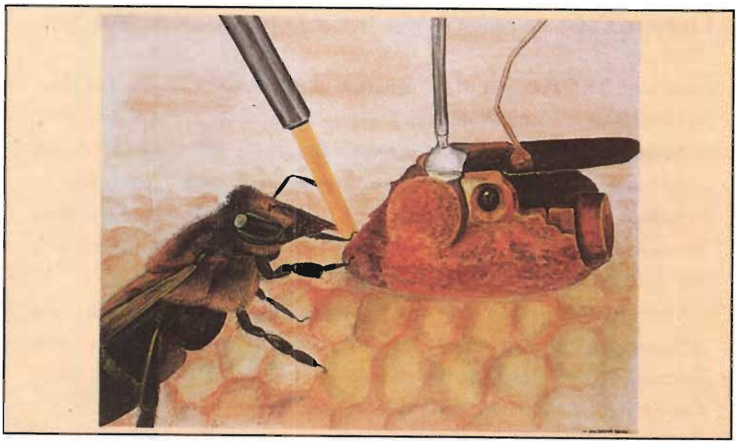
light, at the appropriate distance) where he was confident the recruits would go and sure enough he was rewarded by the arrival of the bees! Notice that the bees should have gone to the correct location, 60 degrees to the right of the real sun if they had relied on the scent of the dancers on the way to and at the location of the food. Although von Frisch retained the Nobel Prize, even this elegant experiment did not set the controversy to rest.

## The Robot Bee — A Novel Solution

The main problem is that we cannot claim to know exactly what it is that the dancer is telling the recruits. What we need is to be able to talk to bees in their own language and restrict communication to only those elements of the language that we have deciphered. Sounds impossible, does it not? Well, not quite. A Michelsen and B B Andersen from Denmark and Wolfgang Kirchner and Martin Lindauer from Germany have constructed a mechanical "robot" bee that talks to the real bees through a computer, programmed by the scientists based on their idea of the bee dance language and, believe it or not, the bees understand! The robot bee was made of brass and was about the size of a real bee *(Figure 5)*. It was coated with a thin layer of wax and made to sit in the nest among the real bees for about 12 hours and thus came to smell like the bees. It had wings made of razor blades which when vibrated produced acoustic signals similar to those

**A Michelsen and B B Andersen from Denmark and Wolfgang Kirchner and Martin Lindauer from Germany have constructed a mechanical "robot" bee that talks to the real bees through a computer.**



SANJEEVA NAYAK / MARK MOFFETT

***Figure 5** Robot bee offering food to a real bee.*

*greater than the second to be written as a sum of two like powers. I have a truly marvellous demonstration of this proposition which this margin is too narrow to contain".* Thus, it was in 1670 that the world learnt of what has come to be termed Fermat's Last Theorem (FLT): The equation

$$X^n + Y^n = Z^n$$

has no solutions in non-zero integers if $n \geq 3$. Fermat himself had given a proof of this assertion for $n = 4$ using *infinite descent*, a method he invented, and Euler proved the case $n = 3$. Thus to prove FLT we need to show that $X^p + Y^p = Z^p$ has no solutions in non-zero integers whenever $p$ is a prime greater than 3 (do you see why?).

After more than three centuries of effort by some of the best mathematicians, Gerhard Frey, J -P Serre, Ken Ribet and Andrew Wiles have finally succeeded in proving Fermat's assertion, each of them making a decisive contribution with Wiles delivering the *coup de grace*. The proof, as it finally came to be, is in some sense a triumph for Fermat. *Elliptic curves and infinite descent* play significant roles and it was Fermat who pioneered the use of elliptic curves in solving diophantine equations and it is to him that we owe the method of infinite descent.

