A Brief History of Fermat's Last Theorem

Kenneth A. Ribet

Center for Advanced Mathematical Sciences
November 8, 2021

Background

Fermat’s Last Theorem states that

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

has no solutions in non-zero integers if $n \geq 3$.

Pierre de Fermat thought that he proved it when he wrote his famous 17th century marginal note.

Background

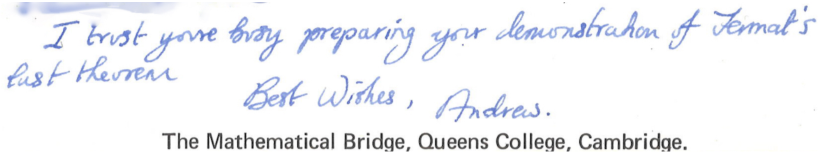
Later in life, using his method of “infinite descent,” Fermat proved that there are no non-zero solutions to Fermat’s equation $x^n + y^n = z^n$ with $n = 4$. Because ruling out non-zero solutions to Fermat’s equation for a given exponent rules out solutions for all *multiples* of the exponent, his proof reduced the Last Theorem to the case where the exponent is an odd prime number.

Background

Later in life, using his method of “infinite descent,” Fermat proved that there are no non-zero solutions to Fermat’s equation $x^n + y^n = z^n$ with $n = 4$. Because ruling out non-zero solutions to Fermat’s equation for a given exponent rules out solutions for all *multiples* of the exponent, his proof reduced the Last Theorem to the case where the exponent is an odd prime number.

In the 18th century, Euler treated the case $n = 3$, thereby reducing to the case of a prime exponent ≥ 5.

The problem remained open until the 1990s.



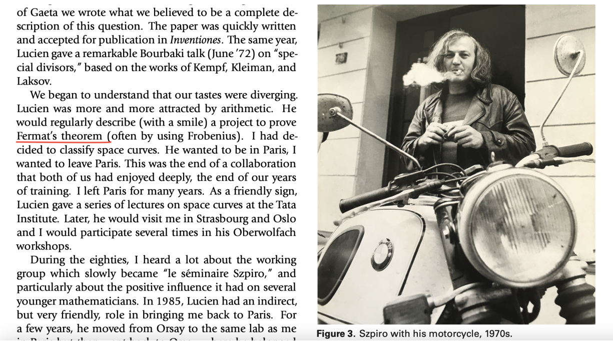
I trust youre busy preparing your demonstration of Fermat's last theorem

Best Wishes, Andrew.

The Mathematical Bridge, Queens College, Cambridge.

Fermat’s Last Theorem and modern arithmetic

In the 1970s, there was a growing feeling that the 20th century techniques of arithmetic algebraic geometry (pioneered by Siegel and Weil) might be fruitful in studying the algebraic curve $x^p + y^p = z^p$. In fact, Barry Mazur’s 1977 study of the family of modular curves $\{X_0(N)\}$ (one for every prime number N) was regarded by some as a prelude to the study of Fermat curves.



of Gaeta we wrote what we believed to be a complete description of this question. The paper was quickly written and accepted for publication in *Inventiones*. The same year, Lucien gave a remarkable Bourbaki talk (June ’72) on “special divisors,” based on the works of Kempf, Kleiman, and Laksov.

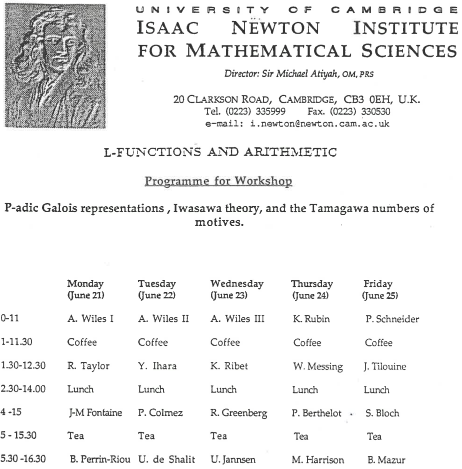
We began to understand that our tastes were diverging. Lucien was more and more attracted by arithmetic. He would regularly describe (with a smile) a project to prove Fermat’s theorem (often by using Frobenius). I had decided to classify space curves. He wanted to be in Paris, I wanted to leave Paris. This was the end of a collaboration that both of us had enjoyed deeply, the end of our years of training. I left Paris for many years. As a friendly sign, Lucien gave a series of lectures on space curves at the Tata Institute. Later, he would visit me in Strasbourg and Oslo and I would participate several times in his Oberwolfach workshops.

