INTRODUCTION

Pierre de Fermat (1601 - 1665) was born at Beaumont-de-Lomagne in France and was the son of a leather merchant, Dominique Fermat, the second consul of Beaumont. His early education was at home, and later he went to Toulouse to study for his eventual career in the magistry.

This information would be of no interest to us today except for the fact that when he died, Fermat was one of the most famous mathematicians in Europe. His outstanding contributions were in many fields of mathematics, including optics, the theory of tangents, quadrature, maxima and minima, the beginnings of analytic geometry, and, most importantly as far as the famous theorem that bears his name is concerned, number theory.

Fermat believed that the theory of numbers had been neglected. He complained that hardly anyone understood arithmetical questions and believed that number theory had been too closely allied to geometry (see [4], page 274). In making good these deficiencies, Fermat showed his brilliance and became the greatest number theorist since Diophantus.

The object of this essay is to trace the history of one of his conjectures, the now famous "Fermats Last Theorem". This 'theorem' has had a long and chequered career, with many people either claiming to have a proof, or working towards a proof, as the following pages will show.

In 1670, five years after the death of Pierre de Fermat, a new edition of C. G. Bachet's (1581 - 1638) edition of Diophantus' Arithmetica was published. This book was the first step taken by Fermat's son Samuel in having his famous father's mathematical discoveries, commentaries and correspondences put in publishable form. Samuel, along with many mathematicians of his time, recognized the greatness of Fermats work, and no doubt feared that he would be forgotten and much valuable information lost unless the work was published posthumously.

The reason for publishing the new edition of Diophantus was that it included Fermat's marginal notes as an appendix. The second of the 48 "Observations on Diophantus" was written in the margin next to problem 8 in Book II, which was "to divide a given square number into two squares," to which Fermat added the comment; "In contrast, it is impossible to divide a cube into two cubes, or a fourth power into two fourth powers, or in general any power beyond the square into powers of the same degree; of this I have discovered a very wonderful demonstration (demonstrationen mirabilem sane detexi). This margin is too narrow to contain it." (see [8], page 27) This statement, originally written nearly thirty years before Fermat's death is now known as FERMAT'S LAST THEOREM.

Its fame is probably due to the fact that it is one of the very few unsolved problems in mathematics that can be understood by anyone with an elementary knowledge of mathematics. Additionally, although it is generally accepted that the Last Theorem is of "but slight interest today, its importance in the development of arithmetic and modern algebra has been very great". (see [2] p.157).

.../2.

The reason for the name Fermat's Last Theorem (hereafter, abreviated to FLT) is unclear. One possible explanation is that of the many unproved theorems that Fermat stated, this is the last one that remains unproved (see [3], p.2) It should also be noted that Fermat may not have been the first person to consider the proposition. As early as 970, the work of Abu Dschafar Muhamed Ibn Allusain implies that the Arab mathematician Alhogendi tried unsuccessfully to prove the case for $n = 3$. (see [9], page 278). Thus it is probable that other mathematicians prior to Fermat had reached his conclusion, but his name is associated with it because he claimed to have a proof.

It is, of course, assumed that Fermat meant, in stating his theorem, that there are no rational numbers x, y, z such that $x^n + y^n = z^n (n > 2)$. This follows because Diophantus dealt exclusively with rational numbers, and if irrationals were permitted the simple solution of $z = \sqrt[n]{x^n + y^n}$ would follow. Further, we can restrict the discussion to whole number or integer solutions, since if d is the lowest common denominator of x, y and z then we would have

$$\begin{aligned}(xd)^n + (yd)^n &= (x^n + y^n)d^n \\ &= (zd)^n\end{aligned}$$

Additionally, we can also assume that we are dealing with positive numbers, as Diophantus and Fermat both dealt with positive numbers, and negative numbers and zero were still viewed with suspicion even in Fermat's time.

Hence, we can state FLT as claiming that if n is an integer greater than 2, then it is impossible to find positive whole numbers x, y and z such that $x^n + y^n = z^n$.

Although Fermat did not give the general solution of his

.../3.

theorem, he did prove the case of $n = 4$ and this was included by Samuel in the posthumously published works as part of Observation 45 on Diophantus.

The following is a proof of the case $n = 4$. Although not the same as that of Fermat, it does use the method of infinite descent, an invention of Fermat. Briefly stated this method says, "Suppose that the assumption that a given positive integer has a set of properties implies that there is a smaller positive integer with the same set of properties. Then no positive integer can have this set of properties". (see [3], p.9).

