THE ABEL PRIZE

Gerd Faltings
Abelprisvinner 2026

Rasjonale løsninger av diofantiske likninger

Uttrykket diofantisk ligning refererer til Diofantos av Alexandria, en hellenistisk matematiker fra det 3. århundre. Diofantos var en pioner innenfor heltallsløsninger til polynomligninger med heltallskoeffisienter, og navnet hans har siden den gang vært knyttet til å finne heltalls- og rasjonale løsninger av slike ligninger.

Diofantos av Alexandria
(foto: famousmathmaticians.net)

Problemet med å finne rasjonale løsninger av polynomligninger går flere hundre år tilbake i tid. Allerede i oldtiden var det kjent at den pytagoreiske ligningen $x^2 + y^2 = z^2$ har uendelig mange heltallsløsninger. Løsningene er fullstendig beskrevet ved formelen

$$x = p^2 - q^2 \quad y = 2pq \quad z = p^2 + q^2$$

for vilkårlige positive heltall p og q.

Pythagoras-ligningen er en kvadratisk ligning, og det faktum at det finnes uendelig mange heltallsløsninger kan sees på som et tegn på den relativt hyppige forekomsten av kvadrater blant heltallene. Å øke graden av ligningen vil generelt føre til et minkende antall rasjonale løsninger. Antallet kan falle fra uendelig til endelig, og kanskje også til null, noe som betyr at for en generell ligning med heltallskoeffisienter finnes det ingen rasjonale løsninger i det hele tatt.

David Hilbert, 1862-1943
(Photo: Wikipedia)

På den internasjonale kongressen for matematikere i Paris i 1900 la den tyske matematikeren David Hilbert fram en liste med 10 uløste problemer i matematikk. Senere publiserte han en utvidet liste som inkluderte 23 problemer, alle ansett som svært innflytelsesrike for matematikken i det 20. århundre. Noen av problemene er fortsatt åpne, noen er løst. Hilbert innleder sine 23 problemer med følgende ord: "Hvem av oss ville ikke med glede løfte på sløret som skjuler framtida; å kaste et blikk på de neste framskrittene i vår vitenskap og på hemmelighetene bak dens utvikling i fremtidige århundrer? Hvilke spesielle mål vil de ledende matematiske sjelene i kommende generasjoner strebe mot? Hvilke nye metoder og nye fakta innen det brede og rike feltet av matematisk tankegang vil de nye århundrene avsløre?"

Et av Hilberts problemer, kjent som Hilberts tiende problem, gjelder løsningene av diofantiske ligninger. "Gitt en diofantisk ligning i et vilkårlig antall ukjente og med rasjonale heltallige koeffisienter: Å utvikle en prosess slik at det ved hjelp av et endelig antall operasjoner kan avgjøres om ligningen har rasjonale løsninger."

Hilbert er ikke opptatt av å finne løsninger på ligningen, spørsmålet hans går mer ut på å avgjøre om det i det hele tatt finnes noen løsninger. Poincaré viste også interesse

for denne typen problemer. I 1901 formulerte han en formodning om rasjonale løsninger av elliptiske kurver, dvs. kurver av grad 3. Hans påstand er at mengden av rasjonale punkter på en elliptisk kurve danner en endelig generert abelsk gruppe, en påstand Mordell skulle bevise rundt tjue år senere.

I mellomtiden publiserte tallteoretikerne flere resultater som dreide seg om løsning av diofantiske ligninger. I 1909 viste den norske matematikeren Axel Thue (blant annet) at ligningen $y^3 - 2x^2 = -1$ bare har endelig mange heltallsløsninger. Det ble senere bevist at ligningen har nøyaktig én løsning, gitt ved $x = 78$ og $y = 23$.

Axel Thue, 1863-1922
(Foto: Wikipedia)

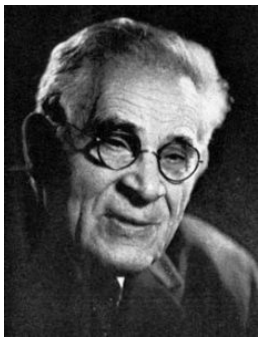
Thues mer generelle resultat er kjent som Thues teorem. Det sier at hvis $f(x,y)$ er et homogent polynom med heltallskoeffisienter, irreduserbart over de rasjonale tallene og av grad ≥ 3, så vil ligningen $f(x,y) = k$ bare ha endelig mange heltallsløsninger for vilkårlig valg av heltallet k.

