The Solving of Fermat’s Last Theorem

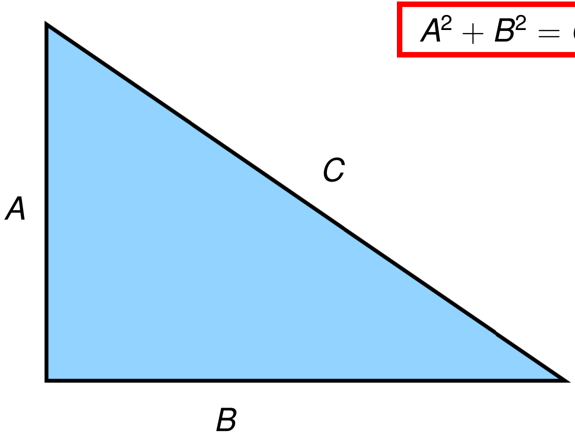
Karl Rubin
Edward and Vivian Thorp Professor of Mathematics

UCIrvine
SCHOOL OF PHYSICAL SCIENCES

March 20, 2007
Physical Sciences Breakfast Lecture

Pythagorean Theorem

$$\boxed{A^2 + B^2 = C^2}$$



$$3^2 + 4^2 = 5^2$$

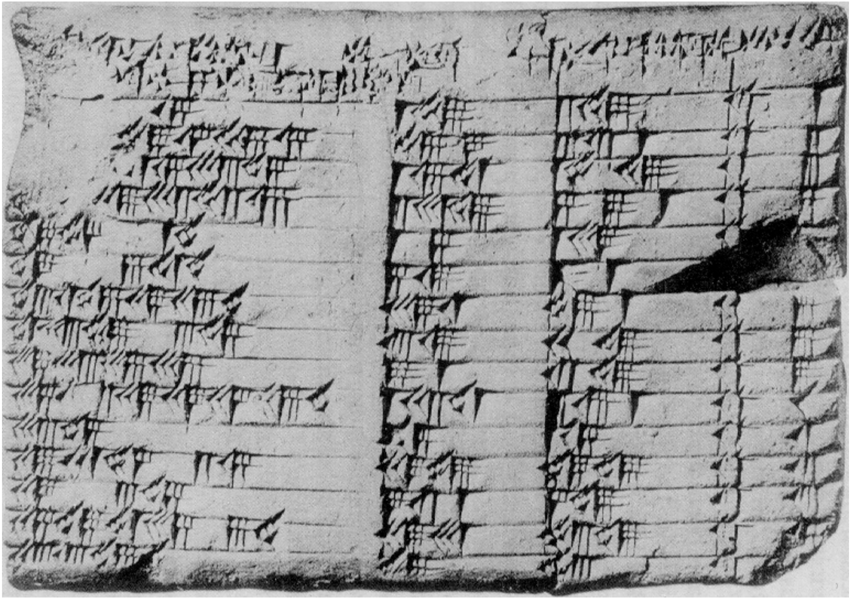
$$5^2 + 12^2 = 13^2$$

$$8^2 + 15^2 = 17^2$$

$$39^2 + 80^2 = 89^2$$

$$\dots$$

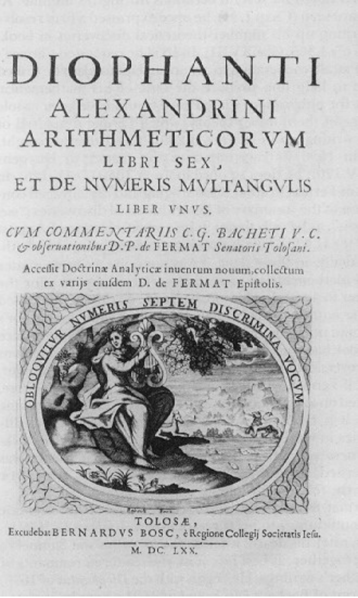
Plympton 322



Plympton 322

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

Diophantus


OBLOQVITVR NVMERIS SEPTEM DISCRIMINA VOCVM

DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.

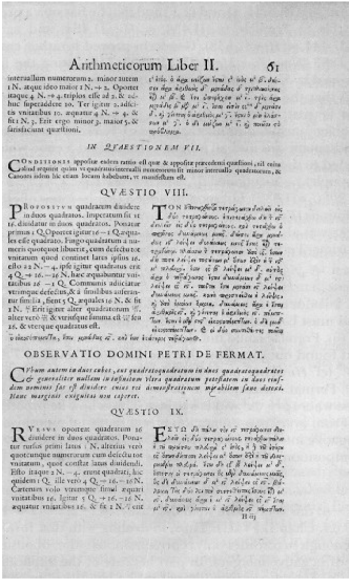
CVM COMMENTARIIS C. G. BACHETI V. C.
& obſeruationibus D. P. de FERMAT *Senatoris Toloſani.*

Acceſſit Doctrinæ Analyticæ inuentum nouum, collectum
ex varijs eiuſdem D. de FERMAT Epiſtolis.

TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Ieſu.
M. DC. LXX.

Fermat

PETRVS DE FERMAT SENATOR THOLOSANVS



Arithmeticorum Liber II. 61

interuallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos eſſe ad 2. & adhuc ſuperaddere 20. Ter igitur 2. adſcitis vnitatibus 10. æquatur 4 N. + 4. & fit 1 N. 3. Erit ergo minor 3. maior 5. & ſatisfaciunt quæſtioni.

[illegible]

IN QVAESTIONEM VII.

CONDITIONIS appoſitæ eadem ratio eſt quæ & appoſitæ præcedenti quæſtioni, nil enim aliud requirit quàm vt quadratus interualli numerorum ſit minor interuallo quadratorum, & Canones iidem hic etiam locum habebunt, vt manifeſtum eſt.

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

ΤΟΝ ἐπιταχθέντα τετράγωνον διελεῖν εἰς δύο τετραγώνους. [illegible]

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.

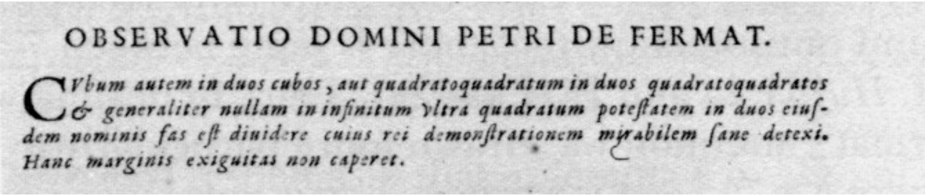
QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rurſus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot conſtat latus diuidendi. Eſto itaque 2 N. − 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. − 16 N. Cæterum volo vtrumque ſimul æquari vnitatibus 16. Igitur 5 Q. + 16. − 16 N. æquatur vnitatibus 16. & fit 1 N. $\frac{16}{5}$ erit

ΕΣΤΩ δὴ πάλιν [illegible]

H iij

Fermat



OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum 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.

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."

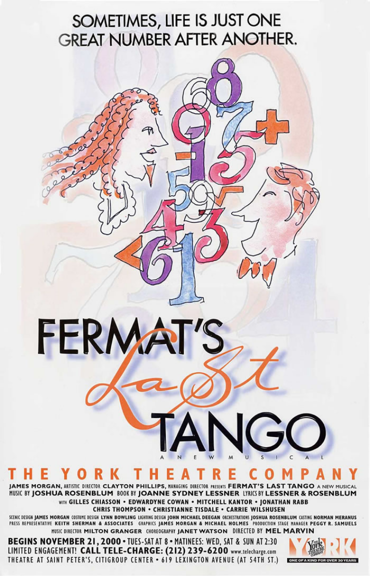
Fermat's Last Theorem

If $n > 2$ then $a^n + b^n = c^n$ has no whole number solutions.

