DORIAN GOLDFELD

Beyond the Last Theorem

In May of last year two mathematicians published a proof of Fermat's conjecture, the most famous mathematical brainteaser of all time. So what comes next?

On August 8, 1900, at the International Congress of Mathematics in Paris, the German mathematician David Hilbert stood before his peers and posed twenty-three difficult, unsolved problems that he believed should guide the future of mathematics.

Hilbert was thirty-eight years old and a professor at the prestigious University of Göttingen. As an extraordinary generalist with a passion for order and rigor, he was just the man to make the other mathematicians of his day sit up and take notice. The year before, with the publication of his book *Grundlagen der Geometrie* (*The Foundations of Geometry*), he had embarked on the project that was to occupy the remainder of his career: to make rock solid the foundations of mathematics. Mathematicians, he declared, should devote themselves to reducing mathematical concepts to rigorous axioms—lists of fundamental terms, relations and rules—which could then be proved consistent, ensuring that mathematical discovery is anchored in unassailable principles.

Some of the problems Hilbert proposed to the congress (such as number four, the "problem of the straight line as the shortest distance between two points") reflected his own back-to-basics approach to mathematics. Others had nagged at mathematicians for generations. Problem ten dealt with *Diophantine equations*, algebraic equations in several variables whose solutions are required to be rational numbers—that is, whole numbers or fractions, the ratios of whole numbers.

Diophantine equations take their name from the Greek mathematician Diophantus of Alexandria, who probably lived in the third century of our era and who discussed such problems at length in his treatise *Arithmetica*. Typical among them is a problem that fascinated the Greeks, namely, finding right triangles the lengths of whose sides are in whole-number ratios to one another. To state the matter in the form of an equation, the right-triangle problem is to find whole numbers x, y and z that satisfy the Pythagorean relation $x^2 + y^2 = z^2$. And as many schoolchildren learn, the numbers 3, 4 and 5 are the simplest triplet that solve the problem—though an infinite number of other such right triangles can be generated.

Hilbert's tenth problem posed a challenge of breathtaking generality:

Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.

It was an ambitious goal. Diophantine equations include some of the oldest and most tenacious problems in number theory. Diophantus himself had already raised the study of such equations to quite sophisticated heights. In the *Arithmetica* he noted that he had found four whole numbers x, y, z and u that satisfy the equation $x^4 + y^4 + z^4 = u^2$. (An infinite number of solutions can be derived from the Pythagorean right triangles; the simplest is given by the numbers 12, 15, 20 and 481, for x, y, z and u, respectively.) That finding proved to seed a pivotal event in the history of mathematics, though many centuries were to pass before the seed came into bloom. Some time around 1637, Pierre de Fermat, a French provincial lawyer and passionate amateur mathematician, encountered Diophantus's result in his copy of a translation of Diophantus. "Why," wrote Fermat in the margin of the book, "did not Diophantus seek two fourth powers such that their sum is a square? This problem is, in fact, impossible, as by my method I am able to prove with all rigor."

In fact, Fermat was to make a much stronger assertion, and the margin of his copy of the *Arithmetica* (now apparently lost) went on to proclaim:

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 two powers of the like degree; I have discovered a truly remarkable proof which this margin is too small to contain.

For the "biquadrate" (fourth power) case, Fermat's earlier assertion is sufficient to imply the later one: if two fourth powers cannot sum to a perfect square, they cannot sum to a fourth power either (since any fourth power, say w^4, is also a perfect square, namely, the square whose side measures u^2). But Fermat was asserting much more. In modern notation Fermat's assertion—known to mathematicians as Fermat's last theorem, or FLT for short—states that the equation $x^n + y^n = z^n$ has no solution if x,

DORIAN GOLDFELD is a professor of mathematics at Columbia University. This article is based on a talk he gave on May 4, 1995, before the section of mathematics at the New York Academy of Sciences.

