Fermat’s Last Theorem:
A non-trivial and beautiful note is not complete necessarily

Michael Albanese  Tronnolone, Hayden

School of Mathematical Sciences
University of Adelaide

11 May 2012
Abstract

There are many elegant, powerful, and enlightening theorems in mathematics, so what makes Fermat’s Last Theorem worthy of an AUMS Student Talk? Well, it is not just the theorem itself that merits discussion but the journey, spanning over 350 years from an amateur mathematician’s scribbled notes in a book to one of the most famous theorems of all time.

First we stated the theorem in the title. We will outline the rich history of the problem, introduce some of the mathematics that is involved in the proof, and present a real-world application of the theorem.
We stated the theorem, right?

A non-trivial and beautiful note is not complete necessarily.
We stated the theorem, right?

A non-trivial and beautiful note is not complete necessarily

\[ a^n + b^n \neq c^n \]
Pierre de Fermat

- Pierre de Fermat (c. 1601–1665) was a lawyer and amateur mathematician from France.
- He was a councillor in the High Court of Judicature in Toulouse for most of his life.
- Fermat was fluent in several languages including Latin, classical Greek, Italian and Spanish. He was often consulted to translate Greek texts.
Fermat’s mathematics

- Fermat communicated most of his mathematics via letters to friends. He often omitted proofs of his results.

- Because of this method, there were some disputes with other mathematicians, such as Descartes, regarding who first discovered certain results.

- In a series of letters in 1654, Fermat and Blaise Pascal discussed a problem related to gambling. In order to resolve the problem, the two invented probability theory. Fermat is said to have performed the first probability calculation.
Fermat’s mathematics

- Fermat worked in a variety of other fields.
  - He developed a method for calculating extrema and tangents to curves that predated calculus.
  - He computed integrals of power functions by reducing the problem to the sum of a geometric series.

These would later go on to influence Newton and Leibniz in their development of calculus.

- Best known for his work in number theory.
- Fermat studied perfect numbers, amicable numbers and Fermat numbers. He discovered several theorems such as Fermat’s Little Theorem and the polygonal number theorem.
- Again, few proofs of his results were ever made public (if any existed).
Arithmetica

- Fermat read and annotated a copy of *Arithmetica* by Diophantus, a third century Greek mathematician. *Arithmetica* contained 130 problems on algebra and methods for their solution.
- This text had a huge influence on mathematics, especially Arabic mathematics, and drove the development of modern algebra.
While Diophantus allowed rational solutions, Fermat was interested in integer solutions.

Because of this, a polynomial equation that requires integer solutions is referred to as a Diophantine equation.

In 1637 Fermat was reading *Arithmetica* and came across problem II.VIII, which describes how a perfect square can be split into two smaller squares. Diophantus only solved this problem for 16, but the result can be generalised.

Among his many annotations, Fermat wrote a (non-trivial and beautiful) note next to this problem...
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 marvellous proof of this, which this margin is too narrow to contain.
Fermat’s Last Theorem

- In 1670, after Fermat’s death, his son published a new edition of *Arithmetica* that included Fermat’s annotations.

- Mathematicians worked through the many results stated by Fermat and, one by one, all of them were proved except for one; Fermat’s note next to problem II.VIII.

- Because of this, the result became known as Fermat’s Last Theorem and may be stated as follows:

**Fermat’s Last Theorem**

The equation $a^n + b^n = c^n$ has no solutions in positive integers for $n > 2$. 
Arithmeticorum Liber II.

interallam numerorum 2. minor autem
1 N. atque ideo maior 1 N. + 2. Oportet
itaque 4 N. + 2, triplos esse ad 2, & ad-
buc superaddere 10. Ter igitur 2, adsci-
tis vinatibus 10. aquatur 4 N. + 4, &
fit N. 3. Erit ergo minor 3, maior 5, &
farasistant quastioni.

IN QVAESTIONEM VII.

CONDITIONIS apposite admodum ratio est que & apposite procedenti quasitioni, nihil ini-
 causi retinet quam ve quadraturi interallium numerorum fit minor interallium quadraturi, &
Canones idem hic etiam locum habebunt, ut manifissem eff.

QVAESTIO VIII.

