Zeitschrift: Elemente der Mathematik
Band: 50 (1995)

Artikel: Reflections on Fermat's last theorem
Autor: Murty, M. Ram
DOI: https://doi.org/10.5169/seals-46338

El. Math. *50* (1995)

0013-6018/95/010003-09$1.50 + 0.20/0

Reflections on Fermat's Last Theorem

M. Ram Murty*

M. Ram Murty obtained his Ph.D. in 1980 from MIT under the direction of Harold Stark. Presently, he is Professor of Mathematics at McGill University in Montreal. His research interests are number theory and automorphic forms. He is also a Fellow of the Royal Society of Canada.

Quest and question are cognates. In our quest for truth and understanding, the method is the way of questioning. By inquiry, by asking pertinent questions, we gain some understanding. This may not be the best method, but it is the only method we have and one that has withstood the test of time. From Socrates to Einstein, the means for gaining knowledge has always been the way of inquiry.

In our daily life, we take many things for granted and never inquire into their nature or origins. You may find it odd, if I say that mathematics plays a vital role in the daily life of every individual. In fact, civilization as we know it would collapse, if it wasn't for the concepts and ideas that were discovered by mathematics and have now become part of our daily life.

Each day we count and manipulate the decimal system, glibly unaware of its origins or meaning. Yet, there was a time when the decimal system was unknown to humanity. In fact, our number system has its genesis in the discovery of the concept of zero. If we reflect for a moment, we quickly realize the concept of zero is a profound concept and that its discovery represents a major advance in human civilization.

Every mathematical discovery has two components: the set of concepts and the 'calculus' of concepts. In the above example, the numerals would be the concepts and arithmetic, the usual operations of addition, subtraction, multiplication and division would represent the 'calculus' of these concepts. I shall clarify this through further examples.

It was not long after the natural numbers came into vogue that the early Greek mathematicians began to inquire into the nature of these numbers. For instance, they found that some numbers can be factored into smaller numbers, like

$$60 = 2 \times 2 \times 3 \times 5,$$

*) This paper is based on the H.H.J. Nesbitt lecture delivered on November 20, 1992 at Carleton University, Ottawa, Canada

whereas a number like 59 could not be decomposed further. Natural numbers that could not be decomposed further, they called prime numbers. They soon discovered there were infinitely many such prime numbers and that each natural number could be factored *uniquely* into a product of prime numbers. Thus, the prime numbers are the building blocks of all natural numbers. If the concept of a number represented a major advance in civilization, then the concept of prime number was equally so, because out of this concept grew the branch of mathematics called number theory.

My purpose here is to focus on one long-standing problem, namely Fermat's Last Theorem, and discuss how through it mathematics has evolved. It is indeed a prototype of many of the unresolved questions of mathematics.

Let us however begin with a question posed in 1980 by Masser and Oesterlé. Suppose that we have three natural numbers A, B, C which are mutually coprime (that is, no two numbers have a common prime divisor). Suppose that[1])

$$A + B = C.$$

Then, the conjecture is that

$$C \leq \left(\prod_{p|ABC} p \right)^2,$$

where the product on the right hand side is over the prime numbers p dividing ABC. This is a special case of a conjecture popularly known as the ABC conjecture. It looks like an idle question, but as we shall see, its motivation lies elsewhere. To this day, the ABC conjecture is unresolved.

Let us go back many centuries to a theorem that everyone learns in grade school. This is the famous theorem of Pythagoras: in a right angled triangle with adjacent and opposite sides of length a and b and hypotenuse c, we must have $c^2 = a^2 + b^2$.

There is an elegant proof which I have not seen in the literature. Construct the appropriate squares on each of the sides as indicated in Fig. 1. Now fold the square on the hypotenuse inward and compute the area of the resulting figure in the obvious two different ways. We obtain:

$$b^2 + a^2 + \frac{ab}{2} + ab = c^2 + \frac{3\,ab}{2}$$

which gives

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

In a work written by Diophantus in the 3rd century B.C., he asks for all integer solutions of

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

---

1) The more precise formulation of this conjecture is that if $A + B = C$, then for any $\varepsilon > 0$, there is a constant $K(\varepsilon)$ such that

$$C \leq K(\varepsilon) \left(\Pi_{p|ABC}\, p \right)^{1+\varepsilon}$$

For the sake of simplicity, we have stated a weaker version of it in the above discussion.

