The Solving of Fermat’s Last Theorem

Karl Rubin
Edward and Vivian Thorp Professor of Mathematics

UCIrvine
School of Physical Sciences

March 20, 2007
Physical Sciences Breakfast Lecture
Pythagorean Theorem

\[ A^2 + B^2 = C^2 \]

- \[ 3^2 + 4^2 = 5^2 \]
- \[ 5^2 + 12^2 = 13^2 \]
- \[ 8^2 + 15^2 = 17^2 \]
- \[ 39^2 + 80^2 = 89^2 \]

...
<table>
<thead>
<tr>
<th></th>
<th>(A)</th>
<th>B</th>
<th>C</th>
<th>angle</th>
</tr>
</thead>
<tbody>
<tr>
<td>120</td>
<td>119</td>
<td>169</td>
<td>45.2</td>
<td></td>
</tr>
<tr>
<td>3456</td>
<td>3367</td>
<td>4825</td>
<td>45.7</td>
<td></td>
</tr>
<tr>
<td>4800</td>
<td>4601</td>
<td>6649</td>
<td>46.2</td>
<td></td>
</tr>
<tr>
<td>13500</td>
<td>12709</td>
<td>18541</td>
<td>46.7</td>
<td></td>
</tr>
<tr>
<td>72</td>
<td>65</td>
<td>97</td>
<td>47.9</td>
<td></td>
</tr>
<tr>
<td>360</td>
<td>319</td>
<td>481</td>
<td>48.5</td>
<td></td>
</tr>
<tr>
<td>2700</td>
<td>2291</td>
<td>3541</td>
<td>49.7</td>
<td></td>
</tr>
<tr>
<td>960</td>
<td>799</td>
<td>1249</td>
<td>50.2</td>
<td></td>
</tr>
<tr>
<td>600</td>
<td>481</td>
<td>769</td>
<td>51.3</td>
<td></td>
</tr>
<tr>
<td>6480</td>
<td>4961</td>
<td>8161</td>
<td>52.6</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>45</td>
<td>75</td>
<td>53.1</td>
<td></td>
</tr>
<tr>
<td>2400</td>
<td>1679</td>
<td>2929</td>
<td>55.0</td>
<td></td>
</tr>
<tr>
<td>240</td>
<td>161</td>
<td>289</td>
<td>56.1</td>
<td></td>
</tr>
<tr>
<td>2700</td>
<td>1771</td>
<td>3229</td>
<td>56.7</td>
<td></td>
</tr>
<tr>
<td>90</td>
<td>56</td>
<td>106</td>
<td>58.1</td>
<td></td>
</tr>
</tbody>
</table>
OBSERVATIO DOMINI PETRI DE FERMAT.

Cvrum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.
Fermat’s Last Theorem

“It is impossible to separate a cube into two cubes,

\[ a^3 + b^3 = c^3 \] has no whole number solutions

or a fourth power into two fourth powers,

\[ a^4 + b^4 = c^4 \] has no whole number solutions

or in general any power greater than the second into two like powers.”

**Fermat’s Last Theorem**

*If* \( n > 2 \) *then* \( a^n + b^n = c^n \) *has no whole number solutions.*
“I have discovered a truly marvelous proof of this, which this margin is not large enough to contain.”
Early progress

<table>
<thead>
<tr>
<th>exponent</th>
<th>solver</th>
<th>year</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Fermat</td>
<td>1640</td>
</tr>
<tr>
<td>3</td>
<td>Euler</td>
<td>1753</td>
</tr>
<tr>
<td>5</td>
<td>Legendre</td>
<td>1825</td>
</tr>
<tr>
<td>7</td>
<td>Lamé</td>
<td>1839</td>
</tr>
<tr>
<td>&lt;37</td>
<td>Kummer</td>
<td>1847</td>
</tr>
<tr>
<td>&lt;100</td>
<td>Kummer</td>
<td>1857</td>
</tr>
<tr>
<td>&lt;125,000</td>
<td>Wagstaff</td>
<td>1978</td>
</tr>
<tr>
<td>&lt;4,000,000</td>
<td>Buhler et al.</td>
<td>1993</td>
</tr>
</tbody>
</table>
If $n$ is large, then a large integer is very unlikely to be an $n$-th power.

