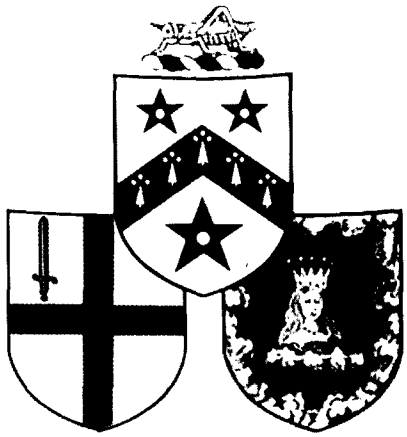
G R E S H A M

C O L L E G E



FERMAT'S FINAL FLING

LAST DAYS OF THE LAST THEOREM

A Lecture by

PROFESSOR IAN STEWART MA PhD FIMA CMath
Gresham Professor of Geometry

4 December 1995

GRESHAM COLLEGE

Policy & Objectives

An independently funded educational institution, Gresham College exists

- to continue the free public lectures which have been given for 400 years, and to reinterpret the 'new learning' of Sir Thomas Gresham's day in contemporary terms;

- to engage in study, teaching and research, particularly in those disciplines represented by the Gresham Professors;

- to foster academic consideration of contemporary problems;

- to challenge those who live or work in the City of London to engage in intellectual debate on those subjects in which the City has a proper concern; and to provide a window on the City for learned societies, both national and international.

Gresham College, Barnard's Inn Hall, Holborn, London EC1N 2HH
Tel: 020 7831 0575 Fax: 020 7831 5208
e-mail: enquiries@gresham.ac.uk

Gresham Geometry Lecture
4 December 1995

Fermat's Final Fling

last days of the last theorem

Some time around 1637 Pierre de Fermat made the most famous marginal note in the history of mathematics: 'To resolve a cube into the sum of two cubes, a fourth power into two fourth powers, or in general any power higher than the second into two of the same kind, is impossible; of which fact I have found a remarkable proof. The margin is too small to contain it.' This statement came to be known as *Fermat's Last Theorem.*

On Wednesday 23 June 1993 Andrew Wiles announced a proof, which was widely acclaimed by experts. Early in 1994 a number of difficulties emerged, among them a subtle logical gap. By the autumn of 1994 some experts were estimating that it would take at least three years of hard work to complete the proof, and others thought the gap might not be filled at all. Then, in October 1994, Wiles announced that he had overcome this final stumbling block.

The lecture will describe the history of Fermat's Last Theorem from ancient Greece to the present day, discuss Wiles's methods, and examine the current status of his proof. No specialist knowledge will be assumed.

Prelude

The Isaac Newton Institute in Cambridge is a newly founded international research centre for mathematics. In June 1993 it was running a conference on number theory. The organizers could have had no conception of how their small meeting was going to redraw the map of mathematics, but soon after the meeting started, rumours began to circulate. Prof. Andrew Wiles, a quiet, rather diffident Englishman working at Princeton University, had announced a series of three lectures on the topic 'Modular forms, elliptic curves, and Galois representations'. Only an insider could read between the lines. Wiles seldom gave lectures; three in a row was unprecedented. And the target of his rather technical researches was something far less esoteric and far more dramatic: nothing less than Fermat's Last Theorem.

Mathematics has a small number of notorious unsolved problems — problems asked often centuries ago, but which the concerted efforts of the world's mathematicians have been unable either to prove or disprove. The puzzle posed by Fermat is somewhere in the top three or four, and it is some 356 years old. Any mathematician would give his eye teeth to be the one who solved it, but few ever try: the task is too daunting, the risk of failure too great.

Wiles's series of talks was scheduled for Monday 21-Wednesday 23 June, one lecture per day. Early on he explained that he had solved a very special case of the so-called Taniyama-Weil conjecture, a highbrow but very important assertion about 'elliptic curves'. One consequence of a more general case of the Taniyama-Weil conjecture — for so called semistable elliptic curves — would be Fermat's Last Theorem. How far had

Wiles got?

The tension mounted as Wiles approached the third and final lecture, having revealed absolutely nothing about just how far his work had progressed. According to Karl Rubin of Ohio State University 'The excitement was increasing each day.' Then, on the Wednesday, Wiles revealed what was up his sleeve. He had found a clever way to take his very special case of the Taniyama-Weil conjecture, and extend it to a proof of the semistable case. Although the audience was well aware of the implication, Wiles quietly spelled it out. There was a sudden silence. Then the entire room burst into spontaneous applause.

Fermat's Last Theorem

What is Fermat's Last Theorem, and why is it such a great prize? And who was Fermat?

