n=4 Case of Fermat's Last Theorem

Anthony Dokanchi

August 21, 2023

1 Fermat's Last Theorem

1.1 Overview

Fermat's Last Theorem states that there are no natural numbers a, b, c, n that satisfy $a^n + b^n = c^n$ and $n > 2$.

For $n = 0$, the equation simply reads $a + b = c$ which trivially has solutions. For $n = 1$, the equation takes the familiar form $a^2 + b^2 = c^2$, which has been long known to have infinitely many solutions.

However, for values of n greater than 2, no solutions have been found, and in the 1990s, it was shown that no solutions exist.

1.2 Cases

Using the property of exponents $x^a b = (x^a)^b$, it can be easily shown that many values of n are redundant cases. For example, any a, b, c that satisfy $a^6 + b^6 = c^6$ must also satisfy both $(a^3)^2 + (b^3)^2 = (c^3)^2$ and $(a^2)^3 + (b^2)^3 = (c^2)^3$. In general, for any $k = pq$, any a, b, c that satisfy $a^k + b^k = c^k$ must also satisfy both $(a^p)^q + (b^p)^q = (c^p)^q$ and $(a^q)^p + (b^q)^p = (c^q)^p$. Thus, for any value of n to have integer solutions, there must also exist integer solutions for all factors of that n. Therefore, to prove Fermat's Last Theorem, it suffices to prove that there are no integer solutions in the cases where n is equal to either 4 or any odd prime.

2 Euclid's Formula for Pythagorean Triples

Lemma 1. *For any primitive triple a, b, c, one of a, b must be even and the other must be odd. Consequently, c must also be odd.*

Proof. If a, b are both even, then $a^2 + b^2$ is also even, which forces c to be even. This contradicts our assumption that the triple is primitive.

If a, b are both odd, then $a^2 + b^2$ is also even, which forces c to be even. Thus, a, b, c can be written in the forms $a = 2x + 1, b = 2y + 1, c = 2z$. We obtain the following equations:

$$(2x + 1)^2 + (2y + 1)^2 = (2z)^2$$

$$4x^2 + 4x + 4y^2 + 4y + 2 = 4z^2$$
$$2x^2 + 2x + 2y^2 + 2y + 1 = 2z^2$$
$$2(x^2 + x + y^2 + y) + 1 = 2(z^2)$$

The LHS of the equation produces an odd number, while the RHS produces an even number. Thus, we arrive at a contradiction. This means that a, b cannot both be odd in a Pythagorean triple.

Therefore, in a Pythagorean triple, a, b cannot have the same parity, so one must be even and one must be odd.

QED

Lemma 2. *If natural numbers a, b, c form a Pythagorean triple, then a, b take the form $p^2 - q^2, 2pq, with c = p^2 + q^2$ for natural numbers p, q with $(p, q) = 1$, and one of p, q is odd while the other is even.*

Proof. Since $c > a$, it can be written in the form $c = a + \frac{bq}{p}$ with relatively prime p, q. From the equation $a^2 + b^2 = c^2$, we get the following identities:

$$a^2 + b^2 = (a + \frac{bq}{p})^2 \implies a^2 + b^2 = a^2 + \frac{2abq}{p} + \frac{b^2q^2}{p^2}$$
$$\implies b^2 = \frac{2abq}{p} + \frac{b^2q^2}{p^2} \implies b = \frac{2aq}{p} + \frac{bq^2}{p^2}$$
$$bp^2 = 2apq + bq^2 \implies (a)(2pq) = (b)(p^2 - q^2)$$
$$\therefore \frac{a}{b} = \frac{p^2 - q^2}{2pq}$$

Since p and q were defined to be relatively prime, $p - \frac{q^2}{p}$ is not an integer, so $p^2 - q^2$ is not divisible by p. The same reasoning shows that $p^2 - q^2$ is not divisible by q. Thus, the only factors that can be shared between $p^2 - q^2$ and $2pq$ are 1 and 1.

If $p^2 - q^2$ shares no common factor with $2pq$ other than 1, which occurs if one of p, q is even while the other is odd, then the previous identity forces $a = p^2 - q^2$ and $b = 2pq$.

