Fermat, Taniyama–Shimura–Weil and Andrew Wiles, Part I

John Rognes

University of Oslo, Norway

May 13th 2016

The Norwegian Academy of Science and Letters has decided to award the Abel Prize for 2016 to **Sir Andrew J. Wiles**, University of Oxford

for his stunning proof of Fermat’s Last Theorem by way of the modularity conjecture for semistable elliptic curves, opening a new era in number theory.

Sir Andrew J. Wiles

Sketch proof of Fermat's Last Theorem:

- Frey (1984): A solution

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

  to Fermat's equation gives an elliptic curve

$$y^2 = x(x - a^p)(x + b^p)\,.$$

- Ribet (1986): The Frey curve does not come from a modular form.
- Wiles (1994): Every elliptic curve comes from a modular form.
- Hence no solution to Fermat's equation exists.

Point counts and Fourier expansions:

$$\begin{tikzcd}
\text{Elliptic curve} \arrow[dr, "\text{Hasse–Witt}"] & \\
& L\text{-function} \\
\text{Modular form} \arrow[ur, "\text{Mellin}"'] &
\end{tikzcd}$$

Modularity:

$$\begin{tikzcd}
\text{Elliptic curve} \arrow[dd, dashed, "?"'] \arrow[dr] & \\
{} \arrow[r, phantom, "\circ"] & L\text{-function} \\
\text{Modular form} \arrow[ur] &
\end{tikzcd}$$

Wiles' Modularity Theorem:

$$\begin{tikzcd}
\text{Semistable elliptic curve defined over } \mathbb{Q} \arrow[dd, "\text{Wiles}"'] \arrow[dr] & \\
\arrow[r, phantom, "\circ"] & L\text{-function} \\
\text{Weight 2 modular form} \arrow[ur] &
\end{tikzcd}$$

Wiles' Modularity Theorem:

$$\begin{tikzcd}
\text{Semistable elliptic curve over } \mathbb{Q} \text{ of conductor } N \arrow[d, "\text{Wiles}"'] \arrow[dr] \arrow[dr, phantom, "\circ"] & \\
\text{Weight 2 modular form of level } N \arrow[r] & L\text{-function}
\end{tikzcd}$$

Frey Curve (and a special case of Wiles' theorem):

$$\begin{tikzcd}
\text{Solution to Fermat's equation} \arrow[d, "\text{Frey}"'] & \\
\begin{array}{c}\text{Semistable elliptic curve} \\ \text{over } \mathbb{Q} \text{ with peculiar properties}\end{array} \arrow[dd, "\text{Wiles}"'] \arrow[dr] & \\
{} \arrow[r, phantom, "\circ"] & L\text{-function} \\
\begin{array}{c}\text{Weight 2 modular form} \\ \text{with peculiar properties}\end{array} \arrow[ur] &
\end{tikzcd}$$

(A special case of) Ribet's theorem:

$$
\begin{tikzcd}
\text{Solution to Fermat's equation} \arrow[d, "\text{Frey}"'] & \\
\text{Semistable elliptic curve over } \mathbb{Q} \text{ with peculiar properties} \arrow[dd, "\text{Wiles}"'] \arrow[dr] & \\
{} \arrow[r, phantom, "\circ"] & L\text{-function} \\
\text{Weight 2 modular form with peculiar properties} \arrow[ur] & \\
\text{Weight 2 modular form of level 2} \arrow[u, "\text{Ribet}"'] &
\end{tikzcd}
$$

Contradiction:

$$
\begin{tikzcd}
\text{Solution to Fermat's equation} \arrow[d, "\text{Frey}"'] & & \\
\begin{array}{c}\text{Semistable elliptic curve}\\ \text{over } \mathbb{Q} \text{ with peculiar properties}\end{array} \arrow[dd, "\text{Wiles}"'] \arrow[drr] & & \\
 & \circ & L\text{-function} \\
\begin{array}{c}\text{Weight 2 modular form}\\ \text{with peculiar properties}\end{array} \arrow[urr] & & \\
\text{Weight 2 modular form of level 2} \arrow[u, "\text{Ribet}"] & & \text{Does not exist} \arrow[ll]
\end{tikzcd}
$$

Blaise Pascal (1623–1662)

Je n’ai fait celle-ci plus longue que parce
que je n’ai pas eu le loisir de la faire plus courte.

Blaise Pascal, Provincial Letters (1656)

(I would have written a shorter letter,
but I did not have the time.)

Perhaps I could best describe my experience of doing mathematics in terms of entering a dark mansion. You go into the first room and it's dark, completely dark. You stumble around, bumping into the furniture. Gradually, you learn where each piece of furniture is. And finally, after six months or so, you find the light switch and turn it on. Suddenly, it's all illuminated and you can see exactly where you were. Then you enter the next dark room . . .

Andrew Wiles (ca. 1994)

Fermat’s equation

Johann Wolfgang von Goethe (by J. H. Tischbein)

Wer nicht von dreitausend Jahren
sich weiß Rechenschaft zu geben,
bleib im Dunkeln unerfahren,
mag von Tag zu Tage leben.

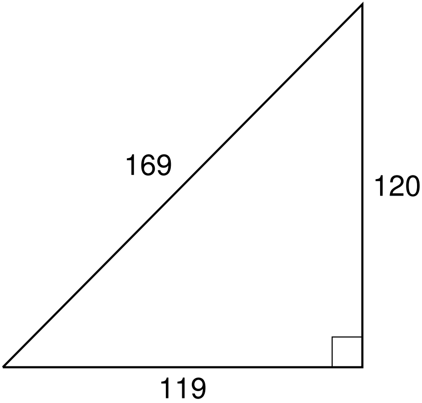
Goethe, West-östlicher Divan (1819)

Den som ikke kan føre sitt regnskap
over tre tusen år,
lever bare fra hånd til munn.

