Mathematics Letters
2024; 10(1): 1-6
http://www.sciencepublishinggroup.com/j/ml
doi: 10.11648/j.ml.20241001.11
ISSN: 2575-503X (Print); ISSN: 2575-5056 (Online)

A Result on Odd Powers in Fermat's Last Theorem

Kelvin Muzundu

Department of Mathematics and Statistics, University of Zambia, Lusaka, Zambia

Email address:
kmzundu@gmail.com

To cite this article:
Kelvin Muzundu. (2024). A Result on Odd Powers in Fermat's Last Theorem. *Mathematics Letters*, *10*(1), 1-6.
https://doi.org/10.11648/j.ml.20241001.11

Received: December 5, 2023; **Accepted**: January 9, 2024; **Published**: January 23, 2024

Abstract: In this work, a partial proof of Fermat's Last Theorem (FLT) relying on elementary number theory is presented. The main result asserts that when certain natural assumptions are placed on the variables involved in the equation of the statement of FLT, then FLT holds for any prime number greater than 9, and consequently for any positive integer greater than 9. The proof of the main and supporting results is by the method of contradiction. It is first proved that if there is a prime number greater than 9 for which FLT is false under a natural assumption on the variables of the equation of FLT, then there is a set of equations that the variables must satisfy. From this set of equations, it is proved that the variables of the equation of FLT are further constrained by an additional set of equations and inequalities, which ultimately results in a contradiction. The elementary number theoretic methods employed are centered around the theory of greatest common divisors, the binomial theorem, the theory of indices, and the theory of polynomials over the ring of all integers. The algebraic operations involved are those defined on the ring of all integers, and those defined on the field of all rational numbers. The elementary order properties of the set of integers as a subset of the totally ordered field of real numbers are also applied. The cancellation and unique prime power factorization properties of the integers are taken for granted.

Keywords: Fermat's Last Theorem, Odd Powers, Integers

1. Introduction

Fermat's Last Theorem (FLT) is the statement 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. It was first stated in 1637 by French mathematician Pierre de Fermat and was proved by British mathematician Andrew Wiles (see [14, 17]) using advanced and relatively modern number theoretic techniques. Before Wiles' proof, various authors including some prominent mathematicians proved FLT for some specific values or classes of n. Fermat himself proved FLT for the cases $n = 3$ and $n = 4$, after developing and applying a technique known as the method of infinite descent, which is a form of proof by contradiction where one assumes 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 lead to a contradiction.

In 1770, Euler also proved FLT for $n = 3$ and $n = 4$ by different methods, although the proof for $n = 3$ had a gap. Euler's methods were adopted by other mathematicians, who corrected Euler's proof for $n = 3$ and applied them in other problems. Sophie Germain in 1823 proved FLT for $n = 5$, and in 1825, Dirichilet and Lagrange also proved it for $n = 5$ by different techniques. In 1839, Lame` established FLT for the case $n = 7$.

Another important breakthrough came in 1847 when Kummer proved FLT for a class of prime numbers known as the regular primes. Following Kummer's work, FLT was known to hold for odd primes below100, except 37, 59 and 67. Further work from various authors proved FLT for the cases $n = 6, 8, 9, 10$ and 14. Another milestone came in 1983 when Germany mathematician Gerd Faltings proved a result in arithmetic geometry, one of whose 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 are adhoc in nature and cannot be generalized to arbitrary n. For a complete historical account of FLT, the reader is referred to [9, 13].

Wiles' proof of FLT relies mainly on modularity theory and

the theory of elliptic curves. Since the publication of the proof in 1995, there have been great developments in modularity theory and the theory of elliptic curves (see for instance [3, 8, 10, 11, 15, 18]).

In this work, elementary number theory will be used to establish a result that describes conditions under which Equation (1) does not hold for any odd integer n greater than 9. The result does not establish a new proof of FLT but only asserts 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 in general, it is well known and can easily be verified that it is enough to consider it only for positive integers. In addition, it will suffice to prove our main result only for prime values of n since if n is not prime, Equation (1) can be re-arranged and written in terms of a prime exponent and powers of the original integers x, y and z. Some of the ideas employed in the proofs of results find their inspiration in the works [1, 2, 4-7, 12, 16].

