BROWN

Fermat's Last Theorem

Problems from the History of Mathematics

Lecture 13 — March 9, 2018

Brown University

Fermat's Last Theorem

Problem II.8 of Diophantus' *Arithmeticae* asks how a given square might be written as the sum of two squares.[1] Diophantus only considers the specific problem $x^2 + y^2 = 16$, but the generalization to other squares is clear from context.

Fermat wrote the following in the margin beside Problem II.8 in his copy of *Arithmeticae* in 1637:

> *"It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain."*

[1] While $k = x^2 + y^2$ is not always solvable over $\mathbb{Q}$, the condition that k be square implies that it does have a solution.

Fermat's Actual Contribution to FLT

In modern notation,

Conjecture (Fermat, 1637):

The Diophantine equation $x^n + y^n = z^n$ has no positive integer solutions (x, y, z) unless $n \leq 2$.

Fermat's name became attached to this conjecture after his son edited and published a new edition of *Arithmeticae* in 1670 which included Fermat's remarks throughout.

However, it seems extremely unlikely that Fermat had any sort of general proof of this claim. There are two extremely convincing pieces of evidence in support of this:

1. The only known solution to FLT was proven in 1994 using mathematics far beyond the grasp of Fermat.
2. Fermat was an incessant braggart, but he made no claims to have solved FLT in the later years of his life.

Fermat's Actual Contribution to FLT

Fermat's actual contribution to the FLT consisted of proving that the $n = 4$ case had no solutions. (This settles the FLT for any exponent which is a multiple of 4 as well.) Fermat did this by showing that

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

has no solutions (by infinite descent).

Proof: We prove a more general statement, that there does not exist a Pythagorean triple in which two sides are squares or twice squares. Suppose (x, y, z) is such a triangle, and write

$$x = 2ab, \quad y = a^2 - b^2, \quad z = a^2 + b^2$$

with $(a, b) = 1$ and a, b of different parity. Before we consider cases, note that y, z are both odd, so not twice squares, and that if x is a square or twice a square, the same holds for a and b.

Fermat's Actual Contribution to FLT

$$x = 2ab, \quad y = a^2 - b^2, \quad z = a^2 + b^2$$

(y, z): If y, z are both squares, the triple $(\sqrt{yz}, b^2, a^2)$ is Pythagorean.

(x, y): Then y is square, so $(b, \sqrt{y}, a)$ is Pythagorean. But a and b are squares or twice squares.

(x, z): Then z is square, so $(a, b, \sqrt{z})$ is Pythagorean. But a and b are squares or twice squares.

In each case, we produce a new triangle with smaller hypotenuse. By infinite descent, no such triangle exists.[2]

[2] This gives another proof of Fermat's Right Triangle theorem. Suppose that 1 is congruent and that $x^2 - y^2$ and $x^2 + y^2$ are both square. Then $(x^2 - y^2)(x^2 + y^2)$ is square, ie. $x^4 - y^4 = z^2$. Contradiction.

Proofs for Other Exponents

The next case to be established in FLT was the $n = 3$ case, which was settled by Euler in a series of increasingly rigorous proofs between 1753 and 1770. Euler uses infinite descent.

The $n = 5$ case was settled by Legendre and Dirichlet around 1825 and the $n = 7$ case was settled by Lamé in 1839.

These proofs use a result of Sophie Germain from 1823:

Theorem (Germain, 1823):

Let p be an odd prime and suppose that $x^p + y^p = z^p$. Suppose that there exists an auxiliary prime θ such that

1. No two non-zero pth powers differ by 1 mod θ;
2. p is not a pth power mod θ

Then one of x, y, z must be divisible by p^2.

This is arguably the first result towards a general proof of FLT.

Unique Factorization in Cyclotomic Number Fields

One promising attack on FLT (and perhaps the "marvelous proof" that Fermat had in mind) begins with a factorization of $z^n - y^n = x^n$ over the cyclotomic integers $\mathbb{Z}[\zeta_n]$, where ζ_n is a primitive nth root of 1.

In the case $n = 3$, we have

$$x^3 = z^3 - y^3 = (z - y)(z - \zeta_3 y)(z - \zeta_3^2 y).$$

Suppose that π divides both $(z - y)$ and $(z - \zeta_3 y)$. Then $\pi \mid (1 - \zeta_3)y$ so that $\pi \mid y$ or $\pi \mid (1 - \zeta_3)$ because π is prime. But $\pi \mid y$ violates primitivity of (x, y, z), so $\pi \mid (1 - \zeta_3)$ and $\pi \sim 1 - \zeta_3$ since the latter is prime.

This implies that $3 \mid (z - y)$, whence $3 \mid x$. Otherwise, the terms $z - \zeta_3^j y$ are coprime and therefore cubes...[3]

[3] Continued on HW.

Unique Factorization in Cyclotomic Number Fields

In 1847, Lamé announced a proof of FLT based on the factorization of $x^n - y^n$ over $\mathbb{Z}[\zeta_n]$. His proof assumed unique factorization in $\mathbb{Z}[\zeta_n]$, which turns out to fail.[4]

This led Kummer to the idea of the ideal class group but did not lead into a gapless proof of FLT.

[4] The smallest example is $n = 23$. You can prove that 47 has multiple prime factorizations in $\mathbb{Z}[\zeta_{23}]$.

Proof of Fermat's Last Theorem

The Taniyama–Shimura Conjecture

In 1955, Taniyama made a bold conjecture linking the fields of algebraic geometry and analytic number theory. Roughly, the conjeture claims that elliptic curves can be used to define functions which turn out to be modular forms of weight 2.

The Taniyama–Shimura conjecture gained notoriety when Frey suggested that a counterexample to FLT implied that a certain elliptic curve (the Frey curve) was not modular.

In 1985, Serre showed that the Frey curve was non-modular under the assumption of the ϵ-conjecture. Ribet proved the ϵ-conjecture in 1986, which showed at last that Taniyama–Shimura implied FLT.

Resolution of the Taniyama–Shimura Conjecture

Despite this, the Taniyama–Shimura conjecture was thought intractable.

In 1993, Andrew Wiles presented a proof of FLT which relied on a proof of the Taniyama–Shimura conjecture for semistable elliptic curves.[5] This proof had an error, and in 1994 Wiles recruited Richard Taylor to help him fix the proof.

Their work on the semistable case was successful in 1995, and the FLT was proven. The full proof of the Taniyama–Shimura conjecture (now known as the Modularity Theorem) was completed in 2001.

[5] Those with square-free conductor.

Questions?