Mordell viste selv allerede i 1913 at ligningen

$$y^2 = x^3 + k$$

hvor k er et heltall, har bare et endelig antall heltallsløsninger.

Hovedresultatet i Mordell's avhandling fra 1922 er det som senere har blitt kalt Mordell's teorem: Gruppa $E(\mathbb{Q})$ av $\mathbb{Q}$-punkter på en elliptisk kurve E er endelig generert. Dette resultatet kom som et svar på Poincarés spørsmål fra 1901.



Louis Mordell, 1888-1972
(Foto: Universitetet i Manchester)

Mordell's teorem refererer til det faktum at en elliptisk kurve, gitt som løsningsmengden til en 3.gradslikning

$$y^2 = x^3 + px + q$$

har en tilleggsstruktur som en abelsk gruppe. Gruppeloven kalles ofte korde- og tangentregelen, siden konstruksjonen er gitt ved en ren geometrisk oppskrift som involverer korder og tangenter. Mordell viser resultatet ved bruk av den klassiske uendelig nedstignings-metoden. Hvis det er uendelig mange løsninger, kan de alle spores tilbake ved hjelp av korde- og tangent-regelen til kun et endelig antall genererende løsninger. Mordell viser også resultatet som er avgjørende for hans resultat, nemlig at summen av to rasjonale punkter på den elliptiske kurven igjen er et rasjonelt punkt.

Basert på formen på løsningsmengden til en generell 3.gradsligning, blir elliptiske kurver også referert til som kurver av genus 1. Kurver av høyere genus er definert av ligninger av høyere grad, og løsningsmengden blir også mer komplisert.

Mordells formodning, som også ble presentert i artikkelen fra 1922 "On the Rational Solutions of the Indeterminate Equations of the Third and Fourth Degree", sier at mengden av rasjonale punkter på kurver av genus ≥ 2 er endelig. Dette gjelder ikke for elliptiske kurver. Endelig generert er ikke det samme som endelig, fordi rasjonale punkter på kurven kan ha uendelig orden.

Den norske matematikeren Trygve Nagell var elev av Axel Thue. Han fant et kriterium for at et rasjonelt punkt på en elliptisk kurve er av endelig orden. Resultatet er kjent som Nagell-Lutz-teoremet, til ære for Nagell og Elisabeth Lutz. Elisabeth Lutz var en fransk matematiker som oppdaget teoremet uavhengig av Nagell. Nagell-Lutz-teoremet beskriver rasjonale punkter av endelig orden på elliptiske kurver over heltallene: Anta at ligningen

Trygve Nagell, 1895-1988
(Photo: Wikipedia)

$$y^2 = x^3 + px + q, \quad p, q \in \mathbb{Z}$$

definerer en ikke-singulær elliptisk kurve med diskriminant

$$\Delta = 4p^3 + 27q^2 \neq 0$$

Hvis $P = (x,y)$ er et rasjonalt punkt av endelig orden på E, så må x og y være heltall og enten så er $y = 0$, og da har P orden 2, eller så vil y dele Δ, som betyr at også y^2 deler Δ.

La E være en elliptisk kurve gitt ved

$$y^2 = x^3 - 4x + 9, \quad \Delta = -256 + 2187 = 1931$$

Det er lett å se at $P = (2,3)$ er et rasjonalt punkt på E. Tallet 1931 er åpenbart ikke delelig med 3 og punktet P har derfor uendelig orden i henhold til Nagell-Lutz-teoremet.

Et annet eksempel er likningen $y^2 = x^3 - x$ som kun har 4 rasjonale punkter, inkludert den additive identiteten 0 i det uendelig fjerne; $P = (1,0)$, $Q = (-1,0)$, $P + Q = (0,0)$, og de oppfyller $2P = 2Q = 0$, dvs. $E(\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Sammen illustrerer de to eksemplene at det blant alle elliptiske kurver både er kurver med endelig mange rasjonale punkter, såvel som kurver med uendelig mange rasjonale punkter.

Axel Thue og Jean Mordell var begge tallteoretikere. Metodene deres er enten rent aritmetiske eller mer approksimative. Etter Faltings og Wiles har vi innsett at løsningene på tallteoriproblemer ofte kan finnes i andre felt av matematikken enn internt innen tallteori.