2. Materials and Methods

The results in this work will involve statements about positive integers in relation to FLT. Then proofs of these statements will be established by standard elementary number theoretic techniques.

3. Results

The main result of this section is Theorem 3.4, which establishes that Equation (1) does not hold under certain assumptions on x, y and z for any odd integer $n > 9$. To prove it, the next three lemmas will be needed.

Lemma 3.1

If there are positive integers x, y and z such that $p = z - x$ does not divide y and $z^n = x^n + y^n$ holds for any prime positive integer $n > 9$, then there are positive integers u and v, which are relatively prime and satisfy the equations $y = (u/v)p$, $p = s^n$ and $p = sv$ for some positive integer s.

Proof. Suppose that positive integers x, y and z exist such that $z^n = x^n + y^n$ holds for an odd positive integer $n > 9$, and satisfying the hypotheses above. Assume without loss of generality that x, y and z are in their lowest terms. Now, since Equation (1) holds, it is clear that $z > x$ and so $p = z - x > 0$. Equation (1) may then be written as

$$z^n = x^n + npx^{n-1} + \cdots + np^{n-1}x + p^n,$$

which when compared with Equation (1) yields that

$$y^n = npx^{n-1} + \binom{n}{2}p^2x^{n-2} \ldots + np^{n-1} + p^n, \qquad (2)$$

so that y and p have a common factor. Since p does not divide y by hypothesis, there are positive integers u and v that have no common factor and satisfy the relations $p > v$, $y > u$ and

$$y = (u/v)p. \qquad (3)$$

Since, obviously, v divides p, there is a positive integer s such that $p = sv$. It follows from Equation (3) that $y = su$, which together with $p = sv$ imply that Equation (2) may be written as

$$s^n u^n = n(sv)x^{n-1} + (n(n-1)/2)(sv)^2x^{n-2} + \cdots + n(sv)^{n-1}x + (sv)^n. \qquad (4)$$

First, suppose that s does not divide v. Then the first possibility is that s has a factor w that has no common factor with v. If w does not divide nx^{n-1}, then Equation (4) is inconsistent since dividing both sides of the equation by the highest power of w in s leaves the left hand side divisible by w while the right hand side is not. Therefore w must divide nx^{n-1} and if w and x^{n-1} have a common factor, then p and x will have a common factor. This will lead to x, y and z having a common factor, contradicting the fact that they are in their lowest terms. Therefore w and x have no common factor, and so w must divide n. This means that w^3 divides the second term $(n(n-1)/2)(sv)^2x^{n-2}$ in the sum on the right hand side of Equation (4). This in turn implies that w^2 divides n, which contradicts the fact that n is a prime number.

Now consider the second possibility for s not dividing v, which is that s has a factor r that occurs with a higher power in s than in v. If r does not divide nx^{n-1} as before, it is deduced that Equation (4) is inconsistent as dividing both sides by the highest power of r in sv leaves the left hand side divisible by r while the right hand side is not. Therefore r must divide nx^{n-1}, and then as before, r^2 will divide n, contradicting the fact that n is prime. Since both cases fail when s does not divide v, it is concluded that s must divide v.

Let s^j be the highest power of s in v. If $j \geq n$, then Equation (4) is inconsistent as dividing both sides by s^n will leave the right hand side divisible by s while the left hand side is not. Similarly, if $n > j + 1$, then again Equation (4) is inconsistent as dividing both sides by s^{j+1} will leave leave the left hand side divisible by s while the right hand side is not. Now suppose that $n = j + 1$ and let v' be a positive integer such that $v = s^j v'$. If $v' > 1$, because u and v are relatively prime, Equation (4) is inconsistent since dividing both sides by $s^n = s^{j+1}$ will leave the right hand side divisible by v' while the left hand side is not. It follows that $v' = 1$, so that $v = s^j = s^{n-1}$, which leads to $p = sv = s^n$.

Lemma 3.2

If there are positive integers x, y and z such that $p = z - x$ does not divide y, $q = z - y = 1$ and $z^n = x^n + y^n$ holds for any prime $n > 9$, then there are positive integers a, b and c such that $x + y = ab$, $z = ac$, and $b < a^{n-1}$.