Norsk oversettelse: Jostein Gaarder (1991)

Plimpton 322 (from Babylon, ca. 1800 BC)

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



The first entry

Integers a, b, c with

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

are called Pythagorean triples.

(May assume a, b, c relatively prime, and a odd.)

Theorem (Euclid)

Each such triple appears in the form

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

for integers p, q.

Geometric proof:

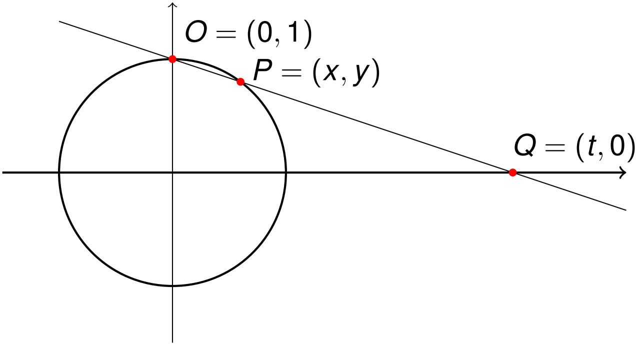
Each Pythagorean triple a, b, c corresponds to a pair

$$x = \frac{a}{c} \qquad y = \frac{b}{c}$$

of rational numbers x, y with

$$x^2 + y^2 = 1 \,.$$

So (x, y) is a rational point on the unit circle.



Rational parametrization of the circle

$$t = \frac{y}{1-x} \qquad \text{vs.} \qquad x = \frac{t^2-1}{t^2+1} \qquad y = \frac{2t}{t^2+1}$$

Each rational point $(t, 0)$ on the line, with

$$t = \frac{p}{q}$$

gives a rational point (x, y) on the circle, with

$$x = \frac{p^2 - q^2}{p^2 + q^2} \qquad y = \frac{2pq}{p^2 + q^2}$$

and a Pythagorean triple a, b, c, with

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

Algebraic proof:

$$a^2 = c^2 - b^2 = (c+b)(c-b)$$

is a square, so by unique factorization

$$c+b = d^2 \qquad c-b = e^2$$

are squares. Therefore

$$c = \frac{d^2+e^2}{2} = p^2 + q^2 \qquad b = \frac{d^2-e^2}{2} = 2pq$$

with

$$p = (d+e)/2 \qquad q = (d-e)/2\,.$$

Pierre de Fermat (by Roland Le Fevre)

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 vero $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

ΤΟΝ ἐπιταχθέντα τετράγωνον διελεῖν εἰς δύο τετραγώνους. ἐπιτετάχθω δὴ τὸν ις̄ διελεῖν εἰς δύο τετραγώνους. καὶ τετάχθω ὁ πρῶτος δυνάμεως μιᾶς. δεήσει ἄρα μονάδας ις̄ λείψει δυνάμεως μιᾶς ἴσας εἶναι τετραγώνῳ. πλάσσω τὸν τετράγωνον ἀπὸ ςς̄. ὅσων δή ποτε λείψει τοσούτων μο ὅσων ἐστὶν ἡ τοῦ ις̄ μο πλευρά. ἔστω ςς β̄ λείψει μο δ̄. αὐτὸς ἄρα ὁ τετράγωνος ἔσται δυνάμεων δ̄ μο ις̄ λείψει ςς ις̄. ταῦτα ἴσα μονάσι ις̄ λείψει δυνάμεως μιᾶς. κοινὴ προσκείσθω ἡ λεῖψις, καὶ ἀπὸ ὁμοίων ὅμοια. δυνάμεις ἄρα ε̄ ἴσαι ἀριθμοῖς ις̄. καὶ γίνεται ὁ ἀριθμὸς ις̄. πέμπτων. ἔσται ὁ μὲν σνς̄ εἰκοστοπέμπτων. ὁ δὲ ρμδ̄ εἰκοστοπέμπτων, καὶ οἱ δύο συντεθέντες ποιοῦσι ῡ εἰκοστόπεμπτα, ἤτοι μονάδας ις̄. καὶ ἔστιν ἑκάτερος τετράγωνος.

OBSERVATIO DOMINI PETRI DE FERMAT.

CVbum 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

Fermat's claim: The equation

$$a^n + b^n = c^n$$

has no solutions in positive integers for $n > 2$.

Proof?

If $n = pm$ we can rewrite the equation as

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

so it suffices to verify the claim

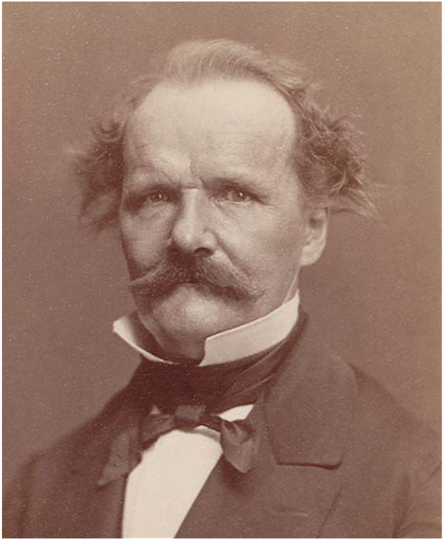
- for $n = 4$ (done by Fermat), and
- for $n = p$ any odd prime.

