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, conditions to satisfy the number identity, $a^n=c^n-b^n$, are changed to conditions to satisfy the polynomial identity, $f(x)=g(x)$, which lead to a trivial solution, $a=c,b=0$, when $n\geq 3$.

1. Introduction

FLT was inferred in 1637 by Pierre de Fermat [1], and was proved by Andrew John Wiles in 1995 [2]. But the proof is not easy even for mathematicians, requiring more simple proof.

In this thesis, to change 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 the polynomial identity, $f(x)=g(x)$, permit only a trivial solution, $a=c,b=0$, when $n\geq 3$.

2. Fatorings of Constant Terms

Lemma 2.1. Below (2.1) is the irreducible factoring of (1.1) over the complex field [3].

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

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

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 $-a^n$ is shown in (2.2). ■

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

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

Proof. The n roots of $b^n-c^n=0$, with respect to b, are $b=ce^{\frac{2k\pi i}{n}}, 1\leq k\leq n$, so, (2.3) is the irreducible factoring of b^n-c^n over the complex field. ■

When $n=1,2$, (2.2) and (2.3) have only integer 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. The solution which satisfies the polynomial identity $f(x) = g(x), n \geq 3$, is a trivial solution, $a = c, b = 0$.

Proof. The constant terms of $f(x)$ and $g(x)$ are rewritten as follows..

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

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

The polynomial $p(x)$ whose roots are all factors of (3.1) is (3.2).

$$p(x) = \prod_{k=1}^{n}\{x - (ce^{\frac{2k\pi i}{n}} - b)\}. \tag{3.2}$$

In graph view, $f(x) = g(x)$ means the $f(x)$ and $g(x)$ graphs overlap. By moving the $p(x)$ graph, we can easily make it overlap the $g(x)$ graph. But, by moving the $p(x)$ graph to overlap the $f(x)$ graph, the following three conditions should be satisfied.

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

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

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

The only case the above three conditions are satisfied is when $ae^{\frac{2k\pi i}{n}} = ce^{\frac{2k\pi i}{n}} - b, 1 \leq k \leq n$. By Euler's identity $e^{ix} = cosx + isinx$ [4], we have

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

The complex number identity states that if $x + iy = u + iv$, then, $x = u, y = v$ [5]. So,

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

$$a = c, \tag{3.3}$$

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

$$b = 0. \tag{3.4}$$

(3.3) and (3.4) 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] https://en.wikipedia.org/wiki/Fermat%27s_Last_Theorem.

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

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

[4] https://en.wikipedia.org/wiki/Euler%27s_identity

[5] https://en.wikipedia.org/wiki/Complex_number