During the eighties, I heard a lot about the working group which slowly became “le séminaire Szpiro,” and particularly about the positive influence it had on several younger mathematicians. In 1985, Lucien had an indirect, but very friendly, role in bringing me back to Paris. For a few years, he moved from Orsay to the same lab as me

Figure 3. Szpiro with his motorcycle, 1970s.

Jubilation in 1993

Andrew Wiles announced a proof of Fermat's Last Theorem in June, 1993, at an Isaac Newton Institute workshop on *p*-adic representations, Iwasawa theory, and the Tamagawa numbers of motives.



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

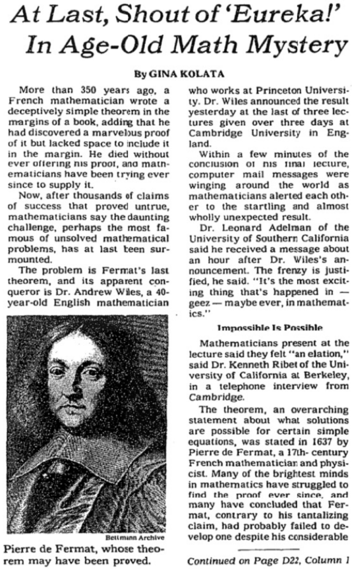
L-FUNCTIONS AND ARITHMETIC

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

The announcement was a great moment for mathematics.



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

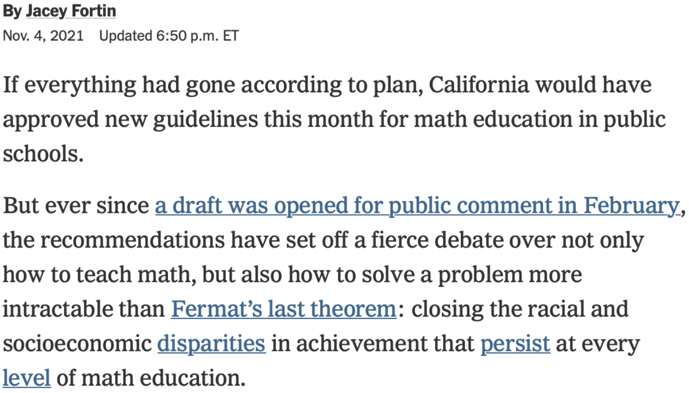
Mathematicians present at the lecture said they felt "an elation," said Dr. Kenneth Ribet of the University of California at Berkeley, in a telephone interview from Cambridge.

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

New York Times—June 24, 1993

Echoes of the “great moment”



By Jacey Fortin

Nov. 4, 2021 Updated 6:50 p.m. ET

If everything had gone according to plan, California would have approved new guidelines this month for math education in public schools.

But ever since a draft was opened for public comment in February, the recommendations have set off a fierce debate over not only how to teach math, but also how to solve a problem more intractable than Fermat’s last theorem: closing the racial and socioeconomic disparities in achievement that persist at every level of math education.

Gina Kolata’s June, 1993 article is referenced in a current New York Times article about K–12 mathematics in California.

Andrew Wiles, June 5, 2002

The gap, and then resolution

Soon after the announcement, Nick Katz was puzzled by a detail as he read Wiles's manuscript.

The "gap" that he had identified left the proof in doubt for 15 months.

A gap-avoiding proof was presented by Richard Taylor and Andrew Wiles in the fall of 1994.

The completed proof consisted of a revision of Wiles's manuscript, along with new work by Taylor and Wiles.

