On the equation $(XY)^n = X + Y$ and Fermat's Last Theorem

Tatenda Isaac Kubalalika

February 28, 2017

ABSTRACT. In 1637, Pierre de Fermat (1601−1665), asserted that the equation $A^r + B^r = C^r$ has no positive integer solutions for $r \geq 3$. For the purposes of this paper, we restrict r to be odd. Perez-Cacho [8] then showed in 1946 that Fermat's conjecture for the exponent r is equivalent to the statement that the equation $(XY)^n = X + Y$ has only the trivial solution $XY = 0$ in $\mathbb{Q}$, where $r = 2n-1$. In this note, we demonstrate by elementary arguments the truth of the latter statement, hence present an elementary proof of Fermat's Last Theorem.

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 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 often 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 no 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

$$a^p + b^p + c^p = 0$$

implies $abc = 0$.
It is believed by some that 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 300 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 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 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 successfully 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 not known whether there exists an infinitude of regular primes, whereas in the other direction, Jensen(1915) established the existence of infinitely many irregular ones. Notable progress towards the resolution of Fermat's conjecture was also made by French woman, Sophie Germain, who initially used the pseudonym Antoine Le Blanc in her correspondences with her male colleagues, particularly Carl Friedrich Gauss, who later became her mentor. Germain proved the conjecture for primes like 3, 5 and 11. These primes have the special property that, if p is prime, then $2p+1$ is also prime. However, whether or not there exists infinitely many such primes is still an open problem.

Proof of Fermat's Last Theorem

A result of Perez-Cacho [8] (also see [6, p.70] and [7, p.247 − 248]) says Fermat's Last Theorem is equivalent to the statement that:

The equation $(XY)^n = X + Y$ *has only the trivial solution* $XY = 0$ *in* $\mathbb{Q}$*, where* $n \geq 2$ *is an integer.*

With the idea of deriving a contradiction, we assume the existence of a rational solution $XY \neq 0$ to the above equation for some integer $n \geq 2$. That is, $X = a/b$ and $Y = c/d$, where a, b, c, d are nonzero integers with $\gcd(a, b) = \gcd(c, d) = 1$. This gives

$$(ac)^n = (bd)^{n-1}(ad + bc)$$

Begin by observing that $ad + bc \neq \pm 1$, otherwise we would have

$$(ac)^n = \pm(bd)^{n-1}$$

from which it would follow that $a^n = \pm d^{n-1}$ and $c^n = \pm b^{n-1}$. Define $u = \pm d/a$ and $v = \pm b/c$, so that $u^{n-1} = \pm a$, $u^n = \pm d$, $v^{n-1} = \pm c$ and $v^n = \pm b$.
One can quickly deduce from this information that u and v are both integers.
Substituting back into $ad + bc = \pm 1$ yields

$$\pm u^{2n-1} \pm v^{2n-1} = \pm 1$$

whose only integral solutions for any integer $n \geq 2$ are $uv = 0$, and a contradiction is reached.
This vindicates our observation that $ad + bc \neq \pm 1$.

Now since $ad + bc$ divides $(ac)^n$, it follows that there exists some prime p such that $p \mid a$ and $p \mid c$. This implies that ac cannot divide bd, otherwise we would have $a \mid d$ hence $p \mid d$ and $p \mid c$. We would also have $c \mid b$ leading to $p \mid b$ and $p \mid a$. Both of these are inconsistent with the assumption that $\gcd(a, b) = \gcd(c, d) = 1$.
Therefore, ac indeed does not divide bd, so that $(ac)^{n-1}$ cannot divide $(bd)^{n-1}$. As a consequence ac has to divide $ad + bc$, which gives $a \mid c$ and $c \mid a$ thus $a = \pm c$. After substituting this back into

the original equation and simplifying, one obtains

$$\pm a^{2n-1} = (bd)^{n-1}(b \pm d)$$

from which it follows that $b \mid a^{2n-1}$. But this is impossible due to the coprimality of a and b, unless $b = \pm 1$, for which the preceding equation would become

$$\pm a^{2n-1} = \pm d^{n-1}(d \pm 1)$$

Because d^{n-1} and $d \pm 1$ are relatively prime, we should have some integers (r, s) such that $d = r^{2n-1}$ and $d \pm 1 = s^{2n-1}$, giving $s^{2n-1} \mp r^{2n-1} = 1$, whose only *integral* solutions for any integer $n \geq 2$ are $rs = 0$, which leads to a contradiction.

This completes the proof.

About the author: Tatenda Kubalalika is a financially limited but very ambitious *prospective undergraduate* mathematics student from Zimbabwe, who is also deeply passionate about study and research in the fields of algebraic and analytic number theory. Actually, his initial goal was not to prove Fermat's Last Theorem for *all* exponents, but to come up with a novel proof for some particular exponent, in an aim to establish a track record for his future work to be taken seriously. To his great surprise, the argument indeed worked for all exponents!
Amongst other things, he hopes to be involved in the fascinating subject of Random Matrix Theory in the future, and use it to analyse the suitably normalized spacings of the zeros of automorphic $L-$ functions, in the spirit of Montgomery, Odlyzko, Rudnick, Sarnak *et al.*

References

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

[2] D. Burton, Elementary Number Theory, 1980, Allyn and Bacon.

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

[4] Inkeri, K., On certain equivalent statements for Fermat's Last Theorem - with requisite corrections. Ann. Univ. Turkuenis, Ser. AI, **186**, (1984), 12 - 22; reprinted in collected papers of Kustra Inkeri (editor P. Ribenboim), Queen's papers in Pure and Applied mathematics, Vol. 91, Kingstone, Ontario, 1992.

[5] J. Jones and G. Jones, Elementary Number Theory, Springer Verlag.

[6] P. Ribenboim, 13 Lectures on Fermat's Last Theorem, Springer - Verlag, Berlin Heiderlberg, 1979.

[7] P. Ribenboim, Fermat's Last Theorem for amateurs, Springer - Verlag, New York, 1997.

[8] Perez - Cacho, L. El ultimo teorema de Fermat y los numeros de Marsenne, Rev. Real Acad. Cienc. Exact. Fiis. y Nature., Madrid, **40**, (1946), 39 - 57.