- The probability that $a^n + b^n$ is an $n$-th power is less than $1/b^{n-1}$.
- If $a^n + b^n$ is an $n$-th power, then $a, b \geq n$.
- So the probability that some $a^n + b^n$ is an $n$-th power, for some exponent $n \geq 4,000,000$, is less than

$$\sum_{n \geq 4,000,000} \sum_{a \geq n} \sum_{b > a} \frac{1}{b^{n-1}} < 10^{-26,000,000}.$$
By this argument, the chance that Fermat’s Last Theorem is *false* is less than 1 in 26,000,000.

This might be enough to convince someone, but it is *not* a proof of Fermat’s Last Theorem!

*What if Fermat’s Last Theorem were true just for “probabilistic” reasons, and not for a “structural” reason that could lead to a proof?*
An *elliptic curve* is a curve defined by an equation of the form

\[ y^2 = x^3 + Ax^2 + Bx + C \]

with integer constants \( A, B, C \).

The elliptic curve \( y^2 = x^3 − x \) was studied by Fermat.
Elliptic curves

\[ y^2 = x^3 - x \]

\((-1, 0)\) \( (0, 0) \) \( (1, 0) \)
**Theorem (Fermat)**

The only pairs of rational numbers (fractions) $x$ and $y$ that satisfy the equation

$$y^2 = x^3 - x$$

are $(0, 0)$, $(1, 0)$, and $(-1, 0)$.

Fermat used this fact to prove that $a^4 + b^4 = c^4$ has no whole number solutions. It was one of the few complete proofs that he did fit in the margin of his *Diophantus*. 
Elliptic curves

Problems mathematicians study about elliptic curves:

- Given an elliptic curve,
  - find all solutions in integers $x, y$,
  - find all solutions in rational numbers $x, y$.

- Study the collection of all elliptic curves by classifying their important properties.
Elliptic curves and Fermat’s Last Theorem

Suppose Fermat’s Last Theorem is false, so there are $a, b, c$, and $n \geq 3$ such that $a^n + b^n = c^n$. Define an elliptic curve

$$E_{a,b,c} : y^2 = x(x - a^n)(x + b^n).$$

Idea (Frey, 1985)

The elliptic curve $E_{a,b,c}$ has such strange properties that it cannot exist!

If correct, Frey’s idea shows that no such $a, b, c$, and $n$ can exist, and hence Fermat’s Last Theorem is true.
An elliptic curve can be *modular*.

**Conjecture (Shimura, Taniyama, ~1960)**

*Every elliptic curve is modular.*
Modularity

**Theorem (Ribet, 1986)**

\[ a^n + b^n = c^n, \text{ then } E_{a,b,c} \text{ is not modular.} \]

This finally reduces the truth of Fermat’s Last Theorem to a “structural” question about elliptic curves!
Modularity

Theorem (Wiles +, 1994)

If $A$ and $B$ are whole numbers, then the elliptic curve

$$y^2 = x(x - A)(x + B)$$

is modular.
Proof by contradiction:

If Fermat’s Last Theorem is false, then there are $a, b, c$ and $n \geq 3$ such that $a^n + b^n = c^n$. If so, then:

**Theorem (Ribet)**

$E_{a,b,c}$ is not modular.

**Theorem (Wiles)**

$E_{a,b,c}$ is modular.

This contradiction shows that no such $a, b, c, n$ can exist, so Fermat’s Last Theorem is true.
Timeline

Summer 1986
After Ribet’s work, Wiles begins to work on the Shimura-Taniyama conjecture.

Spring 1993
Wiles completes draft manuscript of his proof.

June 21-23, 1993
Wiles announces his proof in three lectures on Modular forms, elliptic curves, and Galois representations at a workshop at the Newton Institute in Cambridge, England.
The announcement

UNIVERSITY OF CAMBRIDGE
ISAAC NEWTON INSTITUTE
FOR MATHEMATICAL SCIENCES

Director: Sir Michael Atiyah, OM, FRS

20 CLARKSON ROAD, CAMBRIDGE, CB3 0EH, U.K.
Tel. (0223) 335999 Fax. (0223) 330530
e-mail: i.newton@newton.cam.ac.uk

L-FUNCTIONS AND ARITHMETIC

Programme for Workshop

P-adic Galois representations, Iwasawa theory, and the Tamagawa numbers of motives.

