Andrew Wiles, modularitetsformodningen og Fermats siste sats

John Rognes

Universitetet i Oslo

Hamar, 15. september 2016

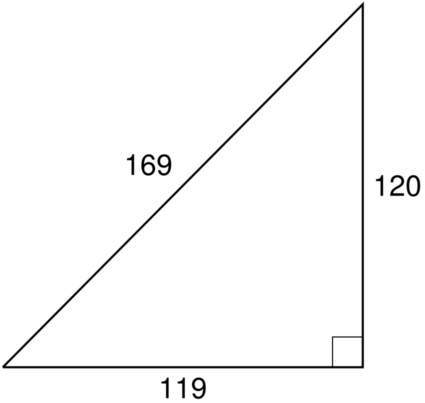
Andrew Wiles

Det Norske Videnskaps-Akademi har besluttet å tildele Abelprisen for 2016 til **Sir Andrew J. Wiles**, Universitetet i Oxford,

for hans oppsiktsvekkende bevis av Fermats siste sats, ved hjelp av modularitetsformodningen for semistabile elliptiske kurver, noe som innledet en helt ny æra innen tallteorien.

Plimpton 322 (fra Babylon, ca. 1800 f.Kr.)

$$119^2 + 120^2 = 169^2$$



Den første linjen

Hele tall a, b, c med

$$a^2 + b^2 = c^2$$

kalles pytagoreiske tripler.

(Vi kan anta at a, b, c er relativt primiske, og at a er odde.)

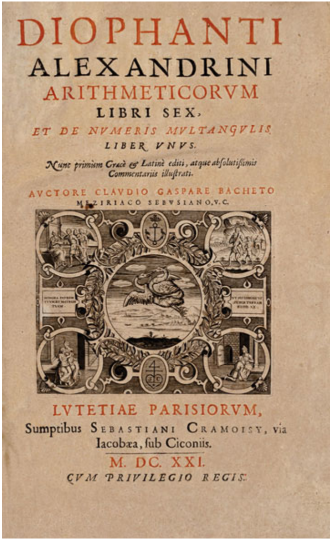
Teorem (Euklid)

Ethvert slikt trippel kan skrives på formen

$$a = p^2 - q^2 \qquad b = 2pq \qquad c = p^2 + q^2$$

for hele tall p, q.

Pierre de Fermat (1601–1665)



DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.

Nunc primùm Græcè & Latinè editi, atque abſolutiſſimis Commentariis illuſtrati.

AVCTORE CLAVDIO GASPARE BACHETO MEZIRIACO SEBVSIANO, V.C.

LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, ſub Ciconiis.

M. DC. XXI.

CVM PRIVILEGIO REGIS.

Diofants *Arithmetica*, i latinsk oversettelse (1621)

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto à 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

ΤΟΝ ἐπιταχθέντα τετράγωνον διελεῖν εἰς δύο τετραγώνους. ἐπιτετάχθω δὴ τὸν ιϛ διελεῖν εἰς δύο τετραγώνους. καὶ τετάχθω ὁ πρῶτος δυνάμεως μιᾶς. δεήσει ἄρα μονάδας ιϛ λεῖψει δυνάμεως μιᾶς ἴσας εἶναι τετραγώνῳ. πλάσσω τὸν τετράγωνον ἀπὸ ςς. ὅσων δή ποτε λεῖψει τοσούτων μο ὅσων ἐστὶν ἡ τῶν ιϛ μο πλευρά. ἔστω ςς β λεῖψει μο δ. αὐτὸς ἄρα ὁ τετράγωνος ἔσται δυνάμεων δ μο ιϛ λεῖψει ςς ιϛ. ταῦτα ἴσα μονάσι ιϛ λεῖψει δυνάμεως μιᾶς. κοινὴ προσκείσθω ἡ λεῖψις, καὶ ἀπὸ ὁμοίων ὅμοια. δυνάμεις ἄρα ε ἴσαι ἀριθμοῖς ιϛ. καὶ γίνεται ὁ ἀριθμὸς ιϛ πέμπτων. ἔσται ὁ μὲν σνϛ εἰκοστοπέμπτων. ὁ δὲ ρμδ εἰκοστοπέμπτων, καὶ οἱ δύο συντεθέντες ποιοῦσι υ εἰκοστόπεμπτα, ἤτοι μονάδας ιϛ. καὶ ἔστιν ἑκάτερος τετράγωνος.

