

Automorphic Functions And Fermat's Last Theorem (2)

Chun-Xuan Jiang

P. O. Box 3924, Beijing 100854, P. R. China

Jiangchunxuan@vip.sohu.com

Abstract

In 1637 Fermat wrote: “It is impossible to separate a cube into two cubes, or a biquadrate into two biquadrates, or in general any power higher than the second into powers of like degree: I have discovered a truly marvelous proof, which this margin is too small to contain.”

This means: $x^n + y^n = z^n$ ($n > 2$) has no integer solutions, all different from 0 (i.e., it has only the trivial solution, where one of the integers is equal to 0). It has been called Fermat's last theorem (FLT). It suffices to prove FLT for exponent 4. and every prime exponent P . Fermat proved FLT for exponent 4. Euler proved FLT for exponent 3.

In this paper using automorphic functions we prove FLT for exponents $6P$ and P , where P is an odd prime. The proof of FLT must be direct. But indirect proof of FLT is disbelieving.

In 1974 Jiang found out Euler formula of the cyclotomic real numbers in the cyclotomic fields

$$\exp\left(\sum_{i=1}^{2n-1} t_i J^i\right) = \sum_{i=1}^{2n} S_i J^{i-1} \quad (1)$$

where J denotes a $2n$ th root of unity, $J^{2n} = 1$, n is an odd number, t_i are the real numbers.

S_i is called the automorphic functions (complex hyperbolic functions) of order $2n$ with $2n-1$ variables [5,7].

$$S_i = \frac{1}{2n} \left[e^{A_1} + 2 \sum_{j=1}^{\frac{n-1}{2}} (-1)^{(i-1)jB_j} \cos\left(\theta_j + (-1)^j \frac{(i-1)j\pi}{n}\right) \right] + \frac{(-1)^{(i-1)}}{2n} \left[e^{A_2} + 2 \sum_{j=1}^{\frac{n-1}{2}} (-1)^{(i-1)j} e^{D_j} \cos\left(\phi_j + (-1)^{j+1} \frac{(i-1)j\pi}{n}\right) \right], \quad (2)$$

where $i = 1, \dots, 2n$;

$$A_1 = \sum_{\alpha=1}^{2n-1} t_\alpha, \quad B_j = \sum_{\alpha=1}^{2n-1} t_\alpha (-1)^{\alpha j} \cos \frac{\alpha j \pi}{n}, \quad \theta_j = (-1)^{(j+1)} \sum_{\alpha=1}^{2n-1} t_\alpha (-1)^{\alpha j} \sin \frac{\alpha j \pi}{n},$$

$$A_2 = \sum_{\alpha=1}^{2n-1} t_\alpha (-1)^\alpha, \quad D_j = \sum_{\alpha=1}^{2n-1} t_\alpha (-1)^{(j-1)\alpha} \cos \frac{\alpha j \pi}{n},$$

$$\phi_j = (-1)^j \sum_{\alpha=1}^{2n-1} t_\alpha (-1)^{(j-1)\alpha} \sin \frac{\alpha j \pi}{n}, \quad A_1 + A_2 + 2 \sum_{j=1}^{\frac{n-1}{2}} (B_j + D_j) = 0 \quad (3)$$

From (2) we have its inverse transformation[5,7]

$$e^{A_1} = \sum_{i=1}^{2n} S_i, \quad e^{A_2} = \sum_{i=1}^{2n} S_i (-1)^{1+i}$$

$$e^{B_j} \cos \theta_j = S_1 + \sum_{i=1}^{2n-1} S_{1+i} (-1)^{ij} \cos \frac{ij\pi}{n},$$

$$e^{B_j} \sin \theta_j = (-1)^{(j+1)} \sum_{i=1}^{2n-1} S_{1+i} (-1)^{ij} \sin \frac{ij\pi}{n},$$

$$e^{D_j} \cos \phi_j = S_1 + \sum_{i=1}^{2n-1} S_{1+i} (-1)^{(j-1)i} \cos \frac{ij\pi}{n}$$

$$e^{D_j} \sin \phi_j = (-1)^j \sum_{i=1}^{2n-1} S_{1+i} (-1)^{(j-1)i} \sin \frac{ij\pi}{n} \quad (4)$$

(3) and (4) have the same form.

From (3) we have

$$\exp \left[A_1 + A_2 + 2 \sum_{j=1}^{\frac{n-1}{2}} (B_j + D_j) \right] = 1 \quad (5)$$

From (4) we have

$$\exp \left[A_1 + A_2 + 2 \sum_{j=1}^{\frac{n-1}{2}} (B_j + D_j) \right] = \begin{vmatrix} S_1 & S_{2n} & \cdots & S_2 \\ S_2 & S_1 & \cdots & S_3 \\ \cdots & \cdots & \cdots & \cdots \\ S_{2n} & S_{2n-1} & \cdots & S_1 \end{vmatrix}$$

$$= \begin{vmatrix} S_1 & (S_1)_1 & \cdots & (S_1)_{2n-1} \\ S_2 & (S_2)_1 & \cdots & (S_2)_{2n-1} \\ \cdots & \cdots & \cdots & \cdots \\ S_{2n} & (S_{2n})_1 & \cdots & (S_{2n})_{2n-1} \end{vmatrix} \quad (6)$$

where $(S_i)_j = \frac{\partial S_i}{\partial t_j}$ [7].