P R O P O S I T U M quadratum diuidere
in duos quadratos. Imperatur sit ve
16. diuidatur in duos quadratos. Pontatur
primus 1 Q. Oportet igitur 16 = Q.
aequare esset quadrato. Fingo quadratum ad
metis quaquadrato libitum. cum defeqto tot
quinatur quod contineat latum ipsi 16.
efuerit a 1 N. 4. igitur igitur quadratur 16,
4 Q. = 16 16 = N. huc aquatur
vinatibus 16 = 1 Q. Communis adiciatur
vrumqve defectus, & a familiaris afeuen-
tur familiaris, fient 5 Q. aequalis 16 N. &
fit 1 N. Erit igitur alter quadratem 5,
alter vero 3, & vrumque hamma est 16,
& vterque quadratur eff.

E x e c o n o m i e n T . h , e u n o m e o e s . n. k a l h o n i c a r t i e r s . t r a n a m .

OBSERVATIO DOMINI PETRI DE FERMAT.

C f l u m autem in duos cubus, aut quadratoquadratum in duos quadratoquadratos
et generali iterum nullum in infinitum utra quadratum potestatem in duos eius-
dem nominis fas est diuidere eum rei demonstrationem mirabilem sanet detexit,
hanc marginitis exiguitas non ipsei.

QVAESTIO IX.

R e circulo oporteat quadratum 16
diuidere in duos quadratos, Ponta-
tur radius primus latus 1 N. alterius vero
quotcunque numerorum cum defecto tot
vinatur, quod conflat latus diuidendi.
Elfo itaque 2 N. 4. erunt quadrati, hic
quidem 1 Q. illte vero 4 Q. + 16 = 16 N.
Caterum volo vrumque simul aquari
vinatibus 16. Igitur 5 Q. + 16 = 16 N.
aquatur vinatibus 16. & fit 1 N. h eff

E x e c o n o m i e n T . h , e u n o m e o e s . n. k a l h o n i c a r t i e r s . t r a n a m .
Why is it important only to consider positive integers?

Suppose we allow complex solutions. Then, given $a$ and $b$ it is trivial to calculate $c = \sqrt[n]{a^n + b^n}$.

If $a$ and $b$ are real and $a^n + b^n \geq 0$, then it is also possible to find a solution in real numbers.
One ring to rule them all

- Any solution in rational numbers can be reduced to a solution in integers by multiplying through by the denominators.

\[
\left( \frac{a}{d} \right)^n + \left( \frac{b}{e} \right)^n = \left( \frac{c}{f} \right)^n \times (def)^n \rightarrow (aef)^n + (bdf)^n = (cde)^n
\]

- Any solution in integers is either trivial \((abc = 0)\), or can be rearranged to give a corresponding solution in positive integers.

**Example:** Suppose \(n\) is odd, \(a, c > 0\) and \(b < 0\). Then

\[
\begin{align*}
    a^n + b^n &= c^n \\
    a^n - (-b)^n &= c^n \\
    a^n &= (-b)^n + c^n
\end{align*}
\]
For $n = 1$, the problem just reduces to adding two positive integers to get a third. Hopefully everyone can solve this.

For $n = 2$, the solutions are Pythagorean triplets. There are an infinite number of solutions.
Fermat’s results

- What was Fermat’s marvellous proof?
- Fermat sent the $n = 3$ and $n = 4$ cases to other mathematicians as challenges, but did not include solutions.
- Only one of Fermat’s results was recorded.
Infinite descent and Fermat’s only proof

Fermat’s only proof comes from a letter to Christian Huygens in 1659. He outlined a proof that there is no right-angled triangle with integer sides whose area was a perfect square.

Fermat reduced this to finding positive integer solutions to $x^4 - y^4 = z^2$.

He proved there are no solutions using infinite descent:
- Assume there is a solution $(x, y, z)$ in positive integers.
- Show that this implies the existence of a smaller solution.

Since the positive integers are bounded below, there cannot be an infinite number of smaller solutions.

Let $x = c$, $y = b$, $z = a^2$. Then the equation can be rearranged to give

$$a^4 + b^4 = c^4.$$
Fermat also noted that the problem could be simplified using primes.

Suppose \( n \) is not prime. We can write \( n = kp \) where \( p \) is prime. Then

\[
a^n + b^n = c^n \implies (a^k)^p + (b^k)^p = (c^k)^p
\]

We need only consider \( n = 4 \) and the odd primes.
Euler or nothing

- No progress was made until 1770 when Leonhard Euler published a proof for $n = 3$ using infinite descent.

- It contained a mistake, but could be fixed with his other results.