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

. . . cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Fermats påstand:

Det finnes ingen naturlige tall a, b, c og $n > 2$, slik at

$$a^n + b^n = c^n \,.$$

Bevis?

Dette var den siste av Fermats påstander som forble ubevist—derfor “Fermats siste sats”.

Hvis $n = pm$ kan vi skrive om likningen som

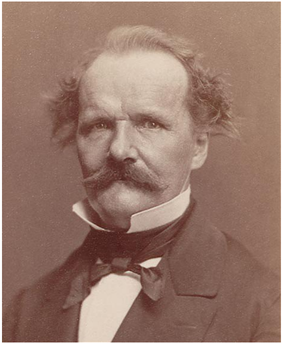
$$(a^m)^p + (b^m)^p = (c^m)^p$$

så det er tilstrekkelig å betrakte tilfellene

- $n = 4$, og
- $n = p$ et vilkårlig odde primtall.

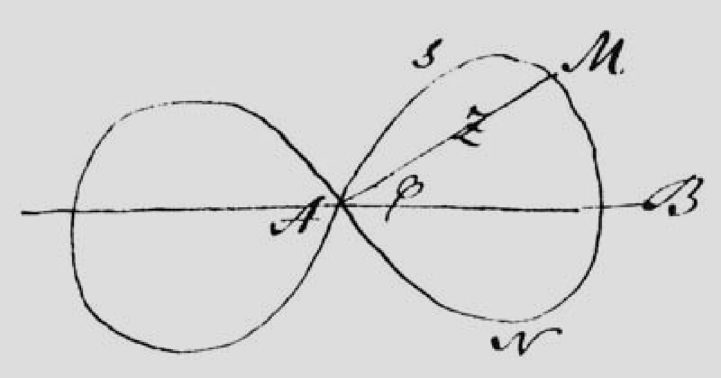
Fermat kunne bevise tilfellet $n = 4$.

Sophie Germain (1776–1831)



Ernst Kummer (1810–1893)

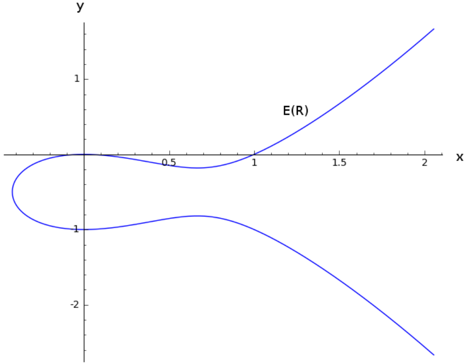
- Innen 1993 var Fermats påstand bevist for alle odde primtall $p < 4.000.000$.
- Uendelig mange tilfeller stod igjen.



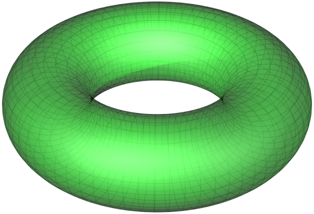
Niels Henrik Abels tegning av en lemniskate