From (5) and (6) we have circulant determinant

$$\exp \left[A_1 + A_2 + 2 \sum_{j=1}^{\frac{n-1}{2}} (B_j + D_j) \right] = \begin{vmatrix} S_1 & S_{2n} & \cdots & S_2 \\ S_2 & S_1 & \cdots & S_3 \\ \cdots & \cdots & \cdots & \cdots \\ S_{2n} & S_{2n-1} & \cdots & S_1 \end{vmatrix} = 1 \quad (7)$$

If $S_i \neq 0$, where $i = 1, 2, 3, \dots, 2n$, then (7) have infinitely many rational solutions.

Let $n = 1$. From (3) we have $A_1 = t_1$ and $A_2 = -t_1$. From (2) we have

$$S_1 = \text{ch } t_1 \quad S_2 = \text{sh } t_1 \quad (8)$$

we have Pythagorean theorem

$$\text{ch}^2 t_1 - \text{sh}^2 t_1 = 1 \quad (9)$$

(9) has infinitely many rational solutions.

Assume $S_1 \neq 0, S_2 \neq 0, S_i \neq 0$, where $i = 3, \dots, 2n$. $S_i = 0$ are $(2n-2)$ indeterminate equations with $(2n-1)$ variables. From (4) we have

$$\begin{aligned} e^{A_1} &= S_1 + S_2, \quad e^{A_2} = S_1 - S_2, \quad e^{2B_j} = S_1^2 + S_2^2 + 2S_1S_2(-1)^j \cos \frac{j\pi}{n}, \\ e^{2D_j} &= S_1^2 + S_2^2 + 2S_1S_2(-1)^{j+1} \cos \frac{j\pi}{n} \end{aligned} \quad (10)$$

Example. Let $n = 15$. From (3) and (10) we have Fermat's equation

$$\exp[A_1 + A_2 + 2 \sum_{j=1}^7 (B_j + D_j)] = S_1^{30} - S_2^{30} = (S_1^{10})^3 - (S_2^{10})^3 = 1 \quad (11)$$

From (3) we have

$$\exp(A_1 + 2B_3 + 2B_6) = [\exp(\sum_{j=1}^5 t_{5j})]^5 \quad (12)$$

From (10) we have

$$\exp(A_1 + 2B_3 + 2B_6) = S_1^5 + S_2^5 \quad (13)$$

From (12) and (13) we have Fermat's equation

$$\exp(A_1 + 2B_3 + 2B_6) = S_1^5 + S_2^5 = [\exp(\sum_{j=1}^5 t_{5j})]^5 \quad (14)$$

Euler prove that (19) has no rational solutions for exponent 3 [8]. Therefore we prove that (14) has no rational solutions for exponent 5.

Theorem. Let $n = 3P$ where P is an odd prime. From (7) and (8) we have Fermat's equation

$$\exp(A_1 + A_2 + 2 \sum_{j=1}^{\frac{3P-1}{2}} (B_j + D_j)) = S_1^{6P} - S_2^{6P} = (S_1^{2P})^3 - (S_2^{2P})^3 = 1 \quad (15)$$

From (3) we have

$$\exp\left(A_1 + 2 \sum_{j=1}^{\frac{P-1}{2}} B_{3j}\right) = \left[\exp\left(\sum_{j=1}^5 t_{jP}\right)\right]^P \quad (16)$$

From (10) we have

$$\exp\left(A_1 + 2 \sum_{j=1}^{\frac{P-1}{2}} B_{3j}\right) = S_1^P + S_2^P \quad (17)$$

From (16) and (17) we have Fermat's equation

$$\exp\left(A_1 + 2 \sum_{j=1}^{\frac{P-1}{2}} B_{3j}\right) = S_1^P + S_2^P = \left[\exp\left(\sum_{j=1}^5 t_{jP}\right)\right]^P \quad (18)$$

Euler prove that (15) has no rational solutions for exponent 3[8]. Therefore we prove that (18) has no rational solutions for prime exponent P [5,7].

Remark. It suffices to prove FLT for exponent 4. Let $n = 4P$, where P is an odd prime. We have the Fermat's equation for exponent $4P$ and the Fermat's equation for exponent P [2,5,7]. This is the proof that Fermat thought to have had. In complex hyperbolic functions let exponent n be $n = \Pi P$, $n = 2\Pi P$ and $n = 4\Pi P$. Every factor of exponent n has the Fermat's equation [1-7]. In complex trigonometric functions let exponent n be $n = \Pi P$, $n = 2\Pi P$ and $n = 4\Pi P$. Every factor of exponent n has Fermat's equation [1-7]. Using modular elliptic curves Wiles and Taylor prove FLT [9, 10]. This is not the proof that Fermat thought to have had. The classical theory of automorphic functions, created by Klein and Poincare, was concerned with the study of analytic functions in the unit circle that are invariant under a discrete group of transformation. Automorphic functions are the generalization of trigonometric, hyperbolic, elliptic, and certain other functions of elementary analysis. The complex trigonometric functions and complex hyperbolic functions have a wide application in mathematics and physics.

Acknowledgments. We thank Chenny and Moshe Klein for their help and suggestion.