Sophie Germain (1776–1831)

Theorem (Germain (pre-1823))

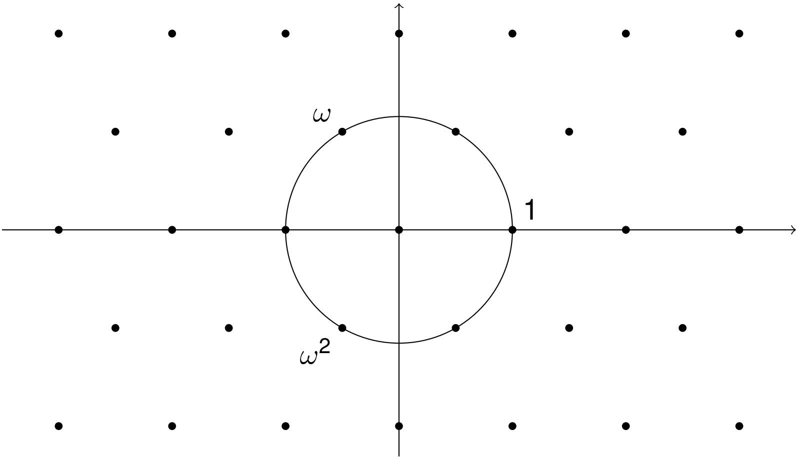
Let p be an odd prime. If there exists an auxiliary prime q such that $x^p + 1 \equiv y^p \mod q$ has no nonzero solutions, and $x^p \equiv p \mod q$ has no solution, then if $a^p + b^p = c^p$ then p^2 must divide a, b or c.

- Any such auxiliary prime q will satisfy $q \equiv 1 \mod p$.
- If $q = 2p + 1$ is a prime, then both hypotheses are satisfied.
- Showing that $p \mid abc$ is called the First Case of Fermat's Last Theorem.



Ernst Kummer (1810–1893)

Suppose
$$a^p + b^p = c^p\,.$$
Using $\omega = \exp(2\pi i/p) = \cos(2\pi/p) + i\sin(2\pi/p)$ we can factorize
$$a^p = c^p - b^p = (c-b)(c-\omega b)\cdots(c-\omega^{p-1}b)\,.$$
If unique factorization holds in $\mathbb{Z}[\omega]$, then each factor
$$(c-b), (c-\omega b), \ldots, (c-\omega^{p-1}b)$$
must be an p-th power. Therefore $\ldots$



The number system $\mathbb{Z}[\omega]$ for $p = 3$

Kummer carried this strategy through to prove Fermat's claim for all regular primes p. (The only irregular primes less than 100 are 37, 59 and 67). Led to:

- the study of new number systems, like $\mathbb{Z}[\omega]$,
- the invention of ideal numbers (ideals) in rings, and
- an analysis of the subtleties of unique factorization (ideal class groups).

The number systems $\mathbb{Q}(\omega)$ with $\omega = \exp(2\pi i/n)$ are called cyclotomic fields. The powers of ω divide the circle into n equal parts.

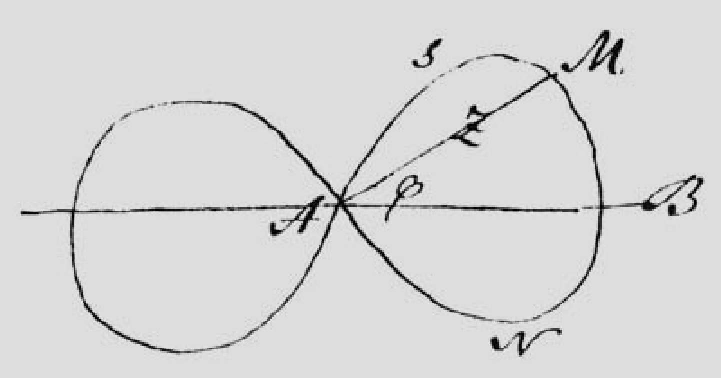
The systematic study of the ideal class groups of cyclotomic fields is called Iwasawa theory.

The Main Conjecture of Iwasawa Theory was proved by Barry Mazur and Andrew Wiles in 1984.

[Ralph Greenberg and] Kenkichi Iwasawa (1917–1998)

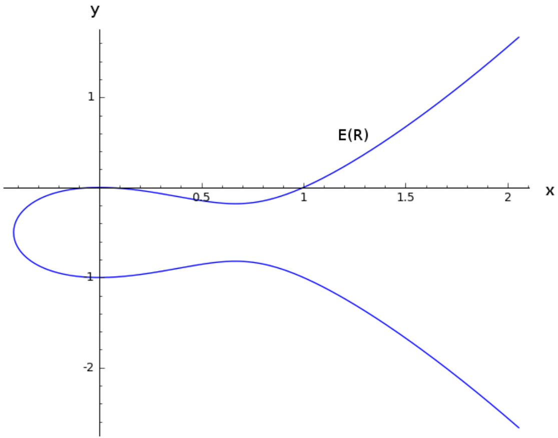
Fermat's equation

Elliptic curve

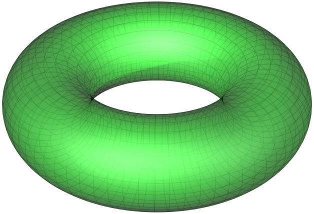


Niels Henrik Abel’s drawing of a lemniscate

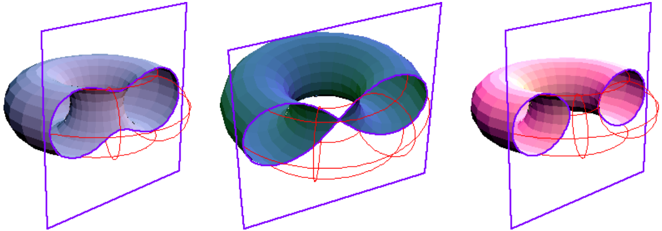
The “first elliptic curve in nature” is $E\colon y^2 + y = x^3 - x^2$.



