Fermat's Last Theorem Remains Unproved

When a Japanese mathematician recently offered a proof of Fermat's Last Theorem, it seemed that one of mathematics' most famous open problems might at last have been solved, but the excitment proved to be premature

THE RECENT ATTEMPT by an eminent Japanese mathematician to solve the famous problem known as Fermat's Last Theorem fell short of the mark, the victim of an assumption that turned out to be unwarranted. Less than 6 weeks after the proof first became publicly known, its author, Yoichi Miyaoka, retracted it, and experts in the theory see little chance that the obstacle that was discovered will be overcome any time soon. Miyaoka's work sheds light on a difficult field of mathematics, but "without a new idea, Fermat's Last Theorem will not be solved this way," according to one observer.

News that Miyaoka, a professor of mathematics at Tokyo Metropolitan University, had possibly proved Fermat's Last Theorem electrified the world mathematics community. Miyaoka's proof was based on new ideas that make arithmetical analogs of results in geometry. The trouble is caused by a critical geometric component that does not seem to have a good analog. Miyaoka tried an ingenious "geometric" substitute, but closer examination revealed that the ersatz component is not up to the task.

Fermat's Last Theorem is undoubtedly the most famous open problem in mathematics. The theorem states quite simply that the equation $x^n + y^n = z^n$ has no positive integer solutions x,y,z if the exponent n is greater than 2. Pierre de Fermat formulated this conjecture around 1637. It is called a theorem only because Fermat claimed to have "a marvelous proof," which he said was too long to squeeze into the margin of his book.

The problem has withstood the efforts of generations of mathematicians, yielding only individual cases, which by now include all exponents up to 150,000. (The theorem need only be proved for the exponent $n = 4$ and exponents that are prime numbers, because if it is true for a given exponent then it is also true for any multiple of that exponent. For instance, if $x = a$, $y = b$, $z = c$ were a solution to the equation $x^6 + y^6 = z^6$, then $x = a^2$, $y = b^2$, $z = c^2$ would be a solution to the equation $x^3 + y^3 = z^3$.)

Fermat did find room to write down a proof for the exponent $n = 4$, and the Swiss mathematician Leonhard Euler gave a proof for $n = 3$ in the 18th century. In the 1840s, several mathematicians worked on a general proof which, like Miyaoka's, foundered on an unwarranted assumption: they had assumed that the unique factorization of integers into primes (such as $60 = 2 \times 2 \times 3 \times 5$) would hold for number systems that extend beyond the ordinary integers. In actuality, unique factorization is rather rare. For instance, 2×3 and $(1 + \sqrt{-5})(1 - \sqrt{-5})$ are distinct factorizations of 6 in a number system that treats $\sqrt{-5}$ as an integer.

"Without a new idea, Fermat's Last Theorem will not be solved this way"

Ernst Eduard Kummer went on to systematize the violation of unique factorization, and developed a theory that allowed him to prove Fermat's Last Theorem for a large number of prime exponents. Kummer's work has grown into a major branch of mathematics known as algebraic number theory. It is much too early to know if the gap in Miyaoka's proof will lead to any similar developments, but Fermat's Last Theorem is generally regarded as more important for the theories that have grown around it than for the result in itself.

The announcement of Miyaoka's proof was not a complete surprise. Considerable progress in number theory has made the prospect of proving Fermat's Last Theorem seem less unlikely than it had before. In particular, there are two new routes to the theorem that mathematicians believe stand the best chance yet of eventually yielding a proof. Each approach shows that Fermat's Last Theorem is a consequence of another deeper and far more important unsolved problem in number theory. In other words, while the truth of Fermat's Last Theorem is of no direct benefit, a counterexample to the theorem would entail all kinds of unpleasant mathematical consequences.