Pierre de Fermat was born in 1601. His father Dominique Fermat sold leather, his mother Claire de Long was the daughter of a family of parliamentary lawyers. In 1631 he married his mother's cousin Louise de Long. In 1648 he became a King's Councillor in the local parliament of Toulouse, where he served for the rest of his life, dying in 1665, just two days after concluding a legal case. He never held an academic position of any kind, and certainly not in mathematics. But mathematics was his passion. Eric Temple Bell called him 'the Prince of amateurs'. Most of today's professionals would be happy with half his ability.

Fermat worked in many fields of mathematics. He worked out many of the basic ideas of calculus, half a century before Isaac Newton and Gottfried Leibniz independently sorted out the whole subject. He formulated the Principle of Least Time, which says that a ray of light takes the shortest path available; this was a forerunner of the variational calculus, one of the most powerful tools of mathematical physics. But his most influential ideas were in number theory, the study of ordinary whole numbers, or *integers*. It is an area in which it is easy to observe patterns, and guess that they are generally valid, but amazingly difficult to pin them down with a proper proof. A typical theorem of Fermat's is that any prime number that is one greater than a multiple of four is always a sum of two integer squares. Anybody can check special cases — for example, $13 = 2^2+3^2$. But Fermat could not only dig such patterns out of the numerical mire: he could polish them up with a shiny proof.

Fermat didn't invent number theory. Arguably that honour goes to Diophantus of Alexandria. We know very little about him: he was probably Greek, and if an ancient puzzle is to be believed he died aged 84. He flourished around AD 250, and he wrote a book called the *Arithmetica*. It was about what are now called Diophantine equations — equations that must be solved in whole numbers. A typical problem from Diophantus is Book III, Problem 6:

find three numbers such that their sum,
and the sum of any two, is a perfect square.

(*Answer at the end.*)

One problem to which Diophantus gave a completely general answer is that of finding 'Pythagorean triangles': three integers x, y, z satisfying the 'Pythagorean equation' $x^2+y^2 = z^2$. Thanks to Pythagoras' Theorem, such triples of numbers are the lengths of sides of a right triangle. Examples are $3^2+4^2 = 5^2$ and $5^2+ 12^2 = 13^2$. The general solution was known in Euclid's time, 500 years earlier — it wasn't invented by Diophantus.

