Sums of Higher Powers and Fermat's Last Theorem

Sums of Higher Powers and Fermat's Last Theorem

We have discovered that the equation

$$a^2 + b^2 = c^2$$

has lots of solutions in whole numbers a, b, c. It is natural to ask whether there are solutions when the exponent 2 is replaced by a higher power. For example, do the equations

$$a^3 + b^3 = c^3 \qquad \text{and} \qquad a^4 + b^4 = c^4 \qquad \text{and} \qquad a^5 + b^5 = c^5$$

have solutions in nonzero integers a, b, c? The answer is "NO." Sometime around 1637, Pierre de Fermat showed that there is no solution for exponent 4. During the eighteenth and nineteenth centuries, Carl Friedrich Gauss and Leonhard Euler showed that there is no solution for exponent 3 and Lejeune Dirichlet and Adrien Legendre dealt with the exponent 5. The general problem of showing that the equation

$$a^n + b^n = c^n$$

has no solutions in positive integers if $n \geq 3$ is known as "Fermat's Last Theorem." It has attained almost cult status in the 350 years since Fermat scribbled the following assertion in the margin of one of his books:

> It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general any power higher than the second into powers of

> like degree. I have discovered a truly remarkable proof which this margin is too small to contain.[1]

Few mathematicians today believe that Fermat had a valid proof of his "Theorem," which is called his Last Theorem because it was the last of his assertions that remained unproved. The history of Fermat's Last Theorem is fascinating, with literally hundreds of mathematicians making important contributions. Even a brief summary could easily fill a book. We will be content with a few brief remarks.

One of the first general results on Fermat's Last Theorem, as opposed to verification for specific exponents n, was given by Sophie Germain in 1823. She proved that if both p and $2p + 1$ are primes then the equation $a^p + b^p = c^p$ has no solutions in integers a, b, c with p not dividing the product abc. A later result of a similar nature, due to A. Wieferich in 1909, is that the same conclusion is true if the quantity $2^p - 2$ is not divisible by p^2. Meanwhile, during the latter part of the nineteenth century a number of mathematicians, including Richard Dedekind, Leopold Kronecker, and especially Ernst Kummer, developed a new field of mathematics called algebraic number theory and used their theory to prove Fermat's Last Theorem for many exponents, although still only a finite list. Then, in 1985, L.M. Adleman, D.R. Heath-Brown, and E. Fouvry used a refinement of Germain's criterion together with difficult analytic estimates to prove that there are infinitely many primes p such that $a^p + b^p = c^p$ has no solutions with p not dividing abc.

> **Sophie Germain** (1776–1831) Sophie Germain was a French mathematician who did important work in number theory and differential equations. She is best known for her work on Fermat's Last Theorem, where she gave a simple criterion that suffices to show that the equation $a^p + b^p = c^p$ has no solutions with abc not divisible by p. She also did work on acoustics and elasticity, especially the theory of vibrating plates. As a mathematics student, she was forced to take correspondence courses from the École Polytechnique in Paris, since they did not accept women as students. For a similar reason, she began her extensive correspondence with Gauss using the pseudonym Monsieur Le Blanc; but when she eventually revealed her identity, Gauss was delighted and sufficiently impressed with her work to recommend her for an honorary degree at the University of Göttingen.

In 1986 Gerhard Frey suggested a new line of attack on Fermat's problem using a notion called modularity. Frey's idea was refined by Jean-Pierre Serre, and Ken

[1] Translated from the Latin: "*Cubum autem in duos cubos, aut quadrato quadratum in duos quadrato quadratos, & generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere; cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.*"

Ribet subsequently proved that if the Modularity Conjecture is true, then Fermat's Last Theorem is true. Precisely, Ribet proved that if every semistable elliptic curve[2] is modular[3] then Fermat's Last Theorem is true. The Modularity Conjecture, which asserts that every rational elliptic curve is modular, was at that time a conjecture originally formulated by Goro Shimura and Yutaka Taniyama. Finally, in 1994, Andrew Wiles announced a proof that every semistable rational elliptic curve is modular, thereby completing the proof of Fermat's 350-year-old claim. Wiles's proof, which is a tour de force using the vast machinery of modern number theory and algebraic geometry, is far too complicated for us to describe in detail.

