The Equation $X^4 + Y^4 = Z^2$ Revisited

Jovan Mikić [1]

J. U. SŠC "Jovan Cvijić", Modriča 74480, *Bosnia and Herzegovina*

Abstract

We give another proof that the equation $X^4+Y^4 = Z^2$ has no solutions in positive integers. We use the fact that the equation $X^4+Y^4 = Z^2$ is equivalent to the equation $(X^2+Y^2+Z)(X^2+Y^2-Z) = (-X^2+Y^2+Z)(X^2-Y^2+Z)$. This proof proves the Fermat Last Theorem for the case $n = 4$.

1 Introduction

The Fermat Last Theorem is one of the hardest problems in mathematics. French mathematician, Pierre Fermat formulated his famous theorem in 1637. Theorem states that, for any positive integer $n > 2$, the equation $X^n + Y^n = Z^n$ has no solutions in positive integers.

Fermat claimed that he had a remarkable proof, but a margin on the paper was so small to contain his proof. The Fermat Last Theorem is finally proved by British mathematician Andrew Wiles [7] in 1995, after 358 years of effort by mathematicians.

The Fermat Last Theorem stimulated the development of the algebraic number theory in the 19th century and the proof of the modularity theorem in the 20th century [6].

However, the case $n = 4$ of the Fermat Last Theorem is considered as the easiest case of this theorem. Fermat was the first [2] who gave a proof of the Fermat Last Theorem for the case $n = 4$. Actually, Fermat showed that right triangle whose sides are integers cannot have its area equals to the square of an integer. Fermat used a method of infinity descent and the parametrization of the Pitagora primitive triplets.

After Fermat, many other mathematicians including Euler [1], Leqendre [5], Lebesque [4] and Hilbert [3] gave a proof of the Fermat Last Theorem for the case $n = 4$. See also [8]. Until now, in total, there are 21 proofs for the case $n = 4$.

We want to prove the Fermat Last Theorem for the case $n = 4$.

We consider the equation

$$X^4 + Y^4 = Z^2 \ ; \tag{1}$$

where X, Y, Z are positive integers.

[1] *E-mail address*: jnmikic@gmail.com

Obviously, if the equation

$$X^4 + Y^4 = Z^4 \tag{2}$$

has solutions in positive integers, than the Eq. (1) also has solutions in positive integers.

Our main theorem is:

Theorem 1. *The Eq. (1) has no solutions in positive integers.*

By contradiction, the Theorem (1) implies that the Eq. (2) has no solutions in positive integers. In other words, a proof of the Theorem (1) is also a proof of the Fermat Last Theorem for the case $n = 4$.

We give a proof of the Theorem (1) by using a method of a contradiction and the fact that the Eq. (1) is equivalent to the equation

$$(X^2 + Y^2 + Z)(X^2 + Y^2 - Z) = (-X^2 + Y^2 + Z)(X^2 - Y^2 + Z). \tag{3}$$

We do not use a well-known parametrization formula for the Pitagora primitive triplets.

2 Notation

Let a, b, and c be integers. We let (a, b) denote the greatest common divisor of a and b. Further, we let $a \equiv b \pmod{c}$ denote a is congruent with b modulo c. Finally, we let LHS denote left hand side; we let RHS denote right hand side.

3 The Proof of the Theorem (1)

We give a proof by a contradiction.

Let us assume that the Eq. (1) has a solution in positive integers, say (X, Y, Z).

Without loss of generality, we may assume that $(X, Y) = 1$, X is even, and Y is odd. Then Z is also odd.

Further, we may assume that a solution (X, Y, Z) of the Eq. (1) is a solution with smallest Z. In other words, if (A, B, C) is any triplet with positive integers such that $C < Z$, then (A, B, C) is not a solution of the Eq. (1).

Let us show that the Eq. (1) implies the Eq. (3).

The LHS of the Eq. (3) becomes, as follows:

$$\begin{aligned}(X^2 + Y^2 + Z)(X^2 + Y^2 - Z) &= (X^2 + Y^2)^2 - Z^2 \\ &= X^4 + 2X^2Y^2 + Y^4 - Z^2 \\ &= 2X^2Y^2\end{aligned}$$

So, the equation

$$(X^2 + Y^2 + Z)(X^2 + Y^2 - Z) = 2X^2Y^2 \tag{4}$$

holds.

