What is... Fermat's last theorem?

Felix Henson

21 Oct 2025

Most images shamelessly ripped from Wikipedia

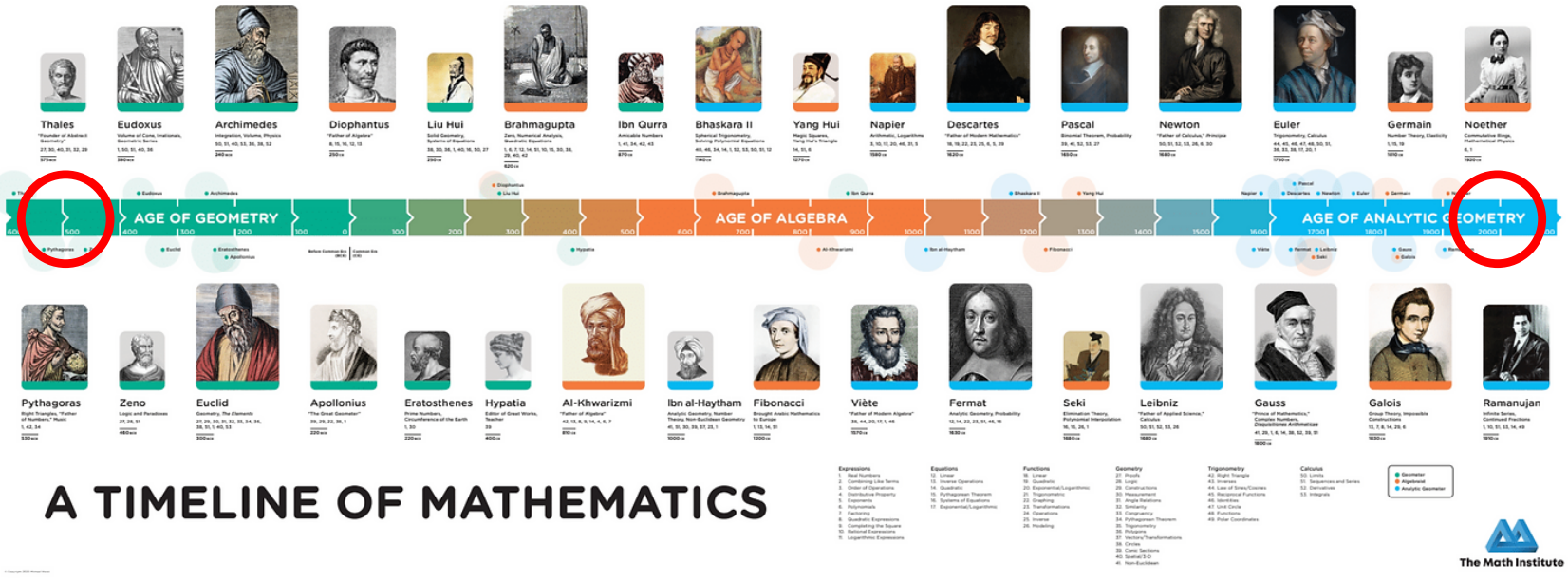
In 1994, Andrew Wiles proved the

Semistable Modularity Theorem

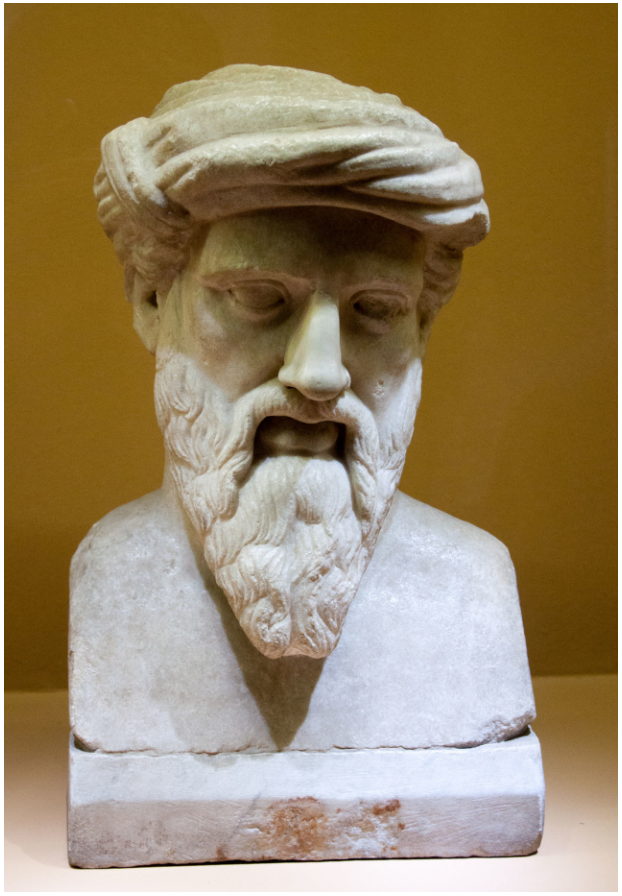
Every semistable elliptic curve over the rational numbers is modular.