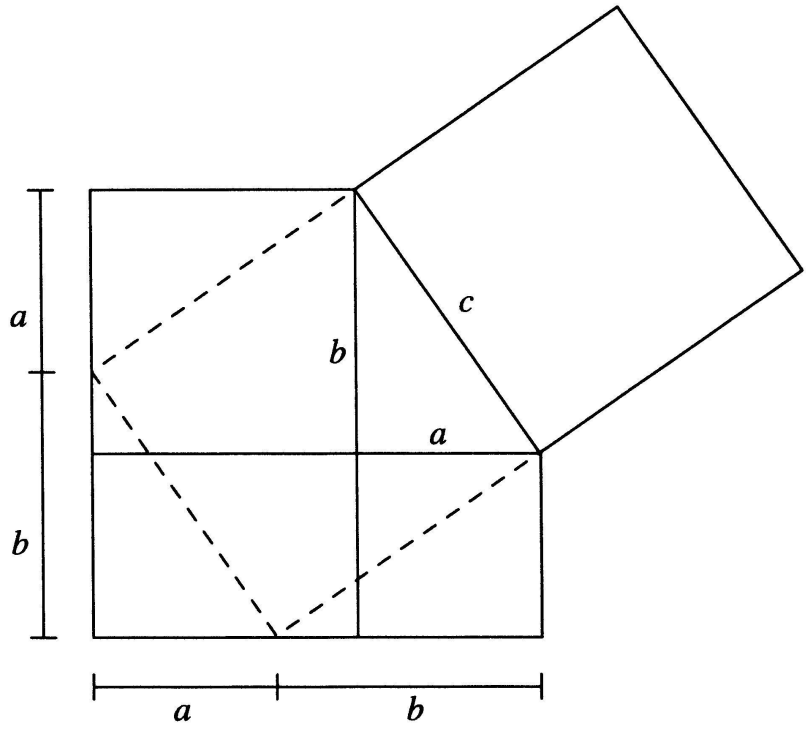

Fig. 1

For example,

$$5^2 = 3^2 + 4^2 ,$$
$$13^2 = 5^2 + 12^2 .$$

Is there a formula for giving *all* the solutions? Indeed, using the unique factorization of natural numbers as a product of prime numbers, he shows that all solutions are given by the following formulas:

$$a = 2\,mnd$$
$$b = (m^2 - n^2)\,d$$
$$c = (m^2 + n^2)\,d ,$$

where $d \in \mathbb{Z}$, m and n are arbitrary integers such that m and n are coprime with $m - n$ odd. For instance, the case $d = 1$, $m = 2$, $n = 1$ gives $(a, b, c) = (4, 3, 5)$ and $d = 1$, $m = 3$, $n = 2$ gives $(a, b, c) = (12, 5, 13)$.

In the 17th century, Pierre de Fermat obtained a copy of Bachet's translation of the work of Diophantus and read the proof giving all solutions of

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

In the margin, Fermat wrote: "On the contrary, it is impossible to separate a cube into two cubes, a fourth power into two fourth powers or generally any power above the second into two powers of the same degree. I have discovered a truly marvellous demonstration which this margin is too narrow to contain." In modern notation, Fermat states that the equation

$$c^n = a^n + b^n , \quad n \geq 3$$

in integers a, b, c implies that $abc = 0$. It is doubtful that Fermat had a proof in our sense of the term. The 17th century was a period when the concept of proof and rigor were slowly evolving in the mathematical circles. (I recall a student of mine saying to me that since Fermat was really a lawyer by profession, he must be telling the truth when he made his assertion, because lawyers are committed to telling the truth!)

The problem has had a tremendous influence on the growth of number theory and in turn, the rest of mathematics. This brings us to a second major theme in mathematics. Unsolved problems are used to focus our concentration to derive the new concepts necessary for widening our understanding of the universe. One should not become obsessed with solving an unsolved problem. Rather, that is a secondary goal, the primary one being the evolution of new concepts. Indeed, if the Fermat conjecture were disproved tomorrow, it would not upset number theory. The conjecture has contributed to the creation of many branches of number theory: a property few conjectures in mathematics share. (In fact, in June 1993, Andrew Wiles announced a proof of Fermat's last theorem. His proof, which is the culmination of the work of many mathematicians, may very well contain a new outlook on problems of this nature.)