Further, the RHS of the Eq. (3) becomes, as follows:

$$\begin{aligned}(-X^2+Y^2+Z)(X^2-Y^2+Z) &= (Z+(Y^2-X^2))(Z-(Y^2-X^2)) \\ &= Z^2-(Y^2-X^2)^2 \\ &= Z^2-(Y^4-2X^2Y^2+X^4) \\ &= Z^2-X^4-Y^4+2X^2Y^2 \\ &= 2X^2Y^2\end{aligned}$$

So, the equation

$$(-X^2+Y^2+Z)(X^2-Y^2+Z) = 2X^2Y^2 \tag{5}$$

holds.

By Eqns. (4) and (5), we conclude that

$$(X^2+Y^2+Z)(X^2+Y^2-Z) = (-X^2+Y^2+Z)(X^2-Y^2+Z).$$

Therefore, the Eq. (1) implies the Eq. (3).

Similarly, we can prove that the Eq. (3) implies the Eq. (1). So, Eqns. (1) and (3) are equivalent.

Let us consider the Eq. (3).

Our proof consists of two parts: $Z \equiv -1 \pmod 4$ and $Z \equiv 1 \pmod 4$.

4 The First Case

Proof. We assume that $Z \equiv -1 \pmod 4$.

We consider numbers on the LHS of the Eq. (3). We introduce the first substitution, as follows:

$$X^2+Y^2+Z = 4M \tag{4.6}$$
$$X^2+Y^2-Z = 2N\,; \tag{4.7}$$

where M and N are positive integers, and N is odd.

From the Eqns. (4.6) and (4.7), we obtain that:

$$X^2+Y^2 = 2M+N \tag{4.8}$$
$$Z = 2M-N\,. \tag{4.9}$$

We assert that $(M,N)=1$.

Let us suppose that $(M, N) > 1$. Then exists a prime number p such that p divide (M, N). The number p must be odd, because N is odd. By the Eq. (4.9), p must divide Z . Let us consider the Eq. (4). The LHS of the Eq. (4) is $8MN$. So, p divide LHS of the Eq. (4). It follows that p must divide RHS of the Eq. (4); p must divide $2X^2Y^2$. Since p is odd, p must divide X^2Y^2. Further, since p is a prime number, p must divide X or Y.

We know that p divide Z. If p divide X, then by the Eq. (1), p must divide Y. It follows that $(X, Y) > 1$. A contradiction! Same argument holds, if p divide Y. Therefore, we conclude that presumption $(M, N) > 1$ is false.

Hence, $(M, N) = 1$.

From the Eq. (4.8), it follows that:

$$X^2 = 2M + N - Y^2 \tag{4.10}$$

By Eqns. (4.6),(4.7), (4.9), and (4.10), the Eq. (3) becomes, as follows:

$$\begin{aligned}
8MN &= (-(2M + N - Y^2) + Y^2 + (2M - N))((2M + N - Y^2) - Y^2 + (2M - N)) \\
8MN &= (-2N + 2Y^2)(4M - 2Y^2) \\
2MN &= (Y^2 - N)(2M - Y^2)\,.
\end{aligned}$$

The last equation above, becomes

$$MN = \frac{Y^2 - N}{2} \cdot (2M - Y^2) \tag{4.11}$$

We introduce the second substitution, as follows:

$$2M - Y^2 = K; \tag{4.12}$$

$$\frac{Y^2 - N}{2} = L, \tag{4.13}$$

where K and L are positive integers, and K is odd.

Then the Eq. (4.11) becomes

$$MN = KL. \tag{4.14}$$

After we eliminate the term Y^2 from Eqns. (4.12) and (4.13), we get

$$2M - N = K + 2L. \tag{4.15}$$

From the fact that $(M, N) = 1$ and from Eqns (4.14) and (4.15), it can be shown that $(K, L) = 1$.

Now, we eliminate M from Eqns (4.14) and (4.15).