Outline of the 1994 proof

☞ Some terms in this description will be defined in a few moments.

I. It's a proof by contradiction. Assume $a^p + b^p = c^p$ with a, b and c non-zero co-prime integers and p a prime ≥ 5. We will derive a contradiction from this assumption.

II. [A technical point: After possibly permuting a, b and c and changing some signs, we can and do assume that b is even and $c \equiv 1$ mod 4.] We then make the *Frey elliptic curve*:

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

This curve turns out to have the required contradictory properties, a key point being that the discriminant of the cubic polynomial $x(x - a^p)(x + b^p)$ is a perfect pth power.

The proof of Fermat's Last Theorem

This curve turns out to have the required contradictory properties, a key point being that the discriminant of the cubic polynomial $x(x - a^p)(x + b^p)$ is a perfect pth power.

III. Using this key property of the discriminant, I proved (in 1986) that E is not *modular*, i.e., not associated with modular forms.

IV. Wiles (plus Taylor–Wiles) proved that E *is* modular. In fact, Wiles + Taylor–Wiles proved that all semistable elliptic curves over $\mathbf{Q}$ are modular; the Frey curve E is easily seen to be semistable. (We learned a few years later that all elliptic curves over $\mathbf{Q}$ are modular.)

The proof of Fermat's Last Theorem

This curve turns out to have the required contradictory properties, a key point being that the discriminant of the cubic polynomial $x(x-a^p)(x+b^p)$ is a perfect pth power.

III. Using this key property of the discriminant, I proved (in 1986) that E is not *modular*, i.e., not associated with modular forms.

IV. Wiles (plus Taylor–Wiles) proved that E *is* modular. In fact, Wiles + Taylor–Wiles proved that all semistable elliptic curves over **Q** are modular; the Frey curve E is easily seen to be semistable. (We learned a few years later that all elliptic curves over **Q** are modular.)

Together, III + IV give the required contradiction.

Now we have to define some terms…

But first here's a photo of Gerhard Frey and me from June, 2016.

What is an elliptic curve?

An *elliptic curve* over a field is a non-singular projective curve of genus 1 over the field, together with a distinguished point on the curve over the field.

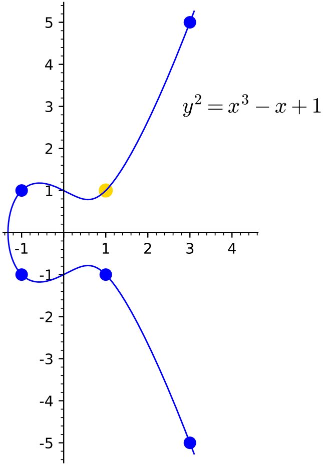
We will take projective curves with affine equation of the form

$$y^2 = \text{a cubic in } x,$$

and use the unique point at infinity in the projective version of each curve as the distinguished point. In order that a curve be non-singular, the defining cubic polynomial in x should have non-zero discriminant.

We already encountered the example $y^2 = x(x - a^p)(x + b^p)$.

The equation $y^2 = x^3 - x + 1$ defines another:



This particular curve happens to have 12 integral points:

$$(-1, \pm 1), (0, \pm 1), (1, \pm 1), (3, \pm 5), (5, \pm 11), (56, \pm 419).$$

Reduction

If E is an elliptic curve over $\mathbf{Q}$ and ℓ is a prime number, we can choose an equation for E with integral coefficients and reduce it mod ℓ. Whenever we succeed in obtaining a non-singular curve in this fashion (for some choice of defining equation), we say that E has *good reduction* mod ℓ.

☞ Bad reduction is the opposite of good reduction.

For example, the elliptic curve with defining equation $y^2 = x^3 - x + 1$ has good reduction at all primes $\neq 2, 23$ and bad reduction at 2 and at 23. (It is relevant that the discriminant of the cubic polynomial $x^3 - x + 1$ is -23.)