In the 19th century, E. Kummer tried to extend the methods of Diophantus for domains other than the integers and succeeded in creating the field of algebraic number theory. He was also successful in proving the Fermat conjecture for many values of n. Through Kummer's work, ideal theory and ring theory were created, setting the stage for the creation of modern abstract algebra. This line of development appears in a book by Edwards [2] and is now classical and well-known. So I will turn to the modern lines of development.

There is a recent theorem of G. Faltings which implies that for each $n \geq 3$, the equation $c^n = a^n + b^n$ can have at most a finite number of solutions in integers. This theorem was proved using modern ideas of algebraic geometry. We refer the reader to Bloch [1] for a readable account of these developments. Still, the theorem of Faltings does not eliminate the possibility of a non-trivial solution.

If we go back to the ABC conjecture mentioned earlier, its proof would imply that there are no non-trivial solutions. Indeed, by ABC, we find

$$c^n \leq \left(\prod_{p|(abc)^n} p \right)^2 = \left(\prod_{p|abc} p \right)^2 \leq (abc)^2$$

which implies

$$c^n \leq c^6$$

or $n \leq 6$. For $n = 3, 4, 5, 6$, we know from the work of Kummer that there are no solutions. (Actually, the full ABC conjecture implies $n \leq 3$.) So the ABC conjecture implies the Fermat conjecture. Now we understand some of the motivation for the ABC conjecture.

One can take a more algebraic-geometric approach to the question. The equation $c^n = a^n + b^n$ can be rewritten

$$\left(\frac{a}{c}\right)^n + \left(\frac{b}{c}\right)^n = 1 ,$$

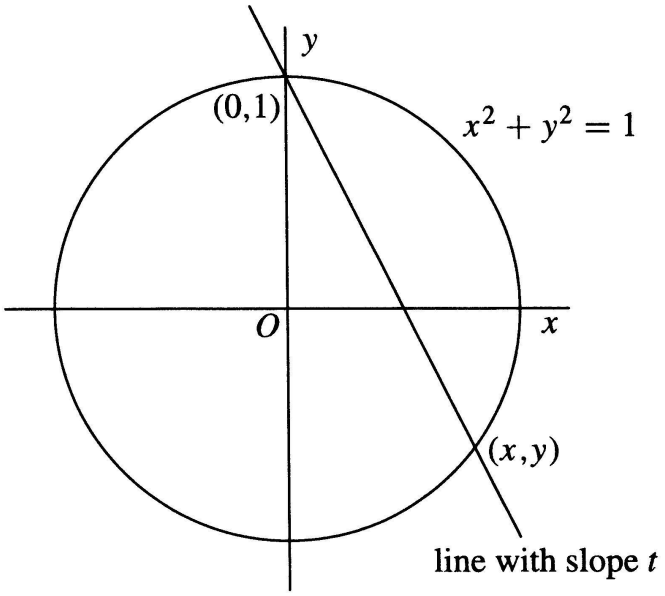

Fig. 2

and so we are seeking rational solutions of the equation

$$x^n + y^n = 1 .$$

In the case $n = 2$, we would like to determine the rational points (that is, points with rational co-ordinates) on the unit circle (see Fig. 2).

The equation of the line passing through $(0, 1)$ with slope t is

$$y = tx + 1 .$$

Where does it intersect the circle? We solve:

$$\begin{aligned} y &= tx + 1 \\ x^2 + y^2 &= 1 \end{aligned}$$

and find

$$x = -\frac{2t}{1 + t^2} ,$$

$$y = \frac{1 - t^2}{1 + t^2} .$$

If t is a rational number, then (x, y) is a rational point. Conversely, if (x, y) is a rational point, the slope of the line through $(0, 1)$ and (x, y) is rational. Thus, there is a one to one correspondence between rational points on the unit circle and lines through $(0, 1)$ with rational slope. Thus, the above formulas give all the rational points on the unit circle. Putting $t = m/n$, with m and n coprime gives the formula of Diophantus for all the Pythagorean triples.