Den “første elliptiske kurven i naturen” er gitt ved likningen

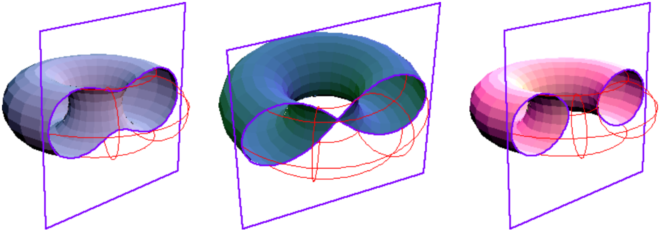
$$E\colon\, y^2 + y = x^3 - x^2\,.$$



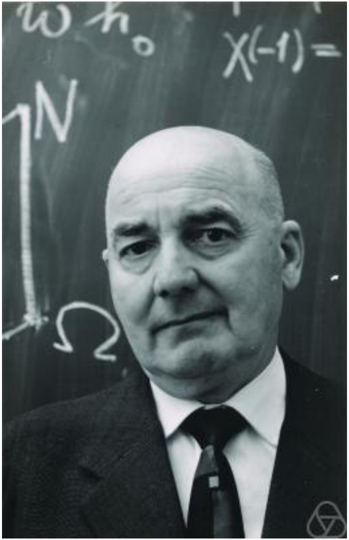
Reell løsningsmengde $E(\mathbb{R})$ med (x, y) i $\mathbb{R}^2 \subset P^2(\mathbb{R})$



Kompleks løsningsmengde $E(\mathbb{C})$ med (x, y) i $\mathbb{C}^2 \subset P^2(\mathbb{C})$



Tre ulike tverrsnitt



Helmut Hasse (1898–1979)

For hvert primtall ℓ gjør sum og produkt modulo ℓ mengden

$$\mathbb{F}_\ell = \mathbb{Z}/(\ell) = \{0, 1, \ldots, \ell - 1\}$$

til en kropp, dvs. et tallsystem med liknende egenskaper som $\mathbb{R}$ og $\mathbb{C}$.

Eksempel: $\mathbb{F}_3 = \{0, 1, 2\}$ har følgende addisjons- og multiplikasjonstabell (modulo 3).

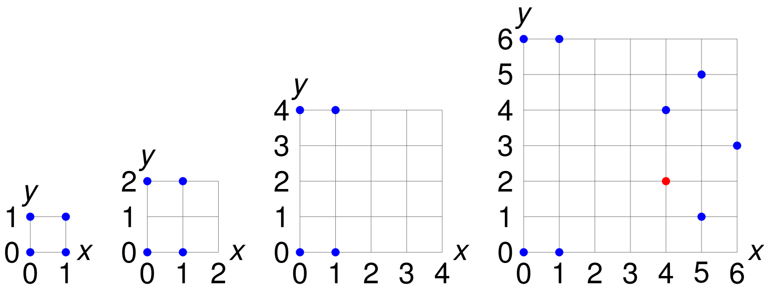
+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Betrakt løsningene (x, y) i $(\mathbb{F}_\ell)^2$ til likningen

$$y^2 + y \equiv x^3 - x^2 \mod \ell\,.$$

Eksempel: $2^2 + 2 = 6 \equiv 48 = 4^3 - 4^2 \mod 7$ så $(4, 2) \in E(\mathbb{F}_7)$.



Modulær løsningsmengde $E(\mathbb{F}_\ell)$ i $\mathbb{F}_\ell^2 \subset P^2(\mathbb{F}_\ell)$ for $\ell = 2, 3, 5, 7$