- This case was later proved by several others.
Other interesting values

- $n = 5$ proved by Legendre (completing a partial proof by Dirichlet).

- $n = 7$ proved by Lamé in 1839.

- $n = 6, 10, \text{ and } 14$ also proved (but don’t really help).

- There was no obvious pattern. Sometimes infinite descent worked, sometimes it did not.
That’s a lot of mathematicians

3 Pierre de Fermat?, Leonhard Euler (1770), Kausler (1802), Adrien-Marie Legendre (1823, 1830), Calzolari (1855), Gabriel Lamé (1865), Peter Guthrie Tait (1872), Günther (1878), Gambioli (1901) Krey (1909), Rychlík (1910), Stockhaus (1910), Carmichael (1915), Johannes van der Corput (1915), Axel Thue (1917), and Duarte (1944)

4 Pierre de Fermat (1659), Frénicle de Bessy (1676), Leonhard Euler (1738), Kausler (1802), Peter Barlow (1811), Adrien-Marie Legendre (1830), Schopis (1825), Terquem (1846), Joseph Bertrand (1851), Victor Lebesgue (1853, 1859, 1862), Theophile Pepin (1883), Tafelmacher (1893), David Hilbert (1897), Bendz (1901), Gambioli (1901), Leopold Kronecker (1901), Bang (1905), Sommer (1907), Bottari (1908), Karel Rychlík (1910), Nutzhorn (1912), Robert Carmichael (1913), Hancock (1931), and Vrangceanu (1966).

5 Adrien-Marie Legendre (1825), Peter Dirichlet (1825), Carl Friedrich Gauss (1875, posthumous), Lebesgue (1843), Lamé (1847), Gambioli (1901), Werebrusow (1905), Rychlík (1910), van der Corput (1915), and Guy Terjanian (1987).

7 Lamé (1839), Lebesgue (1840), Angelo Genocchi (1864, 1874 and 1876), Théophile Pépin (1876), Edmond Maillet (1897).
That’s a lot of mathematicians

3. Pierre de Fermat?, Leonhard Euler (1770), Kausler (1802), Adrien-Marie Legendre (1823, 1830), Calzolari (1855), Gabriel Lamé (1865), Peter Guthrie Tait (1872), Günther (1878), Gambioli (1901), Krey (1909), Rychlík (1910), Stockhaus (1910), Carmichael (1915), Johannes van der Corput (1915), Axel Thue (1917), and Duarte (1944)

4. Pierre de Fermat (1659), Frénicle de Bessy (1676), Leonhard Euler (1738), Kausler (1802), Peter Barlow (1811), Adrien-Marie Legendre (1830), Schopis (1825), Terquem (1846), Joseph Bertrand (1851), Victor Lebesgue (1853, 1859, 1862), Theophile Pepin (1883), Tafelmacher (1893), David Hilbert (1897), Bendz (1901), Gambioli (1901), Leopold Kronecker (1901), Bang (1905), Sommer (1907), Bottari (1908), Karel Rychlík (1910), Nutzhorn (1912), Robert Carmichael (1913), Hancock (1931), and Vrânceanu (1966).

5. Adrien-Marie Legendre (1825), Peter Dirichlet (1825), Carl Friedrich Gauss (1875, posthumous), Lebesgue (1843), Lamé (1847), Gambioli (1901), Werebrusow (1905), Rychlík (1910), van der Corput (1915), and Guy Terjanian (1987).

7. Lamé (1839), Lebesgue (1840), Angelo Genocchi (1864, 1874 and 1876), Théophile Pépin (1876), Edmond Maillet (1897).
The one thing Gauss didn’t do

- Gauss wrote *Disquisitiones Arithmeticae*, which set out modern number theory.

- He planned to work on FLT, but died before getting the chance (although some of his results were found after his death).

- His book inspired Sophie Germain (1776–1831) to work on the problem.
Germain showed that if there was a solution to $a^p + b^p = c^p$ and an auxiliary prime $q$ of the form $2Np + 1 \ (N \in \mathbb{N})$ that satisfies certain conditions then $q$ would divide one of $a, b$ or $c$.

Germain tried to show there are infinitely many such auxiliary primes, but it turns out this is not the case.

However, she went on to classify all possible counterexamples to FLT as one of two cases:

- Case I: $abc$ not divisible by $p$;
- Case II: $abc$ divisible by $p$.