thus proving Fermat's last theorem.

What?


Thales
Eudoxus
Archimedes
Diophantus
Liu Hui
Brahmagupta
Ibn Qurra
Bhaskara II
Yang Hui
Napier
Descartes
Pascal
Newton
Euler
Germain
Noether
AGE OF GEOMETRY
AGE OF ALGEBRA
AGE OF ANALYTIC GEOMETRY
Pythagoras
Zeno
Euclid
Apollonius
Eratosthenes
Hypatia
Al-Khwarizmi
Ibn al-Haytham
Fibonacci
Viète
Fermat
Seki
Leibniz
Gauss
Galois
Ramanujan
A TIMELINE OF MATHEMATICS
The Math Institute

Pythagoras (c.500 BC)



Pythagoras's Theorem

If a right-angled triangle has side lengths x, y, z, where z is the length of the hypotenuse, then $x^2 + y^2 = z^2$.

Generating triples (Euclid, c.300 BC)

Take integers $m > n > 0$. Then

$$x = m^2 - n^2$$
$$y = 2mn$$
$$z = m^2 + n^2$$

give a Pythagorean triple.

Pythagoras (c.500 BC)

In particular, the equation

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

has infinitely many integer solutions $(x, y, z) \in \mathbb{Z}^3$.

Diophantus of Alexandria (c.300 AD)

- Wrote the *Arithmetica* (13 books)
- Invented algebra
- Obsessed with integer solutions to polynomial equations
- *Arithmetica* book 2 problem VIII: solves an equation of the form $x^2 + y^2 = z^2$ for x and y given an integer z

Pierre de Fermat (c.1600)

- Published no mathematics during his life
- Often left proofs out of his letters

> And this proposition is generally true for all series and for all prime numbers; I would send you a demonstration of it, if I did not fear going on for too long.
>
> Fermat, stating his "little theorem" in a letter to Frénicle de Bessy

The Last Theorem

Fermat primes

For every non-negative integer n, the number $2^{2^n} + 1$ is prime.

Fermat's Last Theorem

The equation

$$x^n + y^n = z^n$$

has no integer solutions $(x, y, z) \in \mathbb{Z}^3$ for any integer $n \geq 3$.

The latter was scribbled in the margin of his copy of *Arithmetica*, along with "I have discovered a truly marvelous proof of this, which this margin is too narrow to contain".

The Last Theorem

Fermat not-always-primes

~~For every non-negative integer n, the number $2^{2^n} + 1$ is prime.~~
$2^{2^5} + 1 = 641 \times 6700417$.

Fermat's Last Theorem

The equation

$$x^n + y^n = z^n$$

has no integer solutions $(x, y, z) \in \mathbb{Z}^3$ for any integer $n \geq 3$.

The latter was scribbled in the margin of his copy of *Arithmetica*, along with "I have discovered a truly marvelous proof of this, which this margin is too narrow to contain".

Special Cases

- Fermat proved case $n = 4$ by showing that a counterexample would give a right-angled triangle whose area is a square number.
- Euler (and Gauss) proved case $n = 3$ by factorising the equation using the Eisenstein integers

$$\mathbb{Z}[\zeta_3] = \{a + b\zeta_3 \mid a, b \in \mathbb{Z}\}, \quad \zeta_3 = e^{2i\pi/3}.$$

Gabriel Lamé (1800s)

Why doesn't this work for all n?