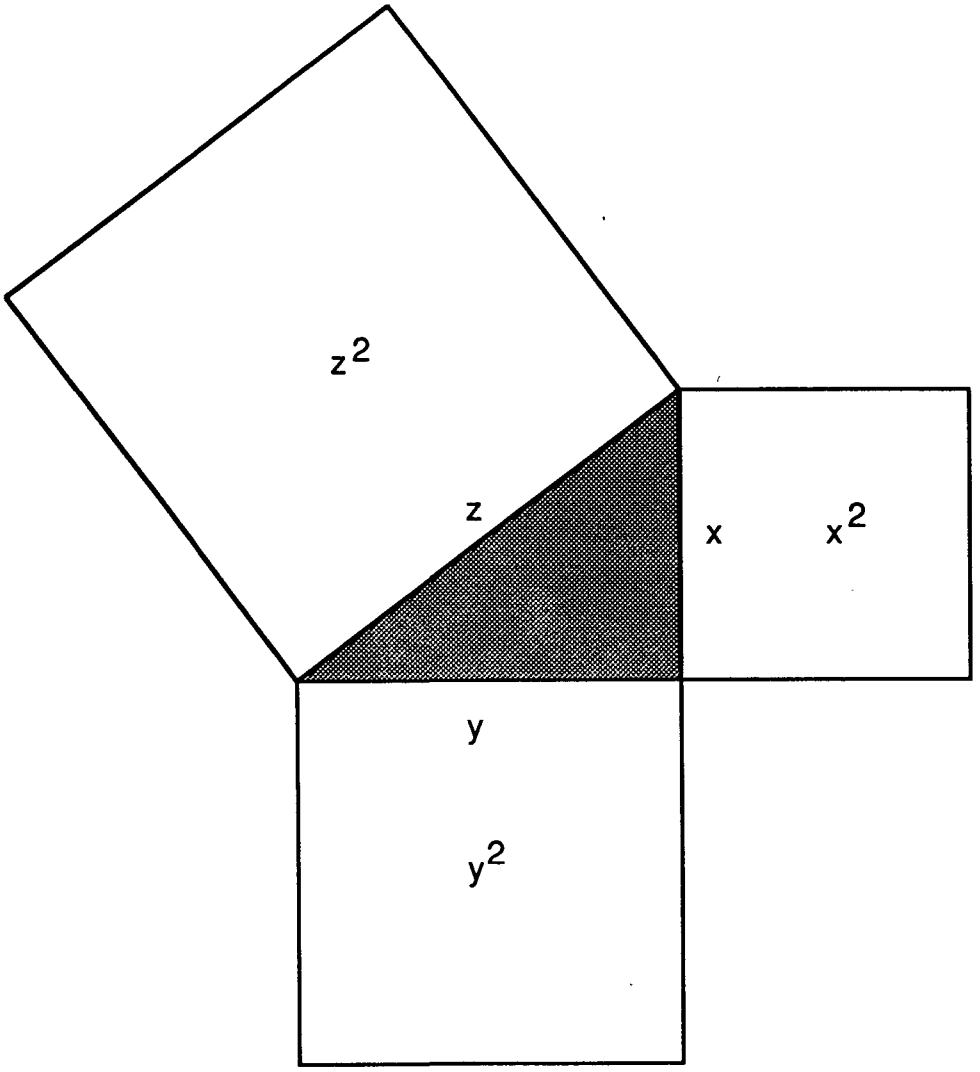


Fig.1 A Pythagorean triangle.

To solve the Pythagorean equation $x^2+y^2 = z^2$, pick any whole numbers k, u, v. Let $x = k(u^2-v^2)$, $y = 2kuv$, $z = k(u^2+v^2)$. Then you've got a solution. For example let $k = 1$, $u = 2$, $v = 1$: then $x = 3$, $y = 4$, $z = 5$. Or let $k = 1$, $u = 3$, $v = 2$, so that $x = 5$, $y = 12$, $z = 13$. This method generates *all* solutions.

Fermat owned a copy of the *Arithmetica*, which inspired many of his investigations. He used to write down his conlcusions in the margin. Some time around 1637 he must have thinking about the Pythagorean equation, and he asked himself what happens if instead of squares you try cubes. He presumably tried some numerical experiments. Is $1^3 + 2^3$ a cube? No, it equals 9 — a square, but not a cube. He was unable to find any solutions, except for 'trivial' ones like $0^3 + 1^3 = 1^3$. The same happened when he tried fourth powers, fifth powers, and so on. In the margin of his copy of the *Arithmetica* he made the most famous note in the history of mathematics:

> *'To resolve a cube into the sum of two cubes, a fourth power into two fourth powers, or in general any power higher than the second into two of the same kind, is impossible; of which fact I have found a remarkable proof. The margin is too small to contain it.'*

Fermat was stating that the 'Fermat equation' $x^n + y^n = z^n$ has no whole number solutions.

This statement has come to be known as his 'last theorem', because for many years it was the only assertion of his that had neither been proved nor disproved by his successors. Nobody could reconstruct Fermat's 'remarkable proof', and it seemed increasingly doubtful that he had ever possessed one.

Algebraic Numbers

At first progress was desparately slow. Fermat himself found a proof for fourth powers, n = 4, using a method that he called 'infinite descent'. He worked with a slightly more general equation, $x^4 + y^4 = z^2$. (It is more general because any fourth power is a square). The numbers x^2, y^2, z form a Pythagorean triangle, and two of its sides are squares. Using the standard formula for Pythagorean triangles, as stated in Diophantus, Fermat found that he could then construct *another* solution of the same equation with smaller numbers. But it is not possible to have an infinite sequence of positive integers that get smaller and smaller. Therefore no solution to the equation can exist.

Fermat also proved the theorem for cubes, n = 3. Independently, Leonhard Euler, a Swiss mathematician and the most prolific who ever lived, proved the same two cases. In 1828 Peter Lejeune-Dirichlet dealt with the case n = 5, and so did Adrien-Marie Legendre in 1830. In 1839 Gabriel Lamé atempted a proof for n = 7, but he made some errors that were corrected by Henri Lebesgue in 1840.

In 1847 Lamé claimed a proof for all n. But Ernst Eduard Kummer pointed out a mistake. It was a very interesting mistake, and in the long run it pointed the way to a solution. But at the time it seemed an insuperable obstacle.

His basic strategy was to introduce *algebraic numbers* — a more general class of numbers. A simple example explains the idea. Suppose we have to solve the equation $y^2+2 = x^3$ in integers. The left hand side can be written as a product of two factors, of a rather curious kind:

$$y^2+2 = (y+\sqrt{-2})(y-\sqrt{-2}).$$

Here $\sqrt{-2}$ is a 'complex' number, involving the square root of a negative quantity; but the really interesting point is that the factors are both of the same general form

$$a + b\sqrt{-2}$$

where a and b are ordinary integers. If you add or multiply numbers of this general form, the result is of the same form (though with differrent values of a and b). So we have an alternative number system, containing a richer supply of numbers than just integers.

For ordinary integers, if a product of two numbers is a cube, and if the numbers have no common factor, then each number is itself a cube. This follows from the uniqueness of prime factorization, which says that every integer is a product of primes *in only one way*. Assuming that such a result also holds good for our new class of numbers $a + b\sqrt{-2}$, it follows that $2+\sqrt{-2}$ must be the cube of such a number. From this a short algebraic calculation leads to the answer: the *only* solution to the original equation is x = 3, y = ±5.

Here are the details, for those who want them.