Fermat’s Last Theorem

“*I have discovered a truly marvelous proof of this, which this margin is not large enough to contain.*”

Fermat’s Last Theorem



THE YORK THEATRE COMPANY

JAMES MORGAN, ARTISTIC DIRECTOR CLAYTON PHILLIPS, MANAGING DIRECTOR PRESENTS FERMAT’S LAST TANGO A NEW MUSICAL
MUSIC BY JOSHUA ROSENBLUM BOOK BY JOANNE SYDNEY LESSNER LYRICS BY LESSNER & ROSENBLUM
WITH GILLES CHIASSON • EDWARDYNE COWAN • MITCHELL KANTOR • JONATHAN RABB
CHRIS THOMPSON • CHRISTIANNE TISDALE • CARRIE WILSHUSEN
SCENIC DESIGN JAMES MORGAN COSTUME DESIGN LYNN BOWLING LIGHTING DESIGN JOHN MICHAEL DEEGAN ORCHESTRATIONS JOSHUA ROSENBLUM CASTING NORMAN MERANUS
PRESS REPRESENTATIVE KEITH SHERMAN & ASSOCIATES GRAPHICS JAMES MORGAN & MICHAEL HOLMES PRODUCTION STAGE MANAGER PEGGY R. SAMUELS
MUSIC DIRECTOR MILTON GRANGER CHOREOGRAPHY JANET WATSON DIRECTED BY MEL MARVIN

BEGINS NOVEMBER 21, 2000 • TUES-SAT AT 8 • MATINEES: WED, SAT & SUN AT 2:30
LIMITED ENGAGEMENT! CALL TELE-CHARGE: (212) 239-6200 www.telecharge.com
THEATRE AT SAINT PETER’S, CITIGROUP CENTER • 619 LEXINGTON AVENUE (AT 54TH ST.)

YORK The York Theatre Company
ONE OF A KIND FOR OVER 30 YEARS

Early progress

exponent	*solver*	*year*
4	Fermat	$\sim$ 1640
3	Euler	1753
5	Legendre	1825
7	Lamé	1839
$<$37	Kummer	1847
$<$100	Kummer	1857
$<$125,000	Wagstaff	1978
$<$4,000,000	Buhler *et al.*	1993

Heuristics

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

$$\sum_{n \geq 4{,}000{,}000} \sum_{a \geq n} \sum_{b \geq a} \frac{1}{b^{n-1}} < 10^{-26{,}000{,}000}.$$

Heuristics

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?

Elliptic curves

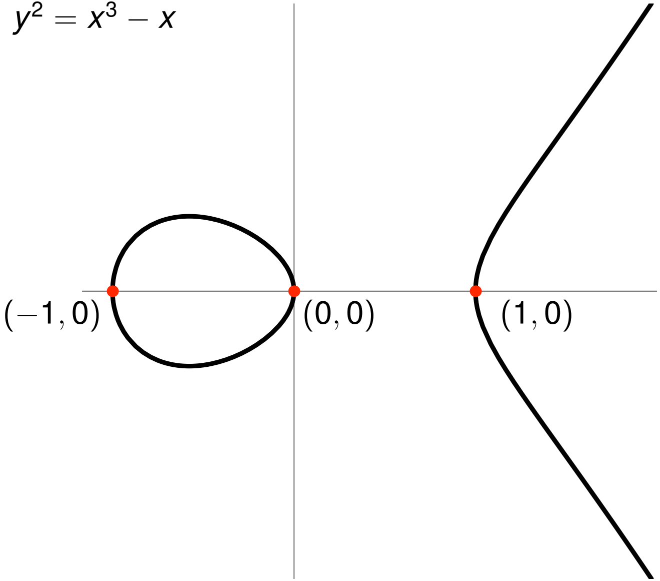
An *elliptic curve* is a curve defined by an equation of the form

$$y^2 = x^3 + Ax^2 + Bx + C$$

with integer constants A, B, C.

The elliptic curve $y^2 = x^3 - x$ was studied by Fermat.

Elliptic curves



Elliptic curves

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!

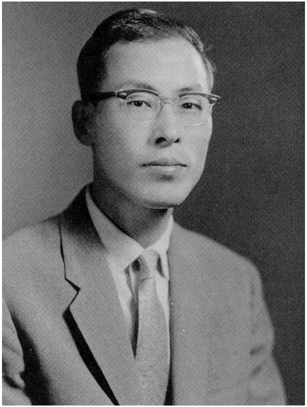
If correct, Frey's idea shows that no such a, b, c, and n can exist, and hence Fermat's Last Theorem is true.

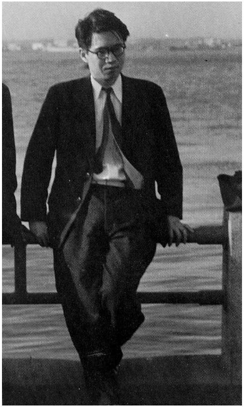
Modularity

An elliptic curve can be *modular*.

Conjecture (Shimura, Taniyama, $\sim$1960)

Every elliptic curve is modular.



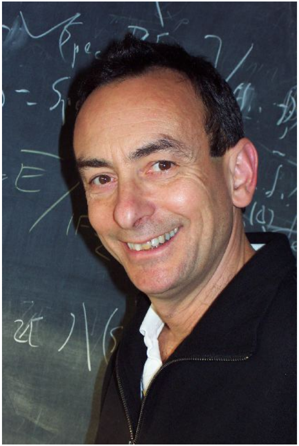


Modularity

Theorem (Ribet, 1986)

If $a^n + b^n = c^n$, then $E_{a,b,c}$ is **not** *modular.*

This finally reduces the truth of Fermat's Last Theorem to a "structural" question about elliptic curves!



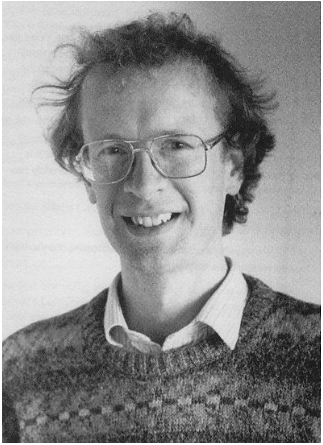
Modularity

Theorem (Wiles +, 1994)

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

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

is *modular.*



Modularity

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.

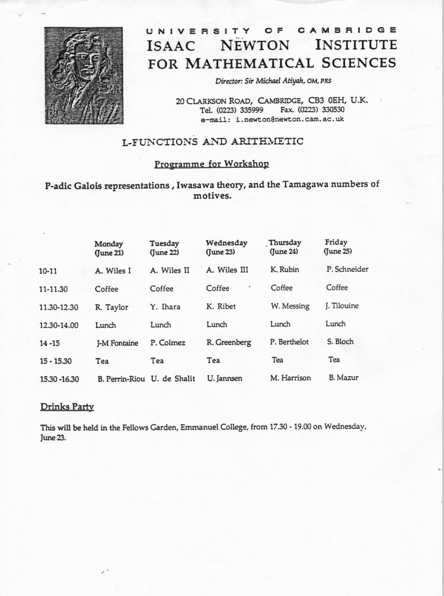
Spring 1993

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 Institue in Cambridge, England.

The announcement



UNIVERSITY OF CAMBRIDGE
ISAAC NEWTON INSTITUTE
FOR MATHEMATICAL SCIENCES

Director: Sir Michael Atiyah, OM, PRS

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.