Proof. Assume that there are positive integers x, y and z such that the hypotheses above are satisfied. As before, it is assumed without loss of generality that x, y, z are in their lowest terms, and that $y > x$. Note also that $z = x + p = y + 1$. Now, since n is odd, $z^n = x^n + y^n$ can 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, and so 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 $z = x+p = y+1$ that $p+1 = 2z-(x+y)$, and because a divides $x+y$ and z, it divides $p+1$. Then $x-1 = y-p = z-(p+1)$ yields that a divides $x-1$ and $y-p$. Since a also divides $p+1$, there are positive integers $d1$ and $d2$ such that $p+1 = ad1$ and $x-1 = y-p = ad2$. Therefore $ad1 + ad2 = p+1+x-1 = x+p = z$, and comparing with $z = ac$, it is deduced that $c = d1 + d2$. In addition, $ab = x+y = x+z-q = ac + ad2$ yields that $b = d1 + 2d2 = c + d2$.

Now, by Lemma 3.1, there are relatively prime positive integers u, v, and an integer s, such that $p = sv$ and $y = su$. It follows from $y-p = x-1 = ad2$ that

$$y - p = x - 1 = (u-v)s = ad2. \tag{5}$$

If a and s have a common factor, then y and z will have a common factor, which contradicts the fact that x, y, z are relatively prime. Therefore a must divide $u-v$, and so there a positive integer t such that $u - v = at$. It follows from Equation (5) that

$$d2 = st \tag{6}$$

Now, writing $x+y = ab$ as $y = ab - x$ and taking n^{th} powers on both sides leads to the equation

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

which on rearrangement and in the light of $z^n = x^n + y^n$ and $z = ac$ becomes

$$a^{n-1}c^n = b((ab)^{n-1} - n(ab)^{n-2}x + \cdots + nx^{n-1}). \tag{7}$$

If b and c have a common factor, then $x+y$ and z will have another common factor other than a, which contradicts the fact that a is their greatest common divisor. Therefore, b and c have no common factor, and so Equation (7) implies that b divides a^{n-1}. Suppose that $b = a^{n-1}$. Then $x+y = ab = a^n$, and since $p = s^n$ by Lemma 3.1, the equation $2z = x+y+p+1$ assumes the form $2z = a^n + s^n + 1$. From $y = su$, $z = ac$ and $z = y+1$, it follows that $ac + su = a^n + s^n$. Since n is odd, this may be written as

$$ac + su = (a+s)(a^{n-1} - a^{n-2}s + \cdots - as^{n-2} + s^{n-1}) = (a+s)g, \tag{8}$$

where $g = (a^{n-1} - a^{n-2}s + \cdots - as^{n-2} + s^{n-1})$. It is easy to deduce from Equation (8) that

$$a(g-c) = s(u-g). \tag{9}$$

Note from $2z = a^n + s^n + 1$ that $a > s$. To see this, suppose that $a \leq s$. Then $2z < 2s^n + 1 = 2p + 1$, and so $z = p + x$ yields that $x < 1/2$, which is not possible. Next, it is shown that $u > c$. Suppose to the contrary that $u \leq c$. The case $u = c$ is ruled out as it would mean that y and z have a common factor. For the case $u < c$, first observe that there are positive integers $s1$ and $u1$ such that $a = s + s1$ and $c = u + u1$, so that $z = ac = su + su1 + us1 + s1u1 = y + su1 + us1 + s1u1$. This is inconsistent with $z = y+1$, and so the inequality $u > c$ is established. Next, it is shown that $c < g < u$. If $c = g$ or $g = u$, Equation (9) yields that $c = u$, which is not possible as it would mean that y and z have a common factor. If $c > g$, then $u > c > g$, which makes Equation (9) inconsistent as the left hand side is negative while the right hand side is positive. Similarly, if $g > u$, then $g > u > c$ and again Equation (9) is inconsistent. Thus, $c < g < u$.