Assume $x^4 + y^4 = z^4$, where no two of x, y and z have a common divisor greater than 1.

Hence, x^2, y^2 and z^2 form a primitive Pythagorean triple and we can write

$$x^2 = 2pq$$
$$y^2 = p^2 - q^2$$
$$z^2 = p^2 + q^2$$

where p and q are relatively prime, of opposite parity and $p > q > o$.

The second equation can be written as

$y^2 + q^2 = p^2$, making y, q and p a primitive Pythagorean triple. So p is odd and q must be even. (p q of opposite parities)

Hence,

$$q = 2ab$$
$$y = a^2 - b^2$$
$$p = a^2 + b^2$$

where a and b are relatively prime, of opposite parity and $a > b > o$.

Thus, $x^2 = 2pq = 4ab(a^2 + b^2)$

Hence, $ab(a^2 + b^2)$ is a square. ie the square of half the even number x.

.../4.

any prime that divided ab would have to divide a or b, but not both & could thus not divide a^2+b^2

Now, ab and $(a^2 + b^2)$ must be relatively prime, therefore they must both be squares.

If ab is a square, then both a and b must be squares, so we can put $a = X^2$ and $b = Y^2$.

Therefore, $X^4 + Y^4 = a^2 + b^2$ is a square. Noting that in our first steps the only assumption that we made about z^4 was that it was a square, the above fact suffices for us to apply the method of infinite descent.

In other words, starting with x and y such that $x^4 + y^4$ is a square, we have found a new pair of positive integers X and Y such that $X^4 + Y^4$ is a square, coupled with the fact that

$X^4 + Y^4 = a^2 + b^2 = p < p^2 + q^2 = z^2 < z^4 = x^4 + y^4$

So we have an infinite descending sequence of positive integers, which is impossible. Hence our assumption is false and FLT holds for $n = 4$.

From this proof it follows that FLT is true for all exponents n that are divisible by 4. Further, we can show that once FLT has been proved in the case $n = 4$ the proof of the general case reduces to the proof of the case in which $n > 2$ is prime.

Although the case $n = 3$ was not proved completely for nearly one hundred years, in his correspondence to Carcavi, Fermat counted the impossibility of solving $x^3 + y^3 = z^3$ among the theorems proved by infinite descent. It has been suggested (see [5], p.345) that he may have believed that this method of infinite descent would work for all cases. However, just as his prime number conjecture (numbers of the form $2^{2^n} + 1$) breaks down for $n = 5$, so too the proof by infinite descent of FLT makes a significant jump in difficulty for

.../5.

$n \geqslant 5$ and fails altogether for $n \geqslant 23$.

The greatest mathematician of the eighteenth century, Leonhard Euler (1707 - 1783) provided the next step in the history of FLT. It is generally understood that Euler provided an incomplete proof for the case $n = 3$ which was subsequently completed by others (see [6], p.510). Admittedly, his proof which appeared in his Algebra (1770), contained a basic fallacy which he apparently did not recognize. However, his elegant proof can be corrected by bringing in arguments which Euler used to prove other propositions of Fermat (see [3], p.40). Additionally, it should be noted that Euler used Fermat's method of infinite descent in his "proof", which was first mentioned in a letter to Goldbach in 1753.

Although progress in number theory was enormous during the next ninety or so years (due in large measure to Lagrange, Gauss and, Legendre), there was not much progress towards a general proof of FLT.

However, this does not mean that there was no interest in FLT. In 1816 the Paris Academy proposed that the proof (or disproof) of FLT was its prize problem for the period 1816-18.

One person who did play a part in the development of the theorem at this time was Sophie Germain (1776 - 1831). She is one of the very few women who have been able to 'make their presence felt' in the world of higher mathematics. Part of her strategy in overcoming the prejudice against women was to correspond with Gauss under the masculine pseudonym of Mr. Leblanc. Fortunately, Gauss' reaction

.../6.

upon discovering of her true identity was one of delight and admiration, and the good relations that she developed with both Gauss and Legendre meant that her discoveries did not go unnoticed or unrecognized.

Her work on FLT led her to split the problem into two parts, which are now known as Case I and Case II of the theorem. Case I is that in which none of the three numbers x, y, z is divisible by n and Case II is that in which one and only one of the three numbers is divisible by n (note that we cannot have two of the numbers divisible by n because then the third number becomes divisible by n).