La

$$\#E(\mathbb{F}_\ell) = \text{antallet punkter i } E(\mathbb{F}_\ell)$$

og definer heltallet a_ℓ ved

$$a_\ell = (\ell + 1) - \#E(\mathbb{F}_\ell)\,.$$

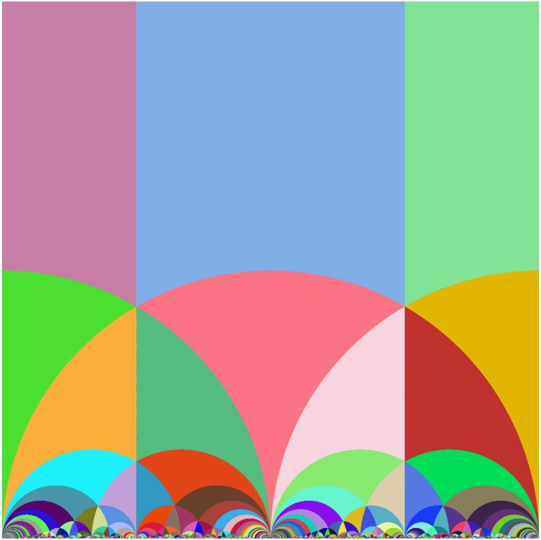
ℓ	2	3	5	7	...
$\#E(\mathbb{F}_\ell)$	5	5	5	10	...
a_ℓ	-2	-1	+1	-2	...

Tallene a_ℓ for $y^2 + y = x^3 - x^2$

Følgen av tall

$$a_\ell = (\ell + 1) - \#E(\mathbb{F}_\ell)$$

husker hvor mange punkter den elliptiske kurven E har, med koordinater i $\mathbb{F}_\ell$, for hvert primtall ℓ.



Symmetrier i det øvre halvplanet $\mathbb{H}$ (av T. Womack)

Gruppen av heltallsmatriser $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ med $ad - bc = 1$ virker som hyperbolske symmetrier på det øvre halvplanet

$$\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{im}(z) > 0\}$$

ved formelen

$$z \longmapsto \frac{az + b}{cz + d}\,.$$

Hver ensfarget trekant sendes til hver annen slik trekant ved en av disse symmetriene.

En modulær form $f(z)$ er en kompleks funksjon

$$\begin{aligned} f \colon \mathbb{H} &\longrightarrow \mathbb{C} \\ z &\longmapsto f(z) \end{aligned}$$

som respekterer (mange av) de hyperbolske symmetriene.

Eksempel: La

$$F(q) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2$$

for $|q| < 1$, og la $f(z) = F(q)$ for $\mathrm{im}(z) > 0$, der $q = e^{2\pi iz}$.

Da er

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z)$$

for enhver heltallsmatrise $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ med $ad - bc = 1$ og $c \equiv 0$ mod 11.

- $f(z)$ er en modulær form av vekt 2 og nivå 11.

Potensrekken

$$F(q) = \sum_{n=1}^{\infty} b_n q^n$$

kan skrives som en Fourier-rekke

$$f(z) = \sum_{n=1}^{\infty} b_n e^{2\pi i n z} .$$

Tallene $(b_n)_n$ er Fourier-koeffisientene til den modulære formen.

Martin Eichler (1912–1992)

$$F(q) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 = \sum_{n=1}^{\infty} b_n q^n$$
$$= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - \dots$$

er den “første modulære formen av vekt 2 i naturen”.

Husk tabellen med antallet punkter med koordinater i $\mathbb{F}_\ell$ for den elliptiske kurven $E\colon\ y^2 + y = x^3 - x$:

ℓ	2	3	5	7	$\dots$
$\#E(\mathbb{F}_\ell)$	5	5	5	10	$\dots$
a_ℓ	-2	-1	+1	-2	$\dots$

$$F(q) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 = \sum_{n=1}^{\infty} b_n q^n$$
$$= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - \dots$$

er den “første modulære formen av vekt 2 i naturen”.

Husk tabellen med antallet punkter med koordinater i $\mathbb{F}_\ell$ for den elliptiske kurven $E\colon\ y^2 + y = x^3 - x$:

ℓ	2	3	5	7	...
$\#E(\mathbb{F}_\ell)$	5	5	5	10	...
a_ℓ	-2	-1	$+1$	-2	...