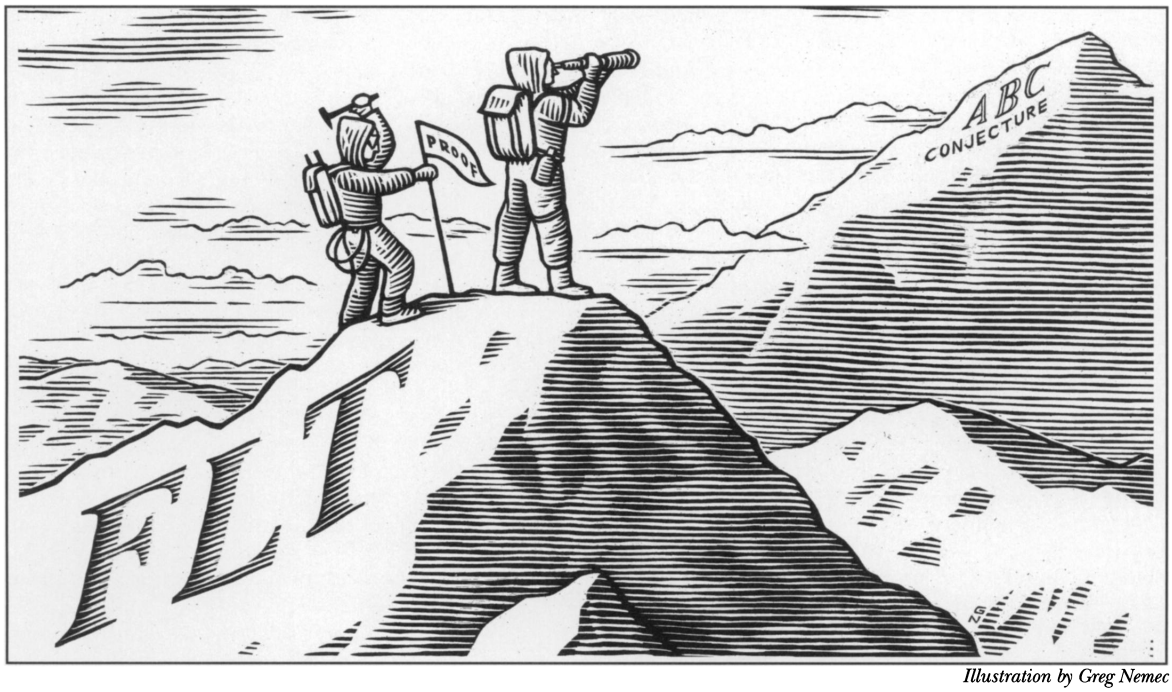


Illustration by Greg Nemec

y and z all are positive integers and n is a whole number greater than 2.

Fermat's last theorem is the consummate Diophantine equation: crisp, clean, easy to state, virtually useless and maddeningly difficult to solve. In the three and a half centuries since its appearance it has attracted a plethora of would-be conquerors, drawn by the desire for fame and the lure, from time to time, of outrageously enormous monetary rewards.

Then, on June 23, 1993, the news media reported that Andrew Wiles, a professor of mathematics at Princeton University, had solved the problem at last. Experts soon uncovered an embarrassing gap in the alleged proof, but in a virtuoso tour de force Wiles and his former student Richard Taylor, a mathematics professor at the University of Cambridge, filled in the hole and cracked the problem. The completed proof, all 130-odd pages of it, was published in May 1995 in the *Annals of Mathematics*. And as far as the media and the nonmathematical public were concerned, that was the end of the matter.

They were wrong, on several counts. For one thing the key proposition proved by Wiles and Taylor was not Fermat's last theorem. It was a radically different theorem, of which FLT was an incidental consequence. That theorem is well worth understanding in its own right, for it is just as beautiful as Fermat's last theorem, and it is vastly more significant. For one thing, it marks the first major step in a long-range program conceived by Robert P. Langlands, a mathematician at the Institute for Advanced Study in Princeton, New Jersey. If successful, the program will culminate in a unified theory of zeta functions, extremely useful mathematical objects that pop up in protean diversity throughout many branches of mathematics and physics. More immediately, and along a different avenue of research, the Wiles–Taylor proof could well trigger the greatest advance yet in the history of Diophantine analysis: a general theory of three-variable Diophantine equations.

That lack of an overarching theory of Diophantine equations was the fundamental problem Hilbert had hoped to correct. Historically, Diophantine problems had always been stated and solved on a case-by-case basis. Over the centuries, mathematicians had devised an assortment of tricks, dodges and *ad hoc* procedures for certain kinds of equations, but a grand pattern eluded them.

