

Arvuteooria antikordamisküsimused

Kevad 2013

Eksamil tuleb osata lahendada ülesandeid, mis kas esinesid mõnes praktikumis mittetärnülesannetena või on nendega analoogiliselt lahendatavad. NB! Nende ülesannete hulka kuuluvad ka tõestusülesanded.

Lisaks peab oskama defineerida kõiki mõisteid, tõestada kõiki tulemusi ja anda ülevaadet kõigist teemadest samas mahus, kui neid käsitleti loengus (seda on kokku veidi vähem, kui kogu loengukonspektis sisalduv materjal),
v.a.

1. Selle algoritmi põhjendamine, mille abil lahendatakse kongruentse algarvu astme järgi (meetodit ennast tuleb osata kasutada);
[loengukonspekti alajaotus 6.4]
2. Teoreem algjuurte leidmisest mooduli p^k järgi;
[loengukonspekti teoreem 7.15]
3. Teoreemid lõplike korpuste konstrueerimisest;
[loengukonspekti lause 8.9 ja teoreem 8.13]
4. Gaussi ruutvastavusseadus.
[loengukonspekti teoreem 9.14]