A SIMPLE PROOF OF FERMAT'S LAST THEOREM
BY
J. C. EDWARDS

Abstract. The proof of Fermat's Last Theorem offered here is relatively simple and well within Fermat's own expertise. Therefore, it can be used to justify Fermat's claim that he was able to prove the theorem himself. The proof recently published by Professor Andrew Wiles takes two hundred pages and the mathematics is so advanced that it could not possibly have been Fermat's own proof.

Around the year 1637 Pierre de Fermat wrote in his copy of the **Arithmetica of Diophantus:**

> "It is impossible to separate a cube into two cubes or a biquadrate into two biquadrates, 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."

Although a detailed history of subsequent attempts to prove the theorem is beyond the scope of this investigation, it may be added that for over three hundred and fifty years mathematicians have failed to prove or disprove this theorem The theorem may be expressed as an equation, and the usual version of this is:

> The equation $x^n + y^n = z^n$, where n is a natural number larger than 2, has no solution in integers all different from 0.

The theorem of Pythagoras determines a one-to-one relationship between the sides of a right triangle and the squares on its three sides, in which the sum of the squares on the two lesser sides is equal to the square on the third side, namely

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

where a, b, c are the sides of the right triangle. For this reason the theorem can be expressed in terms of the right triangle

> If A, B, C are the sides of a right triangle, and $A = a^n$, $b + b^n$, $C = c^n$. then a, b and c cannot be all integers, if n is an integer greater than 1.

This variation of the theorem has the great advantage that we have a formula, which will generate all the three sides of a right triangle in integers.

A fourth variation is even more specific and has the advantage of being easier to prove:

> There are no solutions in integers to the equation $a^n + b^n = c^n$ except when a, b, c are a Pythagorean triple and n is equal to 2.

The Four Theorems on which this Proof of Fermat's Last Theorem is Based

1. Pythagoras' Theorem: The square on the hypotenuse is equal to the squares on the other two sides.

2. The Irrational Number Theorem: When a is not the perfect nth power of some rational number, the equation $x^n = a$ has no rational solutions.

3. The Formula for creating integer right triangles

If p, q are integers, $p > q > 0$, $\gcd(p,q) = 1$, p, q not of the same parity, let

$$a = p^2 - q^2$$

$$b = 2pq$$

$$c = p^2 + q^2.$$

Then (a, b, c) is a primitive triple. And conversely, every primitive triple may so be obtained.

4. De Moivre's Theorem:

$$e^{in\theta} = \cos n\theta + i\sin n\theta = (\cos\theta + i\sin\theta)^n.$$

Table I

Pythagorean triples a, b, c generated from sets (p,q)

p q	c	b	a	p q	c	b	a	p q	c	b	a
2 1	5	4	3	5 4	42	40	45	7 6	85	84	13
3 2	13	12	5	6 1	37	12	35	8 1	65	16	63
4 1	17	8	15	6 5	61	60	11	8 3	73	48	53
4 3	25	24	7	7 2	53	28	45	8 5	89	80	39
5 2	29	20	21	7 4	85	84	13	8 7	113	112	15

It is to be noted that because the product of an irrational number and an integer is itself irrational, therefore what is proved in number theory for primitive triangles is also true for non-primitive or secondary triangles. If a, b, c are triples, then a^n, b^n, c^n are members of a triple as well and for the same side of the triangle. However, as their values are not generated for the same sets (P,Q) they do not appear in the same equation. Here the sets (p,q) generate the basic triple i.e. (a, b, c) and the sets (P,Q) generate $A = a^n$, $B = b^n$, $C = c^n$.

The Formula for Generating the Pairs (P,Q) from (p,q).

$A = (p + q)^n(p - q)^n$, and let $r = (p + q)$, $s = (p - q)$.

$$P = \tfrac{1}{2}(r^n + s^n),\quad Q = \tfrac{1}{2}(r^n - s^n)$$

$B = 2.2^{n-1}.p^n q^n$ for specific values of p and q. 2n-1 can be a factor of either p^n or q^n depending on which of them is the even number.

$C = (p + iq)^n(p - iq)^n = (P + iQ)(P - iQ) = P^2 + Q^2$, where i equals the square root of minus 1.