References

- [1] Jiang, C-X, Fermat last theorem had been proved, Potential Science (in Chinese), 2.17-20 (1992), Preprints (in English) December (1991). <http://www.wbabin.net/math/xuan47.pdf>.
- [2] Jiang, C-X, Fermat last theorem had been proved by Fermat more than 300 years ago, Potential Science (in Chinese), 6.18-20(1992).
- [3] Jiang, C-X, On the factorization theorem of circulant determinant, Algebras, Groups and Geometries, 11. 371-377(1994), MR. 96a: 11023, <http://www.wbabin.net/math/xuan45.pdf>
- [4] Jiang, C-X, Fermat last theorem was proved in 1991, Preprints (1993). In: Fundamental open problems in science at the end of the millennium, T.Gill, K. Liu and E. Trelle (eds). Hadronic

- Press, 1999, P555-558. <http://www.wbabin.net/math/xuan46.pdf>.
- [5] Jiang, C-X, On the Fermat-Santilli theorem, *Algebras, Groups and Geometries*, 15, 319-349(1998)
- [6] Jiang, C-X, Complex hyperbolic functions and Fermat's last theorem, *Hadronic Journal Supplement*, 15, 341-348(2000).
- [7] Jiang, C-X, Foundations of Santilli's Isonumber Theory with applications to new cryptograms, Fermat's theorem and Goldbach's Conjecture. *Inter. Acad. Press*. 2002. MR2004c:11001, <http://www.wbabin.net/math/xuan13.pdf>. <http://www.i-b-r.org/docs/jjiang.pdf>
- [8] Ribenboim, P, *Fermat last theorem for amateur*, Springer-Verlag, (1999).
- [9] Wiles A, Modular elliptic curves and Fermat's last theorem, *Ann of Math*, (2) 141 (1995), 443-551.
- [10] Taylor, R. and Wiles, A., Ring-theoretic properties of certain Hecke algebras, *Ann. of Math.*, (2) 141(1995), 553-572.

Fermat's Last Theorem

Fermat's last Theorem: There is no positive integers x , y , z , and $n > 2$ such that $x^n + y^n = z^n$

was broadcast on 15 January 1996

At the age of ten, browsing through his public library, Andrew Wiles stumbled across the world's greatest mathematical puzzle. Fermat's Last Theorem had baffled mathematicians for over 300 years. But from that day, little Andrew dreamed of solving it. Tonight's HORIZON tells the story of his obsession, and how, thirty years later, he gave up everything to achieve his childhood dream.

Deep in our classroom memories lies the enduring notion that "the square of the hypotenuse is equal to the sum of the squares of the other two sides": Pythagoras's Theorem for right-angled triangles. Written down, it is also the simplest of mathematical equations: $x^2 + y^2 = z^2$

In 1637, a French mathematician, Pierre de Fermat said that this equation could not be true for $x^3 + y^3 = z^3$ or for any equation $x^n + y^n = z^n$ where n is greater than 2. Tantalisingly, he wrote on his Greek text: "I have discovered a truly marvellous proof, which this margin is too narrow to contain." No one has found the proof, and for 350 years attempts to prove "F.L.T." attracted huge prizes, mistaken and eccentric claims, but met with failure.

Simon Singh and John Lynch's film tells the enthralling and emotional story of Andrew Wiles. A quiet English mathematician, he was drawn into

maths by Fermat's puzzle, but at Cambridge in the '70s, FLT was considered a joke, so he set it aside. Then, in 1986, an extraordinary idea linked this irritating problem with one of the most profound ideas of modern mathematics: the Taniyama-Shimura Conjecture, named after a young Japanese mathematician who tragically committed suicide. The link meant that if Taniyama was true then so must be FLT. When he heard, Wiles went after his childhood dream again. **"I knew that the course of my life was changing."** For seven years, he worked in his attic study at Princeton, telling no one but his family. **"My wife has only known me while I was working on Fermat"**, says Andrew. In June 1993 he reached his goal. At a three-day lecture at Cambridge, he outlined a proof of Taniyama - and with it Fermat's Last Theorem. Wiles' retiring life-style was shattered. Mathematics hit the front pages of the world's press.

Then disaster struck. His colleague, Dr Nick Katz, made a tiny request for clarification. It turned into a gaping hole in the proof. As Andrew struggled to repair the damage, pressure mounted for him to release the manuscript - to give up his dream. So Andrew Wiles retired back to his attic. He shut out everything, but Fermat.

A year later, at the point of defeat, he had a revelation. **"It was the most important moment in my working life. Nothing I ever do again will be the same."** The very flaw was the key to a strategy he had abandoned years before. In an instant Fermat was proved; a life's ambition achieved; the greatest puzzle of maths was no more.

PROF. ANDREW WILES:

Perhaps I could best describe my experience of doing mathematics in terms of entering a dark mansion. One goes into the first room and it's dark, completely dark, one stumbles around bumping into the furniture and then gradually you learn where each piece of furniture is, and finally after six months or so you find the light switch, you turn it on suddenly it's all illuminated, you can see exactly where you were.

At the beginning of September I was sitting here at this desk when suddenly, totally unexpectedly, I had this incredible revelation. It was the most, the most important moment of my working life. Nothing I ever do again will... I'm sorry.

NARRATOR:

This is the story of one man's obsession with the world's greatest mathematical problem. For seven years Professor Andrew Wiles worked in complete secrecy, creating the calculation of the century. It was a calculation which brought him fame, and regret.

ANDREW WILES:

So I came to this. I was a 10-year-old and one day I happened to be looking in my local public library and I found a book on math and it, it told a bit about the history of this problem that someone had resolved this problem 300 years ago, but no-one had ever seen the proof, no-one knew if there was a proof, and people ever since have looked for the proof and here was a problem that I, a 10-year-old, could understand, but none of the great mathematicians in the past had been able to resolve, and from that moment of course I just, just tried to solve it myself. It was such a challenge, such a beautiful problem.

This problem was Fermat's last theorem.

NARRATOR:

Pierre de Fermat was a 17th-century French mathematician who made some of the greatest breakthroughs in the history of numbers. His inspiration came from studying the *Arithmetica*, that Ancient Greek text.