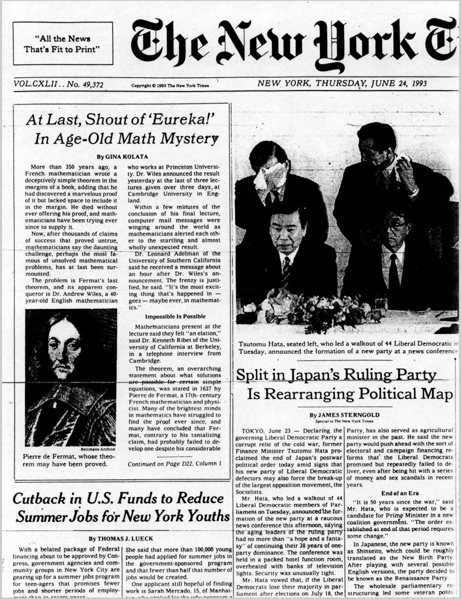
	Monday (June 21)	Tuesday (June 22)	Wednesday (June 23)	Thursday (June 24)	Friday (June 25)
10-11	A. Wiles I	A. Wiles II	A. Wiles III	K. Rubin	P. Schneider
11-11.30	Coffee	Coffee	Coffee	Coffee	Coffee
11.30-12.30	R. Taylor	Y. Ihara	K. Ribet	W. Messing	J. Tilouine
12.30-14.00	Lunch	Lunch	Lunch	Lunch	Lunch
14 -15	J-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 23.

The announcement

The announcement



"All the News
That's Fit to Print"

The New York T

VOL.CXLII . . No. 49,372 Copyright © 1993 The New York Times NEW YORK, THURSDAY, JUNE 24, 1993

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

By GINA KOLATA

More than 350 years ago, a French mathematician wrote a deceptively 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 famous 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 40-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 minutes of the conclusion of his final lecture, computer mail messages were winging around the world as mathematicians alerted each other to the startling and almost wholly unexpected result.

Dr. Leonard Adelman of the University of Southern California said he received a message about an hour after Dr. Wiles's announcement. The frenzy is justified, he said. "It's the most exciting thing that's happened in — geez — maybe ever, in mathematics."

Bettmann Archive

Pierre de Fermat, whose theorem may have been proved.

Impossible Is Possible

Mathematicians present at the lecture said they felt "an elation," said Dr. Kenneth Ribet of the University of California at Berkeley, in a telephone interview from Cambridge.

The theorem, an overarching statement about what solutions are possible for certain simple 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 tantalizing claim, had probably failed to develop one despite his considerable

Continued on Page D22, Column 1

Tsutomu Hata, seated left, who led a walkout of 44 Liberal Democratic
Tuesday, announced the formation of a new party at a news conference

Split in Japan's Ruling Party Is Rearranging Political Map

By JAMES STERNGOLD
Special to The New York Times

TOKYO, June 23 — Declaring the governing Liberal Democratic Party a corrupt relic of the cold war, former Finance Minister Tsutomu Hata proclaimed the end of Japan's postwar political order today amid signs that his new party of Liberal Democratic defectors may also force the break-up of the largest opposition movement, the Socialists.

Mr. Hata, who led a walkout of 44 Liberal Democratic members of Parliament on Tuesday, announced the formation of the new party at a raucous news conference this afternoon, saying the aging leaders of the ruling party had no more than "a hope and a fantasy" of continuing their 38 years of one-party dominance. The conference was held in a packed hotel function room, overheated with banks of television lights. Security was unusually tight.

Mr. Hata vowed that, if the Liberal Democrats lose their majority in parliament after elections on July 18, the Party, has also served as agricultural minister in the past. He said the new party would push ahead with the sort of electoral and campaign financing reforms that the Liberal Democrats promised but repeatedly failed to deliver, even after being hit with a series of money and sex scandals in recent years.

End of an Era

"It is 50 years since the war," said Mr. Hata, who is expected to be a candidate for Prime Minister in a new coalition government. "The order established at end of that period requires some change."

In Japanese, the new party is known as Shinseito, which could be roughly translated as the New Birth Party. After playing with several possible English versions, the party decided to be known as the Renaissance Party.

The wholesale parliamentary restructuring led some veteran politi-

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

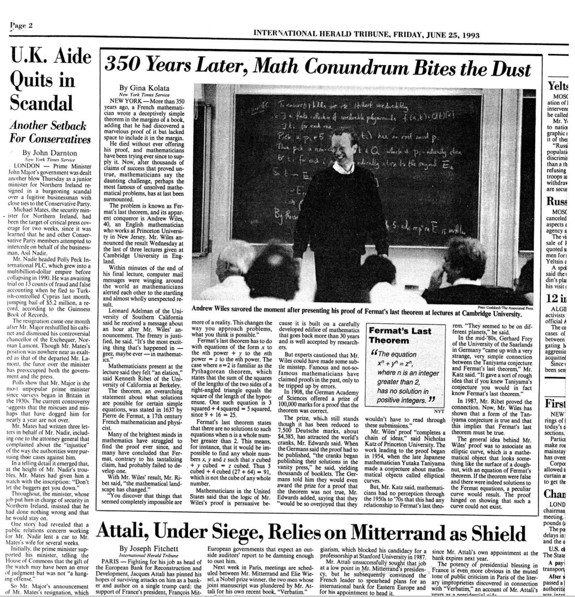
By THOMAS J. LUECK

With a belated package of Federal financing about to be approved by Congress, government agencies and community groups in New York City are gearing up for a summer jobs program for teen-agers that promises fewer jobs and shorter periods of employment than in recent years.

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

One applicant still hopeful of finding work is Sarah Mercado, 15, of Manhattan, who applied for the jobs program a

The announcement



Page 2

INTERNATIONAL HERALD TRIBUNE, FRIDAY, JUNE 25, 1993

U.K. Aide Quits in Scandal

Another Setback For Conservatives

By John Darnton
New York Times Service

LONDON — Prime Minister John Major's government was dealt another blow Thursday as a junior minister for Northern Ireland resigned in a burgeoning scandal over a fugitive businessman with close ties to the Conservative Party.

Michael Mates, the security minister for Northern Ireland, had been the target of critical press coverage for two weeks, since it was learned that he and other Conservative Party members attempted to intercede on behalf of the businessman, Asil Nadir.

Mr. Nadir headed Polly Peck International PLC, which grew into a multibillion-dollar empire before collapsing in 1990. He was awaiting trial on 13 counts of fraud and false accounting when he fled to Turkish-controlled Cyprus last month, jumping bail of $5.2 million, a record, according to the Guinness Book of Records.

The resignation came one month after Mr. Major reshuffled his cabinet and dismissed his controversial chancellor of the Exchequer, Norman Lamont. Though Mr. Mates's position was nowhere near as exalted as that of the departed Mr. Lamont, the furor over the minister has preoccupied both the government and the press.

Polls show that Mr. Major is the most unpopular prime minister since surveys began in Britain in the 1930s. The current controversy suggests that the miscues and mishaps that have dogged him for nearly a year are not over.

Mr. Mates had written three letters in behalf of Mr. Nadir, including one to the attorney general that complained about the "injustice" of the way the authorities were pursuing their cases against him.

In a telling detail it emerged that, at the height of Mr. Nadir's troubles, Mr. Mates had given him a watch with the inscription: "Don't let the buggers get you down."

Throughout, the minister, whose job put him in charge of security in Northern Ireland, insisted that he had done nothing wrong and that he would stay on.

One story had revealed that a public relations concern working for Mr. Nadir lent a car to Mr. Mates's wife for several weeks.