Teorem (Eichler (1954))

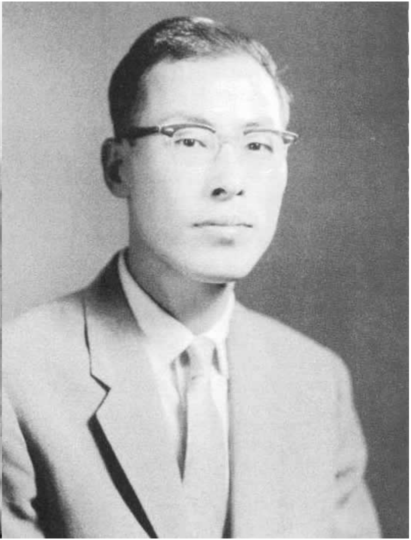
For den "første" elliptiske kurven $E\colon\ y^2 + y = x^3 - x^2$ *og den "første" modulære formen* $f(z)$ *av vekt* 2*, holder likheten*

$$a_\ell = b_\ell$$

for hvert primtall ℓ*.*

- Vi sier at den elliptiske kurven E er modulær.

Yutaka Taniyama (1927–1958)



Goro Shimura

Formodning (Taniyama (1955), Shimura)

For enhver elliptisk kurve

$$E\colon\, y^2 + \alpha_1 xy + \alpha_3 y = x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6\,,$$

med $\alpha_1, \ldots, \alpha_6 \in \mathbb{Q}$ *rasjonale tall, finnes det en modulær form* $f(z)$ *av vekt* 2*, slik at*

$$a_\ell = b_\ell$$

for (nesten) alle primtall ℓ*.*

- Telling av punkter på kurven gir samme tallfølge som Fourier-koeffisientene til en modulær form.

André Weil (1906–1998) [med Atle Selberg (1917–2007)]

Formodning (Hasse–Weil (1967))

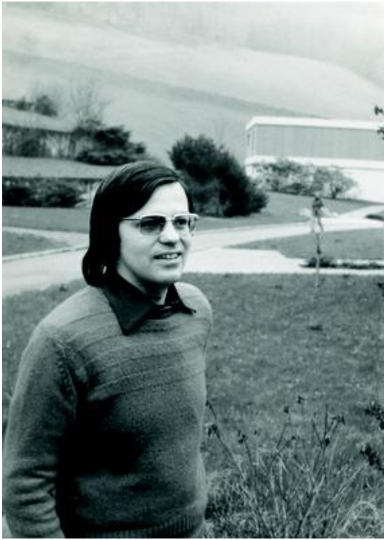
For enhver elliptisk kurve E definert over $\mathbb{Q}$, med konduktør N, finnes det en modulær form $f(z)$ av vekt 2 og nivå N, slik at

$$a_\ell = b_\ell$$

for alle primtall ℓ som ikke deler N.

Ob die Dinge immer, d. h. für jede über $\mathbb{Q}$ definierte Kurve C, sich so verhalten, scheint im Moment noch problematisch zu sein und mag dem interessierten Leser als Übungsaufgabe empfohlen werden.

André Weil (1966)



Gerhard Frey

Konstruksjon (Frey, 1984)

La $p \geq 5$. En løsning

$$a^p + b^p = c^p$$

til Fermats likning gir opphav til en semistabil elliptisk kurve

$$E\colon\ y^2 = x(x - a^p)(x + b^p)$$

med "usedvanlige egenskaper".

- Kurven E er ramifisert over 2, og flat over p, men ellers uramifisert.

Ken Ribet

Teorem (Ribet, 1986)

De "usedvanlige egenskapene" gjør at Frey-kurven ikke er modulær.

- Kurven E ville svare til en kuspidal modulær form $f(z)$ av vekt 2 og nivå 2, og det finnes ingen slike.

Andrew Wiles, 23. juni 1993

Teorem (Wiles, 1994)

Enhver semistabil elliptisk kurve definert over $\mathbb{Q}$ *er modulær.*

- Modularitetsformodningen til Taniyama, Shimura og Weil holder i det semistabile tilfellet.
- Dette kalles nå Wiles' modularitetsteorem.

