A Proof of Fermat's Last Theorem by Relating to Monic Polynomial Properties

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 polymials $x^n - a^n$ and $x^n - (c^n - b^n)$. By doing so, we could inspect whether these two polynomials can be identical when $n \geq 3$, i.e., $x^n - a^n = x^n - (c^n - b^n)$, which satisfies $a^n = c^n - b^n$. By inspecting the properties of two polynomials such as factoring, root structures and graphs, we found that $x^n - a^n$ and $x^n - (c^n - b^n)$ can't be identical when $n \geq 3$, except when trivial cases.

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.

Let a, b, c, n be natural numbers, otherwise specified. We related FLT to the following two monic polynomials.

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

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

If $f(x) = g(x)$ is possible for $n \geq 3$, $a^n = c^n - b^n$ is satisfied, and FLT is false. But the factoring, root structure and graph properties of $f(x)$ and $g(x)$ do not allow $f(x) = g(x)$ when $n \geq 3$. So, $a^n = c^n - b^n$ can't be satisfied for $n \geq 3$.

2. Basic Lemmas

The number of roots of $x^n - a^n$ is as follows, as in Figure 1 [2][3][4].

① **Odd $n \geq 3$:** One integer root and $n - 1$ pairwise complex conjugate roots.

② **Even $n \geq 4$:** Two integer roots and $n - 2$ pairwise complex conjugate roots.

Figure 1. Number of roots examples of $x^n - 1^n$.

(a) Roots of $x^5 - 1^n = 0$.

(b) Roots of $x^6 - 1^n = 0$.

Lemma 2.1. Below (2.1) is the irreducible factoring of (1.1) over the complex field [5].

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

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

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

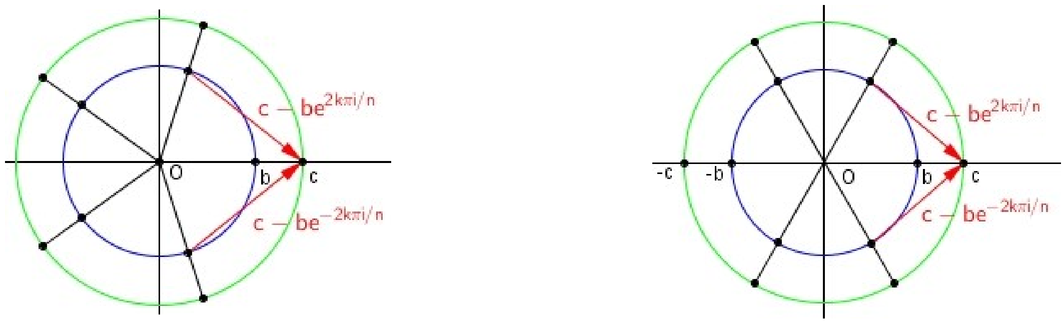
$$h(c,b) = c^n - b^n = \prod_{k=1}^{n}(c - be^{\frac{2k\pi i}{n}}) \tag{2.2}$$

Proof. The n roots of $h(c,b)$ are $c = be^{\frac{2k\pi i}{n}}, 1 \le k \le n$, so, (2.2) is the irreducible factoring of $h(c,b)$ over the complex field. ■

Lemma 2.3. All n factors of (2.2) can't have same magnitude.

Proof. The n factors of (2.2) are $c - be^{\frac{2k\pi i}{n}}, 1 \le k \le n$. Each factor can be considered as the difference vector between $(c, 0)$ and $b(cos\frac{2k\pi}{n}, sin\frac{2k\pi}{n})$, as in Figure 2.

Figure 2. Vector factor examples of (2.2).



(a) *n* = 5 example. (b) *n* = 6 example.

Because $|c - be^{\frac{2k\pi i}{n}}|$ is same only with its complex conjugate $|c - be^{\frac{-2k\pi i}{n}}|$, the magnitude of all factors of (2.2) can't be same for all k. ■

Lemma 2.4. A polynomial whose roots are all factors in (2.2) is (2.3) below.

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

Proof. The n factors of (2.2) are $c - be^{\frac{2k\pi i}{n}}, 1 \le k \le n$, and they are all involved in (2.3) as individual root. So, $p(x)$ is a polynomial whose roots comprise all factors in (2.2). ■

Lemma 2.5. A polynomial with different root magnitude can't be of the form $x^n - a^n, n \ge 3$.

Proof. The n roots of $x^n - a^n$ are all located on a circle of radius a in the complex plane. But, if the magnitude of n roots is not all same, all roots can't be located on a same circle. So, a polynomial with different root magnitude can't be of the form $x^n - a^n, n \ge 3$. ■

Lemma 2.5 implies that $f(x) = g(x)$ can't be achieved for $n \ge 3$, so, $a^n = c^n - b^n$ can't also be satisfied.

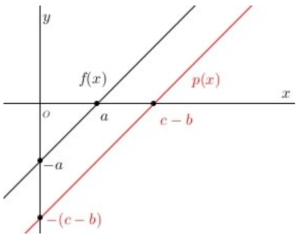
3. Graphical Interpretation of FLT and Proving Lemma

For graphical interpretation of FLT, example graphs of $f(x)$ and $p(x)$ are shown in Figure 3.

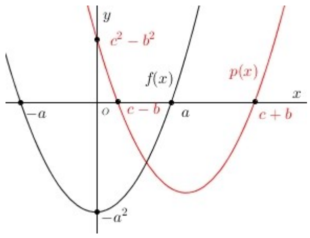
$$f(x) = x^n - a^n. \tag{1.1}$$

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

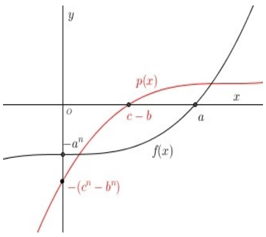
Figure 3. Example graphs of $f(x)$ and $p(x)$.