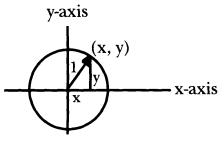
In 1970 the Russian mathematician Yuri Matijasevich of the Steklov Mathematical Institute in Leningrad (now Saint Petersburg) showed that, in a strict sense, such a grand pattern is impossible: no matter what procedure mathematicians devise for solving Diophantine equations, there will always remain some equations whose solutions are undecidable. In other words, there are some equations to which solutions will never be found but for which it will also never be proved that no solutions exist—a dismal conclusion that follows from discoveries about the logic of mathematics made in 1931 by the Austrian logician Kurt Gödel. Hilbert's tenth problem could never be solved.

In a paper that was published in 1974 Matijasevich and the late Julia Robinson showed that the limbo of off-limits problems includes certain Diophantine equations with thirteen or more variables. Before that paper even appeared they further lowered the number to nine: no algorithm can determine whether Diophantine equations in nine unknowns have integer

solutions. For such equations there can be no hope: the theory of logic itself provides an impenetrable barrier to their solution. What about equations with fewer variables? Nobody knows. The magic line between solvability and unsolvability might start as low as four variables or as high as eight. All that mathematicians can say for the present is that the proof of Wiles and Taylor indicates that Diophantine equations in three variables should be solvable.

The proposition proved by Wiles and Taylor was the bulk of a conjecture generally attributed to three mathematicians: Goro Shimura, also of Princeton; the late Yutaka Taniyama; and André Weil of the Institute for Advanced Study. The conjecture, now known as the *STW conjecture*, after the surnames of the three mathematicians, dates back to 1955, when it was published in Japanese as a research problem by Taniyama. It posed a kind of equivalence between the mathematics of objects known as elliptic curves and the mathematics of rigid motions in space. (Elliptic curves are not ellipses; their name stems from the fact that they are useful for calculating the arc length of ellipses—for instance, the distance a planet travels in its orbit around the sun.)

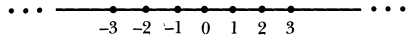
To understand the kind of equivalence posed by the STW conjecture, it is helpful to examine a similar connection between two ways of looking at a circle. In geometry a circle is defined as the set of all points equally distant from one fixed point. Plotted on the familiar perpendicular *x-y* coordinate grid, with the center of the circle at the origin and the distance set equal to 1, that definition translates into the set of all points



Circle

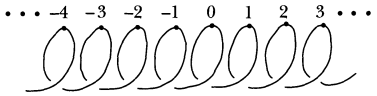
for which $x^2 + y^2 = 1$. In algebraic terms, then, one can think of the circle as the set of solutions to that equation.

But there is another way of looking at a circle. Consider a clock, an antique twenty-four-hour model with a single hand that swings around the dial once a day, pointing first to "high midnight," then to 1:00 a.m. and so on. The clock has no idea what day it is; as far as it is concerned, 3:05 p.m. today is indistinguishable from 3:05 p.m. tomorrow, or next week or on any date you might imagine. In mathematical terms each point on the circular dial sets up an *equivalence class* comprising all the moments in the past, present and future at which the hand points precisely to that point. Schematically, the clock dial takes a time line marked with equally spaced integers (the midnight points),



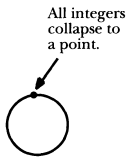
Number line

twists it into a shape like a Slinky, and



Slinky

then collapses the Slinky into a circle.



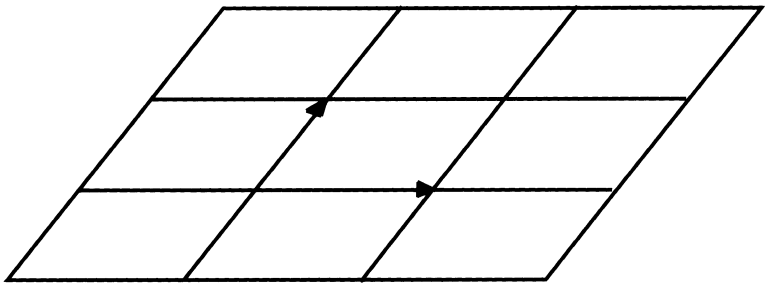
The slinky collapses to a circle.

What the circle does for the one-dimensional flow of time, it can also do for the infinite one-dimensional space of the real number line. In that case the circle becomes a set of equivalence classes of pure numbers. Formally, for any number x, the equivalence class is defined to be the set of all numbers of the form $x + nc$, in which c is the circumference of the circle and n is any positive or negative whole number.