Real solution set $E(\mathbb{R})$ with (x, y) in $\mathbb{R}^2 \subset P^2(\mathbb{R})$

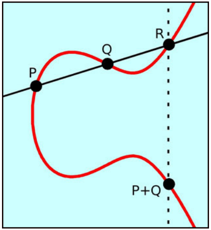


Topology of complex solution set $E(\mathbb{C})$ with (x, y) in $\mathbb{C}^2 \subset P^2(\mathbb{C})$



Cross-sections

For any field K, the solution set $E(K)$ with (x, y) in $K^2 \subset P^2(K)$ is an abelian group. The point at infinity is the zero element.



$$P + Q + R = 0$$

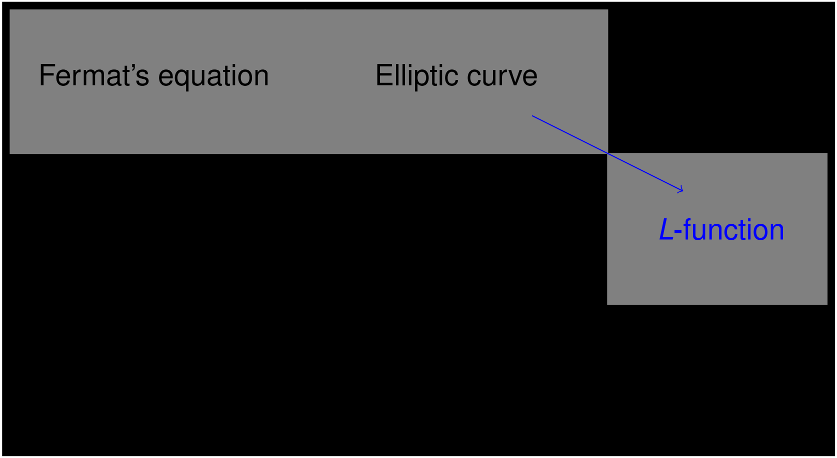
This group structure is related to Niels Henrik Abel's addition theorem, e.g. for curve length on the lemniscate.

The case $K = \mathbb{Q}$ is the most interesting, but also the most difficult.

Theorem (Mordell (1922))

$E(\mathbb{Q})$ is a finitely generated abelian group.

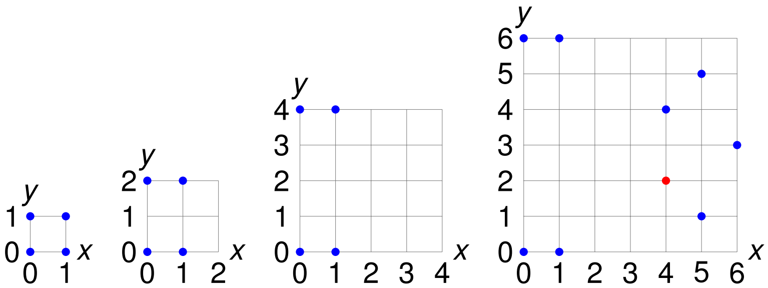
Louis Mordell (1888–1972)


Fermat’s equation
Elliptic curve
L-function

$\mathbb{F}_\ell = \mathbb{Z}/(\ell) = \{0, 1, \ldots, \ell - 1\}$ is a field for each prime ℓ.
Consider solutions (x, y) in $(\mathbb{F}_\ell)^2$ to

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

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



Modular solution sets $E(\mathbb{F}_\ell)$ in $\mathbb{F}_\ell^2 \subset P^2(\mathbb{F}_\ell)$ for $\ell = 2, 3, 5, 7$

A line in $P^2(\mathbb{F}_\ell)$ has ℓ points in $\mathbb{F}_\ell^2$ and 1 point at ∞. Let

$$\#E(\mathbb{F}_\ell) = \text{number of points in } E(\mathbb{F}_\ell)$$

and define the integer a_ℓ so that

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

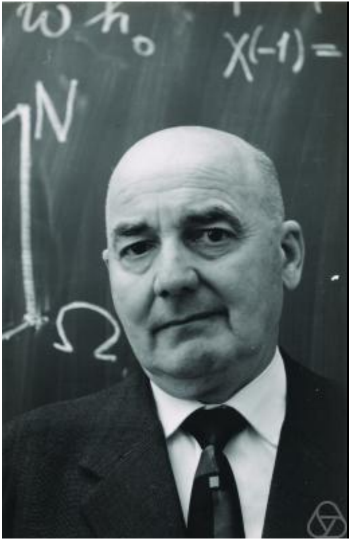
ℓ	2	3	5	7	...
$\#E(\mathbb{F}_\ell)$	5	5	5	10	...
a_ℓ	-2	-1	$+1$	-2	...

The numbers a_ℓ for $y^2 + y = x^3 - x^2$

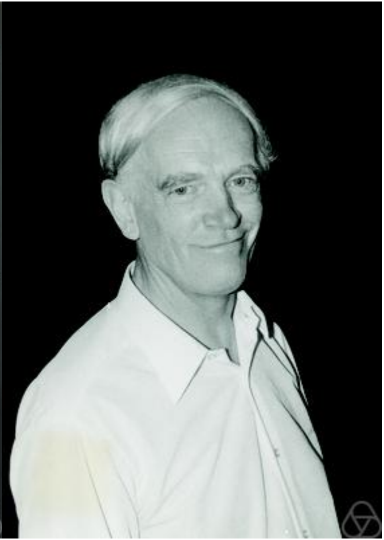
More detailed definitions specify a_n for all $n \geq 1$. The Dirichlet series

