An Elementary Proof Of Fermat's Last Theorem

Bezaliel Anotida Joshua

July 22, 2015

ABSTRACT. In 1995, Princeton professor, Sir Andrew John Wiles, quenched the quest for a proof of Fermat's Last Theorem as he accomplished the task in his 109-page tome *Modular Elliptic Curves and Fermat's Last Theorem*, [1]. However, Fermat's claimed proof, which the margin of the *Arithmetica* was allegedly too narrow to contain, has remained unknown. In this note, we provide an elementary proof of Fermat's Last Theorem via its equivalent reformulation, namely: if $a^p + b^p + c^p = 0$, where a, b, c are integers and $p \geq 3$ is an odd prime, then $abc = 0$. We approach the problem by considering the product $(a+b)(b+c)(a+c)$, and show that if (a, b, c) is a primitive triple and $\mid (b+c)(a+c)(a+b) \mid \geq 2(a+b)$, then $a^p + b^p + c^p$ cannot be equal to zero.

Introduction. Pierre de Fermat (1601-1665) was a judge, living in the French city of Toulose. Although mathematics was not his profession, and although he published virtually nothing during his life, he made fundamental contributions in areas such as calculus, probability theory and number theory, and is generally regarded as one the greatest of all mathematicians. Fermat preferred to communicate his discoveries in letters to friends (usually with no more than the terse statement that he possessed a proof) or to keep them to himself in notes. A number of such notes were jotted down in the margin of his copy of Bachet's translation of Diophantus' *Arithmetica*. By far the most famous of these marginal notes is the one - presumably written around 1637-which states:

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratos, et generaliter nullam in infinitum ultra quadratum potestatum in duos ejusdem nominis fas est dividere: cujes rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

In this tantalising aside, Fermat was simply saying that (English translation) if $n > 2$, then the Diophantine equation

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

has no solution in the integers, other than the trivial solutions in which at least one of the variables is zero. The equation just cited has come to be known as Fermat's Last Theorem, or more accurately, Fermat's conjecture. By the 1800s, all assertions appearing in the margin of his *Arithmetica* had been proved or refuted - with the one exception of the Last Theorem (hence its name). If Fermat really did have a proof, it has never come to light. Fermat did, however, leave a proof for his Last Theorem for the case $n = 4$. The technique used in the proof is a form of induction sometimes called "Fermat's method of infinite descent." In brief, the method may be described as follows: It is assumed that a solution of the problem in question is possible in the positive integers. From this solution, one constructs a new solution in smaller positive integers, which then leads to a still smaller solution, and so on. Because the positive integers cannot be decreased in magnitude indefinitely, it follows that the initial assumption must be false and therefore no solution is possible. One can easily verify that this reduces the problem to the cases where the exponent is an odd prime p, that is, to prove Fermat's Last Theorem, it now suffices to show that: For no odd prime p does the equation

$$a^p + b^p = c^p$$

admit a non-trivial solution in positive integers. At this point, it is useful to replace c with $-c$; since p is odd we have $(-c)^p = -c^p$, so the problem now is to show that

$$a^p + b^p + c^p = 0 \text{ implies } abc = 0$$

In the author's humble view, the advantage of this reformulation is that we now have complete symmetry between a, b and c, and this more than compensates for the slight disadvantage of having to consider negative integers.

Although the problem challenged the foremost mathematicians of the last 350 years, their efforts tended to produce partial results and proofs of individual cases. Euler gave the first proof of the Fermat conjecture for the prime $p = 3$ in the year 1770; the reasoning was incomplete at one stage, but Legendre later supplied the missing steps. Using the method of infinite descent, Dirichlet and

Legendre independently settled the case $p = 5$ around 1825. Not long thereafter, in 1839, Lame proved the conjecture for seventh powers. With the increasing complexity of the arguments came the realization that a successful resolution of the general case called for different techniques.

Then German mathematician Kummer made a major breakthrough. In 1843 he submitted a purported proof Fermat's conjecture based upon an extension of the integers to include the so-called algebraic numbers (that is, complex numbers satisfying polynomials with rational coefficients). Having spent considerable time on the problem himself, Dirichlet was immediately able to detect a flaw in Kummer's reasoning: Kummer had taken for granted that algebraic numbers admit a unique factorisation similar to that of ordinary integers, which is not always true.

Determined to restore unique factorisation to the algebraic numbers, Kummer was led to invent the concept of *ideal numbers.* By adjoining these new entities to the algebraic numbers, Kummer succesfully proved Fermat's conjecture for a large class of primes he termed *regular primes* (that this represented an enormous achievement is reflected in the fact that the only irregular primes less than 100 are 37, 59 and 67). Unfortunately, it is still undecided whether or not there exists an infinite number of regular primes, whereas in the other direction, Jensen(1915) established the existence of infinitely many irregular ones. In 1794, French woman, Sophie Germain came up with an ingenious idea that proved case I the problem for odd primes p such that $2p + 1$ is also a prime. However, it is still an open problem whether or not there exists an infinitude of such primes.

THE ELEMENTARY PROOF

Let (a, b, c) be a primitive triple, $p \geq 3$ be an odd prime and assume without loss of generality that $c < 0$. If $(a+b)(b+c)(a+c)$ divides $a^p + b^p + c^p$, then

$$\mid a^p + b^p + c^p \mid \; = \; \mid (a+b)(b+c)(a+c)d \mid$$

for some integer d.

It is clear that $\mid a^p + b^p + c^p \mid$ is dependant on $(a+b)(b+c)(a+c)$, hence minimising the quantity $\mid (a+b)(b+c)(a+c) \mid$ will also minimise $\mid a^p + b^p + c^p \mid$. But, since $(b+c)(a+c)$ is even, it follows that $min \mid (b+c)(a+c)(a+b) \mid = 2(a+b)$ which requires that $(a, b, c) = (2t-1, 2t, -2t-1)$ for some nonnegative integer $t \geq 2$.

Therefore

$$\mid a^p + b^p + c^p \mid \; \geq \; \mid (2t-1)^p + (2t)^p - (2t+1)^p \mid$$

for some $t \geq 2$. Suppose that

$$(2t-1)^p + (2t)^p = (2t+1)^p$$

This can be rewritten as

$$(2t+1)^p - (2t-1)^p = (2t)^p$$

On binomial expansion, we find that $2t \mid 2$, a contradiction.

Hence we conclude that $\mid (2t-1)^p + (2t)^p - (2t+1)^p \mid \geq 2$, which implies, by the above inequality, that $\mid a^p + b^p + c^p \mid \geq 2$, and we are done.

Remark: For $p = 3$, $(2t-1, 2t, -2t-1) = (5, 6, -7)$ and $\mid 5^3 + 6^3 + (-7)^3 \mid = 2$. Curiously, for the Pythagoras equation, $(2t-1, 2t, 2t+1) = (3, 4, 5)$ and $3^2 + 4^2 - 5^2 = 0$.

Comments: The author, Bezaliel Anotida Joshua, is a prospective BSc (Hons) Mathematics Level 1 student at the University of Zimbabwe. His email address is: bajoshua@gmail.com.

References

[1] A. Wiles, Modular Elliptic Curves and Fermat's Last Theorem, Ann. of Math. **141**, 1995, 443-551

[2] D. Burton, The History of Mathematics: An Introduction, New York: McGraw - Hill, **5**, 2003

[3] D. Cox, Introduction to Fermat's Last Theorem, Amer. Math. Monthly, **101**, (1994), 3 -14