At first glance the two descriptions of a circle—one in terms of algebra, the other in terms of equivalence classes—could hardly be more different. But they are indeed equivalent, linked by the Pythagorean theorem and some elementary geometry. Consider a function $f(x)$, which takes a number x and connects it, or as mathematicians say, maps it, to another number $f(x)$. To be well defined on the equivalence classes that make up the circle, $f(x)$ must be periodic. That is, $f(x + nc)$ must have the same value as $f(x)$ for some number c and for every integer 1. In the case of a circle of radius one, the required periodic functions are just the sine and cosine functions. It is a simple consequence of the Pythagorean theorem that $\cos^2 x + \sin^2 x = 1$. If you then replace $\cos x$ with X and replace $\sin x$ with Y you get the equation $X^2 + Y^2 = 1$—and there you are, back at the original description of a circle. In mathematical parlance, by making that substitution you have parameterized the equation of the circle by periodic functions.

The equivalence that Shimura, Taniyama, and Weil proposed in their conjecture was based on a similar substitution—not for circles, however, but for *elliptic curves*. The equation of an elliptic curve is $y^2 = x^3 + ax + b$, only slightly more complicated than the equation of a circle. And like the equation of a circle, it can be parameterized. The first person to show how to do so was the nineteenth-century German mathematician Weierstrass, who developed the procedure in a classical theorem.

Weierstrass generalized the idea of equivalence classes on a number line to a two-dimensional plane. Imagine the plane as an infinite sheet of extremely thin, clear plastic, governed by the usual coordinate system, a horizontal x axis and a vertical y axis. Next, in your imagination, cover the plane with a grid, drawing regularly spaced parallel lines A units apart in one direction and B units apart in another direction. The lines need not be parallel to the axes, or even perpendicular to one another, but for the sake of simplicity assume they are. The result is a tessellation, or tiling,



Tiling of the plane

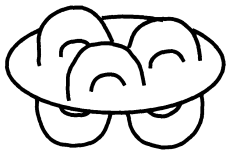
of the plane into an infinite number of identical rectangles.

Now imagine that you pick up a pin, close your eyes and stick the pin at random into the plane. Wherever the pin lands, it will wind up lodged inside or on the boundary of one of the rectangles. Because all the tiles are identical, every other rectangle in the plane must include exactly one point in a position corresponding to that of the pin. (Boundary points on two adjacent sides of each rectangle can be thought of as belonging to that rectangle; boundary points on the other two sides then belong to neighboring rectangles.) Thus any point in the plane can be mapped onto a point in any of the rectangles in the plane; in effect, the whole plane can be collapsed into a single rectangle. The rectangles divide the plane into equivalence classes, just as the integers divide up the number line.

When you encapsulate a plane into a single rectangle, that rectangle takes on some unusual characteristics. For one thing, the parallel sides of the rectangle—top and bottom left and right—become equivalent. Move far enough toward the top, and you reappear on the bottom. Move toward the right, and you reappear on the left. (You get the same effect on the screens of some video games.) As a result, whereas a circle has a single period, the tiling of a plane has two, one horizontal and the other vertical. There is a tidy way of representing that double periodicity. First fold the top and bottom of the rectangle toward each other until they touch, and glue them together to make a cylinder. Then bring the rolled-up sides of the rectangle together, and glue them together, too. The finished product is a doughnut-shaped geometric figure, or torus.

The two periods on a torus are easy to see. They are represented by two circles: one that goes through the hole in the doughnut, and one that goes around the rim. Just as periodic functions can be defined on a circle, doubly periodic functions can be defined on a torus. Weierstrass showed that such doubly periodic functions can be used to parameterize elliptic curves. By choosing suitable lengths for A and B in the original tiling, it is possible to restate any elliptic equation in terms of equivalence classes in a plane.