If $p^2 - q^2$ shares the common factor 2 with $2pq$, then it is possible that a, b, c take the form $a = \frac{p^2-q^2}{2}, b = pq$. In this case, p and q must be both even or both odd. They cannot both be even because that would contradict the definition that p and q are relatively prime, so p and q are odd. We can then define $2r = p + q$ and $2s = p - q$, which causes:

$$a = \frac{p^2 - q^2}{2} = \frac{(p+q)(p-q)}{2} = \frac{(2r)(2s)}{2} = 2rs$$

$$b = pq = \frac{1}{4}(4pq) = \frac{1}{4}(p^2 + 2pq + q^2 - p^2 + 2pq - q^2)$$

$$= \frac{1}{4}(p^2 + 2pq + q^2) - \frac{1}{4}(p^2) - 2pq + q^2 = (\frac{p+q}{2})^2 - (\frac{p-q}{2})^2 = r^2 - s^2$$

Since $a = 2rs$ is odd, $b = r^2 - s^2$ must be even. Therefore, r and s must have opposite parity. Thus, in all cases, a and b take the forms $p^2 - q^2$ and $2pq$.

QED

3 Proof for n=4

Theorem 3. *The equation $a^4 + b^4 = c^4$ has no solutions for natural a, b, c.*

Proof. Any a, b, c that satisfy $a^4 + b^4 = c^4$ also satisfy $a^4 + b^4 = (c^2)^2$. Thus, it suffices to show that the equation $a^4 + b^4 = c^2$ has no solutions for natural a, b, c (and in fact, this is a stronger version of that problem).

We will assume that there exist values of a, b, c that satisfy the above equation, and that $(a, b) = 1$. Lemma 2 allows us to write those variables in this form:

$$a^2 = p^2 - q^2$$

$$b^2 = 2pq$$

where a is odd, b is even, $(p,q)=1$, and one of p,q is even while the other is odd.

The first equation can be written as $a^2+q^2=p^2$, which means a,q,p form a Pythagorean triple. We know that a is odd, which forces q even and p odd.

Since $2pq$ is equal to a square, and $(p,q)=1$, $2q$ and p must both be square. We can define $r^2=p$

Since $p^2-q^2=a^2$, we can write p,q in the forms:

$$p=m^2+n^2$$

$$q=2mn$$

for relatively prime m,n with one even and one odd.

Since $2q=4mn$ is equal to a square, mn must be square. Since $(m,n)=1$, both m and n must be square. Therefore we can set

$$m=x^2$$

$$n=y^2$$

which creates the identity

$$r^2=p=m^2+n^2=x^4+y^4$$

Since $x^4+y^4=r^2$, we have generated a new solution to the equation $a^4+b^4=c^2$

We can write the following identities relating a to x and b to y:

$$a=\sqrt{p^2-q^2}=\sqrt{(m^2+n^2)^2-(2mn)^2}=\sqrt{(m^2-n^2)^2}=m^2-n^2=x^4-y^4=(x^2+y^2)(x^2-y^2)$$

$$\therefore a\geq x^2+y^2 \implies a>x^2 \implies a>x$$

$$\therefore a>x$$

also:

$$b=\sqrt{2pq}=\sqrt{2p(2mn)}=\sqrt{4mnp}=\sqrt{2^2x^2y^2p}=2xy\sqrt{p}$$

$$\therefore b>y$$

Thus, we have shown that if there exist natural a,b where a^4+b^4 is square, it is possible to generate natural $x<a$ and $y<b$ where x^4+y^4

is also square. But this process can be repeated an arbitrary number of times, which implies that there exist natural numbers arbitrarily small. This contradicts the well-ordering property of the natural numbers.

Thus, there do not exist natural values of a, b such that a^4+b^4 is a square. Therefore, there are no integer solutions to $a^4 + b^4 = c^4$

QED

4 Summary

This paper has presented a comprehensive proof that Fermat's Last Theorem holds for n=4. It has done so by showing that any solutions must take a certain form and the existence of a solution would imply the generation of an infinitely long string of strictly decreasing positive integers, a logical impossibility. Thus, one of the cases of Fermat's Last Theorem has been resolved, and our focus shifts to the cases of odd prime values of n.