$$L(E, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

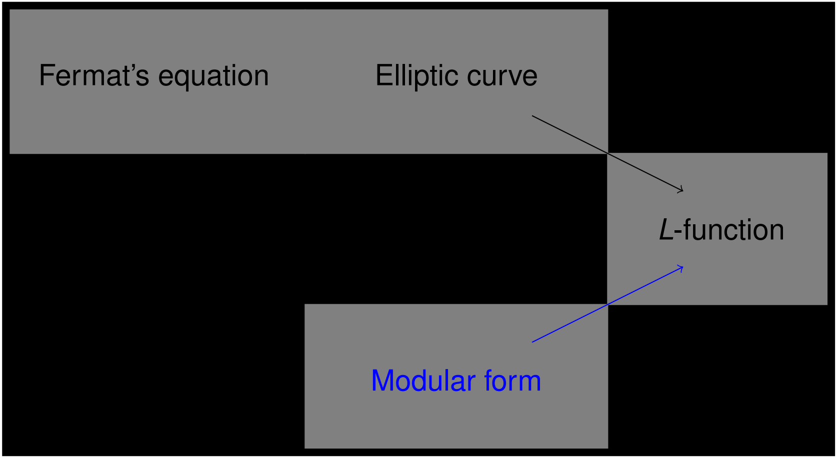
in a complex variable s is the Hasse–Witt L-function of E.

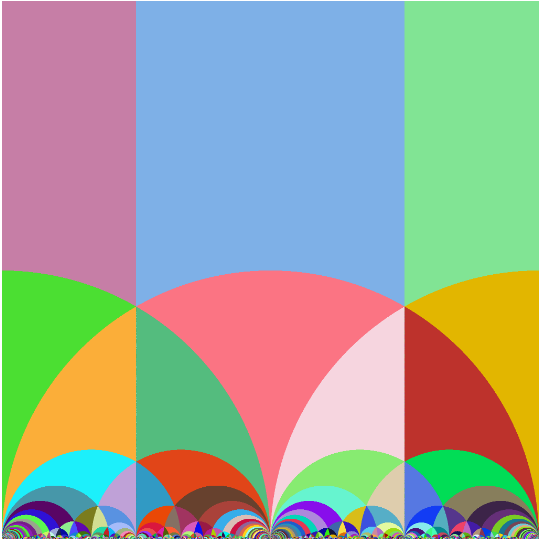


Helmut Hasse (1898–1979)



Ernst Witt (1911–1991)


Fermat's equation
Elliptic curve
L-function
Modular form



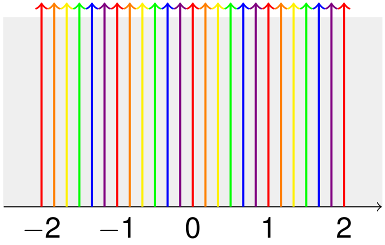
$SL_2(\mathbb{Z})$-symmetry of the upper half-plane $\mathbb{H}$ (by T. Womack)

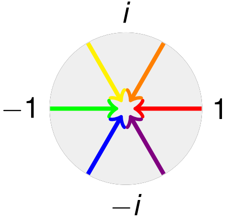
A modular form $f(z)$ is a highly symmetric complex function

$$f\colon \mathbb{H} \longrightarrow \mathbb{C}$$

defined on the upper half $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{im}(z) > 0\}$ of the complex plane.

The exponential map $z \mapsto q = \exp(2\pi i z)$ maps the upper half-plane $\mathbb{H}$ to the unit disc $\{q \mid |q| < 1\}$:





$$z \mapsto q = \exp(2\pi i z)$$

We can write $f(z) = F(q)$ if and only if $f(z) = f(z+1)$.

Amazing property of the discriminant function

$$\Delta(q) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = q - 24q^2 + 252q^3 - 1472q^4 + \dots$$

The holomorphic function $\delta(z) = \Delta(q)$, where $q = \exp(2\pi iz)$, satisfies the symmetry condition

$$\delta(\frac{az+b}{cz+d}) = (cz+d)^{12}\delta(z)$$

for all integer matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $ad - bc = 1$.

- $\delta(z)$ is a modular form of weight 12.

Amazing property of the discriminant function

$$\Delta(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = q - 24q^2 + 252q^3 - 1472q^4 + \ldots$$

The holomorphic function $\delta(z) = \Delta(q)$, where $q = \exp(2\pi i z)$, satisfies the symmetry condition

$$\delta\left(\frac{az+b}{cz+d}\right) = (cz+d)^{12}\delta(z)$$

for all integer matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $ad - bc = 1$.

- $\delta(z)$ is a modular form of weight 12.

Amazing property of the discriminant function

$$\Delta(q) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = q - 24q^2 + 252q^3 - 1472q^4 + \dots$$

The holomorphic function $\delta(z) = \Delta(q)$, where $q = \exp(2\pi iz)$, satisfies the symmetry condition

$$\delta\left(\frac{az+b}{cz+d}\right) = (cz+d)^{12}\delta(z)$$

for all integer matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $ad - bc = 1$.

- $\delta(z)$ is a modular form of weight 12.

The infinite product

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

satisfies $F(q)^{12} = \Delta(q)\Delta(q^{11})$.

The associated function $f(z) = F(q)$ satisfies

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

for all integer matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $ad - bc = 1$ and $c \equiv 0$ mod 11.

- $f(z)$ is a modular form of weight 2 and level 11.

The infinite product

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

satisfies $F(q)^{12} = \Delta(q)\Delta(q^{11})$.

The associated function $f(z) = F(q)$ satisfies

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

for all integer matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $ad - bc = 1$ and $c \equiv 0$ mod 11.

- $f(z)$ is a modular form of weight 2 and level 11.

The infinite product

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

satisfies $F(q)^{12} = \Delta(q)\Delta(q^{11})$.

The associated function $f(z) = F(q)$ satisfies

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

for all integer matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $ad - bc = 1$ and $c \equiv 0$ mod 11.

