Odmevno odkritje treh indijskih znanstvenikov

Problem praštevil končno rešen

Dr. Mojca Pavšič

Trije računalniški znanstveniki z Indijskega tehnološkega inštituta v Kanpurju so avgusta vznemirili mednarodno matematično skupnost, ker so našli rešitev več stoletij starega problema, kako učinkovito določiti, ali je neko število praštevilo. Algoritem, ki so ga odkrili 36-letni profesor Manindra Agarval ter njegova podiplomska študenta Niradž Kajal in Nitin Saksena, je presenetljiv v svoji preprostosti.

Računalniški znanstveniki z Indijskega tehnološkega inštituta v Kanpurju: od leve proti desni Nitin, Niradž in Manindra.

Praštevila so naravna števila, večja od 1, ki so deljiva le z 1 in s samim seboj. S praštevili, ki so »osnovni gradniki« naravnih števil, so se ukvarjali učenjaki vse od antičnih časov naprej. Že okrog leta 240 pr. n. št. se je grški matematik **Eratostenes**, bibliotekar aleksandrijske knjižnice, domislil prve neoporečne metode, s katero je mogoče ugotoviti, ali je neko število praštevilo. Vendar čas, ki ga ta metoda zahteva, narašča eksponentno z dolžino zapisa števila, tako da bi v primeru zelo velikih števil lahko čakali na odgovor dlje, kot je staro vesolje. Enako velja za znano osnovnošolsko metodo, ko dano število po vrsti delimo z manjšimi števili. Zato so matematiki poskušali najti hitrejši algoritem.

Raziskave so postale še posebno intenzivne v zadnjih desetletjih, saj so praštevila ključnega pomena v kriptografiji. Šifrirni sistem RSA, ki se uporablja za zavarovanje internetnih transakcij, potrebuje za svoje delovanje dve veliki (na primer 100-mestni) praštevili. Algoritmi, ki jih računalničarji trenutno uporabljajo za iskanje primernih praštevil, so sicer zelo hitri, vendar se tu in tam lahko zgodi, da sestavljeno število razglasijo za praštevilo. Raziskovalci so si že dolgo zaman prizadevali najti algoritem, ki bi bil ne le hiter, ampak tudi 100-odstotno zanesljiv.

Zdaj pa je **Manindri Agarvalu** in njegovima sodelavcema uspelo najti rešitev. Odkrili so algoritem, ki daje odgovor v smiselnem času in ne dela napak. Njihov uspeh temelji na novem pristopu k reševanju problema. Namesto da bi zastavili eno samo veliko vprašanje, ali je dano število praštevilo, so postavili celo zaporedje manjših vprašanj oziroma »enačb« glede števila, ki so ga želeli preveriti. »Če enačbe veljajo, potem je število praštevilo, če pa katerakoli od teh enačb ne velja, potem število ni praštevilo,« pravi Agarval.

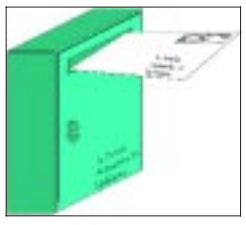
Dokaz, ki so ga indijski znanstveniki objavili na spletnih straneh svojega inštituta, so preverili že številni matematiki. Vsi, ki so Agarvalu poslali povratno informacijo, so algoritem ocenili kot pravilen. Strokovnjaki so sicer že dolgo domnevali, da je hiter algoritem za reševanje tega problema mogoč, vendar niso predvideli izjemne preprostosti trinajstvrstične rešitve, ki so jo predstavili Agarval, Kajal in Saksena.

»To je bil eden od velikih nerešenih problemov v teoretski računalniški znanosti in računalniški teoriji števil,« je o odkritju dejal **Shafi Goldwasser**, profesor računalništva na Massachusetts Institute of Technology v ZDA in na Weizmannovem inštitutu znanosti v Izraelu. »To je najboljši rezultat v zadnjih desetih letih,« pravi Goldwasser.

»Teoretski napredek je pomemben že sam zase, vendar bo ta metoda pomagala matematikom rešiti tudi nekatere probleme, kjer so zaradi uporabe drugih tehnik zašli v slepo ulico,« meni o rešitvi treh indijskih znanstvenikov matematik **Ian Stewart** z Univerze v Warwicku v Veliki Britaniji. Strokovnjak za praštevila **Carl Pomerance**, matematik v Bellovih laboratorijih v New Jerseyju, ZDA, pa pravi, da nas ta preprosta in elegantna rešitev znova opominja, kako lahko je spregledati preproste stvari.