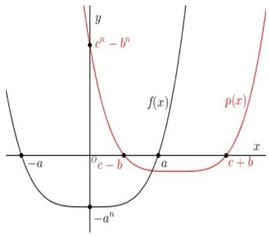
(a) Graphs for $n = 1$.



(b) Graphs for $n = 2$.



(c) Graphs for odd $n \geq 3$.



(d) Graphs for even $n \geq 4$.

We get $f(x)$ by vertically moving $y = x^n$ by $-a^n$. We get $p(x)$ by horizontally moving $y = x^n$ by c and vertically moving by $-(-b)^n$.

$$\begin{aligned} p(x) &= \prod_{k=1}^{n}\{(x - c) - (-be^{\frac{2k\pi i}{n}})\} = \\ &\prod_{k=1}^{n}\{X - (-be^{\frac{2k\pi i}{n}})\} = \\ &X^n - (-b)^n, X = x - c. \end{aligned} \tag{3.1}$$

In graph view, FLT is equivalent to the moving of $p(x)$ to overlap $f(x)$, to find possible solutions that satisfy $a^n = c^n - b^n$. Moving $p(x)$ is equivalent to varying the integer values $(b, c), b \leq a < c$, i.e., moving $p(x)$ vertically or horizontally by integer steps. When any of (b, c) makes two graphs overlap, a solution $a^n = c^n - b^n$ is found, and FLT is false. To make two graphs overlap, the following two steps are required.

① Horizontal movement that makes $X = x - c$ in (3.1) to be $X = x$, i.e., $c = 0$.

② Vertical movement that makes constant terms a^n and $c^n - b^n$ equal.

In Figure 3 (a), when $n = 1$, $p(x)$ always overlaps $f(x)$ for $a = c - b$. In Figure 3 (b), when $n = 2$, $p(x)$ overlaps $f(x)$ for Pythagorean triples, $a^2 = c^2 - b^2 = (c - b)(c + b)$. When $n = 1, 2$, all roots of $f(x)$ and $p(x)$ affect the (x, y)-intercepts of the graphs, and there are infinitely many solutions.

But, when $n \geq 3$, the advent of complex roots, which do not appear in graphs, makes situations quite different from those of when $n = 1, 2$. Figure 3 (c) and (d) show that when $p(x)$ overlaps $f(x)$, $a = c - b$ or $a^2 = c^2 - b^2$ should be satisfied, which contradicts to $a^n = c^n - b^n, n \geq 3$. This is because the complex roots can't affect the (x, y)-intercepts of the graphs. So, any integer step movements of $p(x)$ can't satisfy $p(x) = f(x)$ when $n \geq 3$.

When $n \geq 3$, moving $p(x)$ to overlap $f(x)$ is equivalent to making all n roots in $\prod_{k=1}^{n}(c - be^{\frac{2k\pi i}{n}})$ same as those in $\prod_{k=1}^{n} ae^{\frac{2k\pi i}{n}}$. Hence Lemma 3.1.

Lemma 3.1. When $n \geq 3$, to make every n roots in $\prod_{k=1}^{n}(c - be^{\frac{2k\pi i}{n}})$ exactly match to those in $\prod_{k=1}^{n} ae^{\frac{2k\pi i}{n}}$, $c = 0, a = -b$ must be satisfied.

Proof. The complex number identity states that if $x + iy = u + iv$, then $x = u, y = v$ [6]. To satisfy $\prod_{k=1}^{n} ae^{\frac{2k\pi i}{n}} = \prod_{k=1}^{n}(c - be^{\frac{2k\pi i}{n}})$, keeping all n roots in LHS and RHS identical, $ae^{\frac{2k\pi i}{n}} = c - be^{\frac{2k\pi i}{n}}$ must be satisfied.

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

$$asin\frac{2k\pi}{n} = -bsin\frac{2k\pi}{n},\ a = -b.$$

$$acos\frac{2k\pi}{n} = c - bcos\frac{2k\pi}{n},\ c = 0.$$

So, $c = 0, a = -b$. ■

Lemma 3.1 comprises above mentioned step ① and step ②, where step ① makes $c = 0$ and step ② makes $a^n = c^n - b^n = -b^n$. That is to say, only trivial solutions can satisfy $a^n = c^n - b^n$ for $n \geq 3$.

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 $x^n - a^n$ and $x^n - (c^n - b^n)$. By doing so, the proof of FLT is simplified to the proof of whether the two polynomials can be identical when $n \geq 3$. The properties of the two poynomials such as factoring, root structures and graphs showed that $x^n - (c^n - b^n) = x^n - a^n$ can't be achieved for $n \geq 3$, hence $a^n \neq c^n - b^n$ for $n \geq 3$. When $n = 1, 2$, there can be infinitely many $x^n - a^n = x^n - (c^n - b^n)$ solutions, but when $n \geq 3$, the advent of the complex roots latches further solutions, except for trivial ones. That is to say, as for the solutions of $a^n + b^n = c^n$, $a + b = c$ is the first and last solution for odd n, and $a^2 + b^2 = c^2$ is the first and last solution for even n.

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/Rational_root_theorem

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

[4] https://en.wikipedia.org/wiki/Cyclotomic_polynomial

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

[6] Erwin Kreyszig, Advanced Engineering Mathematics, 10th edition, 2011

List of Figures