***"On the other hand, it is impossible for a cube to be written as a sum of two cubes or a fourth power to be written as sum of two fourth powers or, in general, for any number which is a power greater than the second to be written as a sum of two like powers. I have a truly marvellous demonstration of this proposition which this margin is too narrow to contain".***

## Diophantine Equations

The chief work of Diophantus of Alexandria (c. 250 A.D) known to us is the *Arithmetic*, a treatise in thirteen books, or *Elements*, of which only the first six have survived. This work consists of about 150 problems, each of which asks for the solution of a given set of algebraic equations in positive rational numbers, and so equations for which we seek integer (or rational) solutions are referred to as diophantine equations. The most familiar example we know is $X^2 + Y^2 = Z^2$ whose solutions are *Pythagorean triples;* (3, 4, 5), (5, 12, 13) are examples of such triples. If, instead, we ask for solutions, in integers, of $X^2 + Y^2 = 3Z^2$ we get an example of a diophantine equation for which there are no solutions in non-zero integers. (To see this,'first observe that we may assume $X, Y, Z$ to be pairwise relatively prime, by cancelling common factors, if any; and that any square when divided by 3 leaves remainder 0 or 1.) In fact, it is an interesting exercise to characterize the set of natural numbers $m$ for which the equation $X^2 + Y^2 = mZ^2$ has no solutions in non-zero integers.

To understand the role of *geometry* in solving diophantine equations let us consider the equation $X^2 + Y^2 = Z^2$ . How do we characterize all solutions (in integers) of this equation? We could assume again that $X, Y, Z$ is a *primitive* solution, i.e., $X, Y, Z$ are pairwise relatively prime. Dividing by $Z^2$ and putting $X/Z = x$ and $Y/Z = y$ we get $x^2 + y^2 = 1$, that is to say, we get a *rational point* (a point both of whose coordinates are rational numbers), $(x,y)$, on the unit circle centred at the origin. Conversely, a rational point on the circle $x^2 + y^2 = 1$ will give us a (primitive) Pythagorean triple. So, our problem reduces to finding all rational points on the unit circle. We do this by drawing a line with rational slope passing through the point $(-1, 0)$. This line will meet the circle at one more point and we claim that this point is also rational. I shall leave it to you to figure out why it is so. (You need to use the fact that if one root of a quadratic equation with rational coefficients is rational then the other root is also rational.) This way we obtain all rational points on the circle. Put $t = \tan \theta/2$ in the familiar parametrisation of the circle, $(\cos \theta, \sin \theta)$. Then we get the well-known characterisation of the Pythagorean triples: if $m$ and $n, m > n$, are integers of opposite parity then the numbers

$$m^2 - n^2, 2mn, m^2 + n^2$$

form a primitive Pythagorean triple and every primitive Pythagorean triple arises this way.

This method can be used to find all rational points on a conic section whose defining equation has rational coefficients once we are able to find one such point.

**History of FLT**

- 1640, Fermat himself proved the case $n = 4$
- 1770, Euler proved the case $n = 3$; (Gauss also gave a proof).
- 1823, Sophie Germain proved the *first case* of FLT — first case of FLT holds if there is no solution for $X^p + Y^p = Z^p$ for which $p$ does not divide the product $XYZ$ — for a class of primes, *Sophie Germain primes*: primes p such that $2p + 1$ is also a prime.
- 1825, Dirichlet, Legendre proved FLT for $n = 5$.
- 1832, Dirichlet treated successfully the case $n = 14$.
- 1839, Lamé proved the case $n = 7$.
- 1847, Kummer proved FLT in the case when the exponent is a *regular prime*. But it is not known even today whether there are infinitely many Sophie Germain primes or regular primes.
- 1983, Faltings gave a proof of Mordell's conjecture.
- 1986, Frey - Ribet - Serre: Shimura - Taniyama - Weil conjecture implies FLT.
- 1994, Andrew Wiles: proof of S-T-W conjecture for semistable elliptic curves.

## Elliptic Curves

Consider the following classical problems.

(i) Find all $n$ such that the sum of the squares of first $n$ natural numbers is a square. That is, we have to find natural numbers $n$ and $m$ such that

$$m^2 = n(n+1)(2n+1)/6.$$

(ii) (Diophantus) Find three rational right triangles of equal area.