As just observed, the equation $y^2+2 = x^3$ can be factorized using such numbers: $(y+\sqrt{-2})(y-\sqrt{-2}) = x^3$. Suppose that all the usual properties of prime factors apply. Then the two factors on the left are *relatively prime*: they have no prime factor in common. Now comes the key step: if the product of two relatively prime numbers is a cube, as it is here, then each separately must be a cube. So there must be integers a and b such that

$$y+\sqrt{-2} = (a + b\sqrt{-2})^3.$$

Expanding this and equating coefficients of $\sqrt{-2}$ we see that

$$1 = b(3a^2-2b^2).$$

If a produce of two integers equals 1 then either both equal 1 or both equal -1. Therefore $b = \pm 1$ and $3a^2-2b^2 = 3a^2-2 = \pm 1$. Obviously $b = 1$ and $a = \pm 1$ are the only solutions. Working backwards, we find that $x = 3$, $y = \pm 5$ is the only possibility.

This kind of strategy focuses attention on a broader class of numbers, and asks whether their arithmetical properties are analogous to ordinary whole numbers. For the particular class just introduced, the answer is 'yes'.

Could unique prime factorization fail? A simple example shows that, surprisingly, it could. Consider the system of all whole numbers 1, 5, 9, 13, ..., numbers of the form 4k+1. If you multiply any two such numbers together, you get another of the same form. You can define 'primes' in this system — let's call them *prymes* to show that something weird is going on — to be any number that cannot be obtained by multiplying two numbers *in the system*. So now 9 is pryme — because although we can write 9 = 3×3, the number 3 is *not* in the system under consideration. Indeed every number in the system is a product of prymes.

But not in one way. The number 441 can be factorized in two different ways: 441 = 9×49 = 21×21, and each of 9, 21, and 49 is pryme. Now, it's true that we can expaimn this peculiarity by broadening the class of numbers to include 3, 7, 11, and so on: then the two factorizations are just different groupings of the single factorization 441 = 3×3×7×7. But we can't get uniqueness if we stay inside the chosen system. And once we contemplate enlarging the number system to include algebraic numbers, there is so much freedom to choose that it is not at all clear what happens. With numbers of the form $a+b\sqrt{-2}$, factorization is unique. But with numbers of the form $a+b\sqrt{-5}$ it is not: $6 = 2\times3 = (1+\sqrt{-5})(1-\sqrt{-5})$ and all four factors are prime. What's different about $\sqrt{-2}$ compared to $\sqrt{-5}$? It's hard to tell just by looking.

That's what Lamé got wrong when he tried a similar approach to the Fermat equation. He worked with 'cyclotomic integers', numbers formed algebraically from a complex n^{th} root of 1, so that he could factorize x^n+y^n into n distinct factors, which were relatively prime and whose product was a perfect n^{th} power, namely z^n. Therefore, assuming the usual properties of prime factors, each factor is an n^{th} power. From there he could fairly easily develop a proof that no solution existed.

But Kummer and others pointed out that for n = 23 the cyclotomic numbers *don't* have unique factorization.

Kummer asked *why* cyclotomic numbers could have more than one prime factorization, and eventually he discovered that he could sort the whole thing out by introducing a new kind of gadget altogether, which he called *ideal numbers*. The basic idea is simlar tot he way we extended the numbers of the form 4k+1 to the odd numbers, and resolved the paradox of nonunique factorization. Ideal numbers weren't really numbers, but *sets* of numbers: they provided some 'extra' prime factors to make everything work out right. By 1847 Kummer had used his theory of ideal numbers to dispose of Fermat's Last Theorem for all n up to 100, except n = 37, 59, and 67. By developing extra machinery, Kummer and Dimitri Mirimanoff disposed of those cases too in 1857. By the 1980s similar methods had proved all cases $n \le 150{,}000$.

The Mordell Conjecture

A new idea was needed. And that came by a rather different route.

Some Diophantine equations have infinitely many solutions — such as the Pythagorean equation. Some have none — the Fermat equation for $3 \le n \le 150{,}000$, if we ignore trivial solutions. Some have finitely many — like $y^2+2 = x^3$. In the 1922 the

English mathematician Leo Mordell was trying to work out what distinguished these possibilities, and he started to see a possible pattern. He noticed that if you look at all solutions of such an equation in complex numbers — getting as general as possible, no assumptions about whole numbers at all — then those solutions form a topological surface. The surface has a finite number of 'holes', like a donut or a pretzel. What struck him as remarkable was that equations with infinitely many whole number solutions always had no holes, or just one, when solved in complex numbers. There seemed to be a connection between the topology and the arithmetic.

