Advances in Algebra (AA).
ISSN 0973-6964 Volume 14, Number 1 (2021), pp. 1-2

http://www.ripublication.com/aa.htm

An Elementary Proof of Fermat's Last Theorem

Kelvin Muzundu

Department of Mathematics and Statistics, University of Zambia,
P.O. Box 32379, Lusaka, Zambia.

Abstract

We present an elementary proof of Fermat's Last Theorem, which is the assertion that the equation $z^n = x^n + y^n$ has positive integer solutions for x, y and z only when $n = 1$ and $n = 2$

Mathematics Subject Classification (2020): 11A05; 11C08

Keywords: Fermat's Last Theorem

1. INTRODUCTION

Let n be a natural number. It is well known that the equation

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

has positive integral solutions for x, y and z only for $n = 1$ and $n = 2$. We refer to [1] for the famous proof of this historical result. In this note, we propose an elementary proof of the result. The notation $\gcd(a, b)$ will be used for the greatest common divisor of integers a and b, while $a \mid b$ will mean that a divides b.

2. THE PROOF

Proof. Obviously, when $n = 1$ or $n = 2$, there are positive integers x, y and z satisfying Equation 1. Now suppose that $n \geq 3$ and that Equation 1 is satisfied. We assume without loss of generality that there no positive integers a, b and c satisfying Equation 1

and the inequalities $a < x$, $b < y$ and $c < z$. Now since x, y and z satisfy Equation 1, it is clear that $z > x, z > y$ and $x \neq y$. We may therefore assume that $x < y$. Let p be the positive integer such that $z = x + p$. Then Equation 1 may be written in terms of p as

$$(x + p)^n = x^n + y^n. \tag{2}$$

If $p = 1$, since $x < y$, Equation 2 becomes

$$(x + 1)^n = x^n + (x + q)^n$$

for some positive integer q, which is false. Therefore $p > 1$ and Equation 2 can be rearranged to assume the form

$$\sum_{k=1}^{n} \binom{n}{k} x^{n-k} p^k = y^n,$$

which means that $p \mid y^n$. Now, $\gcd(p, y) = u > 1$ for if not, then $\gcd(p, y^n) = 1$, which is a contradiction. Because $n \geq 3$ we can rearrange Equation 2 to assume the form

$$x^{n-1} = \frac{1}{n}\left(\frac{y^n}{p} - p^{n-1} - \sum_{k=2}^{n-1} \binom{n}{k} x^{n-k} p^{k-1}\right).$$

Clearly,

$$u \mid \frac{1}{n}\left(\frac{y^n}{p} - p^{n-1} - \sum_{n=2}^{n-1} \binom{n}{k} x^{n-k} p^{k-1}\right)$$

and so $u \mid x^{n-1}$. This means that $\gcd(u, x) = v > 1$ and that $v \mid p, v \mid x$ and $v \mid y$. It follows from $z = x + p$ that $v \mid z$. This implies that there are positive integers a, b and c such that $x = av, y = bv$ and $z = cv$, so that Equation 1 reduces to $c^n = a^n + b^n$, which is a contradiction. Hence for $n \geq 3$, there is no positive integer p for which Equation 2 is satisfied, which in turn means that there are no positive integers x, y and z for which Equation 1 is satisfied. □

REFERENCES

[1] Wiles A., 1995, "Modular Elliptic Curves and Fermat's Last Theorem", Annals of Mathematics, 141, pp. 443–551.