But Weierstrass's method is not the only way of parameterizing an elliptic curve. In their conjecture Shimura, Taniyama and Weil proposed another method for elliptic curves $y^2 = x^3 + ax + b$ for which the coefficients a and b are integers. The STW conjecture states that, in addition to a torus, there is another surface that can supply the necessary equivalence. The surface is different for every elliptic curve, but all of them resemble something a child in kindergarten might make out of modeling clay: a blob poked full of holes, like a torus with extra handles grafted

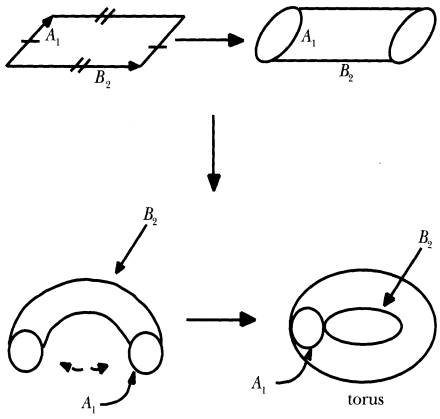


Riemann surface

onto it. To create such a surface (although the procedure can be hard to visualize), all you have to do is take a polygon of the right shape, match up pairs of sides and fold and glue the sides together.

That polygon holds the key to the STW conjecture. Like the rectangle that gives rise to a torus, it represents a method of defining equivalent points. This time, however, the equivalence classes stem not from tiling but from rigid motions of the plane. A rigid motion is a change that moves a plane without stretching or squashing any part of it. For example, imagine that every point in the plane suddenly hops one unit to the right. Or imagine that every point in the plane pivots through a right angle around some imaginary axis. Those are rigid motions. If you pick one point in the plane and trace it through a series of such shifts and rotations, it will correspond to exactly one point for each new position of the plane. Consequently, a sequence of rigid motions creates a set of equivalence classes, one for every point in the plane.

Functions that are periodic with respect to rigid motions are called *modular functions*. Remember how the equivalence classes of a clock dial wrap the number line into a closed circle? In much the same way, if you imagine a curve (a piece of string, if you like) that winds through or around various collections of holes in the blob I described earlier, the



Construction of a torus by folding opposite sides.

equivalence classes of the rigid motions wrap the curve back to its starting point in a closed loop. The theory of modular functions is an important branch of mathematics with many diverse applications, including—not surprisingly, given the terminology—string theory, a branch of theoretical physics that has excited many cosmologists.

Shimura, Taniyama and Weil conjectured that, by picking the right sequence of modular functions, one can create a surface made up of points that constitute solutions to any elliptic curve for which a and b are integers—just as by picking the right set of trigonometric functions (the sine and cosine), one can create a curve, namely, a circle, whose points constitute solutions to the equation $x^2 + y^2 = 1$.

To mathematicians, the statement and proof of the STW conjecture were as revolutionary as the first mingling of waters in the Panama Canal. Until that point, the mathematics of elliptic functions and the mathematics of rigid motions had developed in isolation from each other and in strikingly different ways. The study of elliptic curves was a branch of number theory, small, specialized and provincial—not unlike the study of Diophantine equations. In contrast, the study of rigid motions was a bustling, sophisticated suburb of topology, geometry, and analysis, with many applications to engineering and physics. Mathematicians had been working on rigid motions intensely for a hundred years and had accumulated a vast armamentarium of powerful mathematical machinery. By suggesting that the two fields could be linked, Shimura, Taniyama and Weil delivered that heavy machinery to the construction site of elliptic curves; by proving that the link held, Wiles and Taylor started the engines. The result has been a frenzy of productive mathematical work that has benefited each field and is likely to lead to solutions of outstanding problems in other fields as well.

The cross-fertilization between fields also resulted in the proof of Fermat's last theorem. In the mid-1980s Kenneth A. Ribet of the University of California, Berkeley, showed that if the STW conjecture was true, FLT would follow as an automatic consequence. Ribet's work was based on earlier work by Gerhard Frey of the University of Saarland in Saarbrucken, Germany, and Jean-Pierre Serre of the College of France in Paris. But despite the publicity it has received, FLT could well turn out to be a minor consequence. As charming as FLT was (and three centuries of effort is proof enough of its fascination), much bigger mathematical game is afoot, and there are strong indications that the methods Wiles and Taylor used may soon bring it down.