Sophie Germain's Theorem states (see [3], page 64);
Let n be an odd prime. If there is an auxiliary prime p with the properties that

(1) $x^n + y^n + z^n \equiv 0 \bmod p$ implies $x \equiv 0$ or $y \equiv 0$ or $z \equiv 0 \bmod p$,
and

(2) $x^n \equiv n \bmod p$ is impossible,

then Case I of FLT is true for n.

Case I of FLT was then shown to be true for all primes less than 100 by Sophie Germain, and Legendre extended this result to all odd primes less than 197 as well as others. Thus it became clear that the more difficult part seemed to be Case II as the above was found before FLT was proved for the case n = 5.

In 1825, the case n = 5 was solved by the combined powers of the German mathematician Dirichlet and Legendre. Of interest in this sharing of credit is the fact that Dirichlet was only 20 at the time, while Legendre was past 70, providing a contradiction to the usual contention that mathematics is the domain of younger men.

.../7.

The next cases to follow were n = 14, proved by Dirichlet in 1832, and the difficult case of n = 7, proved by Lamé in 1839. Up until this time, it had been the hope that by finding proof for specific cases, the general case would eventually emerge. Unfortunately, the kinds of arguments that had to be used began to get so involved, and seemed so tied to each specific case, especially with n = 7, that the problem looked worse, rather than better. Thus it was going to take a revolutionary change in the method of attack of the problem to make any significant progress.

This revolutionary change came in the monumental year of 1847, which revealed the brilliance of Ernst Eduard Kummer (1810-1893). Early in the year, FLT had come under considerable discussion in the Paris Academy, with Cauchy and Lamé in particular believing that they were close to proving it. They hoped to be able to decompose $x^n + y^n$ completely into n linear factors using complex numbers and then apply the method of infinite descent. Their enthusiasm was not shared by all the members of the Academy and Liouville, in particular cast doubts on the proposed proof.

The major weakness of the 'proof' was that it presumed unique factorization of certain types of complex numbers. The fact that this presumption was invalid was pointed out by Liouville to the Academy when he read a letter from Kummer, which included material written 3 years earlier, proving that unique factorization fails in the complex case. In his earlier considerations, Kummer had been looking at algebraic numbers, which are formed by the roots of an equation with rational coefficients. Primes in algebraic numbers are defined as in common arithmetic, but the'self-evident' theorem that every integer in every algebraic number field can be built up in essentially one way only by

.../8.

multiplying primes is false. This seemed to be a rather chaotic situation, and it needed a mathematician of the first rank to restore order (see [6], page 512).

This restoration of order was provided by the brilliance of Kummer, who restored unique factorisation by the introduction of a new species of what he called "ideal numbers". This creation led to Kummer's monumental proof of FLT for a large class of prime number exponents which are now known as regular primes. Specifically, Kummer's theorem states: Let p be an odd prime. A sufficient condition for Fermat's Last Theorem to be true for the exponent p is that p not divide the numerators of the Bernoulli numbers B2, B4, ..., Bp-3 (see [3], page V). Possibly moved by the great progress that was made with FLT by Kummer, the Paris Academy in 1849 endowed a gold medal valued at 3000 francs for a complete solution. No paper met the conditions, even on extension of the terminal date, and so the medal was presented to Kummer (see [9], page 278).

The regular primes, p that Kummer's proof deals with may be characterised by the condition that p does not divide the Bernoulli number, B2k, for 2k = 2,4,.... , p-3.

The Bernoulli numbers are defined by the power series expansion

$$\frac{x}{e^x - 1} = \sum_{n=o}^{\infty} Bn \frac{x^n}{n!}$$

The importance of Kummers proof is that it applies to <u>all</u> regular primes, and thus this large class of primes does not have to be considered in any attempt at a general proof.

.../9.

It seems that over 60% of all primes are regular

Unfortunately, it has not yet been established how many regular primes there are, although it is suspected that there are infinitely many of them. However, it has been proved that there are infinitely many irregular primes.

By being able to ignore the regular primes (because of Kummer's result) and concentrate on the irregular primes, it has recently been established (Wagstaff, 1976) that FLT holds for every prime exponent less than 125 000 (see [7], page 230).

Although Kummer's contribution to FLT has probably been the most significant step made towards its proof, this does not mean that there has not been much interest in the theorem since his time. So great has been the interest, that in 1908, Dr. Paul Wolfskehl of Darnstadt offered a prize of 1 000 000 marks for a proof, which must be published and accepted by the Academy of Sciences in Gottingen (see [8], page 278). Naturally, a flood of amateur solutions was submitted until post-world war I inflation devalued the prize. However, the economic recovery of Germany has meant that the prize has now risen back up to the equivalent of about 4 000 American dollars.