Let $\zeta_n = e^{2i\pi/n}$. Then the equation can be written as

$$x^n+y^n = (x+y)(x+\zeta_n y)\cdots(x+\zeta_n^{n-1}y) = z^n.$$

Ernst Kummer

- Had already proved $\mathbb{Z}[\zeta_n]$ didn't have unique factorisation when $n = 23$
- Tried to fix unique factorisation issues using "ideal numbers"
- Proved FLT for all regular primes

The Taniyama-Shimura Conjecture (1955)

Taniyama-Shimura Conjecture

Every elliptic curve over the rational numbers is modular.

Elliptic Curves & Modular Forms

Definition

An *elliptic curve* over $\mathbb{Q}$ is given by the solutions $(x, y) \in \mathbb{Q}$ to an equation of the form

$$y^2 = \text{ a cubic in } x \text{ (with rational coefficients)},$$

(as well as a point "at infinity").
An elliptic curve is called *nonsingular* if the discriminant of the cubic defining it is nonzero.

Elliptic Curves & Modular Forms

Definition

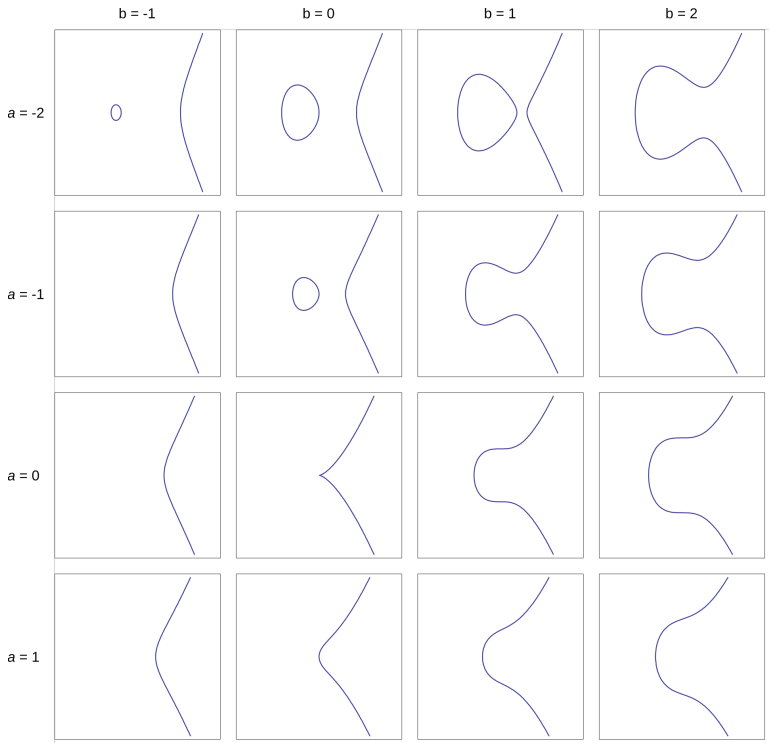
An *elliptic curve* over $\mathbb{Q}$ is given by the solutions $(x, y) \in \mathbb{Q}$ to an equation of the form

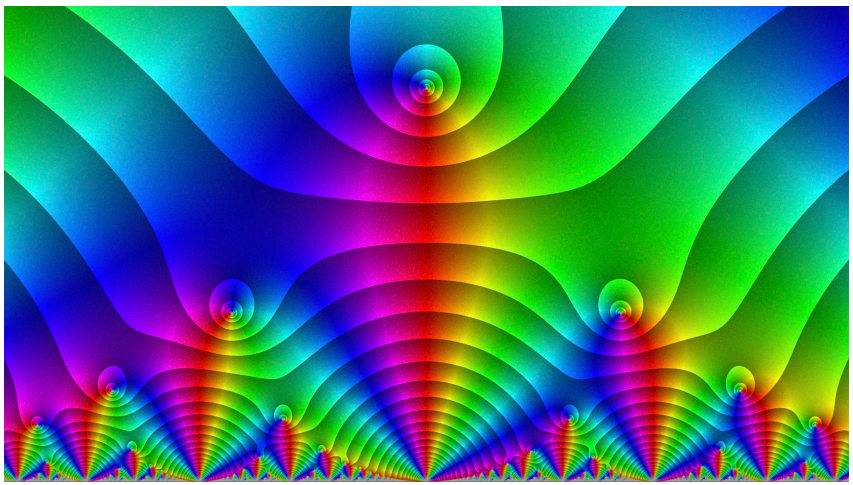
$$y^2 = \text{ a cubic in } x \text{ (with rational coefficients)},$$

(as well as a point "at infinity").
An elliptic curve is called *nonsingular* if the discriminant of the cubic defining it is nonzero.

