Parabola Volume 59, Issue 3 (2023)

Some results on odd exponents in Fermat's Last Theorem

Kelvin Muzundu[1]

1 Introduction

The assertion that the equation

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

has no non-trivial integer solutions for any positive integer n greater than 2 is known as Fermat's Last Theorem (FLT). It was first stated in 1637 by French Mathematician Pierre de Fermat. The famous proof [7] by British Mathematician Andrew Wiles relies on advanced and relatively modern number-theoretic techniques. Prior to Wiles' proof, various authors including some prominent mathematicians proved FLT for specific values or classes of n. Fermat himself proved the result for $n = 3$ and $n = 4$, after developing and applying a technique known as *the method of infinite descent*. This is a form of proof by contradiction where it is assumed that if a statement is true for a given number, then it would be true for a smaller number, which would lead to an infinite descent and ultimately result in a contradiction.

Euler in 1770 also proved FLT for $n = 3$ and $n = 4$ by different methods, although the proof for $n = 3$ had an error. His methods were adopted by others, who corrected the error and also applied them in other problems. In 1823, Sophie Germain proved FLT for $n = 5$, and Dirichlet and Lagrange in 1825 also proved it for $n = 5$ by different methods. Lamé in 1839 established FLT for the case $n = 7$. Another breakthrough came in 1847 when Kummer proved FLT for a class of prime numbers known as the regular primes. After Kummer's work, FLT was known to be true for the odd primes below 100 except 37, 59 and 67.

Faltings's Theorem established in 1983 was another breakthrough in the proof FLT. This is a result in arithmetic geometry, and one its consequences is that Equation (1) has at most finitely many pairwise coprime solutions for any fixed $n \geq 4$. The proofs of FLT for specific values of n tended to be ad hoc in nature and could therefore not be generalized to arbitrary n. For more details on these matters and for a complete historical account, we refer the reader to [5].

In this article, elementary mathematics are used to establish results that describe conditions under which Equation (1) does not hold for odd values of n greater than 9. The results do not establish a new proof of FLT but only assert that Equation (1) does not hold for any odd integer $n > 9$ when certain natural assumptions are placed on x, y and z. Although Equation 1 is stated in terms of non-zero integers, it is well known and can easily be verified that it is enough to consider it only for positive integers.

[1]Kelvin Muzundu is a Lecturer in the Mathematics and Statistics Department, University of Zambia.

2 Results

The main results of the article are presented in this section, which show that when x, y and z satisfy certain conditions, then Equation (1) does not hold. We begin with the following theorem.

Theorem 1. *There are no positive integers x, y, z such that p divides y or $q > 1$ and q divides x, and $z^n = x^n + y^n$ holds for any odd positive integer $n > 9$, where $p = z - x$ and $q = z - y$.*

Proof. Suppose that positive integers x, y and z exist such that Equation (1) holds for an odd positive integer $n > 9$. We assume without loss of generality that x, y and z are in their lowest terms and that $y > x$. It suffices to establish the result for prime values of n, for if n is composite and has a prime factor n_1, then Equation (1) can be written in terms of the prime exponent n_1 and powers of x, y and z.

Now, the equation $p = z - x$ means that $z^n = (x + p)^n$, and so it follows from Equation (1) that

$$y^n = npx^{n-1} + \frac{n(n-1)}{2}p^2x^{n-2} + \cdots + np^{n-1}x + p^n\,, \tag{2}$$

which implies that p divides y^n. If p and x^{n-1} in Equation (2) have a common factor, then x, y and z will have a common factor, which contradicts the fact that they are in their lowest terms. Equation (2) and the assumption that p divides y therefore implies that p must divide n, and because n is odd, p^3 will divide the term $\frac{n(n-1)}{2}p^2x^{n-2}$ in the sum in Equation (2). It follows that p^2 will divide the term nx^{n-1}, and because p and x cannot have a common factor, we deduce that p^2 divides n. But this contradicts the fact that n is prime. This completes the proof of the first part of the result. The second part is proved by using similar arguments. □

In Theorem 1, it was assumed that $q > 1$ and q divides x. In the next result, we establish that Equation (1) still does not hold when $q > 1$ and does not divide x. To prove it, the following lemma will be required.

Lemma 2. *If there are positive integers x, y and z such that $z^n = x^n + y^n$ holds for any odd integer $n > 9$, then there are positive integers b, c, d such that $dy = cx - bq$, where $q = z - y$.*