PROF. JOHN CONWAY:

Fermat owned a copy of this book, which is a book about numbers with lots of problems, which presumably Fermat tried to solve. He studied it, he, he wrote notes in the margins.

NARRATOR:

Fermat's original notes were lost, but they can still be read in a book published by his son. It was one of these notes that was Fermat's greatest legacy.

JOHN CONWAY:

And this is the fantastic observation of Master Pierre de Fermat which caused all the trouble. "Cubum autem in duos cubos"

NARRATOR:

This tiny note is the world's hardest mathematical problem. It's been unsolved for centuries, yet it begins with an equation so simple that children know it off by heart.

CHILDREN:

The square of the hypotenuse is equal to the sum of the squares of the other two sides.

JOHN CONWAY:

Yes well that's Pythagoras's theorem isn't it, that's what we all did at school. So Pythagoras's theorem, the clever thing about it is that it tells

us when three numbers are the sides of a right-angle triangle. That happens just when $x^2 + y^2 = z^2$.

ANDREW WILES:

$x^2 + y^2 = z^2$, and you can ask: well what are the whole numbers solutions of this equation? And you quickly find there's a solution $3^2 + 4^2 = 5^2$. Another one is $5^2 + 12^2 = 13^2$, and you go on looking and you find more and more. So then a natural question is, the question Fermat raised: supposing you change from squares, supposing you replace the two by three, by four, by five, by six, by any whole number 'n', and Fermat said simply that you'll never find any solutions, however, however far you look you'll never find a solution.

NARRATOR:

You will never find numbers that fit this equation, if n is greater than 2. That's what Fermat said, and what's more, he said he could prove it. In a moment of brilliance, he scribbled the following mysterious note.

JOHN CONWAY:

Written in Latin, he says he has a truly wonderful proof "Demonstrationem mirabilem" of this fact, and then the last words are: "Hanc marginis exiguitas non caperet" - this margin is too small to contain this.

NARRATOR:

So Fermat said he had a proof, but he never said what it was.

JOHN CONWAY:

Fermat made lots of marginal notes. People took them as challenges and over the centuries every single one of them has been disposed of, and the last one to be disposed of is this one. That's why it's called the last theorem.

NARRATOR:

Rediscovering Fermat's proof became the ultimate challenge, a challenge which would baffle mathematicians for the next 300 years.

JOHN CONWAY:

Gauss, the greatest mathematician in the world...

BARRY MAZUR:

Oh yes, Galois...

JOHN COATES:

Kummer of course...

KEN RIBET:

Well in the 18th-century Euler didn't prove it.

JOHN CONWAY:

Well you know there's only been the one woman really...

KEN RIBET:

Sophie Germain

BARRY MAZUR:

Oh there are millions, there are lots of people

PETER SARNAK:

But nobody had any idea where to start.

ANDREW WILES:

Well mathematicians just love a challenge and this problem, this particular problem just looked so simple, it just looked as if it had to have a solution, and of course it's very special because Fermat said he had a solution.

NARRATOR:

Mathematicians had to prove that no numbers fitted this equation but with the advent of computers, couldn't they check each number one by one and show that none of them fitted?

JOHN CONWAY:

Well how many numbers are there to beat that with? You've got to do it for infinitely many numbers. So after you've done it for one, how much closer have you got? Well there's still infinitely many left. After you've done it for 1,000 numbers, how many, how much closer have you got? Well there's still infinitely many left. After you've done a few million, there's still infinitely many left. In fact, you haven't done very many have you?

NARRATOR:

A computer can never check every number. Instead, what's needed is a mathematical proof.

PETER SARNAK:

A mathematician is not happy until the proof is complete and considered complete by the standards of mathematics.

NICK KATZ:

In mathematics there's the concept of proving something, of knowing it with absolute certainty.

PETER SARNAK:

Which, well it's called rigorous proof.

KEN RIBET:

Well rigorous proof is a series of arguments...

PETER SARNAK:

...based on logical deductions.

KEN RIBET:

...which just builds one upon another.

PETER SARNAK:

Step by step.

KEN RIBET:

Until you get to...

PETER SARNAK:

A complete proof.

NICK KATZ:

That's what mathematics is about.

NARRATOR:

A proof is a sort of reason. It explains why no numbers fit the equation without having to check every number. After centuries of failing to find a proof, mathematicians began to abandon Fermat in favour of more serious maths.

In the 70s Fermat was no longer in fashion. At the same time Andrew Wiles was just beginning his career as a mathematician. He went to Cambridge as a research student under the supervision of Professor John Coates.

JOHN COATES:

I've been very fortunate to have Andrew as a student, and even as a research student he, he was a wonderful person to work with. He had very deep ideas then and it, it was always clear he was a mathematician who would do great things.

NARRATOR:

But not with Fermat. Everyone thought Fermat's last theorem was impossible, so Professor Coates encouraged Andrew to forget his childhood dream and work on more mainstream maths.

ANDREW WILES:

The problem with working on Fermat is that you could spend years getting nothing so when I went to Cambridge my advisor, John Coates, was working on Iwasawa theory and elliptic curves and I started working with him.

NARRATOR:

Elliptic curves were the in thing to study, but perversely, elliptic curves are neither ellipses nor curves.

BARRY MAZUR:

You may never have heard of elliptic curves, but they're extremely important.

JOHN CONWAY:

OK, so what's an elliptic curve?

BARRY MAZUR:

Elliptic curves - they're not ellipses, they're cubic curves whose solution have a shape that looks like a doughnut.