This was wild stuff — nobody could see any way to get a solid connection between two such different branches of mathematics. But Mordell was sufficiently convinced that he published what is now called the *Mordell conjecture*, which says that equations that give rise to surfaces with two or more holes have only finitely many integer solutions. The number of holes in the surface corresponding to the Fermat equation is (n-1)(n-2)/2, and for $n \geq 3$ this is at least 2. So the Mordell conjecture implies that if the Fermat equation has any integer solutions at all, then it must have only finitely many.

(Incidentally, if x, y, and z form a solution, then so do 2x, 2y, and 2z, or 3x, 3y, and 3z, and so on. That's infinitely many. To avoid this trivial difficulty, Mordell considered only solutions without any common factor.)

In 1962 Igor Shafarevich came up with a new, rather technical conjecture about what happens to solutions of Diophantine equations when you take remainders on division by a prime. In 1968 A.N.Parshin proved that the Shafarevich conjecture implies the Mordell conjecture. Finally in 1983 the young German mathematician Gerd Faltings proved Parshin's conjecture, therefore also Mordell's. Which means that Fermat's Last Theorem is *nearly* true: if for any n there are exceptions, there can be only finitely many of them. His proof uses a version of Fermat's method of infinite descent — but applied to very abstract things called abelian varieties.

Finitely many solutions is not the same as none. But it's a big step to get a potentially infinite number of solutions down to a finite number. You can *do* things with finite numbers — try to find out how big they are, count things, and so forth. Faltings's proof of the Mordell conjecture was a *huge* step forward. Soon afterwards D.R.Heath-Brown modified Faltings' approach to prove that the proportion of integers n for which your conjecture is true approaches 100% as n becomes very large. Fermat's Last Theorem is 'almost always' true.

Elliptic Curves

A more specific, different idea was still lacking. That came from a very beautiful theory that lies at the heart of the modern approach to Diophantine equations. It is the theory of 'elliptic curves'. They are equations of the form $y^2 = ax^3+bx^2+cx+d$ — a perfect square equal to a cubic polynomial. They are called 'curves' because every equation defines a geometric curve by way of coordinate geometry, and 'elliptic' because of a rather vague connection with the problem of finding a formula for the perimeter of an ellipse.

One of the most striking properties of elliptic curves is that, given a few integer solutions of the equation, you can (usually) combine them to get new solutions. More accurately, this is true for *rational* solutions. There is a geometrical construction to build new solutions out of old ones, as follows.

A typical straight line cuts an elliptic curve in three points. If the coordinates of two of those points correspond to whole number solutions of the associated Diophantine equation, then so do the coordinates of the third point. To construct new solutions from

old ones you just take two solutions, draw the line through the corresponding points, and calculate the coordinates of the third point at which this line hits this curve.

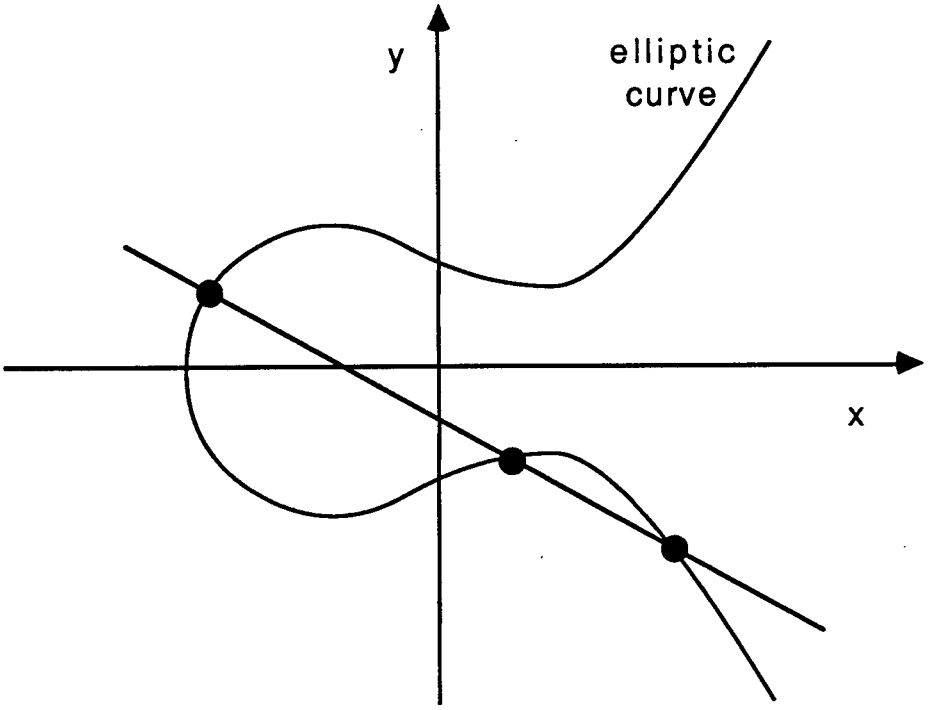


Fig.1 Points on an elliptic curve.

