Om Stein Johansens forklaring av Trell's bevis for Fermats siste teorem

Harald Hanche-Olsen

2003–03–20

For en bakgrunn til denne lille notisen, se `http://www.math.ntnu.no/~hanche/blog/trell/`.

Stein E. Johansen (SEJ)[1] har forfattet og lagt ut på web en artikkel *Tilbakevisning av et forsøk på kritikk av Erik Trells bevis(er) av Fermats siste teorem.* (For en lenke til dette dokumentet, følg URLen ovenfor.) I det følgende vil jeg anta at leseren har SEJs artikkel for hånden; uten den, er det tvilsomt om dette vil være meningsfylt.

La meg ta en rask gjennomgang av den initielle, ukontroversielle delen av beviset. Sentralt står størrelsen

$$\Delta = Z^n - (Z-\lambda)^n = \sum_{k=1}^{n} \binom{n}{k} (-1)^{k-1} \lambda^k Z^{n-k},$$

eller for $n = 3$

$$\Delta = Z^3 - (Z-\lambda)^3 = 3\lambda Z^2 - 3\lambda^2 Z + \lambda^3.$$

Fermats siste teorem sier som kjent at det ikke finnes positive heltallige løsninger X, Y, Z av

$$X^n + Y^n = Z^n \qquad \text{når } n \geq 3.$$

Siden dette åpenbart impliserer $Y < Z$, kan vi i stedet skrive $Y = Z - \lambda$ der $\lambda > 0$ er et heltall, og skrive Fermats ligning som

$$X^n = Z^n - (Z-\lambda)^n, \quad \text{ekvivalent} \quad X^n = \Delta.$$

I likhet med SEJ skal jeg heretter begrense meg til tilfellet $n = 3$, så vi skriver ligningen ovenfor som

$$X^3 = 3\lambda Z^2 - 3\lambda^2 Z + \lambda^3. \tag{1}$$

På dette stadiet innfører SEJ noe han kaller *standard kuberot-teori.*[2] Jeg er litt usikker på hva han mener med dette. Det jeg *er* sikker på, er at ethvert reelt tall har en éntydig reell kubikkrot. I tillegg (for tall forskjellig fra 0) finnes to komplekse kubikkrøtter, men de er ikke relevante her. SEJ snakker om *rasjonelle* røtter,[3] men siden rasjonale tall er reelle er ikke dette noe problem. Vi skal se senere at det kan se ut som SEJ tror på et sterkere teorem, og *det* er et problem.

SEJ skriver nå:

> Standard kuberot-teori angir da at vi bare har én rasjonell kuberot, altså maksimalt én heltallsrot. Vi ser lett at om vi setter $\lambda = Z$, får vi frem denne eneste heltallsroten (som vi vil benevne "x"). HHO hevder imidlertid at dette ikke er noe bevis for at vi ikke kan få frem ANDRE heltallsrøtter for ANDRE λ enn $\lambda = Z$, og følgelig at dette ikke er noe GENERELT bevis for teoremet. Ved å klargjøre Trells prosedyre, skal vi imidlertid se at denne innvendingen ikke holder.

[1] Trell og Johansen omtaler meg konsistent som «HHO». Jeg finner det derfor ikke unaturlig å bruke en tilsvarende forkortelse.

[2] Jeg har aldri støtt på ordet *kuberot* før. I fortsettelsen kommer jeg til å bruke den vanlige betegnelsen *kubikkrot.*

[3] Jeg følger vanlig terminologi og kaller dem *rasjonale.*

Dette virker som en grei (delvis) formulering av min posisjon. Før vi leser videre, kan vi merke oss at dersom man setter $\lambda = Z$, får man $\Delta = \lambda^3 = Z^3$. Denne har ganske riktig en heltallig kubikkrot, nemlig Z.

Vi blar nå om, og finner SEJs ligning (3), som er min ligning (1). SEJ går nå over til å ta ulike kandidater for X en for en.