PETER SARNAK:

It looks so simple yet the complexity, especially arithmetic complexity, is immense.

NARRATOR:

Every point on the doughnut is the solution to an equation. Andrew Wiles now studied these elliptic equations and set aside his dream. What he didn't realise was that on the other side of the world elliptic curves and Fermat's last theorem were becoming inextricably linked.

GORO SHIMURA:

I entered the University of Tokyo in 1949 and that was four years after the War, but almost all professors were tired and the lectures were not inspiring.

NARRATOR:

Goro Shimura and his fellow students had to rely on each other for inspiration. In particular, he formed a remarkable partnership with a young man by the name of Utaka Taniyama.

GORO SHIMURA:

That was when I became very close to Taniyama. Taniyama was not a very careful person as a mathematician. He made a lot of mistakes, but he, he made mistakes in a good direction and so eventually he got right answers and I tried to imitate him, but I found out that it is very difficult to make good mistakes.

NARRATOR:

Together, Taniyama and Shimura worked on the complex mathematics of modular functions.

NICK KATZ:

I really can't explain what a modular function is in one sentence. I can try and give you a few sentences to explain it.

PETER SARNAK:

LAUGHS

NICK KATZ:

I really can't put it in one sentence.

PETER SARNAK:

Oh it's impossible.

ANDREW WILES:

There's a saying attributed to Eichler that there are five fundamental operations of arithmetic: addition, subtraction, multiplication, division and modular forms.

BARRY MAZUR:

Modular forms are functions on the complex plane that are inordinately symmetric. They satisfy so many internal symmetries that their mere existence seem like accidents, but they do exist.

NARRATOR:

This image is merely a shadow of a modular form. To see one properly your TV screen would have to be stretched into something called hyperbolic space. Bizarre modular forms seem to have nothing whatsoever to do with the humdrum world of elliptic curves. But what Taniyama and Shimura suggested shocked everyone.

GORO SHIMURA:

In 1955 there was an international symposium and Taniyama posed two or three problems.

NARRATOR:

The problems posed by Taniyama led to the extraordinary claim that every elliptic curve was really a modular form in disguise. It became known as the Taniyama–Shimura conjecture.

JOHN CONWAY:

The Taniyama–Shimura conjecture says, it says that every rational elliptic curve is modular and that's so hard to explain.

BARRY MAZUR:

So let me explain. Over here you have the elliptic world the elliptic curve, these doughnuts, and over here you have the modular world, modular forms with their many, many symmetries. The Shirmura–Taniyama conjecture makes a bridge between these two worlds. These worlds live on different planets.

It's a bridge, it's more than a bridge, it's really a dictionary, a dictionary where questions, intuitions, insights, theorems in the one world get translated to questions, intuitions in the other world.

KEN RIBET:

I think that when Shirmura and Taniyama first started talking about the relationship between elliptic curves and modular forms people were very incredulous. I wasn't studying mathematics yet. By the time I was a graduate student in 1969 or 1970 people were coming to believe the conjecture.

NARRATOR:

In fact, Taniyama–Shimura became a foundation for other theories which all came to depend on it. But Taniyama–Shimura was only a conjecture, an unproven idea, and until it could be proved, all the maths which relied on it was under threat.

ANDREW WILES:

Built more and more conjectures stretched further and further into the future but they would all be completely ridiculous if Taniyama–Shimura was not true.

NARRATOR:

Proving the conjecture became crucial, but tragically, the man whose idea inspired it didn't live to see the enormous impact of his work. In 1958, Taniyama committed suicide.

GORO SHIMURA:

I was very much puzzled. Puzzlement may be the best word. Of course I was sad that, see it was so sudden and I was unable to make sense out of this.

NARRATOR:

Taniyama–Shimura went on to become one of the great unproven conjectures. But what did it have to do with Fermat’s last theorem?

ANDREW WILES:

At that time no-one had any idea that Taniyama–Shimura could have anything to do with Fermat. Of course in the 80s that all changed completely.

NARRATOR:

Taniyama–Shimura says: every elliptic curve is modular and Fermat says: no numbers fit this equation. What was the connection?

KEN RIBET:

Well, on the face of it the Shimura–Taniyama conjecture which is about elliptic curves, and Fermat’s last theorem have nothing to do with each other because there’s no connection between Fermat and elliptic curves. But in 1985 Gerhard Frey had this amazing idea.

NARRATOR:

Frey, a German mathematician, considered the unthinkable: what would happen if Fermat was wrong and there was a solution to this equation after all?

PETER SARNAK:

Frey showed how starting with a fictitious solution to Fermat’s last equation if such a horrible, beast existed, he could make an elliptic curve with some very weird properties.

KEN RIBET:

That elliptic curve seems to be not modular, but Shimura–Taniyama says that every elliptic curve is modular.

NARRATOR:

So if there is a solution to this equation it creates such a weird elliptic curve it defies Taniyama–Shimura.

KEN RIBET:

So in other words, if Fermat is false, so is Shimura–Taniyama, or said differently, if Shimura–Taniyama is correct, so is Fermat’s last theorem.

NARRATOR:

Fermat and Taniyama–Shimura were now linked, apart from just one thing.

KEN RIBET:

The problem is that Frey didn’t really prove that his elliptic curve was

not modular. He gave a plausibility argument which he hoped could be filled in by experts, and then the experts started working on it.

NARRATOR:

In theory, you could prove Fermat by proving Taniyama, but only if Frey was right. Frey's idea became known as the epsilon conjecture and everyone tried to check it. One year later, in San Francisco, there was a breakthrough.

