An Elementary Problem Whose Solution Can Lead to Fame: Fermat's Last Theorem

H. N. Ng

University of Singapore

Positive integers, also referred to as the natural numbers, form the basis of elementary arithmatic. Some of the deepest and most difficult problems in mathematics concern them, and yet surprisingly, some of these problems are within the comprehension of those who know no more than basic arithmatic. One typical example is the well-known Fermat's (Last) Theorem:

> If $n \geqslant 3$ is a positive integer, then one cannot find positive integers x, y and z satisfying

$$x^n + y^n = z^n. \tag{1}$$

When $n = 2$, the above equation becomes

$$x^2 + y^2 = z^2. \tag{2}$$

Readers who have had basic geometry will note that (2) is "the formula" for the fundamental theorem of Pythagoras on the relationship between the three sides of a right-angled triangle. Now (2) actually has a solution in integers; for example,

$$3^2 + 4^2 = 5^2,$$

corresponding to the right-angled triangle with sides 3, 4 and 5. This shows that the requirement $n \geqslant 3$ is necessary in (1). Although (2) is a special case of (1), it is perhaps interesting to know the circumstances in which Fermat's Theorem arose from (2).

Fermat, born in 1601, was a French jurist by profession until his death in 1665. He dabbled in mathematics only as an amateur. It is all the more admirable that his achievements in pure mathematics equal those of Newton. Fermat liked to write his comments on mathematics in the margins of the books he read. On reading the problem of solving $x^2 + y^2 = z^2$ in positive integers, he wrote down his solution for it and also wrote that $x^n + y^n = z^n$ has no solutions in positive integers for $n \geqslant 3$. He further commented, "I have discovered a truly marvellous demonstration which this margin is too narrow to contain." Although he gave a proof for $n = 4$ using his now well-known method of descent, he did not leave any trace of his "marvellous demonstration" of the general theorem. For nearly 340 years, many generations of mathematicians have not been able to give a proof of Fermat's Theorem or to show that the theorem is not true. Even the most up-to-date computers of today are found to be insufficient to handle the problem. However, in the process of searching for a proof of the theorem, a tremendous amount of techniques and results were created and discovered.

One may ask why does someone not offer a prize for a proof (or disproof) of the theorem. This, in fact, has been done more than once. The French Academy of Sciences set Fermat's Theorem as its competition problem for the "Grand Prize" in 1853. In 1857 the award went to non-competitor Kummer (1810 - 1893) for his incomplete work done on Fermat's Theorem and related subjects. In his many unsuccessful attempts to solve the problem, Kummer introduced his "ideal numbers" and proved some of their fundamental properties. This marked the beginning of modern algebraic number theory, a subject which influenced the development of not only algebra but also the theory of functions. Kummer's earliest work on the theorem dates back to 1835. He continued his work on the same subject until 1874 when he was sixty-four. Although he failed to give a complete solution to Fermat's Theorem, the publication of his partial solutions established him as a great algebraist.

Another prize on Fermat's Theorem was offered as recently as 1909. A wealthy German mathematician, P. Wolfskel, offered 100,000 marks for a published proof (or disproof) of the theorem. This caused an upsurge of interest among amateurs, and thousands of erroneous self-published proofs were submitted. It is known that the great German number theorist, E. Landau (1877 - 1938) of the University of Gottingen, used to have postcards printed with the following message: "Dear Sir or Madam: Your proof of Fermat's Last Theorem has been received. The first mistake is on page...line...", and he gave the cards

to graduate students to be filled and posted. Due to inflation, the prize money amounted to less than one US cent after World War I.

There is a minor incident which is perhaps worth mentioning. The interest on the Wolfskel prize was to be used at the discretion of the Göttingen Scientific Society. Hilbert (1862-1943), who was considered the leading mathematician of his generation, was the chairman of the subcommittee in charge of the money. When asked why did he not try for the big prize himself, Hilbert answered why should he kill the goose that laid the golden egg. It is also worth noting that Fermat's Theorem was not among Hilbert's famous list of twenty-three problems which he claimed, in his address to the Second International Congress of Mathematicians in 1900, would be most earnestly attempted in the twentieth century since their solutions would contribute greatly to the advancement of mathematics.

Another mathematician who did not think that Fermat's Theorem was worth his effort was Gauss(1777-1855) [3], hailed as the Prince of mathematicians by E. T. Bell [1]. When the Paris Academy offered its prize for the 1816-1818 competition on Fermat's Theorem, a friend of Gauss asked him to try for the prize. He replied that Fermat's Theorem was an isolated proposition and as such, he had very little interest in it. Moreover, he said that it would be one of the less interesting consequences of a very deep theory on numbers that he would like to develop but could not find time to do so.

Although Fermat's Theorem has not been proved,

some partial solutions have been obtained. Dickson recorded the work of more than 250 people on the theorem in his famous book The History of the Theory of Numbers [4]. A shorter account of the problem was given in Vandiver's paper, "Fermat's Last Theorem, its History and the Nature of the Known Results Concerning it." [6]. We will only give a brief report.