Først tar han tilfellet $X = 1$: Min ligning (1) er nå:

$$3\lambda Z^2 - 3\lambda^2 Z + \lambda^3 = 1.$$

Jeg siterer igjen:

> Denne ligningen kan bare ha én verdi av λ som heltallsrot. Vi ser umiddelbart at $\lambda = Z$ tilfredsstiller ligningen.

Her er det to grove feil i rask rekkfølge:

For å ta den siste først, så er det *ikke* slik at $\lambda = Z$ tilfredsstiller ligningen. Setter vi inn $\lambda = Z$ får vi nemlig $Z^3 = 1$, og det holder jo ikke dersom $Z > 1$.

Men kanskje viktigere i sammenhengen er påstanden om at ligningen bare kan ha én heltallsrot λ. Det er rett og slett ikke sant at en tredjegradsligning ikke kan ha mer enn én heltallsrot. Ett eksempel er ligningen

$$\lambda^3 - 4\lambda^2 + 5\lambda - 2 = 0,$$

som har røttene 1 og 2.

For meg ser det ut som det er det SEJ kaller «standard kuberot-teori» som her har tatt spranget fra vanlige kubikkrøtter, altså ligningen $X^3 = a$, som høyst kan ha én reell root, til den generelle tredjegradsligningen, som utmerket vel kan ha inntil tre heltallige røtter. Dette blir aldeles åpenlyst når man ser midt på side 3, i oppsummeringen av beviset:

> 5) Sammenhold resultatet i punkt 4), dvs. heltalls-rot for $\lambda = Z$, med at ingen tredjegrads-ligninger kan ha MER enn en heltalls-rot.

Dette er *feil*, og det hjelper ikke samme hvor mye SEJ senere oppsummerer oppsummeringen ved å skrive

> Men den skisserte 9- trinnsprosedyren er fullt ut logisk legitim, både generelt og i dette spesifikke tilfelle.

Jeg bør kanskje skynde meg å legge til at muligheten $X = 1$ kan elimineres av mye enklere grunner enn den SEJ anfører her, men poenget er at han bruker essensielt det samme argumentet for større X, og det er fremdeles like feil.[4]

Angående min andre innvending (at beviset også virker gyldig for $n = 2$, hvor vi vet at resultatet er feil) har SEJ en tilbakevisning av den og, basert på at kvadratiske ligninger, i motsetning til tredjegradsligninger, *kan* ha mer enn én heltallig rot. Men vi har alt sett at tredjegradsligninger godt kan ha flere heltallige røtter, så dette argumentet er irrelevant.

På side 5 er så SEJ klar til å konkludere:

> Konklusjonen er at så langt er det ikke levert NOEN gyldige vitenskapelige argumenter mot Trells "proof"(og slettes ikke mot hans "re-proof"). Den emotivt-invektive kanonaden mot Trell er altså så langt uten noen vitenskapelig ammunisjon.

Det vil være interessant å se om SEJ fortsatt vil mene dette. Jeg mistenker at svaret er «ja», og at det ikke *kan* finnes argumenter som vil overbevise ham. Og før noen påpeker det for meg, så la meg nevne at denne notisen selvsagt ikke behøver være en tilbakevisning Trells bevis, bare av SEJs utlegning av dette beviset. Kanskje SEJ har forstått det like dårlig som jeg har?

Hva menes forresten med «den emotivt-invektive kanonaden mot Trell»? Hvis det er noen som har grepet til invektiver her, må det da være Trell selv, som enhver som leste debatten i Adresseavisen i januar må ha fått med seg. Bare les hva han skrev i Adresseavisen 29. januar:

[4] Standard ligningsteori forteller oss at om λ er en heltallig løsning til (1) der Z og X er heltall, må λ gå opp i X^3, som vi umiddelbart ser ved å skille ut en faktor λ på høyresiden i (1). Dette kan brukes til å eliminere en del λ-kandidater, men langt fra alle i det generelle tilfellet.