The Proof of FLT by the Method of Exclusion

This method entails defining a domain of numbers, within which all possible solutions to the equation,

$$x^n + y^n = z^n$$

must be found. Let X, Y, Z be sets of all possible finite integers, then x^n, y^n, z^n, where n = 0 to infinity, must be sub-sets. A three row matrix can then be created, in which there are three columns and in which there is every possible combination of x, y, z. Every possible solution to the equation must then be represented within this matrix. The domain can then be reduced in size by extracting stage by stage all those sub-sets of numbers, which conform to the theorem, until the only possible solutions in integers to the equation are to be found.

Stage I

The first restriction of the domain is introduced by inserting an addition sign between the X and Y sets of the row of triples, which divides the domain into two separate regions:

$$\text{(i)} \quad X + Y \neq Z$$

and $$\text{(ii)} \quad X + Y = Z.$$

Stage II

The first of these two sub-sets, (i), may be dismissed at once, because of the inequality between the LHS and RHS. Sub-set (ii) corresponds to the equation

$$A + B = C,$$

where $A = a^2$, $B = b^2$, $C = c^2$ and a, b, c form a Pythagorean triple. However, more generally let

$$A = a^n; \; B = b^n; \; C = c^n$$

which is the equation of Fermat's theorem.

Note that although x, y, z are considered to be real numbers, a, b, c. represent the absolute values of the complex equation, $a - ib = c$.

Stage III

This sub-set can again be divided into two more parts by the use of the converse of Pythagoras' theorem. If in the right triangle the sum of the squares on two sides of the triangle is equal to the square on the third then it is true that in the equation $A + B = C$ the square roots of A, B, C form a right triangle, which are the square roots of a^n, b^n, c^n.

Stage IV

This is an important stage in the proof and proves the theorem for all the odd values of n. If n is odd and either $a^{n/2}$ or the others is not a square, then it is an irrational square root. This also applies to a, b, c themselves, because n/2 must also be an integer, and the integer root of an irrational number is itself irrational, but if n is even, then $a^{n/2}$, $b^{n/2}$, $c^{n/2}$ are integers, and not only are they integers, but also they are members of a Pyhtagorean triple. It has already been proved previously elsewhere that if n is even, it cannot be greater than 2. Hence, we are left only with $a^{n/2}$, $b^{n/2}$, $c^{n/2}$ as a Pythagorean triple and n equal to 2.

Stage V

This last stage in the proof is only a matter of comparing $a^n + b^n$ against c^n. When n is equal to 0, $a^n + b^n$ equals 2 on the left-hand side and c^n is equal to 1 on the right-hand side. When $n = 1$, c^n as the hypotenuse is still less than the sum of the other two sides in the right triangle, which is thus formed. When $n = 2$, the LHS = the RHS. After that the RHS is always greater than the LHS. This applies to all such triples, because of the differential growth of their exponentials. If the two sides of the equations are plotted together on the same graph their curves will always intersect when $n = 2$.

Table II

	p	q	n=0	n = 1	n = 2	n = 3
$a^n + b^n$	2	1	2	7	25	91
c^n			1	5	25	125
$a^n + b^n$	3	2	2	17	169	1853
c^n			1	13	169	2197
$a^n + b^n$	5	4	2	49	1681	54728
c^n			1	41	1681	68921
$a^n + b^n$	6	1	2	47	1369	44603
c^n			1	37	1369	50653

The Reasons for Previous Failure to Solve the Problem

Now that the proof has been completed it is not difficult to analyse the cause of previous failure. This was due to the omission of the fourth stage of the proof. The three numbers, x, y, z were considered to be ordinary real numbers taken from the complete set of all possible finite integers. The converse of Pythagoras' theorem that in the equation A + B = C the square roots of these lengths formed a right triangle passed unnoticed. It was not appreciated that out of the set, x, y, z only a, b, c, the Pythagorean triples could solve the equation. In fact, as triples the set does not consist of real numbers only; A is real, B is imaginary and C, the hypotenuse, is a complex number. For the same reason it was not realized that in the equation, $a^n + b^n = c^n$, when n is odd, a, b, c must be irrational unless a^n, b^n, c^n are squares respectively.

Although it was easier to prove the theorem for even numbers of n, it should have been first proved for the odd numbers. Much effort was expended in attempting to prove the theorem for specific values of n as an odd number, but all this was irrelevant, because the proof is complete once n exceeds the number 2.

J.C.Edwards
49 Marsh Crescent
Regina, Saskatchewan S4S 5R3
Canada

Submitted - September 15, 1996