KEN RIBET:

I saw Barry Mazur on the campus and I said let's go for a cup of coffee and we sat down for cappuccinos at this cafe and I looked at Barry and I said you know, I'm trying to generalise what I've done so that we can prove the full strength of Serre's epsilon conjecture and Barry looked at me and said well you've done it already, all you have to do is add on some extra gamma zero of m structure and run through your argument and it still works, and that gives everything you need, and this had never occurred to me as simple as it sounds. I looked at Barry, I looked to my cappuccino, I looked back at Barry and said my God, you're absolutely right.

BARRY MAZUR:

Ken's idea was brilliant.

ANDREW WILES:

I was at a friend's house sipping iced tea early in the evening and he just mentioned casually in the middle of a conversation: by the way, do you hear that Ken has proved the epsilon conjecture? And I was just electrified. I, I knew that moment the course of my life was changing because this meant that to prove Fermat's last theorem I just had to prove Taniyama-Shimura conjecture. From that moment that was what I was working on. I just knew I would go home and work on the Taniyama-Shimura conjecture.

NARRATOR:

Andrew abandoned all his other research. He cut himself off from the rest of the world and for the next seven years he concentrated solely on his childhood passion.

ANDREW WILES:

I never use a computer. I sometimes might scribble, I do doodles I start trying to, to find patterns really, so I'm doing calculations which try to explain some little piece of mathematics and I'm trying to fit it in with some previous broad conceptual understanding of some branch of mathematics. Sometimes that'll involve going and looking up in a book to

see how it's done there, sometimes it's a question of modifying things a bit, sometimes doing a little extra calculation, and sometimes you realise that nothing that's ever been done before is any use at all, and you, you just have to find something completely new and it's a mystery where it comes from.

JOHN COATES:

I must confess I did not think that the Shimura–Taniyama conjecture was accessible to proof at present. I thought I probably wouldn't see a proof in my lifetime.

KEN RIBET:

I was one of the vast majority of people who believe that the Shimura–Taniyama conjecture was just completely inaccessible, and I didn't bother to prove it, even think about trying to prove it. Andrew Wiles is probably one of the few people on earth who had the audacity to dream that you can actually go and prove this conjecture.

ANDREW WILES:

In this case certainly for the first several years I had no fear of competition. I simply didn't think I or any one else had any real idea how to do it. But I realised after a while that talking to people casually about Fermat was, was impossible because it just generates too much interest and you can't really focus yourself for years unless you have this kind of undivided concentration which too many spectators will have destroyed.

NARRATOR:

Andrew decided that he would work in secrecy and isolation.

PETER SARNAK:

I often wondered myself what he was working on.

NICK KATZ:

Didn't have an inkling.

JOHN CONWAY:

No, I suspected nothing.

KEN RIBET:

This is probably the only case I know where someone worked for such a long time without divulging what he was doing, without talking about the progress he had made. It's just unprecedented.

NARRATOR:

Andrew was embarking on one of the most complex calculations in history. For the first two years, he did nothing but immerse himself in the problem, trying to find a strategy which might work.

ANDREW WILES:

So it was now known that Taniyama–Shimura implied Fermat’s last theorem. What does Taniyama–Shimura say? It, it says that all elliptic curves should be modular. Well this was an old problem been around for 20 years and lots of people would try to solve it.

KEN RIBET:

Now one way of looking at it is that you have all elliptic curves and then you have the modular elliptic curves and you want to prove that there are the same number of each. Now of course you’re talking about infinite sets, so you can’t just can’t count them per say, but you can divide them into packets and you could try to count each packet and see how things go, and this proves to be a very attractive idea for about 30 seconds, but you can’t really get much further than that, and the big question on the subject was how you could possibly count, and in effect, Wiles introduced the correct technique.

NARRATOR:

Andrew’s trick was to transform the elliptic curves into something called Galois representations which would make counting easier. Now it was a question of comparing modular forms with Galois representations, not elliptic curves.

ANDREW WILES:

Now you might ask and it’s an obvious question, why can’t you do this with elliptic curves and modular forms, why couldn’t you count elliptic curves, count modular forms, show they’re the same number? Well, the answer is people tried and they never found a way of counting, and this was why this is the key breakthrough, that I found a way to count not the original problem, but the modified problem. I found a way to count modular forms and Galois representations.

NARRATOR:

This was only the first step, and already it had taken three years of Andrew’s life.

ANDREW WILES:

My wife’s only known me while I’ve been working on Fermat. I told her a few days after we got married. I decided that I really only had time for my problem and my family and when I was concentrating very hard and I found

that with young children that's the best possible way to relax. When you're talking to young children they simply aren't interested in Fermat, at least at this age, they want to hear a children's story and they're not going to let you do anything else.

So I'd found this wonderful counting mechanism and I started thinking about this concrete problem in terms of Iwasawa theory. Iwasawa theory was the subject I'd studied as a graduate student and in fact with my advisor, John Coates, I'd used it to analyse elliptic curves.

NARRATOR:

Andrew hopes that Iwasawa theory would complete his counting strategy.

ANDREW WILES:

Now I tried to use Iwasawa theory in this context, but I ran into trouble. I seemed to be up against a wall. I just didn't seem to be able to get past it. Well sometimes when I can't see what to do next I often come here by the lake. Walking has a very good effect in that you're in this state of concentration, but at the same time you're relaxing, you're allowing the subconscious to work on you.

NARRATOR:

Iwasawa theory was supposed to help create something called a class number formula, but several months passed and the class number formula remained out of reach.