- $f(z)$ is a modular form of weight 2 and level 11.

The infinite product

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

satisfies $F(q)^{12} = \Delta(q)\Delta(q^{11})$.

The associated function $f(z) = F(q)$ satisfies

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

for all integer matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $ad - bc = 1$ and $c \equiv 0 \mod 11$.

- $f(z)$ is a modular form of weight 2 and level 11.

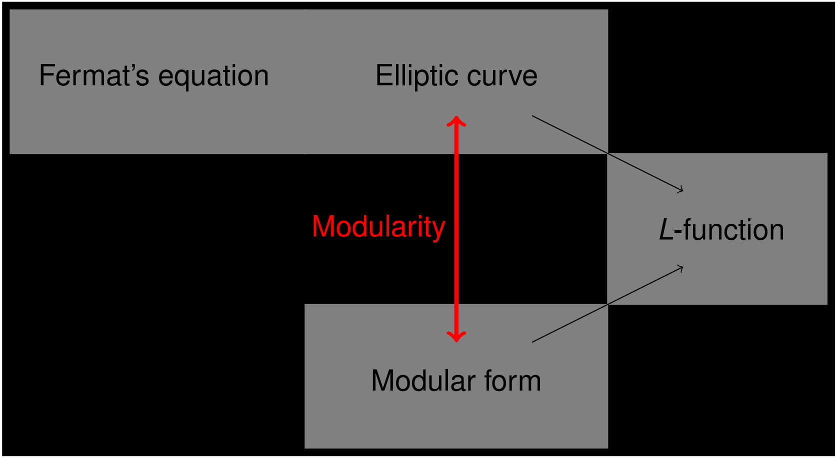
The Fourier expansion

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

contains the same information as the Dirichlet series

$$L(f,s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}\,.$$

We call $L(f,s)$ the Mellin transform of $f(z) = F(q)$.


Fermat's equation
Elliptic curve
Modularity
L-function
Modular form

Martin Eichler (1912–1992)

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

is the "first modular form of weight 2 in nature". Recall the table of point counts for $y^2 + y = x^3 - x$:

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

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

is the “first modular form of weight 2 in nature”. Recall the table of point counts for $y^2 + y = x^3 - x$:

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

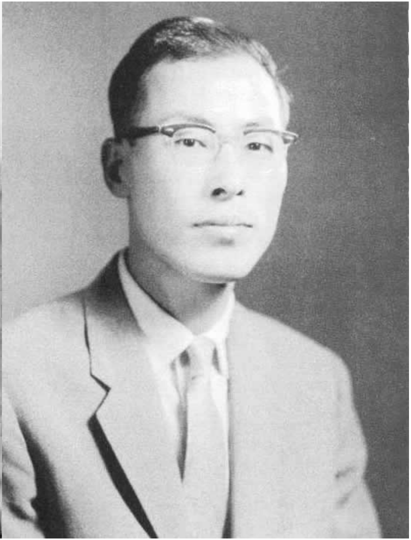
Theorem (Eichler (1954))

For the "first" elliptic curve $E\colon y^2 + y = x^3 - x^2$ *and the "first" modular form* $f(z) = (\Delta(z)\Delta(11z))^{1/12}$ *of weight* 2*, the equality*

$$a_\ell = b_\ell$$

holds for each prime ℓ*.*

- *The L-functions* $L(E, s) = L(f, s)$ *are equal.*



Yutaka Taniyama (1927–1958)

Goro Shimura

Conjecture (Taniyama (1955), Shimura)

For each elliptic curve

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

with $\alpha_1, \ldots, \alpha_6 \in \mathbb{Q}$ *and* $\#E(\mathbb{F}_\ell) = \ell - a_\ell + 1$*, there exists a modular form* $f(z)$ *of weight* 2*, with* $F(q) = \sum_{n=1}^{\infty} b_n q^n$*, such that*

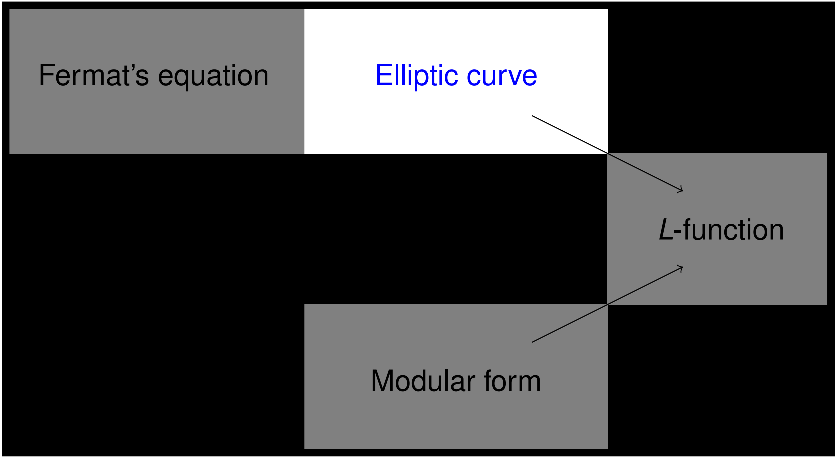
$$a_\ell = b_\ell$$

for almost every prime ℓ*.*

- *The L-functions* $L(E,s) = L(f,s)$ *are equal.*

Conjecture (Taniyama–Shimura)