Let $A$ denote the area of the right triangle with sides $a$ $(= p^2 - q^2)$, $b$ $(= 2pq)$ and $c$ $(=p^2 + q^2)$; thus $A = pq\ (p^2 - q^2)$. Then if we put $x = p/q$ we get a rational point $(p/q, 1/q^2)$ on the curve

$$Ay^2 = x^3 - x.$$

Conversely, if $(a/b, c/d)$ is a rational point on this curve then the right triangle with $d\ (a^2 - b^2)/b^2c$ and $2ad/bc$ as legs also has area equal to $A$.

(iii) (From an Arab manuscript dated before the 9th century) Given a natural number $n$, find a rational number $u$, such that both $u^2 + n$ and $u^2 - n$ are squares (of rational numbers).

If such a $u$ can be found then $n$ is called a congruent number. A number $n$ being congruent is equivalent to the existence of a right triangle with rational sides and area $n$.

Suppose $n$ is a congruent number and let $u$ be such that $u^2 + n = a^2$ and $u^2 - n = b^2$. Multiplying the two equations together we get

$$u^4 - n^2 = (ab)^2.$$

Multiply by $u^2$ throughout to get

$$u^6 - n^2 u^2 = (abu)^2.$$

**What is *elliptic* about elliptic curves?**

Ellipses are not elliptic curves! Elliptic curves are so called because it was in connection with the problem of computing arc lengths of ellipses that they were first studied systematically. When we compute the arc of a circle, we have to integrate the function $1/\sqrt{(1-x^2)}$, which we do in terms of the sin and cos functions. The trigonometric functions are therefore called *circular functions*. Similarly, to compute the arc length of an ellipse we have to integrate functions of the form

$$1/\sqrt{[(1-x^2)(1-k^2x^2)]}.$$

This integral cannot be computed using circular functions and mathematicians worked on this problem for many years before Abel and Jacobi, independently introduced *elliptic functions* to compute such integrals. Just as sin and cos satisfy $x^2 + y^2 = 1$, the elliptic functions satisfy an equation of the form $y^2 = f(x)$ where $f(x)$ is a cubic.

Putting $u^2 = x$ and $abu = y$ we get a rational point on the curve, E, defined by the equation

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

*Exercise:* Conversely, if $(x,y)$ is a rational point on $E$ such that $x$ is a rational square and has even denominator then $n$ (whose square appears as the coefficient of $x$) is a congruent number.

In each of the above problems we were led to consider equations of the form $y^2 = f(x)$, where $f(x)$ is a cubic polynomial in $x$ with rational coefficients and distinct roots. Such equations define *elliptic curves*. We could think of elliptic curves as the set of all rational / real / complex solutions of such equations. The set of all complex solutions of an elliptic curve can be identified with the points on a *torus*. The adjacent figures *(Figure 1)* show what the real and complex points on an elliptic curve look like.

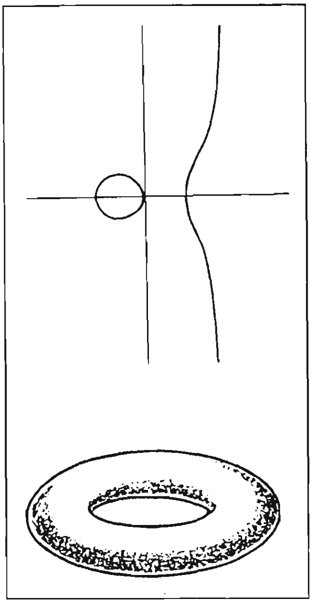


***Figure 1 Typical illustration of how the real / complex points on an elliptic curve look like.***

Finding rational points on an elliptic curve turns out to be a difficult problem and though many deep results have been proved (one of them by Andrew Wiles along with John Coates), a lot remains to be done in this area. The study of elliptic curves is currently a very active field of research involving many different areas of mathematics.