> ... og til det formål har [Baas] sendt ut en av sine løpegutter med en elendig melding i en apokryfisk website fra Ultima Thule, som om den servile poleringen av lederhannens teser var noe annet enn den ynkelige falsifikasjon den i virkeligheten utgjør.

Det er nok jeg som her omtales som en «løpegutt» for professor Baas, og som en som servilt polerer hans (lederhannens!) teser. Jeg frakjennes enhver fri vilje og evne til å tenke selvstendig. Er det rart om jeg blir ørlite grann emosjonell som resultat?

Nåvel. La meg sitere mer fra SEJs artikkel:

> Man kan umiddelbart forundres over hvorfor det er så maktpåliggende å servere slike kanonader i vitenskapens NAVN uten at man har vært i stand til å presentere VITENSKAPELIG gyldige argumenter, verken matematiske eller metamatematiske.

Argumenter har jeg da servert så det skulle holde. Hvorfor er det så maktpåliggende å servere disse kanonader? De fleste av mine kolleger synes jeg kaster bort tiden min på å tilbakevise noe som *alle* matematikere uten unntak skjønner er tøv, og jeg er tildels enig med dem. Men samtidig hører jeg fra flere kanter at det finnes høyt utdannete mennesker, blant dem til og med ingeniører med doktorgrad, som er i tvil. Det skremmer meg faktisk at den kritiske sansen ikke er tilstede i større grad, og dét er hovedgrunnen til at jeg prøver å argumentere så godt jeg kan, med saklige og holdbare argumenter, mot sludderet.

> Emosjoner har sin plass som drivstoff for vitenskapelig virksomhet, men de hører ikke hjemme INNEN den vitenskapelige analyse og argumentasjon. Innen matematikken burde denne skillelinjen være enklere å holde enn i andre disipliner.

Dette må jeg bare si meg enig i. Men det ligger implisitt i sammenhengen at disse ordene er rettet mot meg, og det har jeg vanskelig for å forstå. Ja, matematikk er mitt fag, og jeg *liker* faget mitt. Jeg nyter å se et vakkert bevis, jeg blir irritert over et «stygt» bevis (selv om det er korrekt), men jeg blir direkte arg over å se faget mishandlet. Men jeg klarer utmerket godt å holde emosjonene utenfor en diskusjon om rett eller galt i matematikken, og synes det er direkte fornærmende å bli belært som om jeg ikke skulle være i stand til det eller forstå viktigheten av det.

> Og videre: Er det ikke umiddelbart (altså om vi ser bort fra alt det komplekse strev med å bevise teoremet i den etterfølgende matematikk-historie) større grunn til å TRO på Fermat når han hevdet at han hadde funnet en enkel og elegant løsning, enn å tro at han bløffet eller forregnet seg?

Det er nok liten sjanse for at han *bløffet*. Fermat var i liten grad interessert i å fortelle andre om sine notater, som han gjorde mest for sin egen del. Hvorfor skulle han bløffe for seg selv? Nei, han trodde nok han hadde et bevis. Men alle matematikere har mange ganger i livet konstruert et bevis som viste seg å være feil ved nærmere ettersyn. Hvorfor skulle Fermat være noe unntak?

Det har gjennom tidene vært gjort utallige forsøk på å gjenskape Fermats bevis, enten det var riktig eller galt. Noen spekulasjoner går ut på at metoden kanskje lignet på metoden som kalles «infinite descent», som Fermat brukte med stor suksess for å vise spesialtilfellet $n = 4$ av FLT. Han viste faktisk litt mer: Nemlig at det ikke finnes positive heltallsløsninger x, y, z av

$$x^4 + y^4 = z^2.$$

Ettersom jeg er litt lei av å skrive bare negativt, vil jeg heller bedrive litt *ordentlig* matematikk, og avslutte med å gi en fremstilling av Fermats bevis for denne satsen.