Elliptic curves were one of the things that stimulated Mordell to his conjecture, because the surfaces associated with them have only one hole, or none in degenerate cases. And over the years a very deep and powerful theory of elliptic curves has been developed. You could say they are the one area of Diophantine equations that people really understand pretty well.

The Taniyama Conjecture

Can we drop the word 'almost' from Heath-Brown's near miss?

The answer is 'yes', but its justification is highly technical. Wiles's proof of Fermat's Last Theorem is not the kind that can be written on the back of an envelope, and it takes a real expert to understand it in any detail. However, the general outline of the proof *is* comprehensible, so I'm going to try to give you some of the flavour of this radical development in number theory. At the very least, it will serve to drive home that whatever Fermat had in mind when he claimed to have a proof, it couldn't have been anything remotely like Wiles's argument.

The idea is to reformulate the problem so that the deep theory of ellipic curves can be brought to bear. Elliptic curve theory has its own big unsolved problems, and the biggest of all is called the *Taniyama conjecture.* Indeed it has various names, among them the Taniyama-Shimura conjecture, the Taniyama-Weil conjecture, and the Taniyama-Shimura-Weil conjecture. The surfeit of names reflects the history of the topic, for in 1955 Yutaka Taniyama asked some questions which were generalised and made more

precise by Goro Shimura and by Weil. So we have a choice: use a simple name, or a historically accurate one. I've chosen to go for simplicity, so herafter it's the Taniyama Conjecture — even though Taniyama asked something rather different.

We can grasp the general idea behind the Taniyama conjecture by thinking about one very special case. There is an intimate relationship between the Pythagorean equation $a^2+b^2 = c^2$, the unit circle, and the trigonometric functions 'sine' and 'cosine' (sin and cos). To obtain this relationship, write the Pythagorean equation in the 'dehomogenised' form $(a/c)^2 + (b/c)^2 = 1$. We can interpret this as saying that the point $x = a/c$, $y = b/c$ lies on the unit circle, with equation $x^2 + y^2 = 1$. The theory of trigonometric functions then provides a neat and simple way to represent the unit circle. The fundamental relation between sines and cosines is

$$\cos^2 A + \sin^2 A = 1,$$

which holds for any angle A. This implies that if we set $x = \cos A$, $y = \sin A$, then the point with coordinates (x,y) lies on the unit circle. To sum up: solving the Pythagorean equation in integers is equivalent to finding an angle A such that both cos A and sin A are rational numbers (equal respectively to a/c and b/c). Because the trigonometric functions have all sorts of pleasant properties, this idea is the basis of a really fruitful theory of the Pythagorean equation.

The Taniyama conjecture says, *very* roughly, that the same kind of game — but in a more technical setting — can be played if the circle is replaced by any elliptic curve, but using more sophisticated functions than trigonometric ones, the so-called 'modular' functions. Specifically, it states that *every* elliptic curve can be parametrised by suitable modular functions, just as sin and cos parametrise the 'Pythagorean curve', the unit circle.

Frey's Elliptic Curve

Between 1970 and 1975 Yves Hellegouarch published a series of papers on a connection between Fermat curves $x^n+y^n= z^n$ and elliptic curves, and used them to deduce theorems about elliptic curves from known partial results about Fermat's Last Theorem. Jean-Pierre Serre suggested using the idea in the opposite direction, exploiting properties of elliptic curves to prove results on Fermat's Last Theorem. He found evidence suggesting that this line of attack had the potential to crack the whole problem wide open, and slowly the experts started to believe that Fermat's Last Theorem was on the verge of yielding up its secrets. But it was to be a long, technical struggle.

In 1985, in a lecture at the international mathematical research centre at Oberwolfach, in the Black Forest area of Germany, Gerhard Frey made Serre's suggestion precise by introducing what is now called the *Frey elliptic curve* associated with a presumptive solution of the Fermat equation. The form chosen for this curve goes back to Hellegouarch, but Frey intended to use it in a different way. Suppose that there is a nontrivial solution $A^n + B^n = C^n$ of the Fermat equation. I've used capital letters A, B, C to show we're thinking of some *specific* solution in nonzero integers. For instance A might be 777235, B might be 84153, and C 28994 — except that those number *don't* satisfy the Fermat equation. We choose this presumptive solution, and from that moment on A, B, and C denote fixed (but unknown) integers. All we know about them is that $A^n + B^n = C^n$ for some $n \geq 3$, although we can also do some preliminary tidying and assume that A, B, and C have no common factor.

Now think about the specific (but unknown and possibly non-existent) elliptic curve whose equation is

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

This is Frey's elliptic curve, and it exists if and only if Fermat's Last Theorem is wrong.

So we want to prove that Frey's curve cannot exist. The way to do this it to assume that it does, and fight our way to *some* contradictory conclusion. It doesn't matter what the contradiction is.