**Finding rational points on an elliptic curve turns out to be a difficult problem and though many deep results have been proved (one of them by Andrew Wiles along with John Coates), a lot remains to be done in this area.**

If we try to imitate the method we used for a conic to get more rational points from one such point we are stuck. This is because a line meets a cubic curve, generally, in three points and we cannot conclude that the other points of intersection are rational. That is, if one root of a cubic equation with rational coefficients is rational the other two roots could be irrational; they could be conjugate surds, for instance. What is true is that if you draw the line joining two rational points then the third point where this line meets the cubic will also be a rational point. Thus, we can 'add' two rational points to get a third rational point. It turns out that we could take the 'point at infinity' as the identity or the 'zero' element and obtain a structure of a *group* (in fact, a commutative group) on the set of rational points of an elliptic curve by declaring the sum of three collinear points to be zero; the inverse or 'negative' of the point $(x,y)$ is the point $(x,-y)$. Thus, to add two points $P$ and $Q$ join them by a straight line, find the third point of intersection of the line with the curve and reflect it in the x-axis to get a point, $R$, on the curve which will then be the 'sum' of $P$ and $Q$.

*Exercise:* Consider the elliptic curve, $E$, defined by the equation $y^2 = ax^3 + bx^2 + cx + d$. Obtain an expression for the coordinates, $x_3, y_3$, of the sum of the two points $P = (x_1,y_1)$ and $Q = (x_2,y_2)$ on $E$, in terms of $x_1, x_2, y_1, y_2$.
*Hint:* If $P$ is not equal to $Q$, $x_3 = -x_1 - x_2 - (b/a) + (y_2 - y_1)^2 / a(x_2 - x_1)^2$ and if $P = Q$, $x_3 = -2x_1 - (b/a) + (f'(x_1))^2 / a(2y_1)^2$ where $f(x)$ denotes the cubic.

**The structure of a group on the set of rational points of an elliptic curve provides us with a powerful tool to study diophantine equations.**

The structure of a group on the set of rational points of an elliptic curve provides us with a powerful tool to study diophantine equations. For instance, in problem 2 above if we get one rational point then we could 'double' (i.e. draw a tangent at that point) it to get one more point and then add these two to get yet another point, and so on. In fact, this is what Fermat used to get more solutions to the problem (even Diophantus used this procedure but he gave only three rational points). In the congruent number problem, it turns out that the double of any rational point which is not of order 2 is such that the x-coordinate is a square number with even denominator.

The method we used to show the non-existence of solutions of $X^2 + Y^2 = 3Z^2$ by showing that the equation has no solutions *modulo 3* is a standard method we use in studying diophantine equations. Assume that the equation has integer coefficients by clearing the denominators, if necessary. We *reduce* the equation modulo a prime $p$ by replacing the coefficients of the equation by their remainders when divided by $p$ and consider the set of solutions of the reduced equation in the *finite field* $\{0, 1, 2,.. p\text{-}1\}$. If, for example, we find a prime for which there are no solutions for the reduced equation it follows immediately that the original equation has no rational roots.

Consider an elliptic curve $E$ defined by $y^2 = f(x)$. Except for a finite set of primes depending on the cubic $f(x)$ the reduced equation will also define an elliptic curve. In fact, the *exceptional* set of primes is precisely the set of prime divisors of the discriminant of the cubic $f(x)$. For a prime $p$ not dividing the discriminant let $N_p$ denote the number of points of $E$ modulo $p$, i.e., the number of pairs $(x, y)$, with $x, y$ in $\{0,1,2,..., p-1\}$ , satisfying the equation modulo $p$. Define integers $a_p$ by

$$N_p = p + 1 - a_p.$$

These $a_p$'s could be positive or negative and Hasse proved the following inequality in 1930:

$$|a_p| \leq 2\sqrt{p}.$$

These numbers $a_p$ contain a lot of information about the rational points of the elliptic curve and there are many conjectures concerning their properties among which the Birch – Swinnerton - Dyer conjecture and the Shimura – Taniyama – Weil conjecture are the most important.

The content of the Shimura - Taniyama - Weil (S-T-W) conjecture is that these $a_p$' s are the *Fourier coefficients of a cusp form* (of weight 2 and a certain level $N$). The definition of cusp forms is beyond the scope of this article and we content ourselves by saying that they are certain functions on the upper half-plane (please see *Suggested Reading* at the end). Elliptic curves for which the $a_p$' s satisfy the S-T-W conjecture are called *modular* elliptic curves.