Now, since $g > c$, there are positive integers $c1$ and $g1$ such that $g = cg1 + c1$, where $c > c1$. Then Equation (9) becomes $a(cg1 + c1 - c) = s(u - cg1 - c1)$, which on rearrangement assumes the form $ac(g1-1) + (a+s)c1 + csg1 = su$. From $y = us$ and $z = ac$, it follows that $z(g1-1) + (a+s)c1 + csg1 = y$, and so if $g1 > 1$ then $y > z$. Since this is not possible, it follows that $g1 = 1$, so that $g = c + c1$. This and Equation (9) yield that

$$(su + ac)/(a+s) = (y+z)/(a+s).$$

It follows from $g = c + c1$ that $c + c1 = (y+z)(a+s)$, that is, $ac + ac1 + cs + sc1 = y + z$. Because $ac = z$, this becomes $ac1 + cs + sc1 = y = us$, which implies that s divides $ac1$. Since a and s cannot have a common factor as this would mean that y and z have a common factor, this implies that s divides $c1$. Let $s1$ be a positive integer such that $c1 = ss1$. It follows from $g = c + c1$ that $g = c + ss1$. Equation (9) then leads to

$$u = g + as1 = c + as1 + ss1. \tag{10}$$

Multiplying both sides of Equation (10) by s and using $y = su$ yields that $y = cs + ass1 + s^2s1$. Multiplying both sides of Equation (10) by a and using $z = ac = y + 1$ produces $au = y + a^2s1 + ass1 + 1$. Since $y = cs + ass1 + s^2s1$, the latter equation becomes $au = cs + 2ass1 + a^2s1 + s^2s1 + 1$. Substituting $g - ss1$ for c, it follows that

$$au = sg + 2ass1 + a^2s1 + 1. \tag{11}$$

Multiplying both sides of Equation (10) by c leads to $cu = c^2 + acs1 + css1$. Using Equation (11), the variable u can be substituted for the expression $sg/a + 2ss1 + as1 + 1/a$ in the latter equation, to obtain that

$$c(sg/a + 2ss1 + as1 + 1/a) = c^2 + acs1 + css1,$$

which on rearrangement and simplification leads to $sg + 1 = a(c - ss1)$. Taking $g = c + ss1$, this equation assumes the form $(a-s)c = ss1(a+s) + 1$. From this and the equations $c = d1 + d2$, $d2 = st$ and $p + 1 = ad1$, it follows that $s((a+s)s1 - (a-s)t + d1) = p$. The equation $p = sv$ then yields that $v = (a+s)s1 - (a-s)t + d1$, which from $d2 = st$ and $c = d1 + d2$ becomes $v = (a+s)s1 + c - a$. Therefore

$$g - v = c + ss1 - ((a+s)s1 + c - a) = a(1 - s1). \tag{12}$$

Now, as was noted before, Equation (9) can be written as $(a+s)g = 2y+1$. In view of $z = y+1$, $z = x+p$ and $x+y = ab$, it follows that $(a+s)g = ab+p$, which from $p = sv$ can rearranged as $a(b-g) = s(g-v)$. If $s1 > 1$, Equation (12) means that $v > g$, and then $a(b-g) = s(g-v)$ implies that $g > b$. Therefore $v > b$, which is not possible since $a > s$, $b = a^{n-1}$ and $v = s^{n-1}$. If $s1 = 1$, then Equation (12) and $a(b-g) = s(g-v)$ will yield that $b = g = v$. Since s divides v and y, from the equation $x+y = ab$ it is deduced that s divides x, and so x and y will have a common factor, which leads to a contradiction. It is therefore concluded that the case $b = a^{n-1}$ does not hold, and since b divides a^{n-1}, then $b < a^{n-1}$.

Lemma 3.3

If there are positive integers x, y and z such that $p = z - x$ does not divide y, $q = z - y = 1$ and $z^n = x^n + y^n$ holds for any prime $n > 9$, then there are positive integers a, b and c such that $x + y = ab$, $z = ac$, and $a^{n-2} < b$.

Proof. Suppose that x, y and z are positive integers satisfying the hypotheses above. As before assume without loss of generality that x, y and z are in their lowest terms and that $y > x$. By replicating the arguments in the proof of Lemma 3.2, it is obtained that there are positive integers $a, b, c, d1, d2$ such that $x + y = ab$, $z = ac$, $c = d1 + d2$, $b = c + d2$, $p + 1 = ad1$, $x - 1 = ad2$ and