Each elliptic curve defined over $\mathbb{Q}$ *is modular.*


Fermat's equation
Elliptic curve
L-function
Modular form

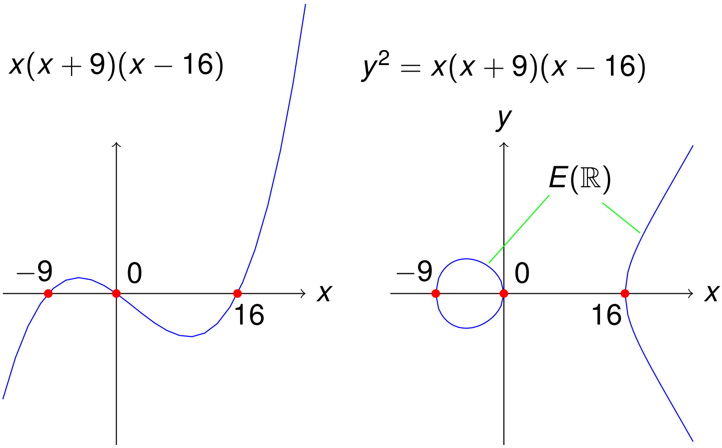
Definition

An elliptic curve is a smooth, projective, algebraic curve E of genus one, with a chosen point O.

- By Riemann–Roch, E is isomorphic to the projective planar curve given by a Weierstraß equation

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

- The origin O corresponds to a single point at infinity.
- If the coefficients $\alpha_1, \ldots, \alpha_6$ lie in a field K, we say that E is defined over K.



A cubic polynomial and an elliptic curve E

If $\alpha_1 = \alpha_3 = 0$, the curve

$$y^2 = x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6$$

is smooth if and only if the right hand side has three distinct roots, r_1, r_2 and r_3.

- An equivalent condition is that

  $$\Delta(E) = 16(r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2$$

  is nonzero.
- In general, the discriminant $\Delta(E)$ of E is an explicit integral polynomial in $\alpha_1, \ldots, \alpha_6$.
- The Weierstraß equation defines an elliptic curve over K if and only if $\Delta(E) \neq 0$ in K.

Let E be an elliptic curve defined over $\mathbb{Q}$.

After a linear change of coordinates (with rational coefficients) we may assume that $\alpha_1, \ldots, \alpha_6 \in \mathbb{Z}$, so that $\Delta(E) \in \mathbb{Z}$.

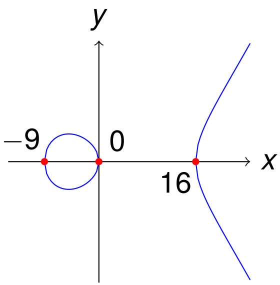
- A choice of equation

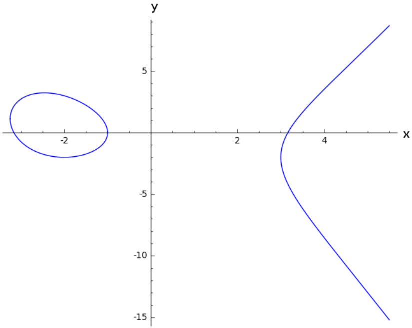
$$y^2 + \alpha_1 xy + \alpha_3 y = x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6$$

  with integral coefficients that minimizes $|\Delta(E)|$ will be called a minimal equation for E.

Example: The minimal equation for $y^2 = x(x+9)(x-16)$ is

$$y^2 + xy + y = x^3 + x^2 - 10x - 10\,.$$





Isomorphic curves, with $\Delta = 2^{12} \cdot 3^4 \cdot 5^4$ and $\Delta = 3^4 \cdot 5^4$

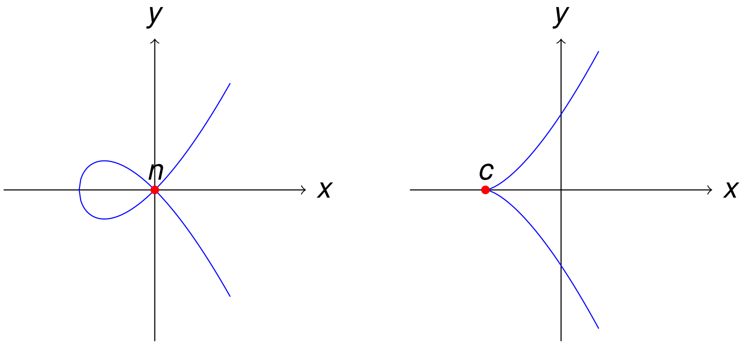
A minimal equation

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

can be viewed as an equation in $\mathbb{F}_\ell$ for $(x, y) \in \mathbb{F}_\ell^2$, for any given prime ℓ.

There are three mutually exclusive cases:

- $E(\mathbb{F}_\ell)$ is elliptic, $\ell \nmid \Delta(E)$, and $\Delta(E) \neq 0$ in $\mathbb{F}_\ell$.
- $E(\mathbb{F}_\ell)$ has a node n, and $E(\mathbb{F}_\ell) \setminus \{n\} \cong \mathbb{F}_\ell^\times$ is the multiplicative group.
- $E(\mathbb{F}_\ell)$ has a cusp c, and $E(\mathbb{F}_\ell) \setminus \{c\} \cong \mathbb{F}_\ell$ is the additive group.



Nodal and cuspidal singularities (real images)

Definition

An elliptic curve E defined over $\mathbb{Q}$ is semistable if for each prime ℓ the curve $E(\mathbb{F}_\ell)$ is smooth or has a node, but does not have a cusp.

Definition

The conductor of a semistable curve E is the product

$$N = \prod_{\ell | \Delta(E)} \ell$$

of the primes ℓ where $E(\mathbb{F}_\ell)$ has a node.

