



Sir Andrew John Wiles,
Abelprisvinner 2016



FERMATS SISTE TEOREM FOR $n = 4$

Den viktigste konsekvensen av modularitetsteoremet er beviset for Fermats siste teorem (forkortet FLT). Selv om Fermat påsto at han hadde funnet et praktfullt bevis for påstanden, er det ikke noen grunn til å tro at dette stemmer. Det vi vet er at Fermat hadde et bevis for teoremet for tilfellet $n = 4$, ved å bruke sin bevismetode omtalt som "infinite descent".



Diofantus av Alexandria

Det enkleste beviset for spesialtilfellene av FLT finner vi for $n = 4$. Det bruker på en smart måte en egenskap ved de positive heltallene kalt Diofants teorem, oppkalt etter Diofantus av Alexandria (levde mellom 200 og 300). Teoremet gir en presis beskrivelse av de såkalte primitive pytagoreiske triplene, dvs. tripler (x, y, z) av positive heltall, uten felles faktor og som tilfredsstiller den pytagoreiske likningen $x^2 + y^2 = z^2$.

Diofants Teorem. *La x, y, z være positive*

heltall uten felles faktor og slik at

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

Da kan vi finne positive heltall $p > q$ uten felles faktor, slik at

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

Vi skal bruke dette resultatet til å bevise at likningen

$$x^4 + y^4 = u^2$$

ikke har noen positive heltallsløsninger. Dette er et sterkere resultat enn FLT for $n = 4$, ved å sette $u = z^2$.

Anta at likningen over har minst én løsning, og betrakt løsningen som har den minste u . Vi observerer først at x, y, u ikke kan ha noen felles faktor. Hvis de hadde hatt det kunne vi faktorisere ut denne, med en ny løsning med en mindre u som resultat.

Videre observerer vi at likningen kan skrives

$$(x^2)^2 + (y^2)^2 = u^2$$

og etter Diofants teorem vet vi at vi kan finne heltall p, q uten felles faktor slik at

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

En annen observasjon er at ethvert kvadrattall har rest 0 eller 1 når vi deler med 4. Den eneste muligheten for å få til dette er at p er et oddetall og q er et partall. Vi skriver $q = 2c$ og får $y^2 = 2pq = 4pc$, eller $(\frac{y}{2})^2 = pc$. Den neste observasjonen er at p og c er kvadrattall. Grunnen til dette er at siden p og q er



Sir Andrew John Wiles, Abelprisvinner 2016



innbyrdes primiske så er også p og c innbyrdes primiske. Lar vi $\frac{y}{2} = p_1 p_2 \cdots p_k$ være primfaktoriseringen til $y/2$ så får vi

$$pc = \left(\frac{y}{2}\right)^2 = p_1^2 p_2^2 \cdots p_k^2.$$

Men p and c har ingen felles faktor og for hver p_i så er enten p_i^2 faktor i p eller så deler ikke p_i tallet p i det hele tatt. Det følger at p og c er kvadrattall. Dermed kan vi skrive $p = d^2, c = f^2$. Ved å bruke $x^2 = p^2 - q^2 = (d^2)^2 - (2c)^2 = (d^2)^2 - (2f^2)^2$, ser vi at

$$x^2 + (2f^2)^2 = (d^2)^2.$$

Det er relativt enkelt å se at $x, 2f^2$ og d^2 ikke har noen felles faktor, og ved å bruke Diofantus teorem en gang til ser vi at

$$x = l^2 - m^2, \quad 2f^2 = 2lm, \quad d^2 = l^2 + m^2,$$

hvor l og m er innbyrdes primiske. Vi bruker den samme teknikken som vi har brukt over på $f^2 = lm$, og det følger at l og m er kvadrater, dvs. $l = r^2, m = s^2$. Vi får at

$$r^4 + s^4 = l^2 + m^2 = d^2$$

Dermed har vi funnet en ny løsning av den opprinnelige likningen $x^4 + y^4 = u^2$, med høyreside $d < u$. Vår innledende antagelse var at u var den minste løsningen. En antagelse som leder til en motsigelse kan ikke være sann, med andre ord har vi bevist at det ikke kan finnes noen heltallsløsning av Fermats likning

$$x^4 + y^4 = u^2$$



1621-utgaven av
Diofantus verk *Arithmetica*.

Diofantus kalles ofte
algebraens far.