Initially, the prime minister supported his minister, telling the House of Commons that the gift of the watch may have been an error of judgment but was not "a hanging offense."

So Mr. Major's announcement of Mr. Mates's resignation, which

350 Years Later, Math Conundrum Bites the Dust

By Gina Kolata
New York Times Service

NEW YORK — More than 350 years ago, a French mathematician wrote a deceptively 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 famous of unsolved mathematical problems, has at last been surmounted.

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

Within minutes of the end of his final lecture, computer mail messages were winging around the world as mathematicians alerted each other to the startling and almost wholly unexpected result.

Leonard Adelman of the University of Southern California said he received a message about an hour after Mr. Wiles' announcement. The frenzy is justified, he said. "It's the most exciting thing that's happened in — geez, maybe ever — in mathematics."

Mathematicians present at the lecture said they felt "an elation," said Kenneth Ribet of the University of California at Berkeley.

The theorem, an overarching statement about what solutions are possible for certain simple 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 tantalizing claim, had probably failed to develop one.

With Mr. Wiles' result, Mr. Ribet said, "the mathematical landscape has changed."

"You discover that things that seemed completely impossible are more of a reality. This changes the way you approach problems, what you think is possible."

Fermat's last theorem has to do with equations of the form *x* to the *n*th power + *y* to the *n*th power = *z* to the *n*th power. The case where $n=2$ is familiar as the Pythagorean theorem, which states that the sum of the squares of the lengths of the two sides of a right-angled triangle equals the square of the length of the hypotenuse. One such equation is 3 squared + 4 squared = 5 squared, since 9 + 16 = 25.

Fermat's last theorem states that there are no solutions to such equations when n is a whole number greater than 2. This means, for instance, that it would be impossible to find any whole numbers *x*, *y* and *z* such that *x* cubed + *y* cubed = *z* cubed. Thus 3 cubed + 4 cubed (27 + 64) = 91, which is not the cube of any whole number.

Mathematicians in the United States said that the logic of Mr. Wiles's proof is persuasive because it is built on a carefully developed edifice of mathematics that goes back more than 30 years and is well accepted by researchers.

But experts cautioned that Mr. Wiles could have made some subtle misstep. Famous and not-so-famous mathematicians have claimed proofs in the past, only to be tripped up by errors.

In 1908, the German Academy of Sciences offered a prize of 100,000 marks for a proof that the theorem was correct.

The prize, which still stands though it has been reduced to 7,500 Deutsche marks, about $4,385, has attracted the world's cranks, Mr. Edwards said. When the Germans said the proof had to be published, "the cranks began publishing their solutions in the vanity press," he said, yielding thousands of booklets. The Germans told him they would even award the prize for a proof that the theorem was not true, Mr. Edwards added, saying that they "would be so overjoyed that they wouldn't have to read through these submissions."

Mr. Wiles' proof "completes a chain of ideas," said Nicholas Katz of Princeton University. The work leading to the proof began in 1954, when the late Japanese mathematician Yutaka Taniyama made a conjecture about mathematical objects called elliptical curves.

But, Mr. Katz said, mathematicians had no perception through the 1950s to '70s that this had any relationship to Fermat's last theorem. "They seemed to be on different planets," he said.

In the mid-'80s, Gerhard Frey of the University of the Saarlands in Germany "came up with a very strange, very simple connection between the Taniyama conjecture and Fermat's last theorem," Mr. Katz said. "It gave a sort of rough idea that if you knew Taniyama's conjecture you would in fact know Fermat's last theorem."

In 1987, Mr. Ribet proved the connection. Now, Mr. Wiles has shown that a form of the Taniyama conjecture is true and that this implies that Fermat's last theorem must be true.

The general idea behind Mr. Wiles' proof was to associate an elliptic curve, which is a mathematical object that looks something like the surface of a doughnut, with an equation of Fermat's theorem. If the theorem were false and there were indeed solutions to the Fermat equations, a peculiar curve would result. The proof hinged on showing that such a curve could not exist.

Peter Goddard/The Associated Press

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."*

NYT

Attali, Under Siege, Relies on Mitterrand as Shield

By Joseph Fitchett
International Herald Tribune

PARIS — Fighting for his job as head of the European Bank for Reconstruction and Development, Jacques Attali has pinned his hopes of surviving attacks on him as a banker and author on a single trump card: the support of France's president, François Mit-

European governments that expect an outside auditors' report to be damning enough to oust him.

Next week in Paris, meetings are scheduled between Mr. Mitterrand and Elie Wiesel, a Nobel prize winner, the two men whose joint manuscript was plundered by Mr. Attali for his own recent book, "Verbatim."

giarism, which blocked his candidacy for a professorship at Stanford University in 1987.

Mr. Attali unsuccessfully sought that job at a low point in Mr. Mitterrand's presidency, but he subsequently convinced the French leader to spearhead plans for an international bank for Eastern Europe and for his appointment to head it.

since Mr. Attali's own appointment at the bank expires next year.

The potency of presidential blessing in France is even more obvious in the muted tone of public criticism in Paris of the literary improprieties discovered in connection with "Verbatim," an account of Mr. Attali's years as a presidential aide.

Yelts
MOSC
ation of l
interven
he called
Mr. Y
to natio
graphic
it of the
"Russ
populati
discrimi
than a th
refusing
troops a
withdra
are secu

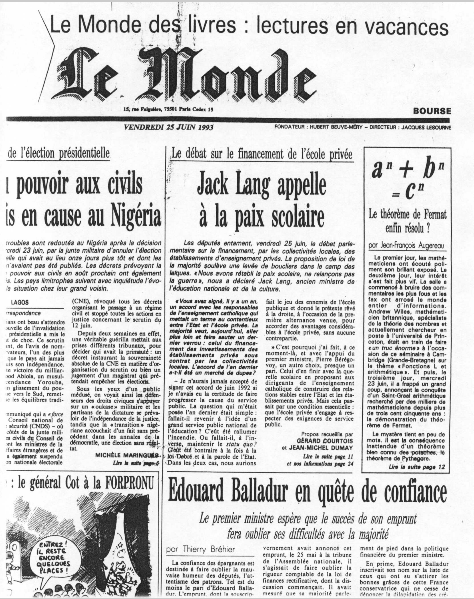
Russ
MOSC
canceled
aspects
agency s
The vi
sale of
quoted s
men for
Yeltsin
A spo
said the
din's pla
his visit

12 in
ALGI
activists
official
The co
cases of
between
gating h
aggressio
acquitted
Since
been sen

First
NEW
rings of
today's
sections.
Partic
make ro
mainstay
has over
Corpo
allowed
curtain a
to get the

Chan
LOND
chairman
meeting.
pounds (
The p
delays in
and the
U.S. c
The State
A pay
transport
After
passed a
authoriti

The announcement


ENTREZ ! IL RESTE ENCORE QUELQUES PLACES !

Le Monde des livres : lectures en vacances

Le Monde

15, rue Falguière, 75501 Paris Cedex 15

BOURSE

VENDREDI 25 JUIN 1993

FONDATEUR : HUBERT BEUVE-MÉRY – DIRECTEUR : JACQUES LESOURNE

de l'élection présidentielle

ı pouvoir aux civils ıs en cause au Nigéria

troubles sont redoutés au Nigéria après la décision rcredi 23 juin, par la junte militaire d'annuler l'élection elle qui avait eu lieu onze jours plus tôt et dont les n'avaient pas été publiés. Les décrets prévoyant la pouvoir aux civils en août prochain ont également ıs. Les pays limitrophes suivent avec inquiétude l'évo- la situation chez leur grand voisin.