Andrew Wiles, 23. juni 1993

Bevis av Fermats siste sats:

- Anta det finnes en løsning $a^p + b^p = c^p$ til Fermats likning, for $p \geq 5$.

Bevis av Fermats siste sats:

- Anta det finnes en løsning $a^p + b^p = c^p$ til Fermats likning, for $p \geq 5$.
- Frey (1984): Den hypotetiske løsningen gir opphav til en elliptisk kurve $y^2 = x(x - a^p)(x + b^p)$ med "usedvanlige egenskaper".

Bevis av Fermats siste sats:

- Anta det finnes en løsning $a^p + b^p = c^p$ til Fermats likning, for $p \geq 5$.
- Frey (1984): Den hypotetiske løsningen gir opphav til en elliptisk kurve $y^2 = x(x - a^p)(x + b^p)$ med "usedvanlige egenskaper".
- Ribet (1986): De "usedvanlige egenskapene" gjør at Frey-kurven ikke er modulær.

Bevis av Fermats siste sats:

- Anta det finnes en løsning $a^p + b^p = c^p$ til Fermats likning, for $p \geq 5$.
- Frey (1984): Den hypotetiske løsningen gir opphav til en elliptisk kurve $y^2 = x(x - a^p)(x + b^p)$ med "usedvanlige egenskaper".
- Ribet (1986): De "usedvanlige egenskapene" gjør at Frey-kurven ikke er modulær.
- Wiles (1994): Enhver elliptisk kurve er modulær.

Bevis av Fermats siste sats:

- Anta det finnes en løsning $a^p + b^p = c^p$ til Fermats likning, for $p \geq 5$.
- Frey (1984): Den hypotetiske løsningen gir opphav til en elliptisk kurve $y^2 = x(x - a^p)(x + b^p)$ med “usedvanlige egenskaper”.
- Ribet (1986): De “usedvanlige egenskapene” gjør at Frey-kurven ikke er modulær.
- Wiles (1994): Enhver elliptisk kurve er modulær.
- Dette er en selvmotsigelse.

Bevis av Fermats siste sats:

- Anta det finnes en løsning $a^p + b^p = c^p$ til Fermats likning, for $p \geq 5$.
- Frey (1984): Den hypotetiske løsningen gir opphav til en elliptisk kurve $y^2 = x(x - a^p)(x + b^p)$ med "usedvanlige egenskaper".
- Ribet (1986): De "usedvanlige egenskapene" gjør at Frey-kurven ikke er modulær.
- Wiles (1994): Enhver elliptisk kurve er modulær.
- Dette er en selvmotsigelse.
- Altså finnes det ingen løsning til Fermats likning!

Andrew Wiles

Bevis av Wiles' modularitetsteorem:

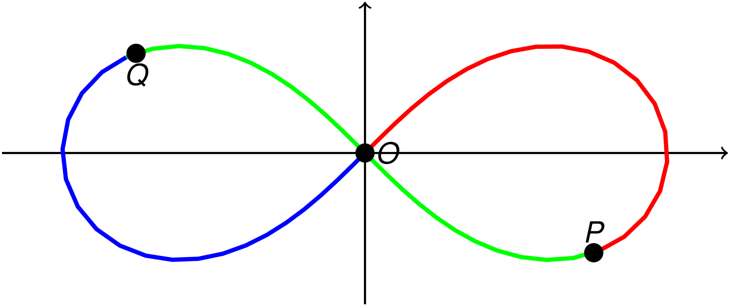
- Wiles oversetter spørsmålet om modularitet for en elliptisk kurve E til et spørsmål om modularitet for en p-adisk Galois-representasjon

$$\rho_p \colon G_{\bar{\mathbb{Q}}} \longrightarrow GL_2(\mathbb{Z}_p)\,.$$

- Reduksjonen

$$\bar{\rho}_p \colon G_{\bar{\mathbb{Q}}} \longrightarrow GL_2(\mathbb{Z}/p)$$

  uttrykker virkningen av Galois-substitusjonene $\sigma \in G_{\bar{\mathbb{Q}}}$ på gruppen $E[p] \cong \mathbb{Z}/(p) \times \mathbb{Z}/(p)$ av p-torsjonspunkter på kurven E.