We have

$$
\begin{aligned}
N &= 2M - K - 2L && \text{(by the Eq. (4.15))}\\
N^2 &= 2MN - (K+2L)N && \text{(multiplication by } N\text{)}\\
N^2 &= 2KL - (K+2L)N && \text{(by the Eq. 4.14)}\\
N^2 + N(K+2L) &= 2KL\\
4N^2 + 4N(K+2L) &= 8KL\\
(2N)^2 + 2(2N)(K+2L) + (K+2L)^2 &= 8KL + (K+2L)^2\\
(2N+K+2L)^2 &= 4L^2 + 12KL + K^2\\
(2N+K+2L)^2 &= (2L+3K)^2 - 8K^2
\end{aligned}
$$

From the last equation above, we obtain that

$$
\begin{aligned}
8K^2 &= (2L+3K)^2 - (2N+K+2L)^2\\
8K^2 &= (2N+4K+4L)(2K-2N)\\
K^2 &= \frac{K-N}{2}\cdot(N+2K+2L) && (K \text{ and } N \text{ are odd}) \qquad (4.16)
\end{aligned}
$$

We assert that $(\frac{K-N}{2}, N+2K+2L) = 1$.

Let us suppose that $(\frac{K-N}{2}, N+2K+2L) > 1$. Then must exist a prime number p such that p divides $\frac{K-N}{2}$ and p divides $N+2K+2L$. Clearly, p must divide $K-N$. By the Eq. (4.16) and the fact that p is a prime, it follows that p divides K. The number p is odd, because K is odd. It follows that p must divide N and $2L$. Since p is odd, p must divide L. We obtain that p must divide both K and L. This implies that $(K, L) > 1$. A contradiction!

Hence, we conclude that $(\frac{K-N}{2}, N+2K+2L) = 1$.

We introduce the third substitution, as follows:

$$\frac{K-N}{2} = V^2, \qquad (4.17)$$

$$N + 2K + 2L = U^2; \qquad (4.18)$$

where U and V are positive integers and $(U, V) = 1$.

Now, we can express all numbers X,Y, Z, M, N, K, and L by numbers U and V.

We start with K.

From the Eq. (4.16), it follows that

$$K = UV. \qquad (4.19)$$

From the Eq. (4.19) and the fact that K is odd, it follows that both U and V are odd.

From Eqns. (4.17) and (4.19), we obtain that

$$N = V(U - 2V). \qquad (4.20)$$

Then, by Eqns. (4.18), (4.19), and (4.20), after short calculation, we obtain that

$$2L = (U - V)(U - 2V). \tag{4.21}$$

By Eqns. (4.15), (4.19), (4.20), and (4.21), after short calculation, we have that

$$2M = U(U - V). \tag{4.22}$$

By Eqns. (4.12), (4.19), and (4.22), we get

$$Y^2 = (U - 2V)U. \tag{4.23}$$

By Eqns. (4.10), (4.20), (4.22), and (4.23), we get

$$X^2 = 2(U - V)V. \tag{4.24}$$

Similarly, by Eqns.(4.9), (4.20), and (4.22), we obtain that

$$\begin{aligned} Z &= U^2 - 2UV + 2V^2 \text{ , or} \\ Z &= (U - V)^2 + V^2. \end{aligned} \tag{4.25}$$

Equations (4.23), (4.24), and (4.25) give the parametrization formula for the primitive solution (X, Y, Z) of the Eq. (1). Let us show that Eqns. (4.23) and (4.24) cannot be both true.

Let us consider the Eq. (4.23). Facts $(U, V) = 1$ and V is odd, imply that $(U-2V, U) = 1$. Then we have:

$$U = U_1^2, \tag{4.26}$$

$$U - 2V = S_1^2; \tag{4.27}$$

where U_1 and S_1 are positive odd integers and $(U_1, S_1) = 1$.

Now, let us consider the Eq. (4.24). Facts $(U, V) = 1$ and V is odd, imply that $(2(U - V), V) = 1$. Then we have:

$$V = V_1^2, \tag{4.28}$$

$$2(U - V) = T^2; \tag{4.29}$$

where V_1 and T are positive integers, V_1 is odd, T is even and $(V_1, T) = 1$.