Frey hacked away at his curve with the powerful general theory of elliptic curves, and discovered that if the Frey curve exists then it is a very curious beast indeed. So curious, indeed, that it seems highly unlikely that such a beast can exist at all — which is exactly what we would like to prove. In 1986 Kenneth Ribet made Frey's idea precise, by proving that if the Taniyama conjecture is true then Frey's elliptic curve definitely cannot exist. Specifically, Frey's curve *cannot* be parametrised by modular functions. If the Taniyama conjecture is true, Fermat's Last Theorem follows.

This is a major, major link in the Fermat chain, for it tells us that Fermat's Last Theorem is not just an isolated curiosity. Instead, it lies at the heart of modern number theory.

Andrew Wiles

As a child, Andrew Wiles had wanted to prove Fermat's last Theorem. But when he became a professional mathematician he decided that it was just an isolated, difficult problem — nice to prove, but not really *important* beyond its notoriety. Then he learned of Ribet's work, changed his view completely, and immediately decided to devote all of his research effort to a proof.

He realised that you don't need the full force of the Taniyama conjecture to make this approach work: you just need one particular special case of it, one that applies to a class of elliptic curves known as 'semistable'. Wiles broke the problem down into six pieces, and piece by piece he solved them, until finally only one held out. Then a lecture by Barry Mazur on something totally different sparked an idea that gave him the final clue. In a 200-page paper he marshalled enough powerful machinery to prove the semistable case of the Taniyama conjecture. This was enough for him to prove the following theorem. Suppose that M and N are distinct nonzero relatively prime integers such that MN(M-N) is divisible by 16. Then the elliptic curve $y^2 = x(x+M)(x+N)$ can be parametrised by modular functions. Indeed the condition on divisibility by 16 implies that this curve is semistable, so the semistable Taniyama conjecture establishes the desired property.

Now apply Wiles's theorem to Frey's curve, by letting $M = A^n$, $N = -B^n$. Then $M-N = A^n + B^n = C^n$, so $MN(M-N) = -A^nB^nC^n$, and we have to show this must be a multiple of 16. But this is easy. At least one of A, B, C must be even — because if A and B are *both* odd then C^n is a sum of two odd numbers, hence even, which implies that C is even. A tactical move is now in order: at this stage of the argument we can make life much easier for ourselves by taking $n \geq 5$, rather than $n \geq 3$, because Euler's proof establishes Fermat's Last Theorem for $n = 3$. Now we merely observe that the fifth or higher power of an even number is divisible by $2^5 = 32$, so $-A^nB^nC^n$ is a multiple of 32, hence certainly a multiple of 16.

Therefore Frey's curve satisfies the hypotheses of Wiles's theorem, implying that it can be parametrised by modular functions. But Frey has proved that it can't be!

This is the contradiction that we have been seeking all along — but this time it is signed, sealed, and delivered. The house of cards that we set up by assuming that there exists a nontrivial solution to the Fermat equation for $n \geq 3$ has collapsed in ruins. Therefore no such solution can exist — so Fermat's Last Theorem is true.

In summary: Wiles's strategy implies the semistable Taniyama conjecture, which implies that Ribet's argument proves that Frey's elliptic curve doesn't exist — and Fermat

was right all along.

Wiles had a huge battery of powerful techniques to work with, but it took him seven years of hard effort to see how to fit the pieces together. He knew what strategy to use, but like any general fighting a major battle, he had to get his tactics right too. And as soon as he announced his proof, of course, there was a new question to ponder. Was it right? It is *so* easy to make mistakes...

Right from the start, a surprisingly large number of experts were willing to commit themselves by saying, publically, that they believed the proof was correct. The strategy made sense, they could see how the tactics were applied, they knew what the sticky points were and what ideas Wiles had invented to get over them. Mazur summed up the consensus view: 'It has the ring of truth'.

But did it?

Fermat's Final Fling

Speculation was rife, but hard facts were thin on the ground. Unusually, Wiles did not release a 'preprint', or informal version, of his proof. Given the amount of interest, this was a reasonable move: coping with the likely demand would have laid low a forest or two. Instead he submitted his work to the world's leading mathematical journal, which sent it out to half a dozen experts to be refereed. Meanwhile, its hunger unsated, the mathematical world's communication lines hummed — technical details gleaned from people who had been at the Newton Institute when Wiles made his historic announcement, comments, queries. Jokes, even. One widely circulated electronic mail message reported a spoof newspaper article about the riotous behaviour that (allegedly) followed the announcement of the proof.