Example: The elliptic curve

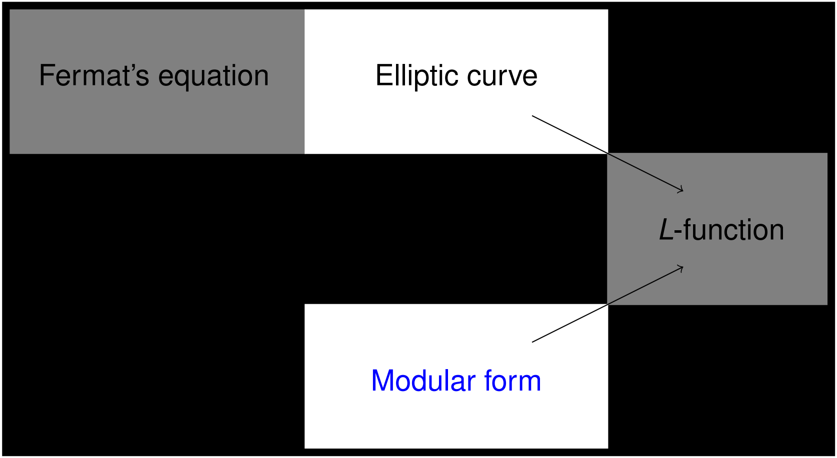
$$y^2 = x(x+9)(x-16)$$

has minimal equation $y^2 + xy + y = x^3 + x^2 - 10x - 10$ of discriminant $\Delta = 3^4 \cdot 5^4$. Both $E(\mathbb{F}_3)$ and $E(\mathbb{F}_5)$ have nodes, so E is semistable. Its conductor is $N = 3 \cdot 5 = 15$.

Example: The elliptic curve

$$y^2 = x(x-9)(x+16)$$

has minimal equation $y^2 = x^3 + x^2 - 160x + 308$ of discriminant $\Delta = 2^{12} \cdot 3^4 \cdot 5^4$. The curve $E(\mathbb{F}_2)$ has a cusp, so E is not semistable.


Fermat's equation
Elliptic curve
L-function
Modular form

Definition

A modular form f of weight 2 and level N is a holomorphic function defined on the upper half-plane $\mathbb{H}$, such that

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

for all $z \in \mathbb{H}$ and all integer matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $ad - bc = 1$ and $c \equiv 0 \mod N$.

- We can write $f(z) = F(q)$ for $q = \exp(2\pi iz)$, because $f(z+1) = f(z)$.
- We require that F is holomorphic at $q = 0$, so that

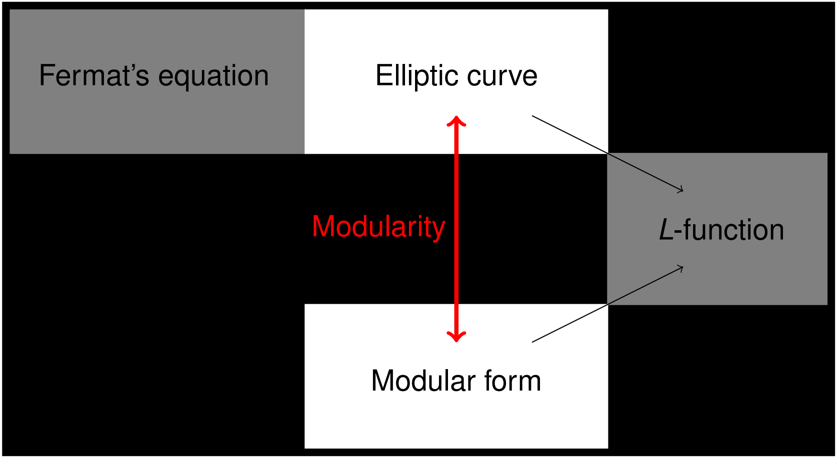
$$F(q) = \sum_{n=0}^{\infty} b_n q^n \, .$$

Technical conditions:

A modular form $f(z) = F(q)$ of level N is

- a cusp form if $f(z) = 0$ “at the cusps”, so that $b_0 = 0$;
- a newform if it is not “induced up” from a modular form of smaller level M;
- an eigenform if it is an eigenvector for each Hecke operator T_n for n relatively prime to N.

Most modular forms considered below will implicitly be assumed to satisfy these three conditions. They give a basis for the most relevant modular forms that are strictly of level N.


Fermat's equation
Elliptic curve
Modularity
L-function
Modular form

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

Conjecture (Hasse–Weil (1967))

For each elliptic curve E defined over $\mathbb{Q}$, with conductor N, there exists a modular form $f(z)$ of weight 2 and level N such that

$$a_\ell = b_\ell$$

for all primes $\ell \nmid N$.

More detailed definitions specify N for all E, and a_n for all $n \geq 1$. The conjecture then asserts that $a_n = b_n$ for all n:

$$L(E,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \sum_{n=1}^{\infty} \frac{b_n}{n^s} = L(f,s) \qquad F(q) = \sum_{n=1}^{\infty} b_n q^n \, .$$

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 (January 1966)

References:

Modular forms and Fermat's last theorem. Edited by Gary Cornell, Joseph H. Silverman and Glenn Stevens. Springer-Verlag, New York, 1997.

Gouvêa, Fernando Q.: "A marvelous proof". Amer. Math. Monthly 101 (1994), no. 3, 203–222.

Rubin, K.; Silverberg, A.: A report on Wiles' Cambridge lectures. Bull. Amer. Math. Soc. (N.S.) 31 (1994), no. 1, 15–38.

Saito, Takeshi: Fermat's last theorem. Basic tools. Translations of Mathematical Monographs, 243. American Mathematical Society, Providence, RI, 2013.

Taylor, Richard; Wiles, Andrew: Ring-theoretic properties of certain Hecke algebras. Ann. of Math. (2) 141 (1995), no. 3, 553–572.

Wiles, Andrew: Modular elliptic curves and Fermat's last theorem. Ann. of Math. (2) 141 (1995), no. 3, 443–551.