Since T is even, we may write $T = 2T_1$; where T_1 is a positive integer. Then the Eq. (4.29) becomes

$$\begin{aligned} 2(U - V) &= 4T_1^2, \text{ or} \\ U - V &= 2T_1^2. \end{aligned} \tag{4.30}$$

By Eqns. (4.26) and (4.28), the Eq. (4.27) becomes

$$U_1^2 - 2V_1^2 = S_1^2 \tag{4.31}$$

By Eqns. (4.26) and (4.28), the Eq. (4.30) becomes

$$U_1^2 - V_1^2 = 2T_1^2 \tag{4.32}$$

We look at Eqns (4.31) and (4.32). Let us eliminate the term V_1^2 from these two equations. We obtain the equation

$$U_1^2 + S_1^2 = 4T_1^2. \tag{4.33}$$

Obviously, RHS of the Eq. (4.33) is divisible by 4. Recall that U_1 and S_1 are odd positive integers. Then it must be $U_1^2 \equiv 1 \pmod 4$ and $S_1^2 \equiv 1 \pmod 4$. It follows that $U_1^2 + S_1^2 \equiv 2 \pmod 4$. So, LHS of the Eq. (4.33) is not divisible by 4. A contradiction!

Therefore, Eqns. (4.23) and (4.24) cannot be both true, at the same time.

We conclude that, if $Z \equiv -1 \pmod 4$, then the Eq. (1) has no solutions.

This proves the first case. □

5 The Second Case

Proof. We assume that $Z \equiv 1 \pmod 4$.

The proof of the second case is similar to the proof of the first case. However, the second case is a little bit harder.

Again, we consider numbers on the LHS of the Eq. (3). We introduce the first substitution, as follows:

$$X^2 + Y^2 + Z = 2M \tag{5.6}$$
$$X^2 + Y^2 - Z = 4N\,; \tag{5.7}$$

where M and N are positive integers, and M is odd.

From the Eqns. (5.6) and (5.7), we obtain that:

$$X^2 + Y^2 = M + 2N \tag{5.8}$$
$$Z = M - 2N\,. \tag{5.9}$$

Similarly, as in the first case, we conclude that $(M, N) = 1$.

From the Eq. (5.8), it follows that:

$$X^2 = M + 2N - Y^2 \tag{5.10}$$

By Eqns. (5.6),(5.7), (5.9), and (5.10), the Eq. (3) becomes, as follows:

$$8MN = (-(M + 2N - Y^2) + Y^2 + (M - 2N))((M + 2N - Y^2) - Y^2 + (M - 2N))$$
$$8MN = (2Y^2 - 4N)(2M - 2Y^2)$$
$$2MN = (Y^2 - 2N)(M - Y^2)\,.$$

The last equation above, becomes

$$MN = (Y^2 - 2N) \cdot \frac{M - Y^2}{2} \tag{5.11}$$

We introduce the second substitution, as follows:

$$Y^2 - 2N = K; \tag{5.12}$$
$$\frac{M - Y^2}{2} = L, \tag{5.13}$$

where K and L are positive integers, and K is odd.

Then the Eq. (5.11) becomes

$$MN = KL. \tag{5.14}$$

After we eliminate the term Y^2 from Eqns. (5.12) and (5.13), we get

$$M - 2N = K + 2L. \tag{5.15}$$

From the fact that $(M, N) = 1$ and from Eqns (5.14) and (5.15), it can be shown that $(K, L) = 1$.

Now, we eliminate N from Eqns (5.14) and (5.15).

We have

$$\begin{aligned}
M &= 2N + K + 2L && \text{(by the Eq. (5.15))}\\
M^2 &= 2MN + (K + 2L)M && \text{(multiplication by } M\text{)}\\
M^2 &= 2KL + (K + 2L)M && \text{(by the Eq. 5.14)}\\
M^2 - M(K + 2L) &= 2KL\\
4M^2 - 4M(K + 2L) &= 8KL\\
(2M)^2 - 2(2M)(K + 2L) + (K + 2L)^2 &= 8KL + (K + 2L)^2\\
(2M - K - 2L)^2 &= 4L^2 + 12KL + K^2\\
(2M - K - 2L)^2 &= (2L + 3K)^2 - 8K^2
\end{aligned}$$

From the last equation above, we obtain that

$$8K^2 = (2L + 3K)^2 - (2M - K - 2L)^2$$
$$8K^2 = (4K + 4L - 2M)(2K + 2M)$$
$$K^2 = \frac{K + M}{2} \cdot (2L + 2K - M) \qquad (K \text{ and } M \text{ are odd}) \tag{5.16}$$

As before, we can conclude that $(\frac{K+M}{2}, 2L+2K-M)=1$.