Fermat used this result to treat the case $n = 4$ of his conjecture. The equation

$$x^4 + y^4 = z^4$$

is a special case of

$$x^4 + y^4 = z^2 ,$$

and it is the latter equation that Fermat addresses. We have $(x^2)^2 + (y^2)^2 = z^2$ and so by the formula of Diophantus,

$$\begin{aligned} x^2 &= 2\,mn \\ y^2 &= m^2 - n^2 \\ z &= m^2 + n^2 . \end{aligned}$$

Hence,

$$n^2 + y^2 = m^2$$

is again a Pythagorean triple. Again by the formula of Diophantus, we can write

$$\begin{aligned} n &= 2\,uv \\ y &= u^2 - v^2 \\ m &= u^2 + v^2 , \end{aligned}$$

so that

$$x^2 = 2\,(2\,uv)\,(u^2 + v^2) ,$$

and the unique factorization of integers implies that u, v and $(u^2 + v^2)$ are perfect squares. Thus,

$$u = \alpha^2 \ , \ v = \beta^2 \ , \ u^2 + v^2 = \gamma^2 .$$

That is,

$$\alpha^4 + \beta^4 = \gamma^2 .$$

But (α, β, γ) is a "smaller" solution than (x, y, z) that we started with in the sense that

$$\max\,(|\alpha|, |\beta|, |\gamma|) < \max\,(|x|, |y|, |z|) .$$

This means, starting from the solution (x, y, z) we obtained another one (α, β, γ) which is "smaller". This cannot go on ad infinitum. So there was no solution to begin with. This method is called the method of infinite descent.

The success in being able to parametrize all solutions for $n = 2$ leads us to ask if it can be done for other values of n. Indeed, for $n = 3$, there is a hidden structure that one can use. For higher values of n, the curve has no structure. The idea is to embed the curve into a larger structure (called the Jacobian of the curve) that has the required algebraic properties. This is the starting point of the Faltings method. Unfortunately, the theorem is ineffective. That is, we do not have any procedure for determining all the solutions (if any) for any given n, though we know there can be only finitely many.

I will conclude by discussing a new theme for attacking the Fermat conjecture that evolved only during the last decade. This involves the subject of elliptic curves. For the purpose of this talk, one can think of an elliptic curve as the locus of solutions of an equation of the form

$$E: \quad y^2 = x^3 + ax + b\,, \quad a, b \in \mathbb{Z}\,.$$

For each prime p, we count the number of solutions (mod p). For example, if E is the curve $y^2 = x^3 + x + 1$, modulo 5, we have:

x	0	1	2	3	4
$x^3 + x + 1$	1	3	1	1	4
y	± 1	no solution	± 1	± 1	± 2

so we find the number of solutions is

$$8 = 5 + 3 = 5 - (-3)\,.$$

In general, one finds a formula for the number of solutions mod p as

$$p - a_p$$

where a_p is a certain integer satisfying the inequality:

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

In the above example, $a_5 = -3$. This defines a_p for all primes p, which are coprime to $4a^3 + 27b^2 = \Delta$. (For primes p dividing $4a^3 + 27b^2$, a slight re-definition is necessary. For these primes, it transpires that $a_p = 0$ or ± 1.)

Set

$$L(s) = \prod_{p|\Delta} \left(1 - \frac{a_p}{p^s}\right)^{-1} \cdot \prod_{p\nmid\Delta} \left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1}$$

and expand the product over the primes on the right hand side to get the (Dirichlet) series

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}\,.$$

This determines the a_n's. (Note the notation is consistent.) Now put

$$f(z) = \sum_{n=1}^{\infty} a_n\, e^{2\pi i n z}$$

where $z \in \mathbb{C}$ and Im $(z) > 0$. In 1956, Y. Taniyama conjectured that there is a natural number N such that for all matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $a, b, c, d \in \mathbb{Z}, ad - bc = 1$ and $N|c$ we have

$$f\left(\frac{az + b}{cz + d}\right) = (cz + d)^2 f(z) .$$

(In technical language, the L-series of the elliptic curve E over $\mathbb{Q}$ is the Mellin transform of a cusp form of weight 2 on $\Gamma_0(N)$ for some N.) This is known as Taniyama's conjecture. In 1985, K. Ribet [3] proved that Taniyama's conjecture implies the Fermat conjecture.