Illustration by Greg Nemec

Traditionally, as I said earlier, the biggest barrier to Diophantine analysis has been that mathematicians must solve each problem on a case-by-case basis. There has been no unifying theory to connect the problems. Now it appears that such a theory may be close at hand. The key is a problem called the *ABC conjecture*, formulated in the mid-1980s by the French mathematician Joseph Oesterle of the University of Paris VI and the English mathematician David W. Masser of the Mathematics Institute of the University of Basel in Switzerland. If the ABC conjecture can be shown to be true, Diophantine analysis will no longer be the mathematical equivalent of fly-fishing; it will be more like fishing with dynamite. That is because the ABC conjecture promises to provide a new way of expressing Diophantine problems, one that translates an infinite number of Diophantine equations into a single mathematical statement. The equations include those for most of the classical problems in three variables, including Fermat's last theorem.

The ABC conjecture, like many problems in number theory, is straightforward enough even for non-mathematicians to understand. It requires only one new concept: that of a *square-free number*, an integer that is not divisible by the square of any number. The numbers 15 and 17 are square free, but 16 and 18 are not. Now for a definition: the *square-free part* of an integer n is the largest square-free number that can be formed by multiplying the factors of n. Mathematicians denote it sqp(n). Thus sqp(15) is 15; sqp(16) is 2; sqp(17) is 17; sqp(18) is 6. In general, if n is square free, the square-free part of n, sqp(n), is just n. Otherwise, sqp(n) is what is left of n after all the factors that create a square have been eliminated. Looked at another way, sqp(n) is the product of the distinct prime numbers that divide n (a prime number is any integer that can be divided only by itself and by 1). To cite two more examples,

$$\text{sqp}(9) = \text{sqp}(3^2) = 3;\ \text{sqp}(1{,}400) = \text{sqp}(2^3 \times 5^2 \times 7) = 2 \times 5 \times 7 = 70.$$

The ABC conjecture deals with pairs of numbers that have no factors in common. Let A and B be two such numbers, and let C be their sum. Now consider the square-free part of $A \times B \times C$. For example, if $A = 3$ and $B = 7$, then C is 10 and sqp(ABC) is $3 \times 7 \times 10$, or 210. If you start plugging in numbers at random, you will find that in most cases sqp(ABC) is greater than C—in other words, sqp(ABC)/C is greater than 1. But that is not always the case. For example:

If A is 1 and B is 8, then $C = 1 + 8 = 9$, and $\text{sqp}(ABC)/C = \text{sqp}(1 \times 2^3 \times 3^2)/9 = (1 \times 2 \times 3)/9 = 6/9 = 2/3$.

If A is 3 and B is 125, then $C = 3 + 125 =$

128, and $\mathrm{sqp}(ABC)/C = \mathrm{sqp}(3\times5^3\times2^7)/128 = (3\times5\times2)/2^7 = 15/64$.

A is 1 and B is 512, then $C = 1 + 512 = 513$, and $\mathrm{sqp}(ABC)/C = \mathrm{sqp}(1\times2^9\times3^3\times19)/513 = (1\times2\times3\times19)/(3^3\times19) = 2/9$.

Masser proved that the ratio $\mathrm{sqp}(ABC)/C$ can get arbitrarily small. That is, if you name any number greater than zero, however minute, then somewhere among the infinitude of positive integers there are numbers A and B for which $\mathrm{sqp}(ABC)/C$ is smaller than that number. Surprisingly, however, it appears that if you change the expression slightly, Masser's statement no longer holds. The ABC conjecture states that $[\mathrm{sqp}(ABC)]^n/C$ does reach a minimum value if n is any number greater than one—even a number such as 1.0000000001 that is only slightly greater than 1.

The remarkable thing about the ABC conjecture is that it provides a way of reformulating an infinite number of Diophantine problems—and, if it is true, of solving them. Fermat's last theorem, for instance, could be shown to result from a straightforward proof by contradiction, as follows:

Assume Fermat's last theorem is false; that is, there are positive integers x, y, z and k (with k greater than two) such that $x^k + y^k = z^k$. It is safe to assume further that x^k and y^k have no common factors (if they did, you could just divide every term by those factors and get an equivalent equation without common factors). Now simplify the formula by setting A equal to x^k, B equal to y^k and C equal to z^k, so that the equation becomes $A + B = C$.

According to the ABC conjecture, for any value of n greater than one, $[\mathrm{sqp}(ABC)]^n/C$ must be greater than some minimum value. At present, with the conjecture still unproved, no mathematician would dare to suggest what that minimum actually is for a given value of n, but that does not matter: the proof will work no matter what it is. So assume that n is two and the minimum is 1 (values that my home computer declares realistic for A and B well into the thousands). That is, $[\mathrm{sqp}(ABC)]^2/C$ is always greater than 1.