Monday (June 25)
Monday (June 25)

Tuesday (June 26)
Tuesday (June 26)

Wednesday (June 27)
Wednesday (June 27)

Thursday (June 28)
Thursday (June 28)

Friday (June 29)
Friday (June 29)

10-11 A. Wiles I A. Wiles II A. Wiles III K. Rubin P. Schneider
11-11.30 Coffee Coffee Coffee Coffee Coffee
11.30-12.30 R. Taylor Y. Ihara K. Ribet W. Messing J. Tilouine
12.30-14.00 Lunch Lunch Lunch Lunch Lunch
14.15 I-M Fontaine P. Colmez R. Greenberg P. Berthelot S. Bloch
15 - 15.30 Tea Tea Tea Tea Tea
15.30 - 16.30 B. Perrin-Riou U. de Shalit U. Jannsen M. Harrison B. Mazur

Drinks Party

This will be held in the Fellows Garden, Emmanuel College, from 17.30 - 19.00 on Wednesday, June 27.
The announcement
At Last, Shout of ‘Eureka!’
In Age-Old Math Mystery

BY GINA BOLATA

More than 350 years ago, a
French mathematician wrote a
decisively simple theorem in
the margins of a book, adding that
he had discovered a marvelous
proof of it but lacked space to
include it in the margin. He died
without ever offering his proof, and
mathematicians have been trying ever
since to supply it.

Now, after thousands of claims
of success that proved untrue,
mathematicians say the daunting
challenge, perhaps the most
intractible of unsolved
mathematical problems, has at last been
surmounted.

The problem is Fermat’s last
theorem, and its apparent
conqueror is Dr. Andrew Wiles, a
60-year-old English mathematician
who works at Princeton University.

Dr. Wiles announced the result
yesterday at the last of three
lectures given over three days, at
Cambridge University in
England.

Within a few months of the
conclusion of his final lecture,
computer-mail messages were
sweeping around the world as
mathematicians pressed each other
in the shouting and almost
wholly unexpected result.

“Dr. Andrew Wiles, a
Professor of Mathematics at the
University of Cambridge, this
morning, in a telephone interview
from Cambridge.

The theorem, an overarching
statement about what solutions
are possible for certain
cubic equations, was stated in 1637 by
Pierre de Fermat, a 17th-century
French mathematician and
physicist. Many of the brightest minds
in mathematics have struggled to
find the proof ever since, and
many have concluded that
Fermat, contrary to his
tonalizing claim, had probably failed to
develop one despite his considerable

Continued on Page D12, Column 1

Cutback in U.S. Funds to Reduce
Summer Jobs for New York Youths

BY THOMAS R. LUCAS

With a belated package of Federal
financing about to be approved by Con-
gress, government agencies and com-
munity groups in New York City are
gearing up for a summer jobs program
for teenagers that promises fewer
jobs and shorter periods of employ-
ment than in past years.

The legislation was said that more than 100,000 young
people had applied for summer jobs in
the various government-sponsored programs
and that fewer than half that number of
jobs would be created.

One applicant still hopeful of finding
work in Sarah Moskowitz, 18, of
Brooklyn, said she was looking forward to
a summer job to make up for the
summer she did not work last year.

The New York T

NEW YORK, THURSDAY, JUNE 24, 1993

VOL.CXLII . NO. 49,372
Copyright © 1993 The New York Times

At Last, Shout of ‘Eureka!’
In Age-Old Math Mystery

BY GINA BOLATA

More than 350 years ago, a
French mathematician wrote a
decisively simple theorem in
the margins of a book, adding that
he had discovered a marvelous
proof of it but lacked space to
include it in the margin. He died
without ever offering his proof, and
mathematicians have been trying ever
since to supply it.

Now, after thousands of claims
of success that proved untrue,
mathematicians say the daunting
challenge, perhaps the most
intractible of unsolved
mathematical problems, has at last been
surmounted.

The problem is Fermat’s last
theorem, and its apparent
conqueror is Dr. Andrew Wiles, a
60-year-old English mathematician
who works at Princeton University.

Dr. Wiles announced the result
yesterday at the last of three
lectures given over three days, at
Cambridge University in
England.