In fact, in 1984, G. Frey noticed the connection in the following way: if

$$C = A + B , \quad A, B, C \in \mathbb{Z} ,$$

then consider the elliptic curve

$$y^2 = x(x + B)(x + C) .$$

This curve has an invariant called the discriminant. The discriminant is not divisible by large powers of primes (if Taniyama's conjecture is true!).

What is central to these ideas is the concept of a modular form (or more generally, an automorphic form) that was alluded to above in Taniyama's conjecture.

So is there any hope for solving the Fermat conjecture? In a sense, the question is irrelevant because that is not our goal, but rather a consequence, a by-product of an investigation. Nevertheless, it is fair to say that our understanding over the centuries has widened and we can enjoy the interplay and the varied hues of the many branches of mathematics that are coming into play to deal with this question. The latest to add to this richness are representation theory and analytic number theory.

By using the theory of automorphic forms one can establish the following: if E is an elliptic curve over $\mathbb{Q}$ and $L(s)$ is its associated L-series (defined above), then suppose that $L(s)$ extends to an entire function and satisfies a functional equation of the form

$$\left(\frac{2\pi}{\sqrt{N}}\right)^{-s} \Gamma(s)L(s) = \left(\frac{2\pi}{\sqrt{N}}\right)^{-(2-s)} \Gamma(2-s)\, L(2-s) .$$

Suppose further that for each character $\chi \pmod q$, the Dirichlet series

$$\sum_{n=1}^{\infty} \frac{a_n \chi(n)}{n^s}$$

also extends to an entire function and satisfies a similar functional equation (the equation must be modified for each $\chi \pmod q$) then the Taniyama conjecture is true!

A close look at the proof of Ribet shows that the full Taniyama conjecture is not necessary to deduce Fermat's Last Theorem. The so-called semi-stable case of the Taniyama

conjecture is sufficient. (For the "semi-expert", semi-stable means the curve has square-free conductor.) Recently, Andrew Wiles established the semi-stable case of the Taniyama conjecture. This is enough to imply Fermat's Last Theorem. The Taniyama conjecture enjoys a conceptual background which is vaster than the Fermat conjecture, and it is from this conceptual standpoint that Fermat's Last Theorem becomes significant. By the remarks above, one would think that to establish any case of the Taniyama conjecture, one has to obtain analytic continuations for an infinite family of Dirichlet series. However, in his proof, Wiles circumvents this by making use of the ingenious theory of deformations of Galois representations. In 1975, Langlands and Tunnell had established the analytic continuations of Dirichlet series attached to two dimensional solvable Galois representations and these arose from modular forms of weight one. By a remarkable lifting lemma, Wiles shows that the Langlands-Tunnell theorem already is enough to imply the semi-stable case of the Taniyama conjecture. The details of this argument occupy 200 pages. Undoubtedly, in the years to come, the proof will be checked and simplified.

Fermat's Last Theorem deserves a special place in the history of civilization. By its simplicity, it has tantalized amateurs and professionals alike and with remarkable fecundity led to the development of many areas of mathematics such as algebraic number theory, ring theory, algebraic geometry, and as indicated above, connecting elliptic curves and representation theory. It is truly fitting that the Wiles proof crowns an edifice composed of the greatest insights of modern mathematics.

Niels Bohr was fond of saying that "every great and deep difficulty bears in itself its own solution. It forces us to change our thinking in order to find it." Fermat's Last Theorem is one luminous example of this aphorism.

References

[1] S. Bloch, The proof of the Mordell conjecture, Math. Intelligencer, Vol. 6, No. 2, (1984) 41–47.

[2] H. Edwards, Fermat's Last Theorem, Springer-Verlag, New York 1977.

[3] K. Ribet, On modular representations of Gal $(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, Inventions Math., 100 (1990) 431–476.

Ram Murty
Dept of Mathematics
McGill University
Montreal H3A 2K6
Canada