The “semistable” hypothesis

If an elliptic curve has bad reduction at a prime ℓ, the reduction may be *additive* or *multiplicative*. An elliptic curve is *semistable* if it has either good or multiplicative reduction at each prime.

Equivalently: every elliptic curve has a *conductor*, which is a positive integer that is divisible by all primes of bad reduction but no primes of good reduction. An elliptic curve is semistable if and only if its conductor is square free.

The elliptic curve defined by $y^2 = x^3 - x + 1$ has multiplicative reduction at 23 and additive reduction at 2. Its conductor is 92.

Modularity

If E is an elliptic curve over **Q**, and ℓ is a prime of good reduction for E, the elliptic curve "E mod ℓ" has a single point at infinity in the projective plane mod ℓ and at most ℓ^2 points in affine 2-space. Thus it has at most $\ell^2 + 1$ points.

Modularity

If E is an elliptic curve over $\mathbf{Q}$, and ℓ is a prime of good reduction for E, the elliptic curve "E mod ℓ" has a single point at infinity in the projective plane mod ℓ and at most ℓ^2 points in affine 2-space. Thus it has at most $\ell^2 + 1$ points.

It is natural to compare the number of points of E over $\mathbf{F}_\ell$ with the number of points of the projective line over $\mathbf{F}_\ell$, namely $\ell + 1$. A theorem of Hasse states that the difference

$$a_\ell = \ell + 1 - |E(\mathbf{F}_\ell)|$$

has absolute value $\leq 2\sqrt{\ell}$.

The *modularity* of E means that the varying numbers a_ℓ are coefficients of a modular form.

The meaning of modularity

The *modularity* of E means that the varying numbers a_ℓ are coefficients of a modular form (of level equal to the conductor of E).

For example, the modular form associated with the elliptic curve $y^2 = x^3 - x + 1$ is a specific Fourier series

$$q - 3q^3 - 2q^5 - 4q^7 + 6q^9 + 2q^{11} - 5q^{13} + 6q^{15} + 4q^{17} - 2q^{19} + \cdots ,$$

where $q = e^{2\pi i \tau}$ with τ in the complex upper half-plane.

That the coefficient of q^7 is -4 indicates that the curve has $7 + 1 + 4 = 12$ points over the field $\mathbf{F}_7$ (including the point at infinity).

12 points over $\mathbf{F}_7$

The assertion is that there are 11 solutions to

$$y^2 = x^3 - x + 1$$

over the field of integers mod 7. The 12 integer solutions

$$(-1, \pm 1), (0, \pm 1), (1, \pm 1), (3, \pm 5), (5, \pm 11), (56, \pm 419)$$

give 10 points mod 7; note that $56 \equiv 0$ and $419 \equiv -1$ mod 7.

The 11th point mod 7 is $(2, 0)$.

The modularity theorem

In 1994, the articles by Wiles and Taylor–Wiles established the modularity of all semistable elliptic curves over $\mathbf{Q}$.

During the period 1994–1999, a group of authors worked individually and then together to enlarge the set of elliptic curves over $\mathbf{Q}$ that were known to be modular. By the summer of 1999, they had proved the *Modularity Theorem*:

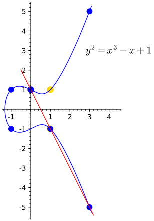
All elliptic curves over $\mathbf{Q}$ *are modular.*

This theorem is the principal result of “On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises” by Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor.

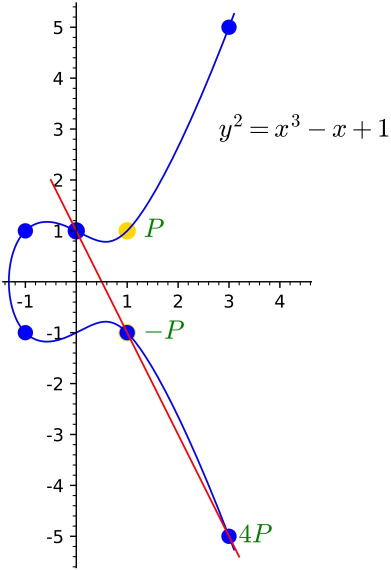
Elliptic curve as group

If E is an elliptic curve, the famous "chord and tangent construction" turns E into a *abelian group*, an algebraic group over $\mathbf{Q}$.