$$a^{n-1}c^n = b((ab)^{n-1} - n(ab)^{n-2}x + \cdots + nx^{n-1}) \ (*).$$

Suppose that $b \leq a^{n-2}$. Since b divides a^{n-1} as was deduced in the proof of Lemma 3.2, the inequality $b \leq a^{n-2}$ and the Equation (*) yield that a and nx^{n-1} have a common factor. Because a and x^{n-1} cannot have a common factor as x, y and z are in their lowest terms, it follows that a and n have a common factor. Since n is prime, the common factor is n itself. Now, note from the equation $a^n c^n = z^n = x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + \cdots - xy^{n-2} + y^{n-1}) = ab(x^{n-1} - x^{n-2}y + \cdots - xy^{n-2} + y^{n-1})$ that a and c are both factors of the sum in the braces, which means that z divides the sum. If y is odd, then $z = y + 1$ is even and x is odd, and the sum in the braces is odd as it will be a sum of an odd number of odd terms, in which case z cannot divide the sum. Thus y must be even, so that z is odd, and so a, b, c, u are odd while s, p, v are even. From $x - 1 = ad2$, it is deduced that $d2$ is even and from $p + 1 = ad1$ that $d1$ is odd.

Now, because n is prime, it divides every term in the sum $\sum_{k=0}^{n} \binom{n}{k}$ apart from the first and last one. Since the first and last terms are both 1 and $\sum_{k=0}^{n} \binom{n}{k} = 2^n$, this implies that n divides $2^n - 2$. Writing $2^n - 2 = 2(2^{n-1} - 1)$, it follows that n divides $2^{n-1} - 1$, and so there is a positive integer f such that $2^{n-1} - 1 = fn$. Since s is even and $p = s^n$ by Lemma 3.2, we can write $p = 2^n w = (2^n - 2 + 2)w = (2^n - 2)w + 2w$, for some positive integer w. Adding 1 on both sides of this equation leads to the equation

$$p + 1 = (2^n - 2)w + 2w + 1. \quad (13)$$

Since n divides a, the equation $p + 1 = ad1$ means that n divides $p + 1$ and since n also divides $2^n - 2$, Equation (13) implies that n divides $2w + 1$ and so

$$2w + 1 = gn \quad (14)$$

for some positive integer g. From $b = c + d2 = d1 + 2d2$, we get that $ab = ad1 + 2ad2$ and then $p + 1 = ad1$ gives $ab = 2ad2 + p + 1$. Using $p = 2^n w$, the latter equation becomes $2ad2 + 2^n w + 1 = ab$ and because n divides a, this implies that n divides $2^n w + 1$. Let h be the positive integer such that

$$2^n w + 1 = hn. \quad (15)$$

If $w = 1$, then Equation (15) establishes that n divides $2^n + 1$, and since it also divides $2^n - 2$, this will mean that n divides 3. However, this is not possible since $n > 9$. Therefore $w > 1$, and so from $p = s^n = 2^n w$, there must be a positive integer $k > 1$ such that $w = k^n$. This implies that $w > 2^{n-1} - 1$ and so it follows from $2^{n-1} - 1 = fn$ and Equations (14) and (15) that $g > f$ and $h > f$. It follows that there exist integers $f1, f2, l1, l2$ with $f > f1, f2$, such that $h = fl1 + f1$ and $g = fl2 + f2$. Then $h - g = (l1 - l2)f + f1 - f2$, so that $fgn = f - g + h$ yields that $(gn - 1)f = (l1 - l2)f + f1 - f2$, or $(gn + l2 - l1 - 1)f = f1 - f2$. Since $f > f1 - f2$, this implies that $f1 - f2 = 0$ and $gn + l2 - l1 - 1 = 0$. Making $l1$ the subject of the formula and using Equation (14) yields that $l1 = 2w + l2$. Together with $f1 = f2$ and $g = fl2 + f2$, this implies that

$$h = fl1 + f1 = (2w + l2)f + f1 = 2wf + g. \quad (16)$$

Now, from $f1 = f2$, $h = fl1 + f1$ and $g = fl2 + f2$, it is established that $h - g = (l1 - l2)f$, or $h = (l1 - l2)f + g$. Comparing with Equation (16), this yields that $l1 - l2 = 2w$. Adding 1 on both sides and using the fact that $2w + 1 = gn$, it follows that $l1 - l2 + 1 = gn$. Using $g = fl2 + f1$ and rearranging, it is obtained that $l1 = (nf + 1)l2 + nf1$. Then $2^{n-1} = nf + 1$ implies that $l1 = 2^{n-1}l2 + nf1$, so that $h = l1f + f2$ produces $h = (2^{n-1}l2 + nf1)f + f1 = 2^{n-1}l2f + nff1 + f1 = 2^{n-1}l2f + (nf + 1)f1 = 2^{n-1}(fl2 + f1) = 2^{n-1}g$.