Few mathematical or scientific discoveries arise in a vacuum. Even Sir Isaac Newton, the transcendent genius not noted for his modesty, wrote that "If I have seen further, it is by standing on the shoulders of giants." Here is a list of some of the giants, all contemporary mathematicians, whose work either directly or indirectly contributed to Wiles's brilliant proof. The diversified nationalities highlight the international character of modern mathematics. In alphabetical order: Spencer Bloch (USA), Henri Carayol (France), John Coates (Australia), Pierre Deligne (Belgium), Ehud de Shalit (Israel), Fred Diamond (USA), Gerd Faltings (Germany), Matthias Flach (Germany), Gerhard Frey (Germany), Alexander Grothendieck (France), Yves Hellegouarch (France), Haruzo Hida (Japan), Kenkichi Iwasawa (Japan), Kazuya Kato (Japan), Nick Katz (USA), V.A. Kolyvagin (Russia), Ernst Kunz (Germany), Robert Langlands (Canada), Hendrik Lenstra (The Netherlands), Wen-Ch'ing Winnie Li (USA), Barry Mazur (USA), André Néron (France), Ravi Ramakrishna (USA), Michel Raynaud (France), Ken Ribet (USA), Karl Rubin (USA), Jean-Pierre Serre (France), Goro Shimura (Japan), Yutaka Taniyama (Japan), John Tate (USA), Richard Taylor (England), Jacques Tilouine (France), Jerry Tunnell (USA), André Weil (France), Andrew Wiles (England).

Exercises

1. Write a one- to two-page biography on one (or more) of the following mathematicians. Be sure to describe their mathematical achievements, especially in number theory, and some details of their lives. Also include a paragraph putting them into an historical context

[2] An elliptic curve is a certain sort of curve, not an ellipse, given by an equation of the form $y^2 = x^3 + ax^2 + bx + c$, where a, b, c are integers. The elliptic curve is semistable if the quantities $3b - a^2$ and $27c - 9ab + 2a^3$ have no common factors other than 2 and satisfy a few other technical conditions.

[3] An elliptic curve is called modular if there is a map to it from another special sort of curve called a modular curve.

by describing the times (scientifically, politically, socially, etc.) during which they lived and worked: (a) Niels Abel, (b) Claude Gaspar Bachet de Meziriac, (c) Richard Dedekind, (d) Diophantus of Alexandria, (e) Lejeune Dirichlet, (f) Eratosthenes, (g) Euclid of Alexandria, (h) Leonhard Euler, (i) Pierre de Fermat, (j) Leonardo Fibonacci, (k) Carl Friedrich Gauss, (l) Sophie Germain, (m) David Hilbert, (n) Carl Jacobi, (o) Leopold Kronecker, (p) Ernst Kummer, (q) Joseph-Louis Lagrange, (r) Adrien-Marie Legendre, (s) Joseph Liouville, (t) Marin Mersenne, (u) Hermann Minkowski, (v) Sir Isaac Newton, (w) Pythagoras, (x) Srinivasa Ramanujan, (y) Bernhard Riemann, (z) P.L. Tchebychef (also spelled Chebychev).

2. The equation $a^2 + b^2 = c^2$ has lots of solutions in positive integers, while the equation $a^3 + b^3 = c^3$ has no solutions in positive integers. This exercise asks you to look for solutions to the equation

$$a^3 + b^3 = c^2 \qquad (*)$$

in integers $c \geq b \geq a \geq 1$.

- **(a)** The equation $(*)$ has the solution $(a, b, c) = (2, 2, 4)$. Find three more solutions in positive integers. [*Hint*. Look for solutions of the form $(a, b, c) = (xz, yz, z^2)$. Not every choice of x, y, z will work, of course, so you'll need to figure out which ones do work.]
- **(b)** If (A, B, C) is a solution to $(*)$ and n is any integer, show that (n^2A, n^2B, n^3C) is also a solution to $(*)$. We will say that a solution (a, b, c) to $(*)$ is *primitive* if it does not look like (n^2A, n^2B, n^3C) for any $n \geq 2$.
- **(c)** Write down four different primitive solutions to $(*)$. [That is, redo (a) using only primitive solutions.]
- **(d)** The solution $(2, 2, 4)$ has $a = b$. Find all primitive solutions that have $a = b$.
- **(e)** Find a primitive solution to $(*)$ that has $a > 10000$.

This page intentionally left blank