The origin (0 point) of the group is the point at infinity, which is generally written "O." Three points on the curve sum to O is an only if they are colinear.



In this example, the group of points of the curve with rational coordinates is infinite cyclic, generated by the gold-colored point $(1, 1)$.



5
4
3
2
1
-1
-2
-3
-4
-5
-1
1
2
3
4
$y^2 = x^3 - x + 1$
P
$-P$
$4P$

Galois representations

If E is an elliptic curve over $\mathbf{Q}$ and n is a positive integer, the set of points

$$E[n] := \{\, P \in E(\overline{\mathbf{Q}}) \mid n \cdot P = O \,\}$$

is the first homology group of E with coefficients in $\mathbf{Z}/n\mathbf{Z}$, the ring of integers mod n. Of note:

- We get the same set whether we use $\overline{\mathbf{Q}}$ or $\mathbf{C}$.
- The set in question is an abelian group of order n^2 that is in fact a free module over $\mathbf{Z}/n\mathbf{Z}$ of rank 2.
- The Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ permutes $E[n]$ in a way that respects the group law on $E[n]$.
- The action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $E[n]$ is given by a homomorphism (or “representation”)

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}\, E[n] \approx \mathbf{GL}(2, \mathbf{Z}/n\mathbf{Z}).$$

A particular Galois representation

Take E to be the Frey curve

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

and $n = p$ (the exponent in Fermat's equation). Then

$$E[p] = \{\, P \in E(\overline{\mathbf{Q}}) \mid p \cdot P = O \,\}$$

is an $\mathbf{F}_p$-vector space of dimension 2 on which $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts (continuously). We thus get a Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}\, E[p] \approx \mathbf{GL}(2, \mathbf{F}_p).$$

Results of Barry Mazur's 1977 "Eisenstein ideal" article imply that ρ is irreducible (i.e., not upper-triangular in any basis).

Barry Mazur

What's wrong with the Galois representation?

If E is modular, then ρ is automatically modular too: the form f attached to E satisfies

$$\operatorname{tr} \rho(\mathrm{Frob}_\ell) \equiv c_\ell \pmod{p}$$

for almost all primes ℓ.

Although we should think of the (ultimately non-existent) elliptic curve E as having a gigantic conductor (the product of the prime numbers dividing abc), ρ has a very tiny conductor because the discriminant of the cubic polynomial

$$x(x - a^p)(x + b^p)$$

is a pth power. In fact, the tiny conductor is 2.

A conjecture of Serre (published in 1987) about irreducible "odd" two-dimensional representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ predicted that ρ is associated to a form of weight 2 on $\Gamma_0(2)$.

A conjecture of Serre (published in 1987) about irreducible "odd" two-dimensional representations of Gal($\overline{\mathbf{Q}}/\mathbf{Q}$) predicted that ρ is associated to a form of weight 2 on $\Gamma_0(2)$.

A conjecture of Serre (published in 1987) about irreducible "odd" two-dimensional representations of Gal($\overline{\mathbf{Q}}/\mathbf{Q}$) predicted that ρ is associated to a form of weight 2 on $\Gamma_0(2)$. There are none.

Level lowering

In 1986, I proved:

> *If ρ arises from a newform of level N—and looks like it should come from a newform of level 2—then in fact ρ does come from a newform of level 2. Since there are no such newforms, it follows that ρ is not modular.*

☞ Moving from (high) level *N* to level 2 is called *level adjustment* or *level lowering*.