Prof. dr. Marko Petkovšek, profesor diskretne in računalniške matematike na Fakulteti za matematiko in fiziko Univerze v Ljubljani ter sodelavec Oddelka za teoretično računalništvo na Inštitutu za matematiko, fiziko in mehaniko v Ljubljani, pa pravi: »Res je presenetljivo, da je rešitev tega temeljnega problema tako preprosta. **Vaughan Pratt** je sicer že leta 1975 pokazal, da za vsako praštevilo obstaja kratek dokaz praštevilskosti, vendar ni bilo jasno, kako bi ta dokaz tudi hitro poiskali. **Gary Miller** pa je leta 1976 objavil algoritem za testiranje praštevilskosti, ki je hiter, če le velja tako imenovana razširjena Riemannova hipoteza. Žal je ta eden od najtežjih nerešenih matematičnih problemov (dokaz Riemannove hipoteze je na primer eden od sedmih problemov, za katerih rešitev je Clayev matematični inštitut iz Bostona v jubilejnem letu 2000 razpisal po milijon ameriških dolarjev nagrade). Prattov in Millerjev rezultat ter še drugi argumenti so kazali, da hiter algoritem za testiranje praštevilskosti najbrž obstaja, vendar smo vsi pričakovali, da bo dolg in zapleten. Navidez težki problemi imajo torej lahko tudi preproste rešitve. Znanstvene rezultate, ki so tako pomembni, da o njih poročajo dnevniki po vsem svetu, pa lahko dosežejo raziskovalci kjerkoli, ne le v vodilnih svetovnih centrih.« ■

Koncept kriptosistema z javnimi ključi



Javno dostopni nabiralnik, ki pa ga lahko odpremo samo z zasebnim ključem.

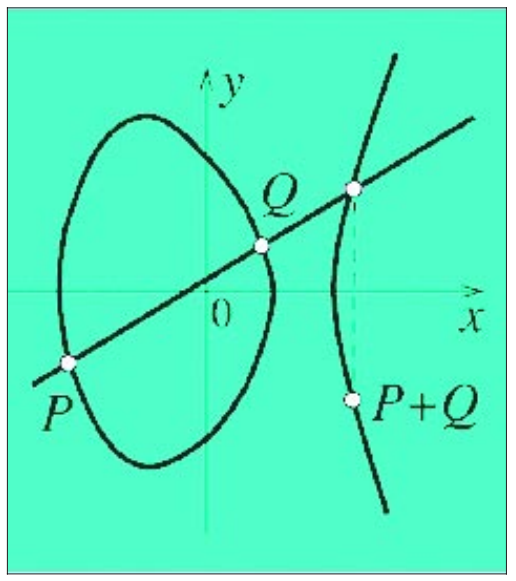
Zgledujmo se po poštnih nabiralnikih. Vsakdo, ki ve, kje je nabiralnik, lahko vanj vrže pošiljko, ne more pa je vzeti ven – to lahko stori le tisti, ki ima ključ nabiralnika. V nasprotju z zasebno (oziroma simetrično) kriptografijo imamo pri javni kriptografiji dva ključa: javnega in zasebnega.

Če želita Anita in Bojan varno komunicirati, objavita svoja javna ključa, zasebna pa zadržita zase. Ko želi Anita poslati sporočilo Bojanu, ga zašifrira z njegovim javnim ključem (t. j. ga vrže v Bojanov nabiralnik), toda samo Bojan ga lahko prebere, saj je edini, ki pozna dešifrirni (zasebni) ključ. Pri javni kriptografiji moramo seveda zahtevati, da iz javnega ključa ne znamo izračunati zasebnega.

Vlogo ključev lahko tudi zamenjamo in dobimo digitalni podpis: če Bojan najprej zašifrira pismo s svojim zasebnim ključem (t. j. ga digitalno podpiše) in objavi dešifrirni ključ, bo vsakdo lahko prebral pismo in se tako prepričal o njegovem izvoru, nihče pa ne bo mogel ponarediti podpisa, saj ima edino Bojan šifrirni ključ. Ko želi Aniti poslati podpisano zasebno sporočilo, ga najprej zašifrira s svojim zasebnim ključem (ga podpiše), nato pa še z Anitinim (šifrirnim) javnim ključem. Anita bo lahko s svojim zasebnim ključem dešifrirala dobljeno sporočilo in nato preverila Bojanov podpis z njegovim javnim dešifrirnim ključem.

Kriptosistemi z eliptičnimi krivuljami – ECC

Množica točk, ki rešijo enačbo $y^2=x^3+ax+b$, imenujemo eliptična krivulja. Točke na krivulji lahko seštevamo po »sekantnem in tangentnem« pravilu, kakor to prikazuje slika.



Skozi točki P in Q potegnemo premico in poiščemo tretje presečišče, ki ga nato še prezrcalimo prek osi x (v primeru podvajanja točke P pa začnemo s tangento v točki P.

Eliptične krivulje se uporabljajo v kriptosistemih z javnimi ključi. Njihova varnost temelji na problemu diskretnega logaritma. Še posebno so privlačne zato, ker so dolžine ključev občutno krajše kot pri RSA-sistemu. 160-bitni ključ v kriptosistemih z eliptičnimi krivuljami zagotavlja enako varnost kot 1024-bitni ključ v RSA-sistemu. To omogoča višje hitrosti. Pomembna prednost je tudi, da za učinkovito izvajanje na pametnih karticah ne potrebujemo posebnih kriptosoprocesorjev, kakor jih na primer potrebuje RSA. Z ECC minimaliziramo programsko kodo, potrebne dolžine ključev in velikost podpisa, zato je za aplikacije na voljo več prostora.

ECC so iz dneva v dan bolje sprejeti kot izbrana metoda za varovanje podatkov v omejenih okoljih in so vključeni v številne standarde (IEEE P1363, ANSI X9, ISO in NIST). Uspešno so jih implementirala razna podjetja po svetu, kot so Siemens, Certicom Corp., Thompson in NeXT Computer.