This means that g divides h, and then Equation (16) establishes that g divides $2wf$. Since g divides $2w + 1$, this means that g and $2w$ cannot have a common factor, and so g must divide f. However, this contradicts the fact that $g > f, and$ it is therefore concluded that the inequality $b \leq a^{n-2}$ does not hold. Hence $a^{n-2} < b$.

Having proved Lemmas 3.1, 3.2 and 3.3, the main result of the paper will now be established, which asserts that the equation $z^n = x^n + y^n$ does not hold when x, y and z satisfy the conditions of Lemma 3.1, 3.2 and 3.3.

Theorem 3.4

There are no positive integers x, y and z such that $p = z - x$ does not divide y, $q = z - y = 1$ and $z^n = x^n + y^n$ holds for any prime $n > 9$.

Proof. Assume that x, y and z are positive integers such that the hypotheses above are satisfied, x, y, z are in their lowest terms and without loss of generality $y > x$. By Lemma 3.1, 3.2 and 3.3, there are positive integers a, b, c such

that $x + y = ab$, $z = ac$ and $a^{n-2} < b < a^{n-1}$. If b has a factor that is relatively prime to a, then the equation

$$a^n c^n = ab(x^{n-1} - x^{n-2}y + \cdots - xy^{n-2} + y^{n-1})$$

implies that b and c have a common factor, which contradicts the fact that a is the greatest common divisor of $x + y$ and$z$. Therefore b has no factor that is relatively prime to a.

First consider the case where a^{n-2} does not divide b. Then either a^{n-2} has a factor that is relatively prime to b or a^{n-2} has a factor that occurs with a higher power in a^{n-2} than in b. For the first case, since no factor of b is relatively prime to a, there are factors $a1$ and $a2$ of a such that $a = a1a2$, $a1$ is relatively prime to b and $b = (a2)^m$ for some positive integer $m > 1$. The equation

$$a^n c^n = ab((ab)^{n-1} + n(ab)^{n-2}x + \cdots + (n(n-1)/2)(ab)x^{n-2} + nx^{n-1}) \quad (17)$$

then becomes

$$(a1a2)^{n-1}c^n = (a2)^m((ab)^{n-1} + n(ab)^{n-2}x + \cdots + (n(n-1)/2)(ab)x^{n-2} + nx^{n-1}),$$

which means that $a1$ dividesnx^{n-1}. Since $a1$ and x cannot have a common factor, it means that $a1$ divides n, and since n is a prime, the latter equation yields that $(a1)^2$ divides the second last term $(n(n-1)/2)abx^{n-2}$. It follows that $(a1)^2$ divides n, which contradicts the fact that n is prime. For the second case, if a^* is a factor of a^{n-2} that occurs with a higher power in a^{n-2} than in b, then Equation (17) will yield that $(a^*)^2$ divides n, again contradicting the fact that n is prime.

Now consider the case where a^{n-2} divides b. Then $b = a^{n-2}a1$ for some positive integer$a1$, and since b divides a^{n-1}, this means that $a1$ is a factor of a. Let $a2$ be the positive integer such $a = a1a2$. It will be shown that $a2 = n$. The equations $a^n c^n = (ab)^n + n(ab)^{n-1}x + \cdots + (n(n-1)/2)(ab)^2x^{n-2} + n(ab)x^{n-1}$ and $b = a^{n-2}a1$ yield that

$$a^n c^n = (a^{n-1}a1)^n + n(a^{n-1}a1)^{n-1}x + \cdots + (n(n-1))2)(a^{n-1}a1)\text{^}2x^{n-2} + n(a^{n-1}a1)x^{n-1}. \quad (18)$$