In 1986, I proved:

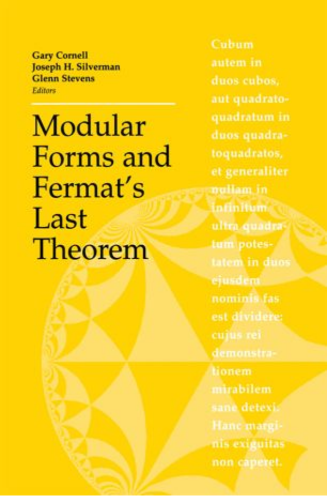
A counterexample to Fermat's Last Theorem would yield a Frey curve whose associated mod *p* Galois representation is not modular. Thus if the Frey curve were known to be modular, we would obtain a contradiction.

In 1986, I proved:

A counterexample to Fermat's Last Theorem would yield a Frey curve whose associated mod p Galois representation is not modular. Thus if the Frey curve were known to be modular, we would obtain a contradiction.

In 1993 and 1994: Wiles + Taylor–Wiles proved that the Frey curve is modular. In fact, they proved that elliptic curves with square free conductor are modular; the Frey curve has this property.

When the proof was new



Gary Cornell
Joseph H. Silverman
Glenn Stevens
Editors

Modular Forms and Fermat's Last Theorem

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.

At Boston University in 1995, experts discussed aspects of the FLT proof. Their lectures are available on Youtube.

Wiles's method

How did we prove that a (semistable) elliptic curve E is modular in 1994? Here is a quick summary:

Wiles's method

How did we prove that a (semistable) elliptic curve E is modular in 1994? Here is a quick summary:

Consider the mod 3 representation attached to E:

$$\rho_3 : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}\, E[3] \approx \mathbf{GL}(2, \mathbf{F}_3).$$

There is no guarantee that ρ_3 is irreducible, but we'll assume that it *is* irreducible to fix ideas. (If not, Wiles would appeal to the "3–5 trick," which in fact was the last element to the proof that he presented in 1993.)

Because $\mathbf{GL}(2, \mathbf{F}_3)$ is a solvable group, we can apply a deep theorem of R. P. Langlands to deduce that ρ_3 is modular. This theorem is the main result of *Base Change for* $\mathbf{GL}(2)$, a 240-page book that was published in 1980.

Wiles's method

Wiles's proof requires an extension of the result of Langlands that was obtained by Jerrold Tunnell in a 1981 Bulletin of the AMS article. People refer to the "Langlands–Tunnell theorem."

Taylor–Wiles

Wiles considered not just ρ_3, but all representations

$$\rho_{3^n} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}\, E[3^n] \approx \mathbf{GL}(2, \mathbf{Z}/3^n\mathbf{Z})$$

for $n \geq 1$. A. Weil (and then Wiles) packaged them together as the 3-adic Galois representation

$$\tilde{\rho}_3 : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}\, E[3^\infty] \approx \mathbf{GL}(2, \mathbf{Z}_3),$$

where $\mathbf{Z}_3$ denotes the 3-adic completion of the ring of integers.

The key contribution of Wiles and Taylor–Wiles is their *relative modularity* or *modularity lifting* theorem, which provides the implication

$$\rho_3 \text{ modular} \implies \tilde{\rho}_3 \text{ modular.}$$

Napa Valley brut after Wiles’s last lecture

Napa Valley brut before my lecture

Taylor–Wiles

The key contribution of Wiles and Taylor–Wiles is their *relative modularity* or *modularity lifting* theorem, which specializes to

$$\rho_3 \text{ modular } \Longrightarrow \tilde{\rho}_3 \text{ modular}$$

in this context.

The modularity of $\tilde{\rho}_3$ is equivalent to the modularity of E. (It is relevant that two integers are equal if they are congruent mod 3^n for all $n \geq 1$.)

Recap (c. 1994)

Begin with $a^p + b^p = c^p$ and form the Frey curve E.

- By Langlands–Tunnell, the mod 3 representation attached to E is modular.
- Modularity lifting implies that E is modular.
- Since E is modular, the mod p Galois representation ρ attached to E is modular.
- By level-lowering, ρ is modular of level 2—contradiction!

Deformations

The proof of relative modularity is organized around the theorem of deformations of Galois representations that was founded by Barry Mazur in the mid-1980s.