The trail taken by Miyaoka was first blazed about a year ago by A. N. Parshin in Moscow. Parshin proved that if an arithmetical analog to a certain inequality in differential geometry were true, then Fermat's Last Theorem would also be true. Parshin's result is part of a program, initiated in Russia by S. Arakelov in the 1970s, to create an arithmetical version of geometry. This theory, which bristles with the technical terminology of modern algebraic geometry (Fermat's "marvelous proof" most likely did not refer to vector bundles, schemes, or cohomology groups), essentially treats the solutions to arithmetical equations as if they were two-dimensional surfaces. The theory achieved a spectacular success in 1983, when Gerd Faltings, now at Princeton University, used the geometric theory to solve a 60-year-old problem known as Mordell's conjecture. Mordell's conjecture states that certain equations which, as surfaces, have two or more "holes," can have at most a finite number of rational solutions.

Faltings's result applies to the Fermat equation by proving that there are at most a finite number of rational solutions to the equation $x^n + y^n = 1$ when n is greater than 3. (Rational solutions to this equation correspond to integer solutions of the Fermat equation by writing $X = x/z$, $Y = y/z$ with a common denominator z.) Unfortunately, Faltings's result does not determine any explicit finite range for the rational solutions to lie in.

Parshin showed that the arithmetical version of a certain inequality involving geometric invariants of surfaces—an inequality that Miyaoka proved for the geometric case in 1974—would lead by a series of steps to a bound on the size of possible exponents for which Fermat's Last Theorem could be false. With luck, the bound would be less than 150,000, in which case the proof would be complete. Otherwise, computers might be called upon to mop up. But it is also possible that the bound itself might be unspecified, in which case the theorem would be true for all "sufficiently large" exponents but an indeterminate number of counterexamples could conceivably survive.

Miyaoka's work is directed at proving the arithmetical inequality. Miyaoka, who is an expert in algebraic geometry but a relative newcomer to the arithmetical theory, proceeded by analogy with the geometric case. But according to Enrico Bombieri, a professor of mathematics at the Institute for Advanced Studies in Princeton, the translation is not straightforward. "Things go over, but with some qualifications," Bombieri says.

"The naïve extension doesn't go through."

The problem, according to Barry Mazur of Harvard University, is the lack of a good arithmetical analog of a crucial geometric object known as the tangent bundle. Mazur, who helped Miyaoka analyze the proof, explains that Miyaoka had "a very interesting idea" to replace the tangent bundle with a "generic" bundle, with the assumption that the generic bundle can be chosen so as to have suitably nice properties. This seems not to be the case.

The effort is not wasted, however. Mazur says that Miyaoka has carried the idea of substituting generic bundles for the tangent bundle back to the original geometric case. "Given any choice of a bundle, you'll get some inequalities," Mazur says. "It's a perfectly reasonable and interesting geometric question to ask what's the structure of this whole complex set of inequalities." Answering such questions will very possibly lead to a deeper understanding of Miyaoka's original geometric proof.

The other promising new route to Fermat's Last Theorem stems from the theory of elliptic curves, which studies a class of equations falling outside of Faltings's result: interpreted as geometric surfaces, elliptic curves have only one hole, whereas Faltings's result applies to surfaces with two or more; the distinction is critical, since the equations corresponding to elliptic curves can and sometimes do have infinitely many rational solutions. In 1986, Gerhard Frey proposed that Fermat's Last Theorem could be proved as a consequence of an important open problem in the theory of elliptic curves known as the Weil-Taniyama conjecture. This conjecture asserts that each elliptic curve has an associated analytic function with very special properties. The conjecture is known to be true for many individual curves, and can be proved for any given curve. It is considered to be important because the properties of the analytic functions contain information related to the solutions of the corresponding equations.

Frey's idea was to show that a counterexample to Fermat's Last Theorem could be used to construct an elliptic curve that is a counterexample to the Weil-Taniyama conjecture. (Curiously, the same elliptic curve plays a role near the end of Parshin's argument.) The connection hinged on yet another conjecture, which Ken Ribet of the University of California at Berkeley managed to prove. The Weil-Taniyama conjecture remains open, but Fermat's Last Theorem is now known to be one of its many consequences. ■ BARRY A. CIPRA

Barry A. Cipra is a mathematician and writer based in Northfield, Minnesota.

When Good Proofs Go Bad

How can there be any doubt over the correctness or incorrectness of a mathematical proof? Why does it take experts to analyze a proof? Isn't it just a matter of checking the logic at each step?