Now $\mathrm{sqp}(ABC)$ is just another way of writing $\mathrm{sqp}(x^k y^k z^k)$, which, by the definition of the square-free-part function, must be less than or equal to xyz. And because x and y are less than z, xyz must be less than z^3. Thus $\mathrm{sqp}(ABC)$ is less than z^3, and so $[\mathrm{sqp}(ABC)]^2/C$ is less than $(z^3)^2/C$, which in turn is the same as z^6/z^k, or $z^{(6-k)}$. But as I just noted, if the ABC conjecture is true, one might as well assume that $[\mathrm{sqp}(ABC)]^2/C$ is greater than 1, and so $z^{(6-k)}$ is also greater than one. But that is a contradiction for any whole number k greater than 5. The only way to remove the contradiction is to remove the assumption that FLT is false, and so (again, assuming the truth of the ABC conjecture) FLT must be true. By retracing the argument with a smaller value of n, you could bring about a contradiction for any whole number k greater than two, thereby proving Fermat's last theorem.

The ABC conjecture is the most important unsolved problem in Diophantine analysis. It is more than utilitarian; to mathematicians it is also a thing of beauty.

The ABC conjecture is the most important unsolved problem in Diophantine analysis. It is more than utilitarian; to mathematicians it is also a thing of beauty. Seeing so many Diophantine problems unexpectedly encapsulated into a single equation drives home the feeling that all the subdisciplines of mathematics are aspects of a single underlying unity, and that at its heart lie pure language and simple expressibility. No wonder mathematicians are striving so hard to prove it—like rock climbers at the base of a sheer cliff, exploring line after line of minute cracks in the rock face in the hope that one of them will offer just enough purchase for the climbers to pick their way to the top. In this case the cracks in the rock face are mathematical statements equivalent to the ABC conjecture, any one of which might yield the proof being sought.

One promising avenue of research focuses on an elliptic curve called the *Frey curve*, after Gerhard Frey. The Frey curve is defined by the equation $y^2 = x(x - A)(x + B)$, where A and B are integers with no common factors. In studying the curve, one of the first things a mathematician does is calculate a number called the discriminant, which gives important information about the shape of the curve, the number of possible solutions to the equation, and where among the realms of real and complex numbers the solutions must reside. If you took high school algebra, your teacher no doubt drummed into your head the formula $b^2 - 4ac$, the *discriminant* of the general quadratic expression $ax^2 + bx + c$. For the Frey curve, the discriminant takes a particularly simple and pleasing form: $(ABC)^2$, where C is equal to A plus B—an expression provocatively similar to the one at the heart of the ABC conjecture. The resemblance is more than esthetic; in fact, the discriminant of the Frey curve may be the key that unlocks the proof of the ABC conjecture.

To see why, remember how Shimura, Taniyama and Weil brought the heavy machinery of rigid motions to the theory of elliptic curves by proposing that every elliptic curve with integer coefficients is related to a set of rigid motions in space. In the formulas that describe rigid motions, every rigid motion is governed by one crucial number, N, known as the conductor. Its exact definition is technical and does not matter here, but what does matter is something that Frey found out about it. He showed that the conductor of the Frey curve is essentially the square-free part of the discriminant: $N = \mathrm{sqp}[(ABC)^2]$. And the square-free part of $(ABC)^2$, of course, is the same as the square-free part of ABC.

continued on page 34

Problem 52: (Quickie) Trigonometric Identity

(i) Case $n = 2m$.

$$\sum_{k=0}^{m-1} \frac{\tan(4k+1)\pi}{8m} = \sum_{j=m}^{2m-1} \frac{\tan(4j+1-4m)\pi}{8m}$$
$$= -\sum_{j=m}^{2m-1} \frac{\cot(4j+1)\pi}{8m},$$

$$\sum_{k=m}^{2m-1} \frac{\tan(4k+1)\pi}{8m} = \sum_{j=0}^{m-1} \frac{\tan(4j+1+4m)\pi}{8m}$$
$$= -\sum_{j=0}^{m-1} \frac{\cot(4j+1)\pi}{8m}.$$

(ii) Case $n = 2m+1$.