Wiles and Taylor–Wiles consider lifts (or *deformations*) of a mod *p* Galois representation ρ to representations

$$\tilde{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, R),$$

where *R* is a complete Noetherian local ring whose residue field is the field over which ρ is defined (so that it makes sense to say that ρ is the reduction of $\tilde{\rho}$). In application, *p* would be 3 and ρ would be ρ_3.

The relative modularity theorem may be paraphrased as follows: if ρ is modular, and $\tilde{\rho}$ satisfies some necessary conditions for modularity, then in fact $\tilde{\rho}$ is modular.

$\mathcal{R} = \mathbf{T}$

Wiles and Taylor–Wiles worked with the “universal” deformation of ρ

$$\rho_{\mathcal{R}} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \mathcal{R})$$

to a representation with the necessary conditions for modularity.

The universality means that all plausibly modular deformations arise (up to isomorphism) from maps $\mathcal{R} \to R$. In this picture, there’s a natural quotient **T** of $\mathcal{R}$ that corresponds to those deformations that are actually modular.

Wiles and Taylor–Wiles proved that the quotient

$$\mathcal{R} \to \mathbf{T}$$

is in fact an isomorphism of rings. In the current lingo, they established the first $\mathcal{R} = \mathbf{T}$ theorem.

Beyond 1994: Lots of $\mathcal{R} = \mathbf{T}$ theorems

A large literature has grown up over the topic of relative modularity. Mark Kisin, in particular, pioneered the generalizations.

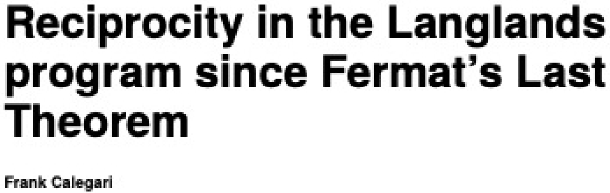
Frank Calegari reports that he was able to identity over 25 articles in top math journals whose main result is an $\mathcal{R} = \mathbf{T}$ theorem.

Beyond 1994: Lots of $\mathcal{R} = \mathbf{T}$ theorems

A large literature has grown up over the topic of relative modularity. Mark Kisin, in particular, pioneered the generalizations.

Frank Calegari reports that he was able to identity over 25 articles in top math journals whose main result is an $\mathcal{R} = \mathbf{T}$ theorem.

Frank Calegari often discusses current developments in this direction in his blog Persiflage.



Reciprocity in the Langlands program since Fermat’s Last Theorem

Frank Calegari

Frank recently submitted a long survey article to the Journal of the European Mathematical Society that discusses developments in this subject since 1993.

Beyond 1994: Potential modularity

Around 2000, Richard Taylor introduced the notion of *potential modularity*, a catchphrase for the strategy of proving that an object over a totally real number field F, which one hopes to be modular over F, is at least modular over some totally real field $F' \supseteq F$.

Taylor's ideas are spelled out in a 2002 article with the innocuous title "Remarks on a conjecture of Fontaine and Mazur."

Beyond 1994: Serre's conjecture is a theorem

Serre's conjecture was proved in 2005 by Shekhar Khare for representations that are ramified only at p ("level 1 case") and in general by Khare and Jean-Pierre Wintenberger in 2008.

Their proof is a tour de force that includes many clever and original arguments to harness theorems on relative modularity and potential modularity to reach their goal.

A skeletal 2020 proof

- Start with (a, b, c).
- Make $E : y^2 = x(x - a^p)(x + b^p)$.
- Introduce the mod p Galois representation arising from E.
- Next, forget about E entirely.
- Apply the theorem of Khare–Wintenberger to the mod p representation to get a contradiction.

We now know a lot

Michael Harris in Quanta Magazine:

> *. . . 10 mathematicians gathered at the Institute for Advanced Study in Princeton, New Jersey, in a successful effort to prove a connection between elliptic curves and modular forms in a new setting. They had all followed different routes to understanding the structure of Wiles' proof, which appeared when some of them were still small children. If asked to reproduce the proof as a sequence of logical deductions, they would undoubtedly have come up with 10 different versions. . . .*

Harris's quotation is from a fairly recent article on the proof of Fermat's Last Theorem by Michael Harris.