Within a few months of the
conclusion of his final lecture,
computer-mail messages were
sweeping around the world as
mathematicians pressed each other
in the shouting and almost
wholly unexpected result.

“Dr. Andrew Wiles, a
Professor of Mathematics at the
University of Cambridge, this
morning, in a telephone interview
from Cambridge.

The theorem, an overarching
statement about what solutions
are possible for certain
cubic equations, was stated in 1637 by
Pierre de Fermat, a 17th-century
French mathematician and
physicist. Many of the brightest minds
in mathematics have struggled to
find the proof ever since, and
many have concluded that
Fermat, contrary to his
tonalizing claim, had probably failed to
develop one despite his considerable

Continued on Page D12, Column 1

Cutback in U.S. Funds to Reduce
Summer Jobs for New York Youths

BY THOMAS R. LUCAS

With a belated package of Federal
financing about to be approved by Con-
gress, government agencies and com-
munity groups in New York City are
gearing up for a summer jobs program
for teenagers that promises fewer
jobs and shorter periods of employ-
ment than in past years.

The legislation was said that more than 100,000 young
people had applied for summer jobs in
the various government-sponsored programs
and that fewer than half that number of
jobs would be created.

One applicant still hopeful of finding
work in Sarah Moskowitz, 18, of
Brooklyn, said she was looking forward to
a summer job to make up for the
summer she did not work last year.

The New York T

NEW YORK, THURSDAY, JUNE 24, 1993

VOL.CXLII . NO. 49,372
Copyright © 1993 The New York Times

At Last, Shout of ‘Eureka!’
In Age-Old Math Mystery

BY GINA BOLATA

More than 350 years ago, a
French mathematician wrote a
decisively simple theorem in
the margins of a book, adding that
he had discovered a marvelous
proof of it but lacked space to
include it in the margin. He died
without ever offering his proof, and
mathematicians have been trying ever
since to supply it.

Now, after thousands of claims
of success that proved untrue,
mathematicians say the daunting
challenge, perhaps the most
intractible of unsolved
mathematical problems, has at last been
surmounted.

The problem is Fermat’s last
theorem, and its apparent
conqueror is Dr. Andrew Wiles, a
60-year-old English mathematician
who works at Princeton University.

Dr. Wiles announced the result
yesterday at the last of three
lectures given over three days, at
Cambridge University in
England.

Within a few months of the
conclusion of his final lecture,
computer-mail messages were
sweeping around the world as
mathematicians pressed each other
in the shouting and almost
wholly unexpected result.

“Dr. Andrew Wiles, a
Professor of Mathematics at the
University of Cambridge, this
morning, in a telephone interview
from Cambridge.

The theorem, an overarching
statement about what solutions
are possible for certain
cubic equations, was stated in 1637 by
Pierre de Fermat, a 17th-century
French mathematician and
physicist. Many of the brightest minds
in mathematics have struggled to
find the proof ever since, and
many have concluded that
Fermat, contrary to his
tonalizing claim, had probably failed to
develop one despite his considerable

Continued on Page D12, Column 1

Cutback in U.S. Funds to Reduce
Summer Jobs for New York Youths

BY THOMAS R. LUCAS

With a belated package of Federal
financing about to be approved by Con-
gress, government agencies and com-
munity groups in New York City are
gearing up for a summer jobs program
for teenagers that promises fewer
jobs and shorter periods of employ-
ment than in past years.

The legislation was said that more than 100,000 young
people had applied for summer jobs in
the various government-sponsored programs
and that fewer than half that number of
jobs would be created.

One applicant still hopeful of finding
work in Sarah Moskowitz, 18, of
Brooklyn, said she was looking forward to
a summer job to make up for the
summer she did not work last year.
By Gita Kolata
New York Times Service
NEW YORK — More than 350 years ago, a French mathematician wrote a deceptive-seeming note, adding that he had discovered a marvelous proof of it but the margin was too narrow to include it in the margin. He died without ever showing his proof, and mathematicians have been trying to prove it ever since.

The problem is known as Fermat’s last theorem, and the first apparent conqueror is Andrew Wiles, 40, an English mathematician who works at Princeton University in New Jersey. Mr. Wiles announced his results Wednesday at the last of three lectures given at Cambridge University in England.