Developed an algorithm to generate auxiliary primes and used it to prove case I of FLT for all $p < 100$.

This was the first step towards a general result.

Legendre extended this to a proof of case I for $p$ up to 197.
Another Lamé attempt Kummer's and goes

- In 1847 Lamé attempted to prove FLT by allowing complex solutions and factoring the equation, i.e. if $\zeta^n = 1$, then
  \[
  x^n + y^n = (x + y)(x + \zeta y) \ldots (x + \zeta^{n-1} y).
  \]

- An error was spotted by Joseph Liouville and highlighted in a paper by Ernst Kummer.

- However, Kummer did manage to modify Lamé’s method and proved FLT for all regular primes. He could not prove it for exceptional primes (about 39% of all primes).
Wolfskehl lays it down

- In 1901 David Hilbert proposed his famous 23 problems. Fermat’s Last Theorem was not one of them.

- In 1908 Paul Wolfskehl bequeathed 100,000 Marks to the Göttingen Academy of Sciences as a prize for a complete proof of FLT.

- The prize had nine rules, one of which said the proof must be completed before the 13th of September, 2007.

- In the first year of the prize 621 proofs were submitted. By the 1970s this had dropped to 3–4 proofs per year. Around 5000 were received.
Mordell and Mordell attempts

- In 1983, Gerd Faltings proved the Mordell conjecture (1920s).
- It implies that the curve $x^n + y^n = 1$ has only a finite number of rational points for $n \geq 4$.
- In 1985, A. Granville and D. Heath–Brown showed FLT was true for “most” $n$. If there are solutions, they become less frequent as $n$ grows.
Computers to the rescue?

- Computers began to be used to prove FLT. Computers could factorise numbers and extend Kummer’s method.

- By 1954, a computer had proved FLT for all primes less than 2521.

- By 1978, it had been shown that any counterexample to FLT must involve \( p > 125,000 \), and \( a, b, c > 125,000^{325,005} \approx 4.5 \times 10^{1,911,370} \).

- By 1993 FLT had been proved for all exponents less than 4 million.
Computers to the rescue?

- Computers began to be used to prove FLT. Computers could factorise numbers and extend Kummer’s method.

- By 1954, a computer had proved FLT for all primes less than 2521.

- By 1978, it had been shown that any counterexample to FLT must involve $p > 125,000$, and $a, b, c > 125,000^{325,005} \approx 4.5 \times 10^{1,911,370}$.

- By 1993 FLT had been proved for all exponents less than 4 million.

- So, why not use MATLAB?
The revised script finished.

MATLAB says that

\[ a = 204290 \]
\[ b = 146996 \]
\[ c = 227033 \]
\[ n = 3 \]

is a counter example to Fermat's last theorem.

With these values, \( a^3 + b^3 = c^3 = 11702185112644936 \).

The script started at 10:21:20 on 11-Apr-12 and terminated at 19:01:40 on 05-May-12. It took 584.6721 hours to run.
(The) Simpsons’ paradox
Where to now?

- Clearly, a better approach is needed.

- We could return to considering curves such as $x^n + y^n = 1$ with rational arguments.

- It turns out progress can be made using elliptic curves.
Elliptic curves

- An elliptic curve over $\mathbb{Q}$ is a curve of the form

$$y^2 = Ax^3 + Bx^2 + Cx + D$$

where $A, B, C$ and $D$ are rational, $A \neq 0$, and the function on the right hand side has distinct roots.

- In 1957 Taniyama and Shimura made the following conjecture about elliptic curves:

  **Taniyama–Shimura conjecture**

  Every elliptic curve is modular.
In 1986, Frey showed that to every counterexample to Fermat’s Last Theorem, there is an associated elliptic curve:

\[ y^2 = x(x - a^p)(x + b^p). \]

Frey noted that this elliptic curve had very strange properties. In particular, he suspected it was not modular.

Later in 1986, Serre proposed the epsilon conjecture. If true, this would show that the so-called Frey curve is not modular.

Ribet proved the epsilon conjecture soon after.
It’s proved Shimura less

Taniyama–Shimura conjecture
Every elliptic curve is modular.

- If FLT is false, there exists a non-modular elliptic curve.
- Taniyama–Shimura $\Rightarrow$ Fermat’s Last Theorem.
Mean Wiles . . .