> 'Math hooligans are the worst,' said a Chicago Police Department spokesman. 'But the city learned from the Bieberbach riots. We were ready for them this time.'
>
> When word hit Wednesday that Fermat's Last Theorem had fallen, a massive show of force from law enforcement at universities all around the country headed off a repeat of the festive looting sprees that have become the traditional accompaniment to triumphant breakthroughs in higher mathematics.
>
> Mounted police throughout Hyde Park kept crowds of delirious wizards at the University of Chicago from tipping over cars on the midway as they first did in 1976 when Wolfgang Haken and Kenneth Appel cracked the long-vexing Four-Color Problem. Incidents of textbook-throwing and citizens being pulled from their cars were described by the university's math department as 'isolated'.

After a few weeks of such excitement, however, rumours of a mistake surfaced. On December 6 1993 Wiles circulated his own e-mail message:

> 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.

(Here Wiles's 'Taniyama-Shimura conjecture' is my 'Taniyama conjecture' as explained earlier.)

It is not unusual for minor tactical errors to emerge when a long and difficult mathematical proof is subjected to the very close scrutiny that is appropriate to a major breakthrough. The question then is: can the errors be repaired, the gaps closed — or is the mistake fatal?

Time passed. The promised repairs did not materialise.

Around Easter 1994 many mathematicians received a remarkable message in their electronic mail:

> There has been a really amazing development today on Fermat's Last Theorem. Noam Elkies has announced a counterexample, so that FLT is not true at all! He spoke about this at the Institute today. The solution to Fermat that he constructs involves an incredibly large prime exponent (larger than 10^{20}), but it is contructive... I wasn't able to get all of the details, which were quite intricate...

Eventually it emerged that this message had originated on April 1st.

The Final Fling Unflung

By the Autumn of 1994 even many experts were becoming pessimistic, estimating that stitching up the hole in Wiles's proof would take at least three years, maybe longer — if at all. Fermat's Last Theorem seemed to be slipping away. Then, on 26 October 1994, Rubin circulated another e-mail message:

> As of this morning, two manuscripts have been released:
>
> *Modular elliptic curves and Fermat's Last Theorem*, by Andrew Wiles.
>
> *Ring theoretic properties of certain Hecke algebras*, by Richard Taylor and Andrew Wiles.
>
> The first one (long) announces a proof of, among other things, Fermat's Last Theorem, relying on the second one (short) for one crucial step.
>
> As most of you know, the argument described by Wiles in his Cambridge lectures turned out to have a serious gap, namely the construction of an Euler system. After trying

unsuccessfully to repair that construction, Wiles went back to a different approach, which he had tried earlier but abandoned in favour of the Euler system idea. He was then able to complete his proof, under the hypothesis that certain Hecke algebras are local complete intersections. This and the rest of the ideas described in Wiles's Cambridge lectures are written up in the first manuscript. Jointly, Taylor and Wiles establish the necessary property of the Hecke algebras in the second paper.

These two papers had been refereed, approved, accepted, and published. The saga of Fermat's Last Theorem has finally come to an end.

Or, more accurately, to a new beginning. Already the proof is being simplified. Wiles's revised argument is shorter and simpler than the first incomplete attempt. Faltings, it is said has already simplified parts of it. More importantly, we now have access to a whole heap of powerful new techniques — in particular the semistable case of the Taniyama conjecture — which we can apply to other questions about elliptic curves and anything we can contrive to link to them.

There is a new power at the heart of number theory.

So: did Fermat really have a proof? There really is no likelihood that Fermat had anything similar in mind to the proof that Wiles has given the world. Big conceptual chunks were not known in Fermat's day — among them elliptic curves and modular functions. The technical machinery that underlies Wiles's approach includes rather a lot of modern algebraic number theory and algebraic geometry. The twentieth century viewpoint would have made no sense in the ninteenth century, let alone the seventeenth.

Which leaves two possibilities. Either Fermat was mistaken, or his idea was quite different. Like virtually all mathematicians, my money is on the first. But sometimes, deep in the night, I awake from strange dreams, and I wonder...

FURTHER READING

Eric Temple Bell, *The Last Theorem* (edited and updated by Underwood Dudley), Mathematical Association of America.

Barry Cipra, Fermat's Last Theorem finally yields, *Science* **261** (2 July 1993) 32-33.

David Cox, Introduction to Fermat's Last Theorem, *American Mathematical Monthly* **101** (1994) 3-14.

Paolo Ribenboim, 13 Lectures on Fermat's Last Theorem, Springer-Verlag, New York 1979.

K.Rubin and A.Silverberg, A report on Wiles' Cambridge lectures, *Bulletin of the American Mathematical Society* **31** (1994) 15-38.

Ian Stewart, *The Problems of Mathematics*, 2nd edition, Oxford University Press, Oxford 1992.

Ian Stewart, Fermat's last time trip, *Scientific American* **269** No. 5, Nov. 1993, 85-88.

Ian Stewart, *From Here to Infinity* [= *The Problems of Mathematics*, 3rd edition], Oxford University Press, Oxford April 1996, to appear.

★★★★★★

(*Solution to Diophantus's Problem:* **41, 80, 320.**)