A Concise Proof of Fermat's Last Theorem[1]

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 offers a concise proof of this theorem using the Euclidean algorithm.

2 Proof

$$x^p + y^p = z^p;\ p\text{: odd prime; } x, y, z\text{: pairwise coprime; } x, y, z \in \mathbb{Z}^+ \text{(positive integer)} \tag{1}$$

From (1) it follows that

$$x^p + y^p = (x+y)f(x,y) = z^p; f(x,y) = x^{p-1} + x^{p-2}(-y) + ... + (-y)^{p-1}. \tag{2}$$

Then, polynomial division of $f(x,y)$ by $x+y$ gives a remainder $r = f(x,-x) = px^{p-1}$. Let $f(x,y) = q(x,y)(x+y) + px^{p-1}$ and $(x+y, f(x,y)) = g$, then $px^{p-1} \mid g$. Hence, according to the Euclidean algorithm $(x+y, f(x,y)) = (x+y, px^{p-1}) = g = p$ or 1 because $x+y \nmid x^{p-1}$. Similarly, $(f(z,-x), z-x), (f(z,-y), z-y) = p$ or 1, if we let $z^p - x^p = (z-x)f(z,-x) = y^p, z^p - y^p = (z-y)f(z,-y) = x^p$.

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

$(x+y, f(x,y)) = p$ means $p \mid z$, because $(x+y)f(x,y) = z^p$. Similarly, $(z-x, f(z,-x)) = p$ means $p \mid y$. $p \mid z$ 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. $(z-x, f(z,-x)) = 1$).[2] For the same reason, when $(x+y, f(x,y)) = p$, at least it is required that $(z-y, f(z,-y)) \neq p$ (i.e. $(z-y, f(z,-y)) = 1$).

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

$$z - x = {y_a}^p \tag{3}$$

$$z - y = {x_a}^p \tag{4}$$

From (3) and (4) it follows that

$$x - y = {x_a}^p - {y_a}^p, \tag{5}$$

where $x - y = x_a x_b - y_a y_b$. ${x_a}^p - {y_a}^p \mid x_a - y_a$. Hence, $x_a x_b - y_a y_b \mid x_a - y_a$. Moreover, $(x_a, y_a) = 1$. It yields $x_b = y_b = 1$ and $p = 1$. 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

$$x + y = {z_a}^p. \tag{6}$$

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 $x^{lp} + y^{lp} = z^{lp}$ (where $l \in \mathbb{Z}^+$). Besides, that no positive integers x, y, z satisfy $x^4 + y^4 = z^4$ was proven by Fermat.([2]) This means according to the laws of exponents that no positive integers x, y, z satisfy $x^{2^m} + y^{2^m} = z^{2^m}$ (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

[1] Wiles, A., Modular elliptic curves and Fermat's Last Theorem, *Ann. Math.* **142**(1995), 443–551.

[2] Freeman, L., Fermat's One Proof, http://fermatslasttheorem.blogspot.kr/, Retrieved 2015-04-18.

[1] Yun, J., Daegu Univ., 712-714, South Korea; jmyun@daegu.ac.kr

[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.