Proof. Suppose that there are positive integers x, y and z such that Equation (1) holds, for some odd $n > 9$. Then $z > x$ and $z > y$, and so there are positive integers p and q such that $z = x + p = y + q$. As before, we assume without loss of generality that $y > x$. Then, clearly, $y > p$, $x > q$ and $p > q$. Now, since $n > 9$ and n is odd, Equation (1) may be written as

$$z^n = (x + y)(x^{n-1} - x^{n-2}y + \cdots - xy^{n-2} + y^{n-1})\,,$$

which implies that $x + y$ divides z^n. Therefore if a is the greatest common divisor of $x + y$ and z, then $a > 1$. Let b and c be positive integers such that $x + y = ab$ and $z = ac$. It follows from $p + q = 2z - (x + y)$ that a divides $p + q$. Then $x - q = y - p = z - (p + q)$ implies that a divides $x - q$ and $y - p$. Since a divides $p + q$ and $x - q = y - p$, there are

positive integers d_1 and d_2 such that $p+q=ad_1$ and $x-q=y-p=ad_2$. Therefore, $ad_1+ad_2=p+q+x-q=x+p=z$, and comparing with $z=ac$, we deduce that $c=d_1+d_2$. In addition, $ab=x+y=x+z-q=ac+ad_2$ implies that $b=d_1+2d_2=c+d_2$. From $z=ac$, $z=y+p$ and $x-q=ad_2$, we get that $\frac{z}{c}=\frac{y+q}{c}=\frac{x-q}{d_2}$, which can be rearranged as $d_2y=cx-(c+d_2)q$. It follows from $b=c+d_2$ that $d_2y=cx-bq$, and taking $d=d_2$, the result follows. □

Theorem 3. *There are no positive integers x, y and z such that $q>1$, q does not divide x and $z^n=x^n+y^n$ holds for any positive odd integer $n>9$, where $q=z-y$.*

Proof. Suppose that positive integers x, y and z exist such that Equation (1) holds for some odd integer $n>9$, and that x, y and z are assumed to be in their lowest terms and $y>x$. Now, the equation $q=z-y$ implies that $z^n=y^n+nqy^{n-1}+\cdots+nq^{n-1}y+q^n$. Comparing with Equation (1) gives $x^n=nqy^{n-1}+\frac{n(n-1)}{2}q^2y^{n-2}+\cdots+nq^{n-1}y+q^n$. Therefore, q divides x^n, and because $q>1$, we have that q and x have a common factor. But since q does not divide x, there are positive integers $e>1$ and $f>1$ with no common factor, such that $q>e$, $x>f$ and

$$x=\frac{f}{e}\,q\,. \tag{3}$$

Equation (3) and Lemma 2 then imply that $d_2ey=(cf-be)q$. If q and y have a common factor, then y and z have a common factor, which leads to a contradiction. If q and y do not have a common factor, then y divides $cf-be$, and so there is a positive integer $g>1$ such that

$$cf-be=gy\,. \tag{4}$$

Multiplying both sides of Equation (4) by a and using $x+y=ab$ and $z=ac$ leads to the equation $fz-e(x+y)=agy$, which in view of $z=q+y$ may be written as $ex-fq=(f-e-ag)y$. But $ex-fq=0$, which implies that $f-e-ag=0$, or $f-e=ag$. It follows from Equation (3) and the equation $x-q=ad_2$ that

$$\frac{f-e}{g}=\frac{(f-e)q}{d_2e}\,,$$

which means that

$$g=\frac{d_2e}{q}\,. \tag{5}$$

Since $x-q=y-p$ and $b=c+d_2$, Equation (4) can be written as $c(f-e)=g(x+q-p)+d_2e$. Equation (5) then implies that $c(f-e)=g(x+q-p)+gq=g(x+2q-p)$. From the equation $f-e=ag$, it is therefore deduced that

$$c(f-e)=\frac{(f-e)}{a}(x+2q-p)\,,$$

which in the light of $z=ac$ becomes $z=x+2q-p$. Then equation $z=x+p$ yields that $p=q$. But this means that $x=y$, which is not possible as it would make z irrational. Hence, Equation (1) does not hold when $q>1$ and does not divide x. □

Theorems 1 and 3 and the well-known fact that Equation (1) does not hold for $n = 4$ lead to the following corollary.

Corollary 4. *There are no positive integers x, y and z such that $p = z - x$ divides y, that $q = z - y > 1$ and that $z^n = x^n + y^n$ holds for any positive integer $n > 9$.*

Proof. If n has an odd factor, then the result follows immediately from Theorems 1 and 3. If n has no odd factor, then 4 divides n since $n > 9$, and in this case the result follows directly from the fact that Equation (1) does not hold for $n = 4$. □

In the light of Theorem 1, Theorem 3 and Corollary 4, to prove that Equation (1) does not hold for every positive integer $n > 9$, one needs to prove that it does not hold when p does not divide y and when $q = 1$.

Acknowledgements

We would like to acknowledge the anonymous reviewer and Thomas Britz for the recommendations and suggestions that have enhanced the presentation of the article.

References

[1] Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[2] G. Faltings, The proof of Fermat's Last Theorem by R. Taylor and A. Wiles, *Notices of the American Mathematical Society* **42**(7) (1995), 743–746.

[3] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, New York, 1990.

[4] H.W. Lenstra, Jr., Euclidean number fields 1, *Math. Intelligencer* **2** (1979), 6–15.

[5] S. Singh, *Fermat's Last Theorem*, Fourth Estate, 1997.

[6] A. van der Poorten, *Notes on Fermat's Last Theorem*, J. Wiley & Sons, New York, 1996.

[7] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Annals of Mathematics* **141** (1995), 443–551.