Beviset er basert på en parametrisering av pythagoreiske talltripler x, y, z, altså slike hvor

$$x^2 + y^2 = z^2.$$

Etter å ha dividert bort felles faktorer, kan man anta at x, y, z er relativt primiske (et slikt pythagoreisk trippel kan vi kalle *irredusibelt*). Siden $(2k)^2 = 4k^2$ og $(2k+1)^2 = 4k^2 + 4k + 1$, er alle kvadrattall kongruent med 0 eller 1 modulo 4. Siden x, y, z ikke alle er partall, følger det umiddelbart at z må være odde, og én av x, y må være et partall. La oss si at x er odde og y er partall. Skriv nå om den pythagoreiske ligningen til formen

$$y^2 = z^2 - x^2 = (z+x)(z-x).$$

Men husk at y er et partall, $y = 2\eta$, og x og z er oddetall, så $z+x$ og $z-x$ er partall. Vi skriver istedet

$$\eta^2 = \Big(\frac{z+x}{2}\Big)\Big(\frac{z-x}{2}\Big).$$

Hvis $\frac{1}{2}(z+x)$ og $\frac{1}{2}(z-x)$ hadde en felles faktor, ville denne også være en faktor i $\frac{1}{2}(z+x) + \frac{1}{2}(z-x) = z$ og i $\frac{1}{2}(z+x) - \frac{1}{2}(z-x) = x$. Siden x og z ikke har noen felles faktor, er altså $\frac{1}{2}(z+x)$ og $\frac{1}{2}(z-x)$ innbyrdes primiske. Siden produktet er et kvadrattall, må de da *begge* være kvadrattall. (Tell opp primfaktorer, og bruk aritmetikkens fundamentalsats om entydig primtallsfaktorisering.) Med andre ord:

$$z+x = 2s^2, \quad z-x = 2t^2$$

for naturlige s og t, som etter litt regning gir

$$x = s^2 - t^2, \quad y = 2st, \quad z = s^2 + t^2.$$

Her er s og t naturlige tall, og det følger av utledningen ovenfor at de er innbyrdes primiske. Vi har vist at *alle irredusible pythagoreiske talltripler kan skrives på formen ovenfor* (med det forbehold at vi kanskje må bytte om på x og y, slik at x blir odde og y blir partall).

La oss nå returnere til ligningen

$$x^4 + y^4 = z^2.$$

Vi kan igjen dividere bort felles primfaktorer, slik at x, y, z er relativt primiske. Ligningen sier nå at x^2, y^2, z danner et irredusibelt pythagoreisk trippel, slik at vi kan skrive

$$x^2 = s^2 - t^2, \quad y^2 = 2st, \quad z = s^2 + t^2, \qquad s,\ t \text{ innbyrdes primiske naturlige tall}$$

(etter eventuelt å ha byttet om x og y). Igjen, siden kvadratet av et partall er kongruent med 0 modulo 4, mens kvadratet av et oddetall er kongruent med 1 modulo 4, må s være odde, mens t er et partall (siden x er odde). Nå har vi av det ovenfor $x^2 + t^2 = s^2$, og x, t, s danner et irredusibelt pythagoreisk trippel, så vi kan skrive

$$x = a^2 - b^2, \quad t = 2ab, \quad s = a^2 + b^2, \qquad a,\ b \text{ innbyrdes primiske naturlige tall}$$

På den annen side, siden s og $2t$ er innbyrdes primiske viser faktoriseringen $y^2 = 2st$ at s og $2t$ begge er kvadrattall, la oss si

$$s = u^2, \quad t = 2v^2.$$

I linjene over finner vi to uttrykk for t, som gir $ab = v^2$, slik at a og b hver må være et kvadrattall, la oss si

$$a = \alpha^2, \quad b = \beta^2.$$

Vi finner nå

$$\alpha^4 + \beta^4 = a^2 + b^2 = s = u^2,$$

så vi har funnet en *ny* løsning av $x^4 + y^4 = z^2$ der z er erstattet med $u < z$. Men da kan vi gjøre det samme med den nye løsningen, og finne nye løsninger med stadig mindre z. Dette kan ikke fortsette i det uendelige, og det er en motsigelse som avslutter beviset.