Perhaps. But mathematicians skip over many routine and familiar steps, much the same way that a practiced musician plays chords without analyzing every finger position—they only back up when something doesn't sound right. "Routine" and "familiar" are relative terms; experts trained in one specialty are oftentimes oblivious to the terminology and techniques of another specialty, even in cases where the two specialties treat the same problems.

Moreover, even if all the steps are given and the proof is in a field familiar to everyone, logical errors can be hard to locate—even if the result is obviously false. The reader is invited to try his or her luck at finding the mistake in the following proof that all triangles are isosceles (in fact, equilateral). The proof, which has appeared in many places, is reprinted here from *An Introduction to Number Theory*, by Harold Stark. (It should not be confused in any way with Miyaoka's work on Fermat's Last Theorem, though, in spite of being a geometric proof in a book on number theory.)

"Let M be the midpoint of BC and let D be the intersection of the perpendicular bisector of BC and the angle bisector of $\angle BAC$ (see Figure 1). Let E be the point on AB such that $AB \perp DE$ and let F be the point on AC such that $AC \perp DF$. Now $BM = CM$ by construction, $\angle BMD = \angle CMD$ (= 90°) by construction and $DM = DM$. Therefore, triangles BMD and CMD are congruent (angle, side, angle theorem). Thus $BD = CD$ and $\angle MBD = \angle MCD$ (corresponding parts of congruent triangles are equal). Next, $DE = DF$ (a point on an angle bisector is equidistant from the sides) and $\angle BED = \angle CFD$ by construction. Therefore, triangles BED and CFD are congruent (two right triangles with two equal sides and equal hypotenuses are congruent—or, by the Pythagorean Theorem, the other sides are also equal and then we can use the side, angle, side, or the side, side, side theorems). Therefore, $\angle DBE = \angle DCF$ (corresponding sides of congruent triangles are equal). Thus $\angle MBE = \angle MCF$ (sums of equals are equal). This says that $\triangle ABC$ is isosceles with equal angles at B and C and thus the sides opposite these angles, AB and AC, are equal.

" . . . It is commonly stated that the error consists of the fact that D is drawn above BC, whereas D is actually below BC. Thus, the reader may enjoy proving that $AB = AC$ from Figure 2 (the letters have the same meaning as before). The proof is practically identical to the one given using Figure 1." ■ B.A.C.

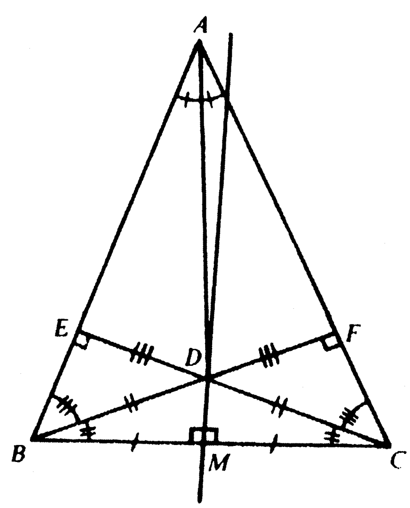

Fig. 1

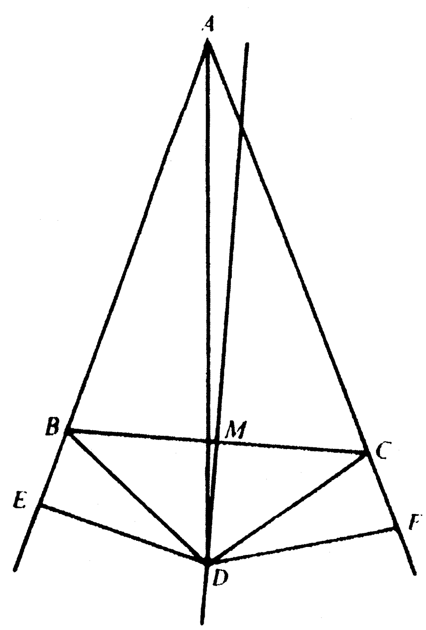

Fig. 2