QUANTIZED COLUMNS

Why the Proof of Fermat's Last Theorem Doesn't Need to Be Enhanced

More from Harris's article:

> *[Proving modularity] was the object of Wiles' seven-year quest. It's hard from our present vantage point to appreciate the audacity of his venture.*

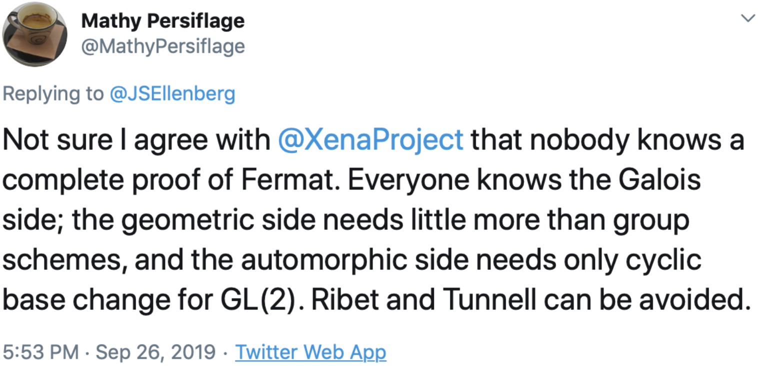
Kevin Buzzard: “The future of mathematics”

Kevin Buzzard has written:

> *I believe that no human, alive or dead, knows all the details of the proof of Fermat’s Last Theorem.*

His comment surprised me, but he does have a point.

Frank Calegari's reply



Mathy Persiflage
@MathyPersiflage

Replying to @JSEllenberg

Not sure I agree with @XenaProject that nobody knows a complete proof of Fermat. Everyone knows the Galois side; the geometric side needs little more than group schemes, and the automorphic side needs only cyclic base change for GL(2). Ribet and Tunnell can be avoided.

5:53 PM · Sep 26, 2019 · Twitter Web App

This Xena Project post contains a more in-depth discussion.

Avoiding Ribet and Tunnell

In an email message to me, Khare sketched out a very compact proof of Fermat's Last Theorem that uses the techniques of the Khare–Wintenberger proof of Serre's conjecture and a theorem of J.-M. Fontaine: the initial mod p Galois representation from the Frey curve lifts to a p-adic representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ that arises ultimately from an abelian variety over $\mathbf{Q}$ with good reduction outside 2 and semistable reduction at 2. Fontaine's work implies that there is no such abelian variety (other than 0).

Conclusion

The techniques of Wiles and Taylor–Wiles have led to immense progress in the Langlands program. We know more about the relationship between Galois representations and automorphic representations of reductive groups than was imaginable 25 years ago.

Conclusion

The techniques of Wiles and Taylor–Wiles have led to immense progress in the Langlands program. We know more about the relationship between Galois representations and automorphic representations of reductive groups than was imaginable 25 years ago.

When I began preparing this talk, I imagined that the current proof of Fermat’s Last Theorem would not be radically dissimilar from the view that we presented in the conference at Boston University in 1995. Indeed, the main ideas of the 1994 proof (including the Taylor–Wiles method) remain present in any recounting of Fermat’s Last Theorem.

Conclusion

The techniques of Wiles and Taylor–Wiles have led to immense progress in the Langlands program. We know more about the relationship between Galois representations and automorphic representations of reductive groups than was imaginable 25 years ago.

When I began preparing this talk, I imagined that the current proof of Fermat's Last Theorem would not be radically dissimilar from the view that we presented in the conference at Boston University in 1995. Indeed, the main ideas of the 1994 proof (including the Taylor–Wiles method) remain present in any recounting of Fermat's Last Theorem.

I realize now that the subject has evolved considerably, and many new ideas have been introduced in the last quarter-century.