We introduce the third substitution, as follows:

$$\frac{K+M}{2} = V^2, \tag{5.17}$$

$$2L+2K-M = U^2; \tag{5.18}$$

where U and V are positive integers and $(U,V)=1$.

Again, we can express all numbers X,Y, Z, M, N, K, and L by numbers U and V.

From the Eq. (5.16), it follows that

$$K = UV. \tag{5.19}$$

From the Eq. (5.19) and the fact that K is odd, it follows that both U and V are odd.

From Eqns. (5.17) and (5.19), we obtain that

$$M = V(2V-U). \tag{5.20}$$

Then, by Eqns. (5.18), (5.19), and (5.20), after short calculation, we obtain that

$$2L = (V-U)(2V-U). \tag{5.21}$$

By Eqns. (5.15), (5.19), (5.20), and (5.21), after short calculation, we have that

$$2N = U(V-U). \tag{5.22}$$

By Eqns. (5.12), (5.19), and (5.22), we get

$$Y^2 = (2V-U)U. \tag{5.23}$$

By Eqns. (5.10), (5.20), (5.22), and (5.23), we get

$$X^2 = 2(V-U)V. \tag{5.24}$$

Similarly, by Eqns. (5.9), (5.20), and (5.22), we obtain that

$$Z = (V-U)^2 + V^2. \tag{5.25}$$

Equations (5.23), (5.24), and (5.25) give the parametrization formula for the primitive solution (X,Y,Z) of the Eq. (1). Let us show that Eqns. (5.23) and (5.24) cannot be both true.

Let us consider the Eq. (5.23). Facts $(U,V)=1$ and V is odd, imply that $(2V-U,U)=1$. Then we have:

$$U = U_1^2, \tag{5.26}$$

$$2V-U = S_1^2; \tag{5.27}$$

where U_1 and S_1 are positive odd integers and $(U_1, S_1) = 1$.

Now, let us consider the Eq. (5.24). Facts $(U, V) = 1$ and V is odd, imply that $(2(V - U), V) = 1$. Then we have:

$$V = V_1^2, \tag{5.28}$$
$$2(V - U) = T^2; \tag{5.29}$$

where V_1 and T are positive integers, V_1 is odd, T is even and $(V_1, T) = 1$.

Since T is even, we may write $T = 2T_1$; where T_1 is a positive integer. Then the Eq. (5.29) becomes

$$2(V - U) = 4T_1^2, \text{ or}$$
$$V - U = 2T_1^2. \tag{5.30}$$

By Eqns. (5.26) and (5.28), the Eq. (5.27) becomes

$$2V_1^2 - U_1^2 = S_1^2 \tag{5.31}$$

By Eqns. (5.26) and (5.28), the Eq. (5.30) becomes

$$V_1^2 - U_1^2 = 2T_1^2 \tag{5.32}$$

We look at Eqns. (5.31) and (5.32). Let us eliminate the term V_1^2 from these two equations. We obtain the equation:

$$U_1^2 = S_1^2 - 4T_1^2. \tag{5.33}$$

We cannot use the same argument as we use at the Eq. (4.33). This makes the second case harder.

We can rewrite the Eq. (5.33) as

$$U_1^2 = (S_1 - 2T_1)(S_1 + 2T_1). \tag{5.34}$$

Recall that U_1 and S_1 are odd and $(U_1, S_1) = 1$. From these facts, it follows that $(S_1 - 2T_1, S_1 - 2T_1) = 1$.

We are forced to introduce the fourth substitution, as follows:

$$S_1 - 2T_1 = P_1^2, \tag{5.35}$$
$$S_1 + 2T_1 = Q_1^2; \tag{5.36}$$

where P_1 and Q_1 are odd positive integers, $Q_1 > P_1$, and $(P_1, Q_1) = 1$.

Now, we want to express all numbers U_1, S_1, T_1 and V_1 by integers P_1 and Q_1.

