SEMINARAS

2016 lapkričio 29 d. 09:00, SRL-I 324 aud.

Raimondas Čiegis

Viešojo rakto RSA algoritmas - matematinė analizė bei įrodymai nagrinėjant moderniąją kriptografijos technologiją

Tęsiame diskusiją apie matematinių įrodymų ir pilnos analizės svarbą matematikos specialistų rengime. Šiame seminare, nagrinėdami labai svarbią šiuolaikinę technologiją, viešojo rakto algoritmus, bandysime sudaryti modelį paskaitos, kai naujos žinios (aktuali, karšta aktualija, nereikalaujanti paaiškinimo, kodėl ji yra aktuali ir teiktina labai užimtiems ir savo vertę žinantiems studentams) yra papildomos pilna pateiktų algoritmų ir teiginių analize su griežtais jų teisingumo įrodymais.

Loginio, konstruktyvaus ir kritinio mąstymo ugdymas yra svarbiausias universitetinio išsilavinimo tikslas. Tai ypač svarbu, kai ruošiame profesionalius matematikus, orientuotus ir pasirengusius spręsti vis naujus virtualiosios realybės ir išmaniųjų technologijų ateities iššūkius. Tiesiog remiuosi asmenine nuostata, kad beprasmiška per daug dėmesio skirti šios dienos technologijoms, jos pasens ir taps vakarykšte diena jau rytoj, o gal net šiandien.

Pagrindinis paskaitos tikslas - nagrinėti situaciją, kai esame priversti paskaitą konstruoti principu "iš viršaus keliaujame žemyn", kai negalime remtis puikiai suderinta ir gyvenimo patikrinta nuostata, jog specialieji dalykai dėstomi padėjus tvirtus bendrųjų dalykų pamatus.

Paskaitoje susitiks modernioji kriptografija - viešasis raktas, matematikos perlas - pirminiai skaičiai, fundamentaliosios matematikos ne pats lengviausias skyrius - grupių teorija, algoritmų sudėtingumo analizė ir netgi Euklido algoritmas, turbūt seniausias iš netrivialiųjų matematinių algoritmų (jau 2500 metų niekam nepavyko jį pagerinti).

Pranešimas yra tęsinys apvaliojo stalo diskusijų, reguliariai bet neprognozuojamu paros laiku vykstančių 424b kabinete (seminaro vadovas MM).

Kviečiame dalyvauti.
Seminaro sekretorius A. Bugajev