Definition

A *modular form* is a function on the complex upper half-plane satisfying certain symmetry and boundedness properties.
Every modular form has a Fourier series.


b = -1
b = 0
b = 1
b = 2
a = -2
a = -1
a = 0
a = 1



From Elliptic Curves to Modular Forms

Given an elliptic curve E,

- Choose a cubic with integer coefficients defining E
- Reduce everything modulo p for each prime p
- For those p which give a non-singular curve, set

$$a_p := p + 1 - \#\{\text{points of } E \text{ modulo } p\}.$$

E is *modular* if

$$f(t) = \sum_p a_p q^p; \quad q = e^{2i\pi t}$$

defines some modular form f.

The Taniyama-Shimura Conjecture

But what does this have to do with Fermat?

The Frey Curve (1980s)

Definition

Suppose $(a, b, c) \in \mathbb{Z}^3$ satisfies $a^p + b^p = c^p$ for some prime $p \geq 5$. The corresponding *Frey curve* is the elliptic curve given by

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

Can we prove that these don't exist?

Two Important Invariants

Every elliptic curve has a *minimal discriminant* Δ and a *conductor* N. For the Frey curve these are

$$\Delta = \frac{(abc)^{2p}}{256},$$
$$N = \prod_{p|abc,\, p \text{ prime}} p.$$

Two Important Invariants

Every elliptic curve has a *minimal discriminant* Δ and a *conductor* N. For the Frey curve these are

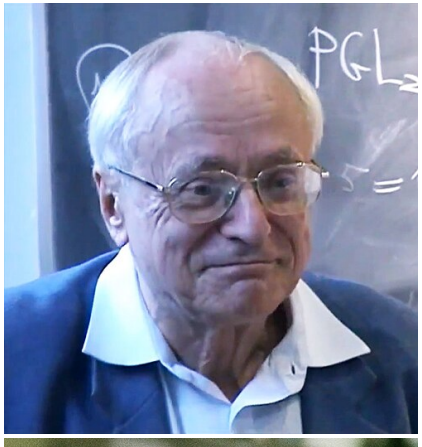
$$\Delta = \frac{(abc)^{2p}}{256},$$
$$N = \prod_{p|abc,\, p \text{ prime}} p.$$

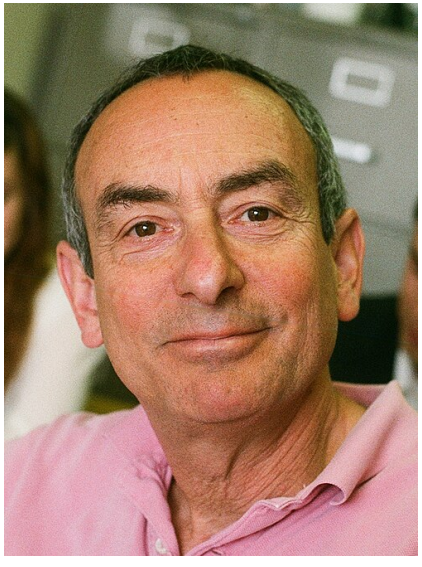
Szpiro's Conjecture

For any $\varepsilon > 0$, the ratio $\frac{\Delta}{N}$ is bounded above by a multiple of $N^{6+\varepsilon}$.

But for the Frey curve, we have $\frac{\Delta}{N} \geq \frac{(abc)^{2p-1}}{256}$ (exponential growth!)