Notwithstanding the fact that no general solution to FLT has been found, many interesting results concerning the theorem have been found since the time of Kummer. One rather fascinating result was proved in 1933 by H. Kapferrer, to the effect that the existence of a solution of the equation $z^3 - y^2 = 3^3.2^{2n-2}.x^{2n}$ in rational integers x, y, z, any two of which have no common factor > 1, is equivalent to the existence of a solution of Fermat's equation

.../10.

$u^n - v^n = w^n$ (see [6], page 510).

The first case of FLT has been extended far beyond the proof for primes less than 125 000 by Brillhart, Tonascia and Weinberger (1971) who have extended this case to include every prime exponent less than 3×10^9. Their result was an extension of work carried out earlier in this century by Wieferich (1909), Mirimanoff (1910) and Frobenius and Vandiver (1914).

However, primes larger than 3×10^9 have been found to satisfy FLT. In fact, the first case has been found to hold for the largest prime known today, this being the Mersenne number $M_q = 2^q - 1$, where $q = 19937$. Following the discovery of its primality, the proof that the first case holds for it followed from the earlier work of Wieferich, mentioned above (see [7], page 234).

Naturally, throughout the centuries since Fermat proposed his famous 'theorem', many people have searched for a counter-example that would prove the theorem wrong. No one has yet come up with one, and some very interesting work has been done to establish how large the numbers in such a counter-example would need to be. For example, in 1856, Grünert showed that if $x^n + y^n = z^n$, where $0 < x < y < z$, then $x > n$. This very effectively shows that it is no use to try to find a counter example with small numbers, for if $n = 101$, the numbers in the counter example would be at least 102^{101}.

Although such a number is large, it is small in comparison with recently found lower bounds for a counter example. In 1953, Inkeri proved that if the first case fails for the exponent p, where x, y, z

.../11.

are integers, $0 < x < y < z$, p does not divide xyz, and $x^p + y^p = z^p$,

then

$$x > \left(\frac{2p^3 + p}{\log(3p)}\right)^p$$

and, for the general case,

$$x > \tfrac{1}{2} p^{3p-4} \qquad \text{(see [7], page 235)}$$

Using the figure of 125000 from Wagstaff's result, we can substitute this for p in the formula for the general case, and we get that x must be greater than a number with 3 billion digits. If this is not already large enough, when we substitute the figure 3×10^9 from Brillhart, Tonasci and Weinberger's results in the formula for the first case, we obtain

$$x > \left(\frac{2 \times 3^3 \times 10^{27} + 3 \times 10^9}{\log\ (9 \times 10^9)}\right)^{3 \times 10^9}$$

and this number has more than 80 billion digits!

Thus it is not surprising that serious mathematicians are concentrating on proving the theorem, not disproving it!

In conclusion, we can see that three centuries of mathematical endeavour has failed to prove FLT. However, the search has by no means been in vain, for it has been instrumental in the development of number theory and has led to many other discoveries in this field. Additionally, although many would conclude that Fermat did not actually have a solution, his use of the phrase "a very wonderful demonstration" leaves a nagging doubt that perhaps there may be a straightforward, elegant proof that will one day be rediscovered.

REFERENCES

[1] E.T. Bell 'Men of Mathematics" Simon and Shuster N.Y. 1937

[2] E.T. Bell "The Development of Mathematics" McGraw-Hill N.Y. 1945

[3] H.M. Edwards "Fermat's Last Theorem - A Genetic Introduction to Algebraic Number Theory" Springer-Verlag 1977

[4] M. Kline 'Mathematical Thought from Ancient to Modern Times" Oxford University Press N.Y. 1972

[5] M.S. Mahoney "The Mathematical Career of Pierre de Fermat 1601 - 1665" Princeton University Press 1973

[6] J. Newman "The World of Mathematics, Volume I" Allen and Unwin 1956

[7] P. Ribenboim "Recent Results on Fermat's Last Theorem" Canadian Mathematical Bulletin Vol. 20 No. 2 June 1977.

[8] P.J. Struik "A Source Book in Mathematics, 1200 - 1800" Harvard University Press

[9] H. Tietze "Famous Problems of Mathematics" Graylock 1965