Since the left hand side of the equation is divisible by a^n, so is the right hand. In particular, a^n divides the last term of the sum on the right, and since a and x cannot have a common factor, this implies that $a = (a1)n$. From $a = a1a2$, it follows that $a2 = n$, and so if both sides of Equation (18) are divided by a^n, it is obtained that a divides $c^n - x^{n-1}$. Since n divides a, this means that n divides $c^n - x^{n-1}$. Writing $c^n - x^{n-1} = c^n - x^{n-1} + 1 - 1$ and using the fact that a divides $x - 1$, it is deduced that n divides $c^n - 1$. Since n divides $x - 1, p + 1$ and$y + 1$, adding each of these quantities to $c^n - 1$ yields that n divides $c^n + x - 2$, $c^n + p$ and $c^n + y$. Let $k1, k2, k3$ and $k4$ be positive integers such that $c^n - 1 = (k1)n$, $c^n + x - 2 = (k2)n$, $c^n + p = (k3)n$ and $c^n + y = (k4)n$. Note that $z = y + 1 = c^n + y - (c^n - 1) = (k4 - k1)n$ and $z = p + x = (k2 + k3)n + 2 - 2c^n = (k2 + k3 - 2k1)n$, from which it follows that

$$k4 = k2 + k3 - k1. \quad (19)$$

It is also easy to check that $p + 1 = (k3 - k1)n = ad1$ and $x - 1 = (k2 - k1)n = ad2$, from which it follows that

$$(k2 - k1)d1 = (k3 - k1)d2. \quad (20)$$

Equations (19) and (20) then yield that $(k4 - k3)d1 = (k3 - k1)d2$, which may be written as $(k4 - k3)d1 = (k3 - k1 + k4 - k4)d2 = (k3 - k4)d2 + (k4 - k1)$.
Using $c = d1 + d2$, the latter equation can be rearranged as $(k4 - k3)c = (k4 - k1)d2$. Multiplying both sides of this equation by a and using $ac = z = y + 1$ and $ad2 = y - p$ produces $(k4 - k3)y + k4 - k3 = (y - p)(k4 - k1)$. Collecting like terms, this becomes $(k3 - k1)y = (k4 - k1)p + k4 - k1$. Writing this equation as $(k3 - k1)y = (k4 - k1)p + k4 - k3 + k3 - k1$ and then rearranging leads to the equation $(k3 - k1)(y + 1) = (k4 - k1)(p + 1)$. It follows from $y + 1 = z = x + p$ that $(k3 - k1)(p + x) = (k4 - k1)(p + 1)$, and the latter equation may be written as $(k4 - k3)(p + 1) = (k3 - k1)(x - 1)$. In the light of Equation (19), this becomes $(k4 - k3)(p + 1) = (k4 - k2)(x - 1)$, which may be written as

$$k1 + (k2)x + (k4)(p + 1) = (k3)p + (k4)x. \quad (21)$$

Now, from $c^n + y = (k4)n$ and $p + 1 = (k3 - k1)n$, Equation (21) may be written as $k1 + (k2)x + (k3 - k1)(c^n + y) = (k3)p + (k4)x$, which on rearrangement becomes $(c^n + y - 1)k1 + (k4 - k2)x = (c^n + y - p)k3$. Since $k4 - k2 = k3 - k1$ by Equation (19), it follows that $(c^n + y - x - 1)k1 = (c^n + y - x - p)k3$, or $(k3 - k1)(c^n + y - x) = k3p - k1$. The latter equation may be written as $(k3 - k1)(c^n + y - x) = (k3)p - k1 - k3 + k3$, which becomes $(k3 - k1)(c^n + y - x - 1) = (p - 1)k3$. Writing this equation as $(k3 - k1)(c^n + y - x - 1) = (p + 1 - 2)k3 = (p + 1)k3 - 2(k3)$ and using $p + 1 = (k3 - k1)n$ yields that $(k3 - k1)((k3)n + x - c^n - y + 1) = 2(k3)$. Since $p = (k3)n - c^n$ and $y - x = p - 1$, it follows that $2(k3 - k1) = 2(k3)$, that is, $k3 - k1 = k3$. This means that $k1 = 0$, and so $c = 1$, which leads to a contradiction. It is therefore concluded that the case where a^{n-2} divides b fails, and since the case where a^{n-2} does not divide b also fails, the result is proved.