LAGOS

rrespondance

ians ont beau s'attendre ouvelle de l'invalidation présidentielle a mis le ıt de choc. Ce scrutin ınt, de l'avis de nom- vateurs, l'un des plus que le pays ait jamais uis son indépendance. te victoire du milliar- ood Abiola, un musul- cendance Yorouba, ın glissement du pou- ue vers le Sud, remet- se les équilibres tradi-

nmuniqué qui a *«force* Conseil national de sécurité (CNDS) – où côtés de la junte mili- es civils du Conseil de ont les ministres de la ffaires étrangères et de a également suspendu on nationale électorale (CNE), révoqué tous les décrets organisant le passage à un régime civil et stoppé toutes les actions en justice concernant le scrutin du 12 juin.

Depuis deux semaines en effet, une véritable guérilla mettait aux prises différents tribunaux, pour décider qui avait la primauté : un décret instaurant la souveraineté absolue de la CNE en matière d'organisation du scrutin ou bien un jugement d'un magistrat qui prétendait empêcher les élections.

Sous les yeux d'un public médusé, on voyait ainsi les défenseurs des droits civiques s'appuyer sur un «oukase» militaire et les partisans de la dictature se prévaloir de l'indépendance de la justice, tandis que la «transition» nigériane accouchait d'un fait sans précédent dans les annales de la démocratie, une élection sans résultat.

MICHÈLE MARINQUES

Lire la suite page 6

Le débat sur le financement de l'école privée

Jack Lang appelle à la paix scolaire

Les députés entament, vendredi 25 juin, le débat parlementaire sur le financement, par les collectivités locales, des établissements d'enseignement privés. La proposition de loi de la majorité soulève une levée de boucliers dans le camp des laïques. «Nous avons rétabli la paix scolaire, ne relançons pas la guerre», nous a déclaré Jack Lang, ancien ministre de l'éducation nationale et de la culture.

«Vous avez signé, il y a un an, un accord avec les responsables de l'enseignement catholique qui mettait un terme au contentieux entre l'Etat et l'école privée. La majorité veut, aujourd'hui, aller plus loin et faire sauter un dernier verrou : celui du financement des investissements des établissements privés sous contrat par les collectivités locales. L'accord de l'an dernier a-t-il été un marché de dupes?

– Je n'aurais jamais accepté de signer cet accord de juin 1992 si je n'avais eu la certitude de faire progresser la cause du service public. La question qui m'était posée l'an dernier était simple : fallait-il revenir à l'idée d'un grand service public national de l'éducation ? C'eût été rallumer l'incendie. Ou fallait-il, à l'inverse, maintenir le *statu quo?* C'eût été contraire à la fois à la loi Debré et à la parole de l'Etat. Dans les deux cas, nous aurions fait le jeu des ennemis de l'école publique et donné le prétexte rêvé à la droite, à l'occasion de la première alternance venue, pour accorder des avantages considérables à l'école privée, sans aucune contrepartie.

» C'est pourquoi j'ai fait, à ce moment-là, et avec l'appui du premier ministre, Pierre Bérégovoy, un autre choix, presque un pari. Celui d'en finir avec la querelle scolaire en proposant aux dirigeants de l'enseignement catholique de construire des relations stables entre l'Etat et les établissements privés. Mais cela passait par une condition essentielle : que l'école privée s'engage à respecter des exigences de service public.

Propos recueillis par
GÉRARD COURTOIS
et JEAN-MICHEL DUMAY

Lire la suite page 11
et nos informations page 24

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

Le théorème de Fermat enfin résolu ?

par Jean-François Augereau

Le premier jour, les mathématiciens ont écouté poliment son brillant exposé. Le deuxième jour, leur intérêt s'est fait plus vif. La salle a commencé à bruire des commentaires les plus fous et les fax ont arrosé le monde entier d'informations. Andrew Wiles, mathématicien britannique, spécialiste de la théorie des nombres et actuellement chercheur en poste à l'université de Princeton, était en train de faire *«un truc énorme»* à l'occasion de ce séminaire à Cambridge (Grande-Bretagne) sur le thème «Fonctions L et arithmétique». Et puis, le troisième jour, mercredi 23 juin, il a frappé un grand coup, annonçant la conquête d'un Saint-Graal arithmétique recherché par des milliers de mathématiciens depuis plus de trois cent cinquante ans : la démonstration du théorème de Fermat.

Le mystère tient en peu de mots. Il est la conséquence inattendue d'un théorème bien connu des potaches, le théorème de Pythagore.

Lire la suite page 12

: le général Cot à la FORPRONU

Edouard Balladur en quête de confiance

Le premier ministre espère que le succès de son emprunt fera oublier ses difficultés avec la majorité

par Thierry Bréhier

La confiance des épargnants est destinée à faire oublier la mauvaise humeur des députés, l'attentisme des patrons. Tel est du moins le pari d'Edouard Balladur. L'emprunt, dont la souscrip- vernement avait annoncé cet emprunt, le 25 mai à la tribune de l'Assemblée nationale, il s'agissait de faire oublier la rigueur comptable de la loi de finances rectificative, dont la discussion commençait. Il avait mesuré que sa majorité parle- ment de pied dans la politique financière du premier ministre.

En prime, Edouard Balladur inscrivait son nom sur la liste de ceux qui ont su s'attirer les bonnes grâces de cette France conservatrice qui ne cesse de dénoncer la dilapidation des cré-

Timeline

Summer 1993

A small number of people check Wiles' manuscript.

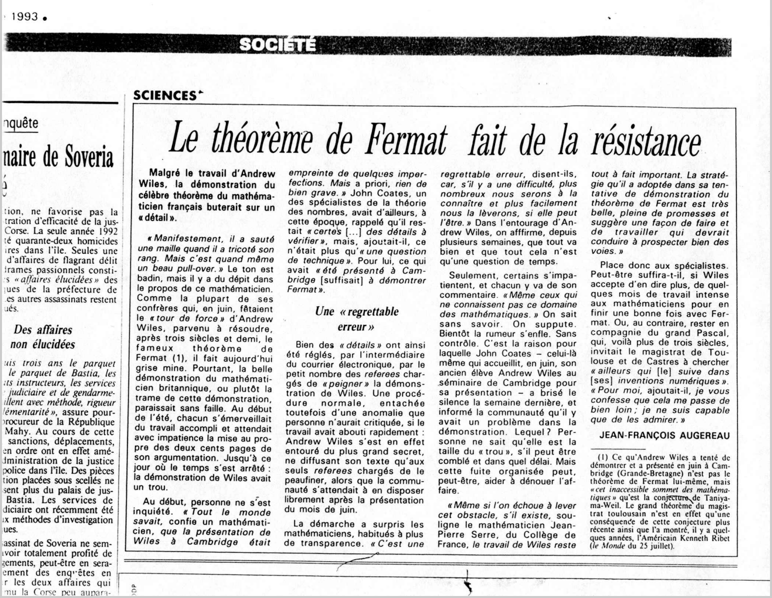
Autumn 1993

Rumors circulate of a "gap" in Wiles' proof.

December 1993

Wiles announces gap.

The “gap”



1993 •

SOCIÉTÉ

nquête

naire de Soveria

tion, ne favorise pas la
tration d'efficacité de la jus-
Corse. La seule année 1992
té quarante-deux homicides
ires dans l'île. Seules une
d'affaires de flagrant délit
lrames passionnels consti-
s *« affaires élucidées »* des
ues de la préfecture de
es autres assassinats restent
ués.