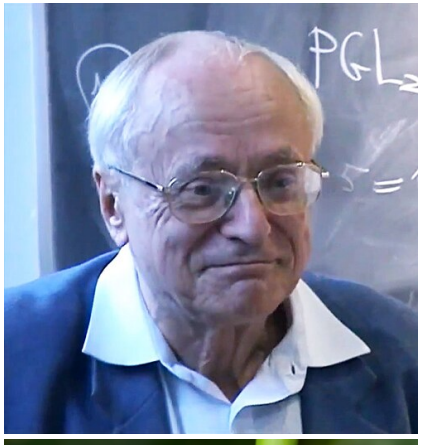
Serre & Ribet





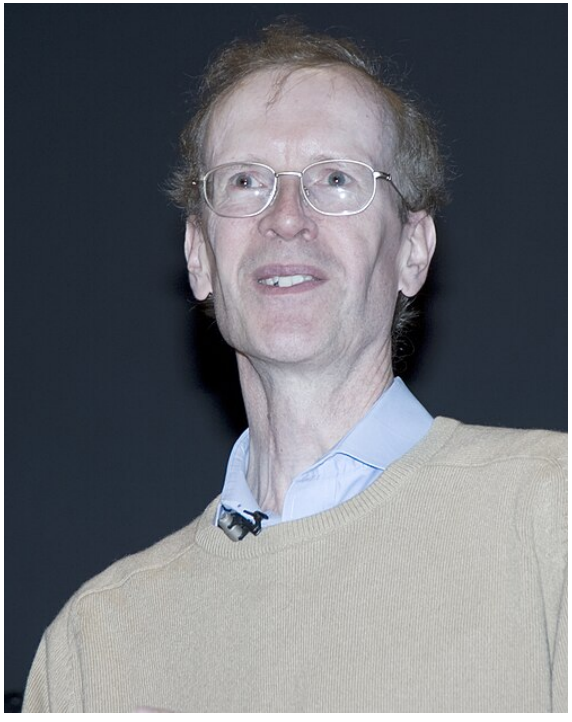
- Serre: If we can prove a small result "ε", then the Taniyama-Shimura conjecture implies Fermat's last theorem
- Ribet: Proved the ε conjecture (not without difficulty!), showing that the Frey curve is not modular.

Serre & Ribet



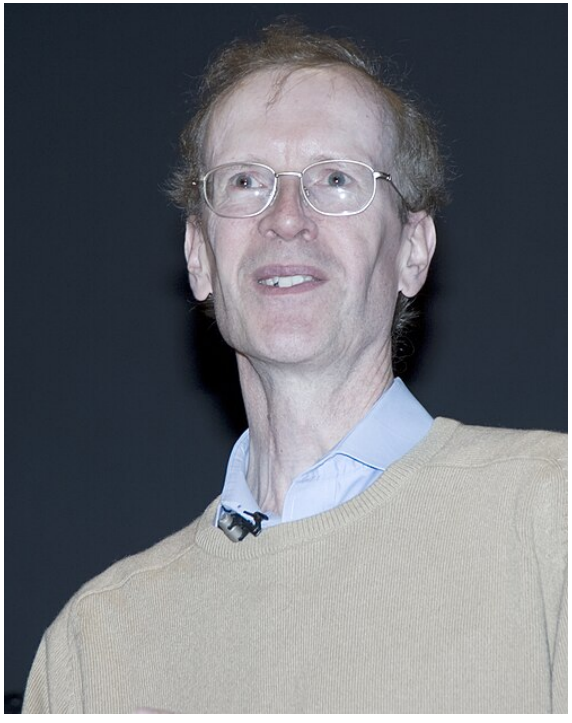
- Serre: If we can prove a small result "ε", then the Taniyama-Shimura conjecture implies Fermat's last theorem
- Ribet: Proved the ε conjecture (not without difficulty!), showing that the Frey curve is not modular.

Andrew Wiles



- Read *The Last Problem* by E.T. Bell as a teenager
- Worked in secret from 1986 to 1993 on proving Fermat's last theorem via the Taniyama-Shimura conjecture

