THE ABEL PRIZE 2021

Bevist utover enhver rimelig tvil

For å få en domfellelse i retten må straffeskyld være bevist utover enhver rimelig tvil. I matematikk er denne graden av bevis vanligvis ikke akseptert som tilstrekkelig. Et matematisk bevis skal være deterministisk og basert på formal logikk. Pythagoras´ læresetning, som sier at kvadratsummen av de to katetene i en rettvinklet trekant er lik kvadratet av hypotenusen, ble bevist allerede i antikken. Bevisene (det er mange av dem) er deterministiske, siden de lar seg reprodusere og gir det samme resultat hver gang.

Utviklingen av elektroniske høyhastighets-datamaskiner utfordret den deterministiske bevis-tradisjonen. Den åpnet også for muligheten til å implementere algoritmer som var utenfor rekkevidde til å gjennomføre for hånd. Nye muligheter åpnet for nye spørsmål. Hva er grensene for det som kan beregnes? Hvor raskt kan vi faktorisere et heltall? Er det mulig å verifisere noe ved å bruke argumenter basert på sannsynlighet?

Det er generelt vanskelig å faktorisere heltall. Hvis du velger et tilfeldig 1000-sifret heltall og har som mål å primtallsfaktorisere det, kan kanskje en datamaskin finne svaret, men det tar tid. Det kan gå både vinter og vår før beregningen er ferdig. På den annen side, hvis du får oppgitt et forslag til en faktorisering, så er det en enkel oppgave for en datamaskin å sjekke om svaret er riktig. Det er mye vanskeligere å finne en nål i en høystakk enn å bekrefte at det faktisk er en nål du har funnet. Dette er essensen av et berømt matematisk problem, det såkalte **P** versus **NP**-problemet, et av de syv millenniumsproblemene i matematikk.

Abelpris-vinnerne László Lovász og Avi Wigderson har hatt ledende roller i utviklingen av det matematiske grunnlaget for teoretisk computer science og dens to store underdisipliner: algoritmedesign og kompleksitetsteori. Både Lovász og Wigderson har gitt vesentlige bidrag til å forstå betydningen av tilfeldigheter i beregninger og i det å utforske hva som er grensene for effektive beregninger.

Lovász-Lenstra-Lenstras reduksjonsalgoritme for gittere

Et eksempel på prisvinnernes bidrag innen algoritmedesign er den såkalte LLL-reduksjonsalgoritmen for gittere, oppkalt etter Lovász og Lenstra-brødrene, Arjen og Hendrik. For et høyere-dimensjonalt heltallsgitter finner denne algoritmen en nesten-ortogonal basis, hvor basisvektorene er ordnet etter lengde. Algoritmen har blitt et viktig verktøy for kryptoanalytikere, og har med suksess knukket flere kryptosystemer. I tillegg var også algoritmen grunnlaget for å motbevise Mertens-formodningen.

Mertens-formodningen ble først formulert av Thomas Joannes Stieltjes i 1885 i et brev til Charles Hermite og igjen på trykk av Franz Mertens i 1897. Formodningen dreier seg om den såkalte Möbius-funksjonen. Möbius-funksjonen $\mu(n)$ er definert for alle positive heltall n og tar verdien -1, 0 eller 1, avhengig av antall primfaktorer i n; hvis n er delelig med et primtallskvadrat, så er verdien 0, mens verdien $\mu(n)$ for et kvadratfritt tall n er -1 hvis n har

et odde antall primfaktorer og +1 hvis antall primfaktorer er et partall. I Mertens-formodningen summeres $\mu(n)$ for alle positive heltall mindre enn et reelt tall x. Vi kaller denne summen $M(x)$. Mertens-formodningen sier at $M(x)$ er mindre enn $\sqrt{x}$ for ethvert positivt tall x.

Mertens-formodningen er et dypt matematisk resultat. Hvis formodningen var sann, ville det bety at Riemann-hypotesen også var sann. Riemann-hypotesen er et annet av de syv milleniums-problemene i matematikk. Dessverre er det kun en enveis sammenhengen mellom de to formodningene, så Mertens-formodningens fall vil ikke ha noen konsekvenser for statusen til Riemann-hypotesen.

