x^2 + 50x - 44 \equiv 0 \pmod{214}$.

4. Olgu a täisarv ja n naturaalarv, kusjuures $n \equiv 5 \pmod{8}$. Tõesta, et kui $\left(\frac{a}{n}\right) = 1$, siis kongruents $x^2 + 2(a+x) + 1 \equiv 0 \pmod{n}$ ei ole lahenduv. Kas kehtib ka vastupidine väide?

5. Tõesta, et arv 3 on algjuur kõigi Fermat' algarvude $p > 3$ jaoks (Fermat' algarv on algarv kujul $2^{2^k} + 1$, kus $k \in \mathbb{N}$).

6. Olgu a ja n naturaalarvud, kusjuures n on paaritu. Kas peab kehtima kongruents

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}?$$

7. Tõesta, et leidub lõpmata palju algarve kujul $5k + 4$, kus $k \in \mathbb{N}$.

8. Olgu a ja b naturaalarvud. Tõesta, et aritmeetiline jada $(a + kb)_{k=1}^{\infty}$ sisaldab lõpmata palju täisruute parajasti siis, kui a on ruutjääk mooduli b järgi.

9*. Olgu $p > 2$ algarv, n naturaalarv ja $(p, n) = 1$. Leia

$$\sum_{i=1}^p \left(\frac{i^2 + n}{p}\right).$$

10**. Olgu a täisarv ja $p > 2$ algarv. Leia kongruentsi

$$x^2 + y^2 + z^2 \equiv 2xyz \pmod{p}$$

lahendite (x, y, z) arv.

1. Näide 8.22.
2. Teoreem 8.14, lemma 8.4.
3. Näide 8.22. Vt ka praktikumi 13 ülesanne 8.
4. Definitsioon 8.1, märkus 8.17, lause 8.21, näide 8.22.
5. Näita, et kõik mitteruutjäägid on algjuured ja 3 on mitteruutjääk.
6. Definitsioon 8.16.
7. Vrdl lausega 8.10.
8. Definitsioon 8.1. Ühe täisruudu abil saab samas aritmeetilises jadas kontrueerida lõpmata palju täisruute.