Des affaires non élucidées

uis trois ans le parquet
le parquet de Bastia, les
ıts instructeurs, les services
judiciaire et de gendarme-
illent avec méthode, rigueur
lémentarité », assure pour-
rocureur de la République
Mahy. Au cours de cette
sanctions, déplacements,
en ordre ont en effet amé-
dministration de la justice
police dans l'île. Des pièces
tion placées sous scellés ne
sent plus du palais de jus-
Bastia. Les services de
diciaire ont récemment été
ıx méthodes d'investigation
ues.

assinat de Soveria ne sem-
ıvoir totalement profité de
gements, peut-être en sera-
ement des enqᵛêtes en
r les deux affaires qui
mu la Corse peu aupara-

SCIENCES

Le théorème de Fermat fait de la résistance

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 dépit 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 *« certes* [...] *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 *referees* chargés 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 *referees* chargés de le peaufiner, alors que la communauté s'attendait à en disposer librement après la présentation du mois de juin.

La démarche a surpris les mathématiciens, habitués à plus de transparence. *« C'est une regrettable erreur*, disent-ils, *car, s'il y a une difficulté, plus nombreux nous serons à la connaître et plus facilement nous la lèverons, si elle peut l'être. »* Dans l'entourage d'Andrew Wiles, on afffirme, depuis plusieurs semaines, que tout va bien et que tout cela n'est qu'une question de temps.

Seulement, certains s'impatientent, et chacun y va de son commentaire. *« Même ceux qui ne connaissent pas ce domaine des mathématiques. »* On sait sans savoir. On suppute. Bientôt la rumeur s'enfle. Sans contrôle. C'est la raison pour laquelle John Coates – celui-là même qui accueillit, en juin, son ancien élève Andrew Wiles au séminaire de Cambridge pour sa présentation – a brisé le silence la semaine dernière, et informé la communauté qu'il y avait 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.

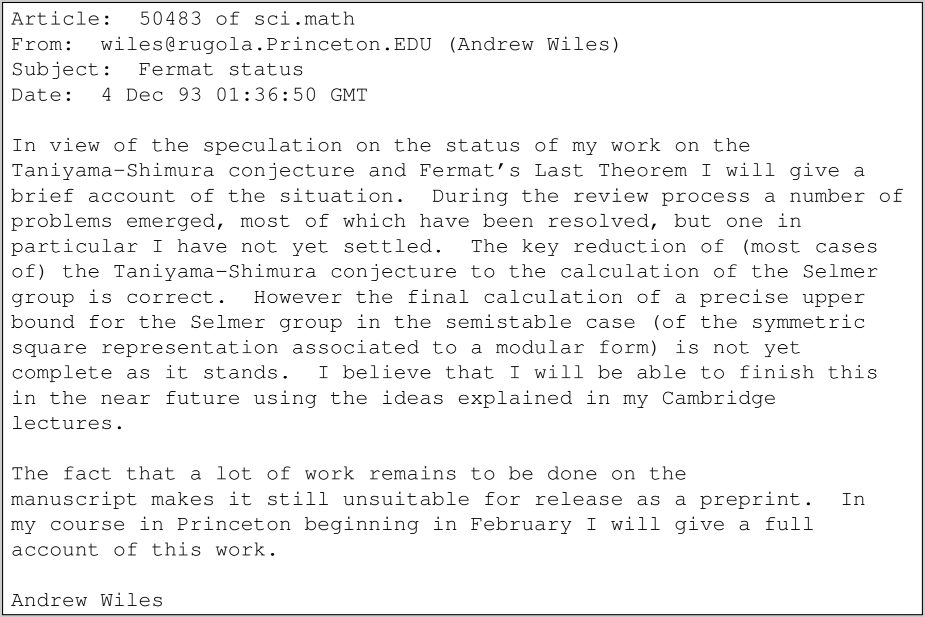
« Même si l'on échoue à lever cet obstacle, s'il existe, souligne le mathématicien Jean-Pierre Serre, du Collège de France, *le travail de Wiles reste tout à fait important. La stratégie qu'il a adoptée dans sa tentative de démonstration du théorème de Fermat est très belle, pleine de promesses et suggère 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 en finir une bonne fois avec Fermat. Ou, au contraire, rester en compagnie du grand Pascal, qui, voilà plus de trois siècles, invitait le magistrat de Toulouse et de Castres à chercher *« ailleurs qui* [le] *suive 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 Cambridge (Grande-Bretagne) n'est pas le théorème de Fermat lui-même, mais *« cet inaccessible sommet des mathématiques »* qu'est la conjecture de Taniyama-Weil. Le grand théorème du magistrat 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 25 juillet).

The “gap”



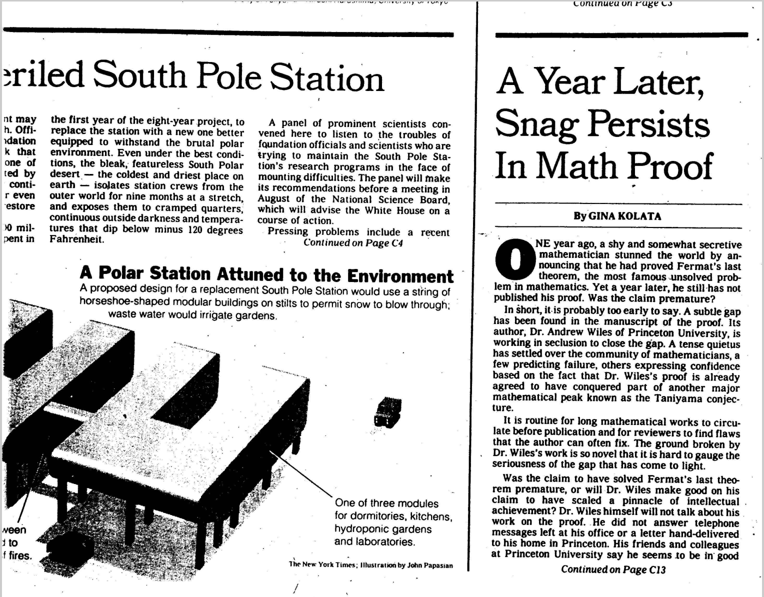
Article: 50483 of sci.math
From: wiles@rugola.Princeton.EDU (Andrew Wiles)
Subject: Fermat status
Date: 4 Dec 93 01:36:50 GMT

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

The “gap”



Continued on Page C3

ɛriled South Pole Station

nt may
h. Offi-
ıdation
k that
one of
ted by
conti-
r even
estore

)0 mil-
pent in

the first year of the eight-year project, to replace the station with a new one better equipped to withstand the brutal polar environment. Even under the best conditions, the bleak, featureless South Polar desert — the coldest and driest place on earth — isolates station crews from the outer world for nine months at a stretch, and exposes them to cramped quarters, continuous outside darkness and temperatures that dip below minus 120 degrees Fahrenheit.

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

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.

ween
d to
f fires.

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

The New York Times; Illustration by John Papasian

A Year Later, Snag Persists In Math Proof

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 quietus 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.