ANDREW WILES:

So at the end of the summer of '91 I was at a conference. John Coates told me about a wonderful new paper of Matthias Flach, a student of his, in which he had tackled a class number formula, in fact exactly the class number formula I needed, so Flach using ideas of Kolyvagin had made a very significant first step in actually producing the class number formula. So at that point I thought this is just what I need, this is tailor-made for the problem. I put aside completely the old approach I'd been trying and I devoted myself day and night to extending his result.

NARRATOR:

Andrew was almost there, but this breakthrough was risky and complicated. After six years of secrecy, he needed to confide in someone.

NICK KATZ:

January of 1993 Andrew came up to me one day at tea, asked me if I could come up to his office, there was something he wanted to talk to me about. I had no idea what, what this could be. Went up to his office. He closed

the door, he said he thought he would be able to prove Taniyama–Shimura. I was just amazed, this was fantastic.

ANDREW WILES:

It involved a kind of mathematics that Nick Katz is an expert in.

NICK KATZ:

I think another reason he asked me was that he was sure I would not tell other people, I would keep my mouth shut, which I did.

JOHN CONWAY:

Andrew Wiles and Nick Katz had been spending rather a lot of time huddled over a coffee table at the far end of the common room working on some problem or other. We never knew what it was.

NARRATOR:

In order not to arouse any more suspicion, Andrew decided to check his proof by disguising it in a course of lectures which Nick Katz could then attend.

ANDREW WILES:

Well I explained at the beginning of the course that Flach had written this beautiful paper and I wanted to try to extend it to prove the full class number formula. The only thing I didn't explain was that proving the class number formula was most of the way to Fermat's last theorem.

NICK KATZ:

So this course was announced. It said calculations on elliptic curves, which could mean anything. Didn't mention Fermat, didn't mention Taniyama–Shimura, there was no way in the world anyone could have guessed that it was about that, if you didn't already know. None of the graduate students knew and in a few weeks they just drifted off because it's impossible to follow stuff if you don't know what it's for, pretty much. It's pretty hard even if you do know what's it for, but after a few weeks I was the only guy in the audience.

NARRATOR:

The lectures revealed no errors and still none of his colleagues suspected why Andrew was being so secretive.

PETER SARNAK:

Maybe he's run out of ideas. That's why he's quiet, you never know why they're quiet.

NARRATOR:

The proof was still missing a vital ingredient, but Andrew now felt confident. It was time to tell one more person.

ANDREW WILES:

So I called up Peter and asked him if I could come round and talk to him about something.

PETER SARNAK:

I got a phone call from Andrew saying that he had something very important he wanted to chat to me about, and sure enough he had some very exciting news.

ANDREW WILES:

Said I, I think you better sit down for this. He sat down. I said I think I'm about to prove Fermat's last theorem.

PETER SARNAK:

I was flabbergasted, excited, disturbed. I mean I remember that night finding it quite difficult to sleep.

ANDREW WILES:

But there was still a problem. Late in the spring of '93 I was in this very awkward position and I thought I'd got most of the curves to be modular, so that was nearly enough to be content to have Fermat's last theorem, but there was this, these few families of elliptic curves that had escaped the net and I was sitting here at my desk in May of '93 still wondering about this problem and I was casually glancing at a paper of Barry Mazur's and there was just one sentence which made a reference to actually what's a 19th-century construction and I just instantly realised that there was a trick that I could use, that I could switch from the families of elliptic curves I'd been using, I'd been studying them using the prime three, I could switch and study them using the prime five. It looked more complicated, but I could switch from these awkward curves that I couldn't prove were modular to a different set of curves which I'd already proved were modular and use that information to just go that one last step and I just kept working out the details and time went by and I forgot to go down to lunch and it got to about teatime and I went down and Nada was very surprised that I'd arrived so late and then, then she, I told her that I, I believed I'd solved Fermat's last theorem.

I was convinced that I had Fermat in my hands and there was a conference in Cambridge organised by my advisor, John Coates. I thought that would be a wonderful place. It's my old home town, I'd been a graduate student

there, be a wonderful place to talk about it if I could get it in good shape.

JOHN COATES:

The name of the lectures that he announced was simply 'Elliptic curves and modular forms' There was no mention of Fermat's last theorem.

KEN RIBET:

Well I was at this conference on L functions and elliptic curves and it was kind of a standard conference and all of the people were there, didn't seem to be anything out of the ordinary, until people started telling me that they'd been hearing weird rumours about Andrew Wiles's proposed series of lectures.

I started talking to people and I got more and more precise information. I've no idea how it was spread.

PETER SARNAK:

Not from me, not from me.

JOHN CONWAY:

Whenever any piece of mathematical news had been in the air, Peter would say oh that's nothing, wait until you hear the big news, there's something big going to break.

PETER SARNAK:

Maybe some hints, yeah.

ANDREW WILES:

People would ask me leading up to my lectures what exactly I was going to say and I said well, come to my lecture and see.

KEN RIBET:

It's a very charged atmosphere a lot of the major figures of arithmetical, algebraic geometry were there. Richard Taylor and John Coates, Barry Mazur.

BARRY MAZUR:

Well I'd never seen a lecture series in mathematics like that before. What was unique about those lectures were the glorious ideas how many new ideas were presented, and the constancy of his dramatic build-up that was suspenseful until the end.

KEN RIBET:

There was this marvellous moment when we were coming close to a proof of

Fermat's last theorem, the tension had built up and there was only one possible punchline.

ANDREW WILES:

So after I'd explained the $3/5$ switch on the blackboard, I then just wrote up a statement of Fermat's last theorem, said I'd proved it, said I think I'll stop there.

