THE
ABEL
PRIZE
2016

Det Norske Videnskaps-Akademi
har besluttet å tildele Abelprisen 2016 til

Sir Andrew J. Wiles

Universitetet i Oxford

"for hans bevis av Fermats siste sats via modularitetsformodningen for semistabile elliptiske kurver, som innledet en ny æra i tallteorien."

Tallteori, en gammel og vakker gren av matematikken, beskjeftiger seg med studiet av heltallenes aritmetiske egenskaper. I dets moderne form er emnet nært forbundet med kompleks analyse, algebraisk geometri og representasjonsteori. Tallteoretiske resultater spiller en viktig rolle i vårt daglige liv, gjennom krypterings-algoritmer for kommunikasjon, finansielle transaksjoner og digital sikkerhet.

Fermats siste sats, først formulert av Pierre de Fermat i det 17. århundre, er utsagnet at for n>2 har likningen $x^n + y^n = z^n$ ikke noen løsninger blant positive hele tall. Fermat beviste påstanden for n=4, Leonhard Euler fant et bevis for n=3, og Sophie Germain beviste det første generelle resultatet som gjelder for uendelig mange primtallseksponenter. Ernst Kummers studie av problemet avslørte flere grunnleggende ideer i algebraisk tallteori, så som ideelle tall og det subtile ved entydig faktorisering. Det fullstendige beviset som Andrew Wiles fant, støtter seg på ytterligere tre begreper i tallteori, nemlig elliptiske kurver, modulære former og Galois-representasjoner.

Elliptiske kurver defineres av tredjegradslikninger i to variabler. De er de naturlige definisjonsområdene for de elliptiske funksjonene som ble introdusert av Niels Henrik Abel. Modulære former er usedvanlig symmetriske analytiske funksjoner som er definert på den øvre halvdelen av det komplekse planet, og de faktoriserer naturlig gjennom visse rom som kalles modulære kurver. En elliptisk kurve sies å være modulær dersom den kan parametriseres ved en avbildning fra en av disse modulære kurvene. Modularitetsformodningen, som ble foreslått av Goro Shimura, Yutaka Taniyama og André Weil på 1950- og 60-tallet, hevder at enhver elliptisk kurve definert over de rasjonale tallene, er modulær.

I 1984 knyttet Gerhard Frey en semistabil elliptisk kurve til ethvert tenkt moteksempel til Fermats siste sats, og fremmet en sterk mistanke om at denne elliptiske kurven ikke ville være modulær. Freys ikke-modularitet ble bevist, via Jean-Pierre Serres epsilon-formodning, av Kenneth Ribet i 1986. Dermed ville et bevis av Shimura, Taniyama og Weils modularitetsformodning også utgjøre et bevis av Fermats siste sats. På den tiden ble imidlertid modularitetsformodningen allment ansett å være fullstendig utilgjengelig. Det var derfor et meget overraskende gjennombrudd da Andrew Wiles, i en banebrytende artikkel som ble publisert i 1995, introduserte sin modularitetsløftningsmetode og beviste det semistabile tilfellet av modularitetsformodningen.

Wiles' modularitetsløftningsmetode handler om Galois-symmetriene til punktene av endelig orden i den abelske gruppestrukturen på en elliptisk kurve. Ved å bygge på Barry Mazurs deformasjonsteori for slike Galois-representasjoner klarte Wiles å identifisere et numerisk kriterium, som sikrer at modularitet for punktene av orden p kan løftes til modularitet for punktene av orden en vilkårlig potens av p, der p er et odde primtall. Denne løftede modulariteten er så tilstrekkelig for å bevise at den elliptiske kurven er modulær. Det numeriske kriteriet ble bekreftet i det semistabile tilfellet ved å bruke en viktig følgeartikkel, skrevet i fellesskap med Richard Taylor. Teoremer av Robert Langlands og Jerrold Tunnell viser i mange tilfeller at Galois-representasjonen gitt ved punktene av orden tre, er modulær. Ved en sinnrik overgang fra ett primtall til et annet klarte Wiles å vise at i de gjenværende tilfellene er Galois-representasjonen gitt ved punktene av orden fem, modulær. Dette fullførte hans bevis av modularitetsformodningen, og dermed også av Fermats siste sats.

De nye ideene Wiles introduserte var avgjørende for den utviklingen som fulgte, deriblant beviset i 2001 av det generelle tilfellet av modularitetsformodningen ved Christophe Breuil, Brian Conrad, Fred Diamond og Richard Taylor. Så sent som i 2015 beviste Nuno Freitas, Bao V. Le Hung og Samir Siksek det tilsvarende modularitetsutsagnet over reelle kvadratiske tallkropper. Få resultater har en så rik matematisk historie og et så dramatisk bevis som Fermats siste sats.