Mr. Wiles’ mission of the end of his final lecture, which many saw as the end of the world as mathematicians know it, was almost immediately and almost universally accepted.

Leonard Adleman of the University of Southern California said he received a message about an hour after Mr. Wiles’ announcement. The message was just a single word: “Yes.”

There are no other mathematicians who could take on the task of proving or disproving Fermat’s last theorem. The theorem, which has been conjectured to be true but has never been proved, states that the equation x^n + y^n = z^n has no solution in positive integers if n is greater than 2.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Andrew Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Andrew Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Andrew Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Andrew Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Andrew Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Andrew Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Andrew Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Andrew Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Andrew Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Andrew Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Andrew Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Andrew Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Andrew Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Andrew Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Andrew Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Andrew Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Andrew Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Andrew Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Andrew Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.

Fermat’s Last Theorem

The equation

x^n + y^n = z^n

where n is an integer greater than 2, has no solution in positive integers.

Ann Wiles savored the moment after presenting his proof of Fermat’s last theorem at lectures at Cambridge University.
Timeline

Summer 1993
A small number of people check Wiles’ manuscript.

Autumn 1993
Rumors circulate of a “gap” in Wiles’ proof.

December 1993
Wiles announces gap.
The "gap"

1993

La enquête

Société

Malgré le travail d’Andrew Wiles, la démonstration du célèbre théorème du mathématicien français buterait sur un "détail".

"Manifestement, il a sauté une maille quand il a tricoté son rang. Mais c’est quand même un beau pull-over. » Le ton est badin, mais il y a du dépité dans le propos de ce mathématicien. Comme la plupart de ses confrères qui, en juin, fêtaient le "tour de force" d’Andrew Wiles, parvenu à résoudre, après trois siècles et demi, le fameux théorème de Fermat (1), il fait aujourd’hui grise mine. Pourtant, la belle démonstration du mathématicien britannique, ou plutôt la trame de cette démonstration, paraissait sans faille. Au début de l’été, chacun s’émerveillait du travail accompli et attendait avec impatience la mise au propre des deux cents pages de son argumentation. Jusqu’à ce jour où le temps s’est arrêté : la démonstration de Wiles avait un trou.

Au début, personne ne s’est inquiété. « Tout le monde savait, confie un mathématicien, que la présentation de Wiles à Cambridge était empreinte de quelques imperfections. Mais a priori, rien de bien grave. » John Coates, un des spécialistes de la théorie des nombres, avait d’ailleurs, à cette époque, rappelé qu’il restait "certains [...] des détails à vérifier", mais, ajoutait-il, ce n’était plus qu’"une question de technique". Pour lui, ce qui avait été présenté à Cambridge "suffisait à démontrer Fermat".

Une « regrettable erreur »

Bien des "détails" ont ainsi été réglés, par l’intermédiaire du courrier électronique, par le petit nombre des références char- mantes et drôles de "peigner" la démonstration de Wiles. Une procédure normale, entachée toutefois d’une anomalie que personne n’aurait critiquée, si le travail avait abouti rapidement : Andrew Wiles s’est en effet entouré du plus grand secret, ne diffusant son texte qu’aux seuls référenes chargés de le peaufiner, alors que la communauté n’aurait demandé qu’un problème dans la démonstration. Lequel ? Personne ne sait qu’elle est la taille du "trou", s’il peut être comblé et dans quel délai. Mais cette fuite organisée peut, peut-être, aider à dénouer l’affaire.

« Même si l’on écoute à lever cet obstacle, s’il existe, sou- ligne le mathématicien Jean-Pierre Serre, du Collège de France, le travail de Wiles reste tout à fait important. La stratégie qu’il a adoptée dans sa tentative de démonstration du théorème de Fermat est très belle, pleine de promesses et suggère une façon de faire et de travailler qui devrait conduire à prospecter bien des voies. »

Place donc aux spécialistes. Peut-être suffira-t-il, si Wiles accepte d’en dire plus, de quelques mois de travail intense aux mathématiciens pour enfin une bonne fois avec Fermat. Ou, au contraire, rester en compagnie du grand Pascal, qui, voilà plus de trois siècles, invitait le magistrat de Tou- louse et de Castres à chercher "ailleurs qui [le] suivent dans [ses] inventions numériques".

"Pour moi, ajoutait-il, je vous confesse que cela me passe de bien loin : je ne suis capable que de les admirer."