- Sir Andrew Wiles (born 1953) is an English mathematician.
- Wiles first encountered FLT when he was ten years old. At that point he decided that he would try to solve it.
- Wiles’ research was in the area of elliptic curves, so when he heard that the epsilon conjecture had been proved he committed himself to proving the Taniyama–Shimura conjecture.
Wiles worked in solitude for seven years, without revealing his plans to anyone.

Finally, in 1993, Wiles gave a lecture series on elliptic curves at a conference in Cambridge.

He concluded the talk by proving the Taniyama–Shimura conjecture, and stated “from which it follows that Fermat’s Last Theorem is true. I think I’ll leave it there.”
...and that's the proof of Fermat's Last Theorem!

Woo!

Spring Break!

Girls Gone Wiles
A Taylor-made solution

- But, there was a problem. Upon review, a minor oversight was found in Wiles’ 100-page proof.

- Wiles, dejected, tried to fix the problem himself.

- After many attempts, he enlisted the help of his former student, Richard Taylor. Together, they managed to repair the original proof (using one of Wiles’ early ideas).

- Thus, after 358 years (not 800 Captain Picard), Fermat’s Last Theorem was proved.

- Andrew Wiles collected the Wolfskehl Prize in 1997.
A real-world application
A real-world application
Can we do it?

- Is the number of cans in a stage $n$ Coke Can-tor Set a perfect $n^{th}$ power?

In a stage $n$ Coke Can-tor Set, there are $3^n - 2^n$ cans.

For $n = 1$, $3^1 - 2^1 = 1$.

For $n = 2$, $3^2 - 2^2 = 5$.

What about for $n > 2$?

$$3^n - 2^n = a^n \Rightarrow a^n + 2^n = 3^n$$

No solutions!

Theorem (Michael Albanese and Tronnolone, Hayden 2012)

The number of cans in a stage $n$ Coke Can-tor Set is a perfect $n^{th}$ power only when $n = 1$. 

M. A. T. H. (University of Adelaide)
Can we do it?

- Is the number of cans in a stage \( n \) Coke Can-tor Set a perfect \( n^{\text{th}} \) power?
- In a stage \( n \) Coke Can-tor Set, there are \( 3^n - 2^n \) cans.
- For \( n = 1 \), \( 3^1 - 2^1 = 1^1 \), and for \( n = 2 \), \( 3^2 - 2^2 = 5 \).
- What about for \( n > 2 \)?
Can we do it?

- Is the number of cans in a stage \( n \) Coke Can-tor Set a perfect \( n^{th} \) power?
- In a stage \( n \) Coke Can-tor Set, there are \( 3^n - 2^n \) cans.
- For \( n = 1 \), \( 3^1 - 2^1 = 1^1 \), and for \( n = 2 \), \( 3^2 - 2^2 = 5 \).
- What about for \( n > 2 \)?

\[
3^n - 2^n = a^n \Rightarrow a^n + 2^n = 3^n
\]
Can we do it?

- Is the number of cans in a stage $n$ Coke Can-tor Set a perfect $n^{th}$ power?
- In a stage $n$ Coke Can-tor Set, there are $3^n - 2^n$ cans.
- For $n = 1$, $3^1 - 2^1 = 1^1$, and for $n = 2$, $3^2 - 2^2 = 5$.
- What about for $n > 2$?

$$3^n - 2^n = a^n \Rightarrow a^n + 2^n = 3^n$$

- No solutions!
Can we do it?

- Is the number of cans in a stage $n$ Coke Can-tor Set a perfect $n^{th}$ power?
- In a stage $n$ Coke Can-tor Set, there are $3^n - 2^n$ cans.
- For $n = 1$, $3^1 - 2^1 = 1^1$, and for $n = 2$, $3^2 - 2^2 = 5$.
- What about for $n > 2$?

$$3^n - 2^n = a^n \Rightarrow a^n + 2^n = 3^n$$

- No solutions!

**Theorem (Michael Albanese and Tronnolone, Hayden 2012)**

The number of cans in a stage $n$ Coke Can-tor Set is a perfect $n^{th}$ power only when $n = 1$. 
Many problems in both elementary and algebraic number theory remain unsolved. Did Fermat have a proof? Did Wiles do the right thing?
A-Fermat-ion

- Many problems in both elementary and algebraic number theory remain unsolved.
Many problems in both elementary and algebraic number theory remain unsolved.

Did Fermat have a proof?
Many problems in both elementary and algebraic number theory remain unsolved.

Did Fermat have a proof?

Did Wiles do the right thing?