Andrew Wiles



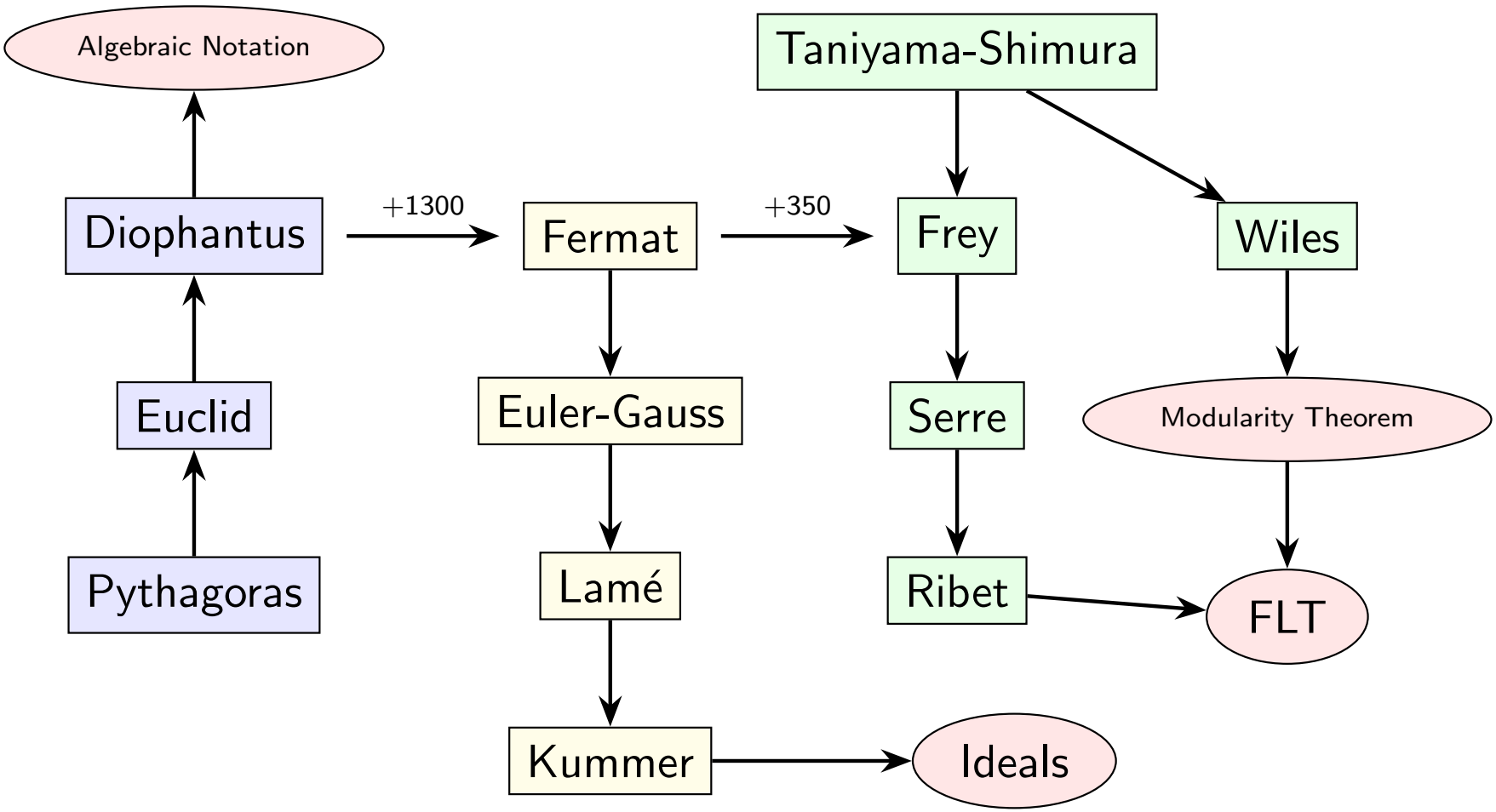
In 1994, Wiles proved the

Semistable Modularity Theorem

Every semistable elliptic curve over the rational numbers is modular.

- So the Frey curve is simultaneously modular and not modular – a contradiction
- So no Frey curve can exist
- So Fermat's last theorem is true.

Recap


Algebraic Notation
Taniyama-Shimura
Diophantus
+1300
Fermat
+350
Frey
Wiles
Euclid
Euler-Gauss
Serre
Modularity Theorem
Pythagoras
Lamé
Ribet
FLT
Kummer
Ideals

Further Reading

- *Fermat's Last Theorem* by Simon Singh
- Lectures on YouTube about FLT: Ribet & Wiles
- Langlands program - Wiles lecture on YouTube