We first observe that we need only show that Fermat's Theorem holds if (1) cannot have solutions in positive integers for any odd prime n. Assume that (1) is not solvable in positive integers whenever n is an odd prime. We will show that (1) is again not solvable for any integer $n \geq 3$. For suppose x_o, y_o and z_o are positive integers and n is a composite (i.e. not a prime) integer greater than 3 such that $x_o^n + y_o^n = z_o^n$. Now either n has an odd prime factor or n is a power of 2. In the first case, $n = pm$ for some odd prime p and a positive integer m. Thus $(x_o^m)^p + (y_o^m)^p = (z_o^m)^p$, contrary to the assumption that (1) has no solutions in positive integers if n is a prime. In the second case, $n = 2^k$ for some integer $k \geq 2$, and so

$(x_o^{2^{k-2}})^4 + (y_o^{2^{k-2}})^4 = (z_o^{2^{k-2}})^4$, contrary to the result of Fermat for the case when $n = 4$. Both cases are impossible and hence (1) has no solutions for any integer $n \geq 3$.

However, this seemingly weaker form of Fermat's Theorem (for n a prime) is not much easier. One of Kummer's major results proved that Fermat's Theorem holds for the class of so-called regular primes. In his theory

of "ideal numbers" - which marked the beginning of the theory of ideals - he has an ideal class number for each prime integer, and a prime p is called regular if p is not a factor of the ideal class number corresponding to p. Although he also proved Fermat's Theorem for some primes which are not regular (i.e. for some irregular primes), he could not solve the problem for all irregular primes, and to date, no one has. Unfortunately, it was subsequently proved by Jensen (1915) that there are infinitely many irregular primes. Although it is not yet known whether the number of regular primes is infinite, there is ample evidence among number theorists that three primes out of five are regular.

One way to dispose of Fermat's Theorem is, of course, to find a solution of (1) for some n by trial and error. This method is humanly impossible for $n \geqslant 5$. However, with the high-speed computers at our disposal, one would think that we now have a better chance for success. The fact just does not turn out that way. In 1967, some mathematicians used computers to prove Fermat's Theorem for all primes less than 25000. It is perhaps interesting to note that in 1955, when computers were not as sophisticated and as fast as those of today, the use of computers could only prove Fermat's Theorem for primes less than 4002.

Fermat's Theorem has attracted many mathematicians for the past 340 years. It is not an exaggeration to say that every well-known mathematician, not only number theorists, has given some thoughts to the

theorem, even though he may admit that its solution will not affect the development of mathematics as a whole. Typical examples were Gauss and Hilbert. The former proved the theorem for $n = 5$ and the latter simplified Kummer's proof for regular primes.

The attempts to prove Fermat's Theorem have connected it with many deep concepts and techniques, some of which were invented with the intention of solving the theorem. In [6], Vandiver quoted at least twenty-five different topics which he found to be related to the theorem. For such a special and isolated problem to have this amount of inspiring effect upon mathematics is certainly very surprising though this is not uncommon in the development of science.

Today most mathematicians believe that the proof by Fermat was probably wrong. In the 1972 Ritt Lecture Series delivered at Columbia University, Professor André Weil of the Institute of Advanced Study at Princeton, one of the world's leading mathematicians, gave a very interesting justification of this belief based on his mathematical knowledge. Perhaps Fermat would be amazed, if he were alive today, to find out how much his Last Theorem has generated mathematical research and influenced the development of modern mathematics.

References

[1] E. T. Bell, Men of Mathematics, Simon and Schuster, 3rd. Printing, New York, 1965.

[2] _____, The Last Problem, Victor Gollancz Ltd., London, 1962.

[3] C. T. Chong, Notes on Mathematicians: 1. Carl Friedlich Gauss, This Medley, vol. 3, No. 1 (1975), 6 - 10.

[4] L. E. Dickson, History of the Theory of Numbers, vol. III, G. E. Stechert & Co., New York, 1934.

[5] C. Reid, Hilbert, Springer Verlag, Berlin, 1970.

[6] H. Vandiver, Fermat's Last Theorem: Its History and the Results Concerning It, Amer. Math. Monthly, vol. 53 (1946), 555 - 578; Supplement in the same journal, vol 60 (1953), 164 - 167.

1975 Inter-school Mathematical Competition[+]

The 1975 Inter-school Mathematical Competition problems are reproduced below. In Paper 1, an asterisk is marked after each correct answer. In Paper 2, solutions of some of the problems or parts thereof are given.

Paper 1

Monday, June 2, 1975 Time 9.00 a.m. - 11.00 a.m.

1. The number $\sqrt{2}$ is

(a) a rational fraction; (b) a finite decimal; (c) 1.41421; (d) an infinite repeating decimal; (e)* an infinite non-repeating decimal.

2. If n is a positive integer greater than or equal to 2,

[+]The Society wishes to thank all those who in one way or another helped to make this competition a success, paticularly the members of its 1975 Competition Subcommittee, comprising Dr. Louis H. Y. Chen (University of Singapore), Mr. Chong Tien Hoo (Institute of Education), Dr. Lee Peng Yee (Nanyang University), Dr. Ng How Ngee (University of Singapore), Dr. Shee Sze Chin (Nanyang University) and Mr. Yeo Kok Keong (Ministry of Education).