Univerza na Primorskem
Titov trg 4
6000 Koper

VABILO NA AKTIVNOSTI PROJEKTA OOOZNANOST!

Najnujnejše o testih praštevilskosti

Kdaj: 18. marec 2026, ob 16.00
Kje: UP Famnit (Glagoljaška 8, 6000 Koper)
Izvajalec: dr. Aleksander Simonič

Opis:

Predstavljajte si, da morate ugotoviti, ali je dano stomestno liho naravno število praštevilo. Morda se ta naloga sliši kot slaba šala pri pouku matematike, vendar je odgovor ključnega pomena za sodobno kriptografijo. Preprost postopek bi bil, da za vsako naravno število d, večje od 1 in manjše od kvadratnega korena danega števila n, preverimo, ali d deli n. To bi zahtevalo približno 1050 operacij deljenja. Tudi če bi vsaka takšna operacija trajala le 1 nanosekundo, bi na odgovor čakali okoli 1033 let, zato to ni učinkovit postopek.

Učinkovit postopek (ali algoritem) je tisti, ki potrebuje p(log n) operacij, kjer je p(x) nek polinom. Na srečo v praksi obstajajo zelo hitri verjetnostni algoritmi, npr. Miller–Rabinov test, ki s precejšnjo verjetnostjo pravilno določijo, ali je število praštevilo. Na predavanju si bomo ogledali nekatere takšne postopke in osnovne ideje v ozadju.

O predavatelju:

Aleksander Simonič je leta 2022 doktoriral iz analitične teorije števil na Univerzi Novega Južnega Walesa (Avstralija). Po doktoratu je bil tam zaposlen kot raziskovalec in predavatelj, kjer je poučeval različne matematične predmete študentom Avstralske vojaške akademije. Trenutno je zaposlen kot asistent na Fakulteti za matematiko, naravoslovje in informacijske tehnologije Univerze na Primorskem, kjer se raziskovalno ukvarja z L-funkcijami ter poučuje dva številsko-teoretična predmeta. Je strasten ljubitelj klasične glasbe in dolgih sprehodov.

Univerza v Mariboru
TRANSFORM 4EUROPE
FACTUMEVENT
Financira Evropska unija

»Financira Evropska unija. Za izražena stališča in mnenja odgovarja samo avtor (ali avtorji) in ne odražajo nujno stališč Evropske unije ali Evropske izvajalske agencije za raziskave. Niti Evropska unija niti Evropska izvajalska agencija za raziskave ne moreta biti odgovorna zanje.«