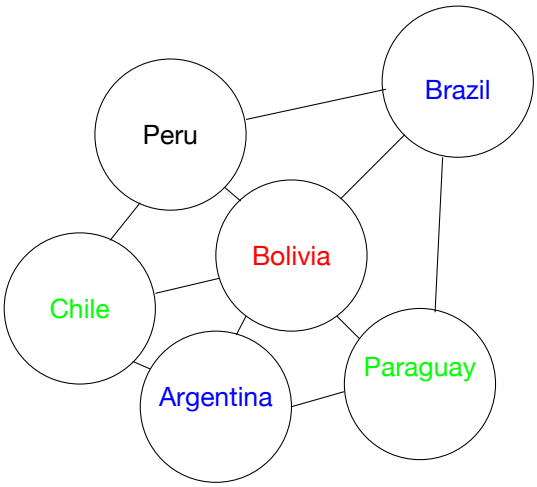
Mertens-formodningen er et godt eksempel på en matematisk formodning som faktisk ikke er riktig, til tross for utallige eksempler som indikerer det motsatte. Etter å ha stått som et åpent spørsmål i nesten et helt århundre, gjorde LLL-reduksjonsalgoritmen det til slutt mulig for Andrew Odlyzko og Herman te Riele å vise at formodningen ikke er riktig.

Null-kunnskapsbevis

Når du skal overføre penger i banken, er autentisering et viktig begrep. Før den kan utføre en transaksjon må banken være sikker på at du er deg, enten du er fysisk til stede eller om du logger deg inn i banken elektronisk. Når du oppgir din personlige kode, må banken med stor sikkerhet være i stand til å bekrefte at du er den virkelige kontoinnehaveren. Av sikkerhetsmessige grunner ønsker imidlertid ikke banken å lagre din personlige kode. Men er det mulig for banken å bekrefte en kode den ikke har lagret? Svaret er faktisk ja, og her er det de såkalte null-kunnskapsbevisene kommer inn.

Null-kunnskapsbevis ble først beskrevet i 1985 av Shafi Goldwasser, Silvio Micali og Charles Rackoff. Noen år senere utviklet Oded Goldreich, Silvio Micali og Abel-prisvinneren Avi Wigderson teorien videre og beskrev blant annet et null-kunnskapsbevis for tre-farge-problemet. Dette var et svært viktig resultat siden eksistensen av et slikt bevis garanterer eksistensen av lignende bevis for ethvert annet problem av samme kompleksitet.

Null-kunnskapsbeviset for tre-farge-problemet kan beskrives som følger: Anta at vi har delt et plant område i sammenhengende regioner, slik som f.eks. på et kart. Vår oppgave er å fargelegge hvert land slik at ingen naboland har samme farge. I 1976 fant Kenneth Appel og Wolfgang Haken det første beviset for at uansett hvordan landene ligger i forhold til hverandre, er det alltid mulig å fullføre fargeleggingen med fire farger. Og fire farger er den nedre grensen for å få dette til. Bolivia og nabolandene er et fint eksempel på dette. Bolivia har 5 naboer, Chile, Argentina, Paraguay, Brasil og Peru. De fem naboene omgir Bolivia fullstendig.



Som vi ser i illustrasjonen, hvor forbindelseslinjene symboliserer felles grenser, er ikke tre farger nok.

Men anta nå at vi har et kart som kan fargelegges med kun tre farger. Er det mulig for Alice å overbevise Bob at dette er tilfellet, uten at hun faktisk viser Bob kartet? Wigderson et al. ga et positivt svar; Alice dekker til kartet slik at Bob bare ser landene og grensene, men ingen farger. Bob velger to naboland og ber Alice vise han fargene. Alice gjør som hun blir bedt om og Bob ser med egne øyne at fargene er forskjellige. Alice dekker til fargene igjen og Bob velger et nytt par naboland for fargesjekking. Igjen viser Alice Bob fargene og Bob er fornøyd med det han ser. Så hvorfor får ikke Bob noen kunnskap om fargene på denne måten? Hemmeligheten er at mellom to farge-avsløringer permuterer Alice de tre fargene. Derfor observere kun Bob at de to nabolandene har forskjellige farger, men hvilke farger landene hadde i utgangspunktet forblir en hemmelighet. Etter å ha gjennomført denne prosedyren et passende antall ganger innser Bob at den eneste muligheten for at Alice kan lykkes i hvert forsøk, er at hun faktisk har klart å fargelegge kartet med bare tre farger.

På denne måten har Alice gitt Bob et null-kunnskapsbevis. Null-kunnskapsbevis baserer seg på sannsynligsbetraktninger, i den forstand at det avgjørende argumentet for Bob er den overveiende sannsynligheten for at Alice har rett. Han godtar Alice's påstand, fordi han finner den bevist utover enhver rimelig tvil.

Denne formen for probabilistisk tilnærming har vist seg å gi en vellykket utvidelse av det matematiske universet, gjennom å bidra med en ny type teknikker og strategier. At den har utvidet vår matematiske kunnskap – er bevist utover enhver rimelig tvil.