**The general feeling among mathematicians following Falting's proof of the Mordell conjecture was one of satisfaction since there was no reason or heuristic basis as to why FLT should be true; *at most finitely many solutions* was good enough.**

## Frey Elliptic Curve and Fermat's Last Theorem

The study of rational points on higher degree curves witnessed a breakthrough in 1983 when Gerd Faltings proved a conjecture of Mordell. As a corollary it followed that the curve $X^n + Y^n = 1$ has only finitely many rational points if $n \geq 5$ which means that there would be at most finitely many solutions to the Fermat equation

$$X^n + Y^n = Z^n.$$

The general feeling among mathematicians following this was one of satisfaction since there was no reason or heuristic basis as to why FLT should be true; *at most finitely many solutions* was good enough.

**Fermat's favourite target for his problems and challenges were the English mathematicians; after all he was French! Thus it is fitting that his most famous challenge has been answered by Wiles, an Englishman, though it took a while (A Wiles!) coming!**

But FLT bounced back soon after in 1985 when Gerhard Frey linked a counter example of FLT, if there is one, with an elliptic curve which did not seem to satisfy the S-T-W conjecture! Frey's was a simple but very ingenious idea: if, for some prime $p > 3$, there are non-zero integers $u,v,w$ such that $u^p + v^p = w^p$ then consider the elliptic curve, now referred to as the *Frey curve*,

$$y^2 = x(x + u^p)(x - v^p).$$

Thus for the first time, FLT for *any exponent* was connected with a *cubic* curve instead of the higher degree curve which the equation itself defines.

Then things started happening fast and in the summer of 1986, building on the work of Frey and Serre, Ribet succeeded in proving that S-T-W implies FLT by showing that the Frey curve could not be modular. Now, FLT was not just a curiosity but was related to a deep conjecture; if it were not true and we had a counter example, the Frey curve would be sticking out like a sore thumb!

Soon after he heard of Ribet's result, Andrew Wiles went to work on the S-T-W conjecture in the late summer of 1986. After working hard on it for seven years, during which even his closest friends did not get to know what he was up to, Wiles stunned the mathematical world by claiming that he had proved the FLT by proving a particular case of the S-T-W conjecture, the case of *semi-stable* elliptic curves. He made the announcement at the end of a series of lectures at the Isaac Newton Institute in Cambridge, England on the morning of Wednesday, June 23, 1993. But experts checking his proof found many gaps of which he could overcome all but one. It is to the credit of Wiles that he did not let this setback deter him. Rather, encouraged and mathematically supported by his students and close friends, notably Henri Darmon, Fred Diamond and Richard Taylor, he circumvented the gap in September 1994. His paper, along with another one of his jointly with Richard Taylor, occupies one whole issue of the leading journal *Annals of Mathematics*, 142 (1995). It should be remarked that the theorem Wiles proves is a very significant result with far-reaching consequences and FLT follows as a simple corollary.

***Figure 2** Andrew Wiles who delivered the final* **coup de grace** *in the proof of FLT.*

Apparently, Fermat's favourite target for his problems and challenges were the English mathematicians; after all, he was French! Thus, it is fitting that his most famous challenge has been answered by Wiles, an Englishman *(Figure 2)*, though it took a while (A Wiles!) coming!

## Suggested Reading

**Paulo Ribenboim. 13 Lectures on Fermat's Last Theorem. Springer-Verlag. 1979.**

**H M Edwards. Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory. Springer-Verlag. 1977.**

**The two books above contain historical accounts of the various attempts to prove FLT and developments stemming from these attempts, especially the work of Kummer.**

**J -P Serre. A Course in Arithmetic. Springer International Student Edition, 1979.**

**This extraordinary book covers in just hundred pages many important theorems in number theory (with proofs) and contains an introduction to modular forms.**

**Neal Koblitz. Introduction to Elliptic Curves and Modular Forms. Springer-Verlag. 1984.**

**This contains a beautiful introduction to elliptic curves and modular forms via the *congruent number problem*.**

*Address for correspondence*
C S Yogananda
Scientist, NBHM (DAE)
Department of Mathematics,
Indian Institute of Science,
Bangalore 560012, India.