A Proof of Fermat's Last Theorem by Relating to Two Polynomial Identity Conditions

Tae Beom Lee

Abstract: Fermat's Last Theorem(FLT) states that there is no natural number set $\{a, b, c, n\}$ which satisfies $a^n + b^n = c^n$ or $a^n = c^n - b^n$, when $n \geq 3$. In this thesis, we related LHS and RHS of $a^n = c^n - b^n$ to the constant terms of two monic polynomials $f(x) = x^n - a^n$ and $g(x) = x^n - (c^n - b^n)$. By doing so, the conditions to satisfy the number identity, $a^n = c^n - b^n$, are transferred to the conditions to satisfy the polynomial identity, $f(x) = g(x)$, which leads to a trivial solution, $a = c, b = 0$, when $n \geq 3$.

1. Introduction

FLT was inferred in 1637 by Pierre de Fermat, and was proved by Andrew John Wiles [1] in 1995. But the proof is not easy even for mathematicians, requiring more simple proof.

In this thesis, to restrict the freedom of number identity to polynomial identity, we related LHS and RHS of $a^n = c^n - b^n$ to the constant terms of two monic polynomials. Let a, b, c, n be natural numbers, otherwise specified.

$$f(x) = x^n - a^n. \tag{1.1}$$

$$g(x) = x^n - (c^n - b^n). \tag{1.2}$$

We proved that the conditions to satisfy $f(x) = g(x)$ permit only a trivial solution, $a = c, b = 0$, when $n \geq 3$.

2. Fatoring of Constant Terms

Lemma 2.1. Below (2.1) is the irreducible factoring of (1.1) over the complex field [2].

$$f(x) = x^n - a^n = \prod_{k=1}^{n}(x - ae^{\frac{2k\pi i}{n}}). \tag{2.1}$$

$$a^n = \prod_{k=1}^{n} ae^{\frac{2k\pi i}{n}}. \tag{2.2}$$

Proof. The n roots of (1.1) are $ae^{\frac{2k\pi i}{n}}, 1 \leq k \leq n$, so, (2.1) is the irreducible factoring of (1.1) over the complex field. The constant term is the multiplication of n roots, as in (2.2). ■

Lemma 2.2. Below (2.3) is the irreducible factoring of $c^n - b^n$ over the complex field.

$$c^n - b^n = \prod_{k=1}^{n}(ce^{\frac{2k\pi i}{n}} - b). \tag{2.3}$$

Proof. The n roots of $c^n - b^n$ are $b = ce^{\frac{2k\pi i}{n}}, 1 \leq k \leq n$, so, (2.3) is the irreducible factoring of $c^n - b^n$ over the complex field. ■

When $n = 1, 2$, (2.2) and (2.3) have only natural number factors. But, when $n \geq 3$, (2.2) and (2.3) have complex number factors, making situations quite different from when $n = 1, 2$.

3. Proof

Lemma 3.1. To satisfy the polynomial identity, $f(x) = g(x)$, all corresponding factors in (2.2) and (2.3), with respect to k, must be same, which leads to a trivial aolution $a = c, b = 0$.

Proof. To satisfy the polynomial identity, $f(x) = g(x)$, the following three conditions must be satisfied.

$$\prod_{k=1}^{n} ae^{\frac{2k\pi i}{n}} = \prod_{k=1}^{n}(ce^{\frac{2k\pi i}{n}} - b). \tag{3.1}$$

$$|ae^{\frac{2k\pi i}{n}}| = |ce^{\frac{2k\pi i}{n}} - b|. \tag{3.2}$$

$$arg(ae^{\frac{2k\pi i}{n}}) = arg(ce^{\frac{2k\pi i}{n}} - b). \tag{3.3}$$

The only case to satisfy above three conditions is when $ae^{\frac{2k\pi i}{n}} = ce^{\frac{2k\pi i}{n}} - b, 1 \leq k \leq n$. So,

$$a\left(cos\frac{2k\pi}{n} + isin\frac{2k\pi}{n}\right) = c\left(cos\frac{2k\pi}{n} + isin\frac{2k\pi}{n}\right) - b,$$

$$asin\frac{2k\pi}{n} = csin\frac{2k\pi}{n},$$

$$a = c, \tag{3.4}$$

$$acos\frac{2k\pi}{n} = ccos\frac{2k\pi}{n} - b,$$

$$b = 0. \tag{3.5}$$

(3.4) and (3.5) is a trivial solution, $a = c, b = 0$. ∎

4. Conclusion

In this thesis, we related LHS and RHS of $a^n = c^n - b^n$ to the constant terms of two monic polynomials $f(x) = x^n - a^n$ and $g(x) = x^n - (c^n - b^n)$. By doing so, FLT is simplified to the problem of finding conditions that will satisfy the polynomial identity, $f(x) = g(x)$, when $n \geq 3$. To satisfy $f(x) = g(x)$, the corresponding factors of the two constant terms of $f(x)$ and $g(x)$ must be exactly same, resulting a trivial solution, $a = c, b = 0$.

References

[1] Andrew John Wiles, Modular elliptic curves and Fermat’s Last Theorem, Annals of Mathematics, 141 (1995), 443-551.

[2] https://en.wikipedia.org/wiki/Absolutely_irreducible