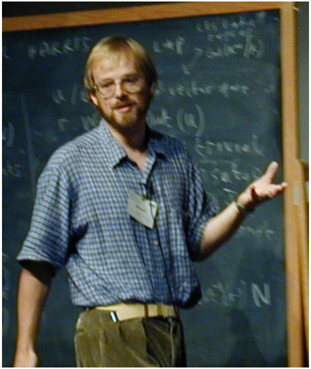
Was the claim to have solved Fermat's last theorem premature, or will Dr. Wiles make good on his claim to have scaled a pinnacle of intellectual achievement? Dr. Wiles himself will not talk about his work on the proof. He did not answer telephone messages left at his office or a letter hand-delivered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

Continued on Page C13

Timeline

October 1994

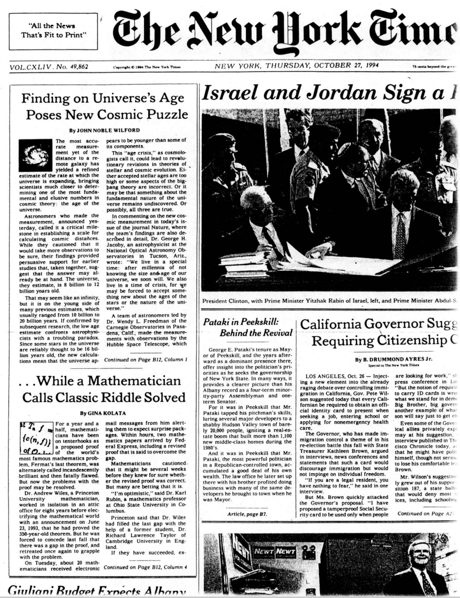
Wiles and Richard Taylor announce a new joint paper, completing the proof of Fermat's Last Theorem



May 1995

Wiles and Taylor-Wiles papers published in *Annals of Mathematics*

Success



"All the News That's Fit to Print"

The New York Time

VOL.CXLIV . No. 49,862 Copyright © 1994 The New York Times NEW YORK, THURSDAY, OCTOBER 27, 1994 75 cents beyond the grea

Finding on Universe's Age Poses New Cosmic Puzzle

By JOHN NOBLE WILFORD

The most accurate measurement yet of the distance to a remote galaxy has yielded a refined estimate of the rate at which the universe is expanding, bringing scientists much closer to determining one of the most fundamental and elusive numbers in cosmic theory: the age of the universe.

Astronomers who made the measurement, announced yesterday, called it a critical milestone in establishing a scale for calculating cosmic distances. While they cautioned that it would take more observations to be sure, their findings provided persuasive support for earlier studies that, taken together, suggest that the answer may already be at hand. The universe, they estimate, is 8 billion to 12 billion years old.

That may seem like an infinity, but it is on the young side of many previous estimates, which usually ranged from 10 billion to 20 billion years. If confirmed by subsequent research, the low age estimate confronts astrophysicists with a troubling paradox. Since some stars in the universe are reliably thought to be 16 billion years old, the new calculations mean that the universe appears to be younger than some of its components.

This "age crisis," as cosmologists call it, could lead to revolutionary revisions in theories of stellar and cosmic evolution. Either accepted stellar ages are too high or some aspects of the big-bang theory are incorrect. Or it may be that something about the fundamental nature of the universe remains undiscovered. Or possibly, all three are true.

In commenting on the new cosmic measurement in today's issue of the journal Nature, where the team's findings are also described in detail, Dr. George H. Jacoby, an astrophysicist at the National Optical Astronomy Observatories in Tucson, Ariz., wrote: "We live in a special time: after millennia of not knowing the size and age of our universe, we soon will. We also live in a time of crisis, for we may be forced to accept something new about the ages of the stars or the nature of the universe."

A team of astronomers led by Dr. Wendy L. Freedman of the Carnegie Observatories in Pasadena, Calif., made the measurements with observations by the Hubble Space Telescope, which

Continued on Page B12, Column 1

. . .While a Mathematician Calls Classic Riddle Solved

By GINA KOLATA

For a year and a half, mathematicians have been on tenterhooks as a proposed proof of the world's most famous mathematics problem, Fermat's last theorem, was alternately called incandescently brilliant and then fatally flawed. But now the problems with the proof may be resolved.

Dr. Andrew Wiles, a Princeton University mathematician, worked in isolation in an attic office for eight years before electrifying the mathematical world with an announcement on June 23, 1993, that he had proved the 350-year-old theorem. But he was forced to concede last fall that there was a gap in the proof, and retreated once again to grapple with the problem.

On Tuesday, about 20 mathematicians received electronic mail messages from him alerting them to expect surprise packages. Within hours, two mathematics papers arrived by Federal Express, including a revised proof that is said to overcome the gap.

Mathematicians cautioned that it might be several weeks before they knew for sure whether the revised proof was correct. But many are betting that it is.

"I'm optimistic," said Dr. Karl Rubin, a mathematics professor at Ohio State University in Columbus.

Princeton said that Dr. Wiles had filled the last gap with the help of a former student, Dr. Richard Lawrence Taylor of Cambridge University in England.

If they have succeeded, ex-

Continued on Page B12, Column 4

Giuliani Budget Expects Albany

Israel and Jordan Sign a

President Clinton, with Prime Minister Yitzhak Rabin of Israel, left, and Prime Minister Abdul-S.

Pataki in Peekskill: Behind the Revival

George E. Pataki's tenure as Mayor of Peekskill, and the years afterward as a dominant presence there, offer insight into the politician's priorities as he seeks the governorship of New York State. In many ways, it provides a clearer picture than his Albany record as a four-term minority-party Assemblyman and one-term Senator.

For it was in Peekskill that Mr. Pataki tapped his pitchman's skills, luring several major developers to a shabby Hudson Valley town of barely 20,000 people, igniting a real-estate boom that built more than 1,100 new middle-class homes during the 1980's.

And it was in Peekskill that Mr. Pataki, the most powerful politician in a Republican-controlled town, accumulated a good deal of his own wealth. The law office he later set up there with his brother profited doing business with many of the same developers he brought to town when he was Mayor.

Article, page B7.

California Governor Sugg Requiring Citizenship C

By B. DRUMMOND AYRES Jr.

Special to The New York Times

LOS ANGELES, Oct. 26 — Injecting a new element into the already raging debate over controlling immigration in California, Gov. Pete Wilson suggested today that every Californian be required to obtain an official identity card to present when seeking a job, entering school or applying for nonemergency health care.

The Governor, who has made immigration control a theme of in his re-election battle this fall with State Treasurer Kathleen Brown, argued in interviews, news conferences and statements that such a card would discourage immigration but would not impinge on individual freedom.

"If you are a legal resident, you have nothing to fear," he said in one interview.

But Ms. Brown quickly attacked the Governor's proposal. "I have proposed a tamperproof Social Security card to be used only when people

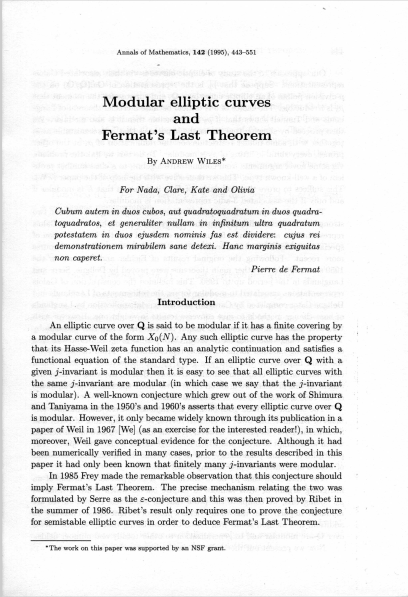
are looking for work," sh
press conference in Lo
"But the notion of requiri
to carry ID cards is wro
what we stand for in dem
Big Brother, big govern
another example of wha
son will say just to get el

Even some of the Gove
ical allies privately exp
may at his suggestion,
interview published in Th
cisco Chronicle today, a
that he might have poli
himself, though not seriou
to lose his comfortable le
Brown.

Mr. Wilson's suggestio
ly grew out of his suppor
sition 187, a state ballo
that would deny most s
ices, including schoolin

Continued on Page A2

Success



Annals of Mathematics, **142** (1995), 443–551

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 quadratoquadratos, 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.