$$\sum_{k=0}^{m} \frac{\tan(4k+1)\pi}{8m+4} = \sum_{j=0}^{m} \frac{\tan(4m+1-4j)\pi}{8m+4}$$
$$= \sum_{j=0}^{m} \frac{\cot(4j+1)\pi}{8m+4},$$

$$\sum_{k=m+1}^{2m} \frac{\tan(4k+1)\pi}{8m+4} = \sum_{j=m+1}^{2m} \frac{\tan(12m+5-4j)\pi}{8m+4}$$
$$= \sum_{j=m+1}^{2m} \frac{\cot(4j+1)\pi}{8m+4}.$$

Editorial note. The proposer conjectured that each of the given sums equals n. This follows from the known identity $\sum_{k=0}^{n-1} \cot(a+k\pi/n) = n \cot na$ and takes more effort to prove.

Problem 54: (Quickie) Diophantine Equations

(1)Define the sequence $\{F_n\}$ by $F_{n+1} = F_n!$ where $F_0 = n$. Since $n(n-1)! = n!$, it follows that an infinite set of solutions to the more general equation $x_0!x_1!\cdots x_m! = x!$ is given by $x_0 = F_0$, $x_1 = F_1 - 1$, $x_2 = F_2 - 1, \ldots, x_m = F_m - 1$, $x = F_m$.

(2) Assuming $a \geq b \geq c \geq d \geq e \geq f$, we have $6a! \geq (a+1)!$ or $5 \geq a$. Hence, the only solutions are $(5,5,5,5,5,5,6)$ and $(3,3,3,2,2,2,4)$.

(3) Assuming $a \geq b \geq c \geq d \geq e \geq f$, we have $6a^a \geq (a+1)^{a+1}$ so that there are no solutions.

Problem 58: (Quickie) Maximum Sum

Since the sum is convex in each of the x_i's, it takes on its maximum value for the x_i's being either 0 or 1. Hence the maximum sum is $n-1$.

[*Continued from page 31*]

Are alarm bells going off? If not, take another look at the ABC conjecture. All it says (hypothetically) is that if the number n is greater than 1, $[\text{sqp(ABC)}]^n/C$ has a lower bound greater than zero. Thanks to Frey's discovery, mathematicians now have a chance to derive the conjecture from any number of relations that might link conductors, discriminants and almost everything else I have talked about so far. It seems almost inevitable that if we mathematicians propose enough plausible-looking relations, one of them will pay off.

In 1988 I discovered one possibility while looking at the two ways of parameterizing the Frey curve: Weierstrass's method (parallelograms and toruses) and the STW method (rigid motions and many-holed surfaces). The relation was a simple ratio: the area of the tiling parallelogram, divided by the conductor raised to some power. If that ratio has a lower bound, I showed, the ABC conjecture is true. More recently, harnessing the techniques pioneered by Wiles and Taylor, I developed some other statements equivalent to the ABC conjecture while working with the French mathematician Lucien Szpiro of the University of South Paris in Orsay. Szpiro has developed an elegant conjecture involving the discriminant and the conductor, from which the ABC conjecture would follow. Szpiro has proved his conjecture for certain special kinds of elliptic curves, and massive computational evidence has borne out the more general case. The signs are that a proof of the ABC conjecture could well be close at hand.

If the ABC conjecture yields, mathematicians will find themselves staring into a cornucopia of solutions to long-standing problems. Some of those problems are of more than theoretical interest. Nowadays many methods of ensuring the security of electronic mail and other computerized transactions depend heavily on number theory, as programmers develop ciphers based on time-consuming problems in arithmetic. For example, a highly popular technique depends on the difficulty of determining all the large prime factors of a very large number. In principle, it should also be straightforward to create a cipher based on the difficulty of solving problems in Diophantine analysis. The major hurdle is the solvability barrier: the number of variables above which a Diophantine equation becomes impervious to attack. Any cipher based on an equation with that many variables should be absolutely secure. But where is the threshold? As I noted earlier, all anyone knows is that it probably lies between three and nine variables. At current or foreseeable processing speeds, a nine-variable cipher is impracticably slow, even for the fastest computers. A four-variable Diophantine cipher, however, would be both practical and extremely useful. If Hilbert's ghost were to return to proclaim twenty-three directions for mathematical research in the twenty-first century, nailing down the solvability barrier would certainly be among them.■