Corollary 3.5

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

Proof. By Theorem 3.4, there are no positive integers x, y and z such that $z^n = x^n + y^n$ holds for any prime $n > 9$, and hence for any positive odd integer $n > 9$. Now suppose that $n > 9$ is even and that $z^n = x^n + y^n$ holds. If n has an odd factor m, then $n = 2^j m$, for a positive integer $j \geq 1$. Then $z^n = x^n + y^n$ becomes $\left(z^{2^j}\right)^m = \left(y^{2^j}\right)^m + \left(x^{2^j}\right)^m$, which does not hold because m is odd and $z^{2^j}, y^{2^j}, x^{2^j}$ are positive integers. If n has no odd factor, then it can be written

as $n = 2^i$, where $i > 3$. Then equation $z^n = x^n + y^n$ is then written as $\left(z^{2^j}\right)^4 = \left(y^{2^j}\right)^4 + \left(x^{2^j}\right)^4$, where $i = j + 2$ and $j \geq 1$. Again, this does not hold because z^{2^j}, y^{2^j} and x^{2^j} are positive integers and it is well known that Equation (1) does not hold for $n = 4$.

4. Discussion

Note that the proofs of Lemma 3.1, 3.2, 3.3, Theorem 3.4 and Corollary 3.5 still hold for any odd $n > 3$. The assumption that $n > 9$ is made only to align with the fact that the cases of odd $n \leq 9$ have already been dealt with by the various authors.

5. Conclusions

This paper deals with the general problem of finding an elementary proof of FLT. As is outlined in Section 1, several elementary partial proofs of FLT have been established over the years by various authors. In this work, another elementary partial proof of FLT has been established, which may not necessarily be viewed as complementary to the ones outlined in Section 1 as it is of a different nature.

Since the partial proof of FLT in this work, which is Corollary 3.5, asserts that there are no positive integers x, y, z satisfying the equation $z^n = x^n + y^n$ for any positive integer $n > 9$, where $p = z - x$ does not divide y and $q = z - y = 1$, the remaining gap to show that there are no positive integers x, y, z satisfying the equation $z^n = x^n + y^n$ for any positive integer $n > 9$, which we recommend for future research, is to show that there are no positive integers x, y, z satisfying the equation $z^n = x^n + y^n$ for any positive integer $n > 9$, where $p = z - x$ does not divide y and $q = z - y > 1$; or p divides y and $q \geq 1$. Together with the fact that elementary proofs of FLT are known for $n \leq 9$, this would then complete an elementary proof of FLT.

ORCID

0000-0001-7192-3169

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Albert, A. A., *Modern Higher Algebra*, Cambridge University Press, 1938.

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

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

[4] Grosswald, E., *Topics from the Theory of Numbers*, Macmillan, New York, 1965.

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

[6] Lenstra, H. W., Jr., Euclidean Number Fields 1, *Math. Intelligencer* 1979, 2, 6-15.

[7] Long, C. T., *Elementary Introduction to Number Theory*, D. C. Heath and Company, 1972.

[8] Maeda, Y., *Modularity of special cycles on unitary Shimura varieties over CM-fields,* Acta Arithmetica 2022, 204(1), 1-18.

[9] Mahoney, M. S., *The Mathematical Career of Pierre de Fermat, 1601-1665*, (2nd ed.), Princeton University Press, 1994.

[10] McLarty, C., *The large structures of Grothendieck founded on finite order arithmetic*, Rev. Symb. Log. 2020, 13(2), 296-325.

[11] Ribet, K., Galois Representations and Modular Forms, *Bulletin of AMS* 1995, 32, 375-402.

[12] Ribenboim, P., *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.

[13] Singh, S. *Fermat's Last Theorem*. Notting Hill: Fourth Estate; 1997.

[14] Taylor, R., Wiles, A., Ring-Theoretic Properties of Certain Hecke Algebras, *Ann. Of Math*. 1995, 141, 553-572.

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

[16] Washington, L., *An Introduction to Cyclotomic Fields*, 2nd ed., Springer-Verlag, New York, 1997.

[17] Wiles, A. Modular elliptic curves and Fermat's Last Theorem. *Ann. Of Math*. 1995, 141, 443-551.

[18] Zhang, S., *On a comparison of Cassels pairings of different elliptic curves*, Acta Arithmetica 2023, 211(1), 1-23.