From Eqns. (5.34), (5.35), and (5.36), after short calculations, we obtain that

$$U_1 = P_1 \cdot Q_1, \tag{5.37}$$

$$S_1 = \frac{Q_1^2 + P_1^2}{2}, \tag{5.38}$$

$$T_1 = \frac{Q_1^2 - P_1^2}{4}. \tag{5.39}$$

Only remains V_1.

Let us consider the Eq. (5.32). By Eqns. (5.37) and (5.39), we have that

$$\begin{aligned} V_1^2 &= U_1^2 + 2T_1^2 \\ &= (P_1 \cdot Q_1)^2 + 2 \cdot (\frac{Q_1^2 - P_1^2}{4})^2 \\ &= P_1^2 \cdot Q_1^2 + 2 \cdot \frac{Q_1^4 - 2Q_1^2 \cdot P_1^2 + P_1^4}{16} \\ &= P_1^2 \cdot Q_1^2 + \frac{Q_1^4 - 2Q_1^2 \cdot P_1^2 + P_1^4}{8} \\ &= \frac{Q_1^4 + 6Q_1^2 \cdot P_1^2 + P_1^4}{8} \end{aligned} \tag{5.40}$$

Then the last Eq. (5.40) becomes, as follows:

$$\begin{aligned} 8V_1^2 &= Q_1^4 + 6Q_1^2 \cdot P_1^2 + P_1^4, \\ 16V_1^2 &= 2(Q_1^4 + 6Q_1^2 \cdot P_1^2 + P_1^4), \\ 16V_1^2 &= (Q_1 + P_1)^4 + (Q_1 - P_1)^4, \text{ or} \\ V_1^2 &= (\frac{Q_1 + P_1}{2})^4 + (\frac{Q_1 - P_1}{2})^4. \end{aligned} \tag{5.41}$$

Recall that P_1 and Q_1 are odd integers, $(P_1, Q_1) = 1$, and $Q_1 > P_1$. Then the Eq. (5.41) implies that a triplet $(\frac{Q_1 - P_1}{2}, \frac{Q_1 + P_1}{2}, V_1)$ is a primitive solution of the Eq. (1).

If we want to find a contradiction, we need to show that $V_1 < Z$.

We make some rough estimates.

From the Eq. (1), it follows that $X^2 < Z$.

Obviously, from the Eq. (5.24), it follows that $X^2 > V$ (because $V > U$).

By the Eq. (5.28), $V = V_1^2$. So, we have: $V_1 <= V_1^2 = V < X^2 < Z$.

Hence, $V_1 < Z$.

We assumed that a triplet (X, Y, Z) is a primitive solution of the Eq. (1) in positive integers, where X is even, Y is odd, and $Z \equiv 1 \pmod 4$. We proved that the Eq. (1) had another primitive solution in positive integers; a triplet $(\frac{Q_1 - P_1}{2}, \frac{Q_1 + P_1}{2}, V_1)$ such that $V_1 < Z$.

A contradiction with the minimality of Z !

This proves the second case.

□

References

[1] L. Euler, *"Theorematum quorundam arithmeticorum demonstrationes"*, Comm. Acad. Sci. Petrop. 10 (1738): 125–146. Reprinted Opera omnia, ser. I, "Commentationes Arithmeticae", vol. I, pp. 38–58, Leipzig:Teubner (1915)

[2] L. Freeman, *"Fermat's One Proof"*. Retrieved 2009-05-23.

[3] D. Hilbert, *"Die Theorie der algebraischen Zahlkörper"*, Jahresbericht der Deutschen Mathematiker-Vereinigung. 4: 175–546., reprinted in 1965 in Gesammelte Abhandlungen, vol. I by New York: Chelsea.

[4] V. A. Lebesque, Introduction à la Théorie des Nombres., Paris: Mallet-Bachelier (1862), pp. 71–73.

[5] A. M. Legendre, Théorie des Nombres (Volume II) (3rd ed.), Paris: Firmin Didot Frères (1830), reprinted in 1955 by A. Blanchard (Paris).

[6] S. Singh, *Fermat's Last Theorem*, 1997.

[7] A. Wiles, *"Modular elliptic curves and Fermat's Last Theorem"*, Annals of Mathematics. 141 (3): pp. 443–551, 1995.

[8] http://math.uga.edu/~pete/4400flt4.pdf