JEAN-FRANÇOIS AUGEREAU

(1) Ce qu’Andrew Wiles a tenté de démontrer et a présenté en juin à Cam- bridge (Grande-Bretagne) n’est pas le théorème de Fermat lui-même, mais "cet inaccessible sommet des mathéma- tiques" qu’est la conjecture de Taniyama-Weil. Le grand théorème du magis- trat toulousain n’est en effet qu’une conséquence de cette conjecture plus récente ainsi que l’a montré, il y a quelques années, l’américain Kenneth Ribet (le Monde du 22 juillet).
In view of the speculation on the status of my work on the Taniyama–Shimura conjecture and Fermat’s Last Theorem I will give a brief account of the situation. During the review process a number of problems emerged, most of which have been resolved, but one in particular I have not yet settled. The key reduction of (most cases of) the Taniyama–Shimura conjecture to the calculation of the Selmer group is correct. However the final calculation of a precise upper bound for the Selmer group in the semistable case (of the symmetric square representation associated to a modular form) is not yet complete as it stands. I believe that I will be able to finish this in the near future using the ideas explained in my Cambridge lectures.

The fact that a lot of work remains to be done on the manuscript makes it still unsuitable for release as a preprint. In my course in Princeton beginning in February I will give a full account of this work.

Andrew Wiles
A Polar Station Attuned to the Environment

A proposed design for a replacement South Pole Station would use a string of horseshoe-shaped modular buildings on stilts to permit snow to blow through; waste water would irrigate gardens.

One of three modules for dormitories, kitchens, hydroponic gardens and laboratories.

The New York Times; Illustration by John Papasan

A panel of prominent scientists convened here to listen to the troubles of foundation officials and scientists who are trying to maintain the South Pole Station's research programs in the face of mounting difficulties. The panel will make its recommendations before a meeting in August of the National Science Board, which will advise the White House on a course of action.

Pressing problems include a recent

Continued on Page C4

Continued on Page C3

By GINA KOLATA

ONE year ago, a shy and somewhat secretive mathematician stunned the world by announcing that he had proved Fermat's last theorem, the most famous unsolved problem in mathematics. Yet a year later, he still has not published his proof. Was the claim premature?

In short, it is probably too early to say. A subtle gap has been found in the manuscript of the proof. Its author, Dr. Andrew Wiles of Princeton University, is working in seclusion to close the gap. A tense quietism has settled over the community of mathematicians, a few predicting failure, others expressing confidence based on the fact that Dr. Wiles's proof is already agreed to have conquered part of another major mathematical peak known as the Taniyama conjecture.

It is routine for long mathematical works to circulate before publication and for reviewers to find flaws that the author can often fix. The ground broken by Dr. Wiles's work is so novel that it is hard to gauge the seriousness of the gap that has come to light.

Was the claim to have solved Fermat's last theorem premature, or will Dr. Wiles make good on his claim to have scaled a pinnacle of intellectual achievement? Dr. Wiles himself will not talk about his work on the proof. He did not answer telephone messages left at his office or a letter hand-delivered to his home in Princeton. His friends and colleagues at Princeton University say he seems to be in good
October 1994

Wiles and Richard Taylor announce a new joint paper, completing the proof of Fermat’s Last Theorem

May 1995

Wiles and Taylor-Wiles papers published in *Annals of Mathematics*
Finding on Universe’s Age Poses New Cosmic Puzzle

BY JOHN WILFORD

The most accurate measurement yet of the age of the universe is a result of a new way to estimate the universe’s age. By combining results from two different methods, the team of astronomers led by Dr. David J. Dunlop of the Carnegie Observatories in Pasadena, Calif., have come up with a new calculation that the universe is 8 billion years old. Since the stars in the universe are still so young, this new calculation means that the universe is not as young as some of its components.

Israel and Jordan Sign a Peace Agreement

President Clinton, with Prime Minister Yitzhak Rabin of Israel, left, and Prime Minister Ahto Savi of Finland, signed a peace agreement in Egypt today. The agreement, known as the Oslo Accords, is designed to end the conflict between Israel and Jordan. The agreement includes a partial recognition of Jordan as an independent state and a commitment to a peaceful resolution of the conflict.