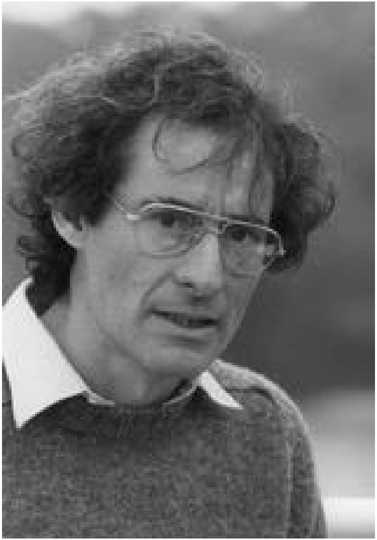
3-torsjonspunkter på lemniskaten (reellt bilde)

Wiles utvikler en løftningsteknikk for modularitet:

Teorem (Wiles, 1994)

Dersom $\bar{\rho}$ er modulær og irredusibel, så er ρ modulær.

- ρ kalles en løftning av $\bar{\rho}$.
- Beviset bruker Mazurs deformasjonsteori for Galois-representasjoner.



Barry Mazur

Teorem (Mazur, 1978)

$\bar{\rho}_p$ er irredusibel for $p = 3$ eller $p = 5$.

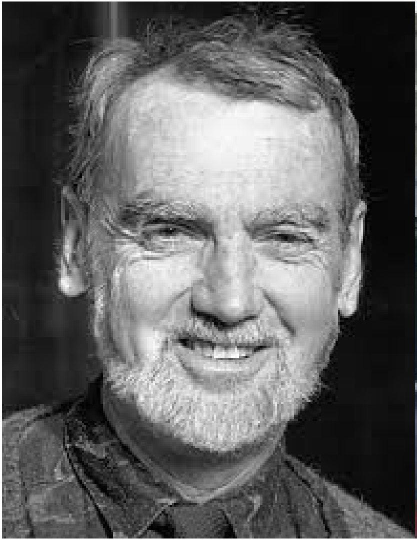
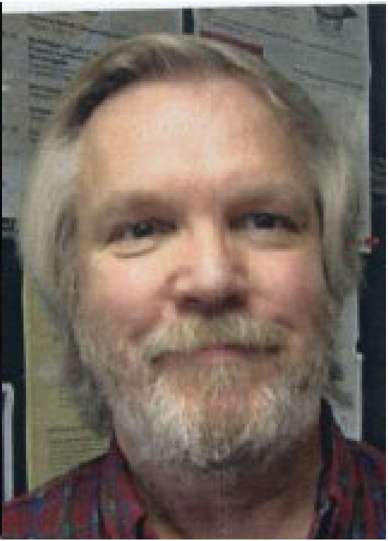
Teorem (Langlands–Tunnell, 1980/81)

Dersom $\bar{\rho}_3$ er irredusibel, så er $\bar{\rho}_3$ modulær.

Teorem (Wiles, 1993)

Dersom $\bar{\rho}_3$ er redusibel, så er $\bar{\rho}_5$ modulær.

Altså er ρ_p modulær for $p = 3$ eller $p = 5$, så E er modulær.
Q.E.D.

Robert Langlands Jerrold Tunnell

Ernst S. Selmer

Ernst Selmer (1920–2006)

Bevis av Wiles' løftningsteorem bygger på en beregning av ordenen til en såkalt Selmer-gruppe.

- Wiles' opprinnelige bevis for dette (fra 1993) inneholdt en feil.
- Et korrekt bevis ble funnet i 1994 av Taylor og Wiles.

Richard Taylor

Goro Shimura