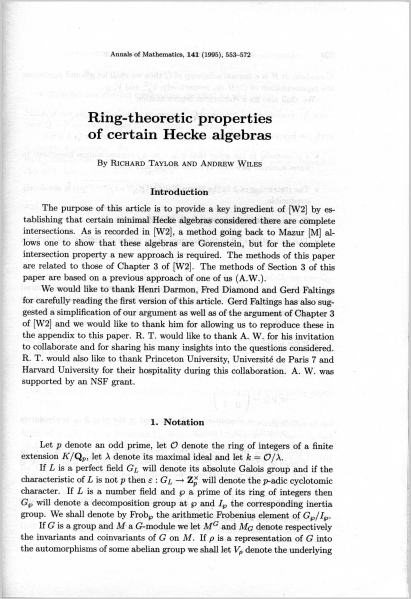
Pierre de Fermat

Introduction

An elliptic curve over **Q** is said to be modular if it has a finite covering by a modular curve of the form $X_0(N)$. 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 **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 **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 ε-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.



Annals of Mathematics, **141** (1995), 553–572

Ring-theoretic properties of certain Hecke algebras

By Richard Taylor and Andrew Wiles

Introduction

The purpose of this article is to provide a key ingredient of [W2] by establishing that certain minimal Hecke algebras considered there are complete intersections. As is recorded in [W2], a method going back to Mazur [M] allows one to show that these algebras are Gorenstein, but for the complete intersection property a new approach is required. The methods of this paper are related to those of Chapter 3 of [W2]. The methods of Section 3 of this paper are based on a previous approach of one of us (A.W.).

We would like to thank Henri Darmon, Fred Diamond and Gerd Faltings for carefully reading the first version of this article. Gerd Faltings has also suggested a simplification of our argument as well as of the argument of Chapter 3 of [W2] and we would like to thank him for allowing us to reproduce these in the appendix to this paper. R. T. would like to thank A. W. for his invitation to collaborate and for sharing his many insights into the questions considered. R. T. would also like to thank Princeton University, Université de Paris 7 and Harvard University for their hospitality during this collaboration. A. W. was supported by an NSF grant.

1. Notation

Let p denote an odd prime, let $\mathcal{O}$ denote the ring of integers of a finite extension $K/\mathbf{Q}_p$, let λ denote its maximal ideal and let $k = \mathcal{O}/\lambda$.

If L is a perfect field G_L will denote its absolute Galois group and if the characteristic of L is not p then $\varepsilon : G_L \to \mathbf{Z}_p^\times$ will denote the p-adic cyclotomic character. If L is a number field and $\wp$ a prime of its ring of integers then $G_\wp$ will denote a decomposition group at $\wp$ and $I_\wp$ the corresponding inertia group. We shall denote by $\mathrm{Frob}_\wp$ the arithmetic Frobenius element of $G_\wp/I_\wp$.

If G is a group and M a G-module we let M^G and M_G denote respectively the invariants and coinvariants of G on M. If ρ is a representation of G into the automorphisms of some abelian group we shall let V_ρ denote the underlying

Success

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.

Success

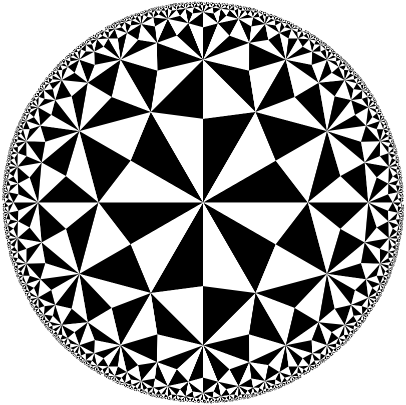
Fermat's Last Theorem is an important milestone. But much more important for the future of mathematics is the substantial progress Wiles made toward the Shimura-Taniyama Conjecture.

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.

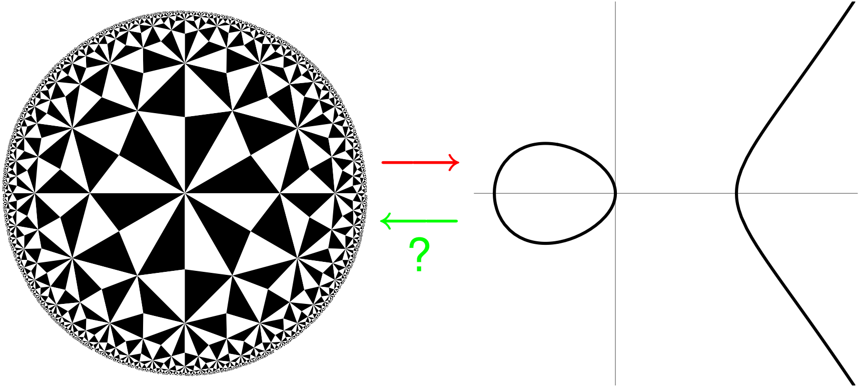
Modularity

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).



Modularity

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

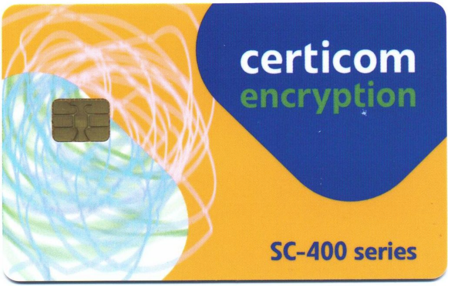
$$\begin{tikzcd}
\left\{\begin{array}{c}\text{Elliptic}\\ \text{curves}\end{array}\right\} \arrow[dr] & & \left\{\begin{array}{c}\text{Cusp}\\ \text{forms}\end{array}\right\} \arrow[ll] \arrow[dl] \\
& \left\{\begin{array}{c}\text{“nice” Galois}\\ \text{representations}\end{array}\right\} &
\end{tikzcd}$$

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

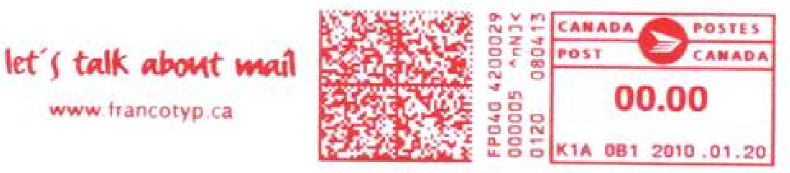
Elliptic curve cryptography is especially well suited for settings where space or computing power are limited, such as

- Cell phones and PDA's

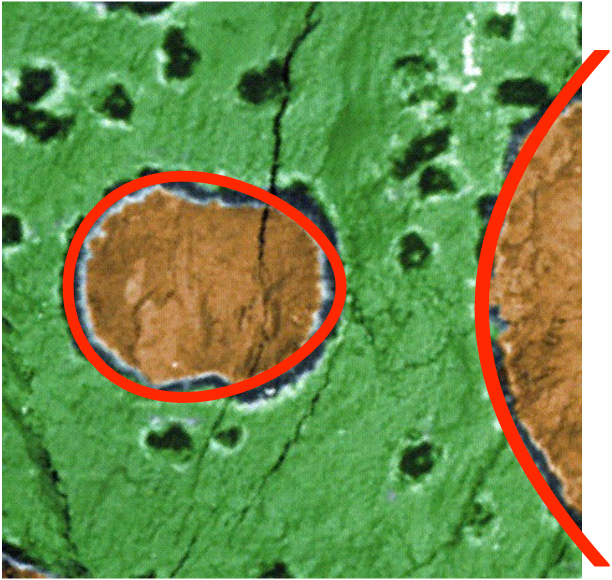
Elliptic curves are everywhere

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