Patton in Peekskill: Behind the Revival

For a year and a half, the state of New York has been struggling with the world’s most famous mathematical problem, Fermat’s Last Theorem. The theorem, which states that no three positive integers a, b, and c can satisfy the equation a^n + b^n = c^n for any integer n greater than 2, has been proved by Andrew Wiles. Wiles presented his proof to the world in 1993, and it has been widely accepted. However, some mathematicians have expressed concern that the proof may be valid.

Students at the prestigious Massachusetts Institute of Technology (MIT) have been trying to verify the proof, and their efforts have been supported by MIT, the Clay Mathematics Institute, and the National Science Foundation. The proof is now widely accepted, but some mathematicians have expressed concern that the proof may be valid.

Karl Rubin (UC Irvine)
Modular elliptic curves
and
Fermat’s Last Theorem

By Andrew Wiles

For Nada, Clare, Kate and Olivia

Cubum autem in duos cubos, aut quadratoquadratum in duos quadra-
toquadras, et generaliter nullam in infinitum ultra quadratum
potestatem in duos ejusdem nominis fas est dividere: cujus rei
demonstrationem mirabilem sane detexi. Hanc marginis exiguitas
non caperet.
Pierre de Fermat

Introduction

An elliptic curve over \( \mathbb{Q} \) is said to be modular if it has a finite covering by
a modular curve of the form \( \mathbb{X}_0(N) \). Any such elliptic curve has the property
that its Hasse-Weil zeta function has an analytic continuation and satisfies a
functional equation of the standard type. If an elliptic curve over \( \mathbb{Q} \) with a
given \( j \)-invariant is modular then it is easy to see that all elliptic curves with
the same \( j \)-invariant are modular (in which case we say that the \( j \)-invariant
is modular). A well-known conjecture which grew out of the work of Shimura
and Taniyama in the 1950’s and 1960’s asserts that every elliptic curve over \( \mathbb{Q} \)
is modular. However, it only became widely known through its publication in a
paper of Weil in 1967 [We] (as an exercise for the interested reader!), in which,
moreover, Weil gave conceptual evidence for the conjecture. Although it had been
numerically verified in many cases, prior to the results described in this paper it had only been known that finitely many \( j \)-invariants were modular.

In 1985 Frey made the remarkable observation that this conjecture should
imply Fermat’s Last Theorem. The precise mechanism relating the two was
formulated by Serre as the \( e \)-conjecture and this was then proved by Ribet in
the summer of 1986. Ribet’s result only requires one to prove the conjecture for
semistable elliptic curves in order to deduce Fermat’s Last Theorem.

*The work on this paper was supported by an NSF grant.
The full Shimura-Taniyama conjecture was proved in 1999, using the methods begun by Wiles:

**Theorem (Breuil, Conrad, Diamond & Taylor, 1999)**

*Every elliptic curve is modular.*
Fermat’s Last Theorem is an important milestone. But much more important for the future of mathematics is the substantial progress Wiles made toward the Shimura-Taniyama Conjecture.

The Shimura-Taniyama Conjecture is part of a more general philosophy:

*There are deep and subtle connections between number theory and other branches of mathematics.*
Modularity

A *modular form* is a function on the unit disk that has special symmetries.

A *cusp form* is a modular form that is zero at the “cusps” (certain boundary points).
Every cusp form gives rise to an elliptic curve. If an elliptic curve comes from a cusp form in this way, we say that the elliptic curve is modular.
Modularity

\[
\{\text{Elliptic curves}\} \quad \rightarrow \quad \{\text{Cusp forms}\}
\]

\[
\{\text{“nice” Galois representations}\}
\]
Number theory at UCI
Elliptic curves are everywhere

Elliptic curve cryptography is especially well suited for settings where space or computing power are limited, such as

- Smartcards
Elliptic curves are everywhere

Elliptic curve cryptography is especially well suited for settings where space or computing power are limited, such as

- Cell phones and PDA's
Elliptic curves are everywhere

Elliptic curve cryptography is especially well suited for settings where space or computing power are limited, such as

- Digital postage
Elliptic curves are everywhere
The Solving of Fermat’s Last Theorem

Karl Rubin
Edward and Vivian Thorp Professor of Mathematics

UCIrvine
School of Physical Sciences

March 20, 2007
Physical Sciences Breakfast Lecture