A Concise Proof of Fermat’s Last Theorem

ABSTRACT. This paper offers a concise proof of Fermat’s Last Theorem using the Euclidean algorithm.

1 Introduction

Fermat’s Last Theorem states that no positive integers \( x, y, z \) satisfy \( x^n + y^n = z^n \) for any integer \( n > 2 \). (cf. [1]) This paper will offer a concise proof of this theorem using the Euclidean algorithm.

2 Proof

\[ x^n + y^n = z^n; \quad p: \text{odd prime; } x, y, z: \text{pairwise coprime; } x, y, z \in \mathbb{Z}^+ \text{ (positive integer)} \]  \hspace{1cm} (1)

From (1) it follows that

\[ x^n + y^n = (x + y) f(x, y) = z^n; \quad f(x, y) = x^n + x^{n-2} (-y) + \ldots + (-y)^{n-1}. \]  \hspace{1cm} (2)

Then, according to the polynomial remainder theorem the division of \( f(x, y) \) by \( x + y \) provides a remainder \( R = f(x, -x) = px^{n-1} \). Furthermore, according to the Euclidean algorithm \( x + y, f(x, y) = (x + y, px^{n-1}) = p \) or 1 because \( x + y \) \( x^{n-1} \). Similarly, \( f(z, -x), f(z, -y), f(z, -y), z - y \) = \( p \) or 1, if we let \( z^n - x^n = (z - x) f(z, -x) = y^n, z^n - y^n = (z - y) f(z, -y) = x^n \).

2.1 In the case \((x + y, f(x, y)) = p \)

\( (x + y, f(x, y)) = p \) means \( p \mid z \), because \( (x + y) f(x, y) = z^n \). Similarly, \( (z - x, f(z, -x)) = p \) means \( p \mid y \). If \( p \mid z \) and \( p \mid y \) cannot be satisfied at once, because \( (z, y) = 1 \). Hence, when \( (x + y, f(x, y)) = p \), at least it is required that \((z - x, f(z, -x)) \neq p \) (i.e. \((z - x, f(z, -x)) = 1 \)).

Now, let \( x = x_a y_b, y = y_a y_b \) (where \( x_a, y_b, y_a, y_b \in \mathbb{Z}^+, (x_a, y_b) = 1, (y_a, y_b) = 1, f(z, -x) = y_b^p, f(z, -y) = x_b^p \), then \( z - x, z - y \) can be written as following (3),(4).

\[ z - x = y_a^p \]  \hspace{1cm} (3)

\[ z - y = x_b^p \]  \hspace{1cm} (4)

From (3) and (4) it follows that

\[ x - y = x_a^p - y_a^p, \]  \hspace{1cm} (5)

where \( x - y = x_a x_b - y_a y_b \). Then, according to (2), (5) must be satisfied even if \((x_a, y_a) = k (2 \leq k \in \mathbb{Z}) \).

Hence, \((k x_a) x_b - (k y_a) y_b = (k x_a)^p - (k y_a)^p \), and so \( k = k^p, p = 1 \). This means that \( p \) cannot exist.

2.2 In the case \((x + y, f(x, y)) = 1 \)

Let \( z = z_a z_b \) (where \( z_a, z_b \in \mathbb{Z}^+, (z_a, z_b) = 1 \)), then when \((x + y, f(x, y)) = 1, x + y \) can be written as

\[ x + y = z_a^p. \]  \hspace{1cm} (6)

When \((x + y, f(x, y)) = 1, \) at least it is required that both \((z - x, f(z, -x)) \neq p \) and \((z - y, f(z, -y)) \neq p \) at once. Hence, either (6) and (3), or (6) and (4) must be satisfied at once. Thus, similar to the case 2.1 above, \( p = 1 \). This means that \( p \) cannot exist.

3 Conclusion

Consequently, no positive integers \( x, y, z \) satisfy \( x^p + y^p = z^p \) (where \( l \in \mathbb{Z}^+ \)). Besides, that no positive integers \( x, y, z \) satisfy \( x^2 + y^2 = z^2 \) was proven by Fermat. (1) This means according to the laws of exponents that no positive integers \( x, y, z \) satisfy \( x^2 + y^2 = z^2 \) (where \( 2 \leq m \in \mathbb{Z}^+ \)).

In conclusion, no positive integers \( x, y, z \) satisfy \( x^n + y^n = z^n \) for any integer \( n > 2 \). QED.

References


\footnote{1} Yun, J., Daegu Univ., 712-714, South Korea; jmyun@daegu.ac.kr

\footnote{2} For reference, even if e.g. \((z - x, f(z, -x)) = 1 \), there still exists the possibility of \( p \mid y \), but \( y, z \) must not have the common prime factor \( p \) like any other positive integers.