JOHN COATES:

The next day what was totally unexpected was that we were deluged by enquiries from newspapers, journalists from all around the world.

ANDREW WILES:

It was a wonderful feeling after seven years to have really solved my problem, I've finally done it. Only later did it come out that there was a, a problem at the end.

NICK KATZ:

Now it was time for it to be refereed which is to say for people appointed by the journal to go through and make sure that the thing was really correct.

So for, for two months, July and August, I literally did nothing but go through this manuscript, line by line and what, what this meant concretely was that essentially every day, sometimes twice a day, I would E-mail Andrew with a question: I don't understand what you say on this page on this line. It seems to be wrong or I just don't understand.

ANDREW WILES:

So Nick was sending me E-mails and at the end of the summer he sent one that seemed innocent at first. I tried to resolve it.

NICK KATZ:

It's a little bit complicated so he sends me a fax, but the fax doesn't seem to answer the question, so I E-mail him back and I get another fax which I'm still not satisfied with, and this in fact turned into the error that turned out to be a fundamental error and that we had completely missed when he was lecturing in the spring.

ANDREW WILES:

That's where the problem was in the method of Flach and Kolyvagin that I'd extended, so once I realised that at the end of September, that there was really a, a problem with the way I'd made the construction I spent the fall trying to think what kind of modifications could be made to the

construction. There, are lots of simple and rather natural modifications that any one of which might work.

PETER SARNAK:

And every time he would try and fix it in one corner it would sort of some other difficulty would add up in another corner. It was like he was trying to put a carpet in a room where the carpet had more size than the room, but he could put it in in any corner and then when he ran to the other corner it would pop up in this corner and whether you could not put the carpet in the room was not something that he was able to decide.

NICK KATZ:

I think he externally appeared normal but at this point he was keeping a secret from the world and I think he must have been in fact pretty uncomfortable about it.

JOHN CONWAY:

Wellyou know we were behaving a little bit like Kremlinologists. Nobody actually liked to come out and ask him how he's getting on with, with the proof, so somebody would say I saw Andrew this morning. Did he smile? Well yes, but he didn't look too happy.

ANDREW WILES:

The first seven years I'd worked on this problem. I loved every minute of it. However hard it had been there'd been, there'd been setbacks often, there'd been things that had seemed insurmountable but it was a kind of private and very personal battle I was engaged in.

And then after there was a problem with it doing mathematics in that kind of rather over-exposed way is certainly not my style and I have no wish to repeat it.

NARRATOR:

Other mathematicians, including his former student Richard Taylor, tried to help fix the mistake. But after a year of failure, Andrew was ready to abandon his flawed proof.

ANDREW WILES:

In September, I decided to go back and look one more time at the original structure of Flach and Kolyvagin to try and pinpoint exactly why it wasn't working, try and formulate it precisely. One can never really do that in mathematics but I just wanted to set my mind at rest that it really couldn't be made to work. And I was sitting here at this desk. It was a Monday morning, September 19th and I was trying convincing myself that it didn't work, just seeing exactly what the problem was when suddenly, totally

unexpectedly, I had this incredible revelation. I, I realised what was holding me up was exactly what would resolve the problem I'd had in my Iwasawa theory attempt three years earlier was, it was the most, the most important moment of my working life. It was so indescribably beautiful, it was so simple and so elegant and I just stared in disbelief for twenty minutes. Then during the day I walked round the department, I'd keep coming back to my desk and looking to see it was still there, it was still there. Almost what seemed to be stopping the method of Flach and Kolyvagin was exactly what would make horizontally Iwasawa theory. My original approach to the problem from three years before would make exactly that work, so out of the ashes seemed to rise the true answer to the problem. So the first night I went back and slept on it, I checked through it again the next morning and by 11 o'clock I satisfied and I went down, told my wife I've got it, I think I've got it, I've found it, and it was so unexpected, she, I think she thought I was talking about a children's toy or something and said got what? and I said I've fixed my proof, I, I've got it.

JOHN COATES:

I think it will always stand as, as one of the high achievements of number theory.

BARRY MAZUR:

It was magnificent.

JOHN CONWAY:

It's not every day that you hear the proof of the century.

GORO SHIMURA:

Well my first reaction was: I told you so.

NARRATOR:

The Taniyama-Shimura conjecture is no longer a conjecture, and as a result Fermat's last theorem has been proved. But is Andrew's proof the same as Fermat's?

ANDREW WILES:

Fermat couldn't possibly have had this proof. It's a 20th-century proof. There's no way this could have been done before the 20th-century.

JOHN CONWAY:

I'm relieved that this result is now settled. But I'm sad in some ways because Fermat's last theorem has been responsible for so much. What will we find to take its place?

ANDREW WILES:

There's no other problem that will mean the same to me. I had this very rare privilege of being able to pursue in my adult life what had been my childhood dream. I know it's a rare privilege but if, if one can do this it's more rewarding than anything I could imagine.

BARRY MAZUR:

One of the great things about this work is it embraces the ideas of so many mathematicians. I've made a partial list: Klein, Fricke, Hurwitz, Hecke, Dirichlet, Dedekind...

KEN RIBET:

The proof by Langlands and Tunnell...

JOHN COATES:

Deligne, Rapoport, Katz...

NICK KATZ:

Mazur's idea of using the deformation theory of Galois representations...

BARRY MAZUR:

Igusa, Eichler, Shimura, Taniyama...

PETER SARNACK:

Frey's reduction...

NICK KATZ:

The list goes on and on...

BARRY MAZUR:

Bloch, Kato, Selmer, Frey, Fermat.