Two Proofs 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 $a^n + b^n = c^n$ when $n \geq 3$. In this thesis, we related the LHS of $a^n = c^n - b^n$ to $x^n - a^n$ and the RHS to $x^n - (c^n - b^n)$. By doing so, we could analyse FLT in view of properties of monic polynomials such as factoring, root structure and graphs.The polynomial properties narrowed the vast possible approaches to FLT to elementary level mathematics. We relied on factoring, rational root theorem and parallel movement of graphs. And we succeeded to find simple proofs of FLT, which many people waited for so long time.

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.

From now on, let $a, b, c, n \geq 3$ and other variables be natural numbers, otherwise specified, and let's relate FLT to two monic polynomials as follows.

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

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

If the graphs of $f(x)$ and $g(x)$ can overlap or $g(a) = a^n - (c^n - b^n) = 0$, then $c^n = a^n + b^n$ is satisfied, proving FLT false. Can $g(x)$ be of the form $x^n - a^n$? The constant term $c^n - b^n$ of $g(x)$ has the form $x^n - a^n$. Of course $a = \sqrt[n]{c^n - b^n}$ is the real root, but, by the rational root theorem [2], the integer root(s) must be involved in the constant terms of $f(x)$ and $g(x)$. For $f(x)$ the constant term explicitly involves a, but for $g(x)$, how a can be involved in $c^n - b^n$? We studied in factoring and graph views, and found that $f(x)$ and $g(x)$ can't be isomorphic(same form) to each other.

2. Two Views on FLT and Lemmas

2.1. Factoring View

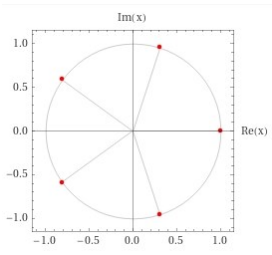
The number of roots of $x^n - 1$ is as follows and depicted in Figure 1 [3][4].

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

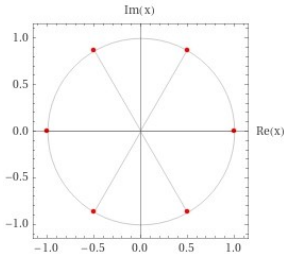
② **Even $n \geq 4$:** Two integer roots and $n - 2$ complex roots, which are pairwise complex conjugate.

Likewise, the number of roots of $x^n - a^n$ is same as the case of $x^n - 1$, for odd n, one integer root and $n - 1$ complex roots, for even n, two integer roots and $n - 2$ complex roots, and all complex roots are pairwise complex conjugate.

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



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



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

Lemma 2.1.1. The below (2.1.1) is the irreducible factoring of (1.1) over the complex field [5].

$$f(x) = x^n - a^n = \prod_{k=1}^{n}(x - ae^{\frac{2k\pi i}{n}}). \tag{2.1.1}$$

Proof. The roots of (1.1) are $ae^{\frac{2k\pi i}{n}}, 1 \le k \le n$, so, (2.1.1) is the irreducible factoring of (1.1) over the complex field. ■

Lemma 2.1.2. The below (2.1.2) is the irreducible factoring of $h(c,b) = c^n - b^n$ over the complex field.

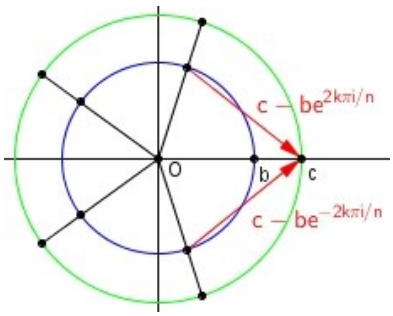
$$h(c,b) = c^n - b^n = \prod_{k=1}^{n}(c - be^{\frac{2k\pi i}{n}}) \tag{2.1.2}$$

Proof. The roots of $h(c,b)$ are $c = be^{\frac{2k\pi i}{n}}, 1 \le k \le n$, so, (2.1.2) is the irreducible factoring of $h(c,b)$ over the complex field. ■

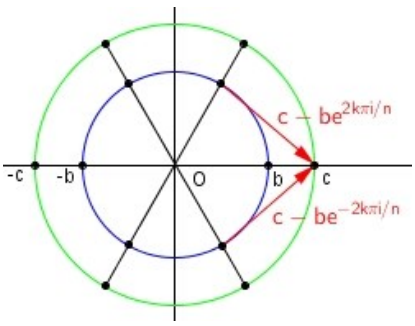
Lemma 2.1.3. All factors of (2.1.2) can't have same magnitude.

Proof. The n factors of (2.1.2) 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 (2.1.2).



(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 (2.1.2) can't be same for all k. ■

Lemma 2.1.4 A polynomial whose roots are all factors in (2.1.2) is (2.1.3) below.

$$p(x) = \prod_{k=1}^{n}\{x - (c - be^{\frac{2k\pi i}{n}})\}. \tag{2.1.3}$$

Proof. The n factors of (2.1.2) are $c - be^{\frac{2k\pi i}{n}}$, so, $p(x)$ is a polynomial whose roots comprise all factors in (2.1.2). ■

Lemma 2.1.5. A polynomial with different root magnitude can't be of the form $x^n - a^n$.

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 $x^n - a^n$. ■

2.2. Graph View

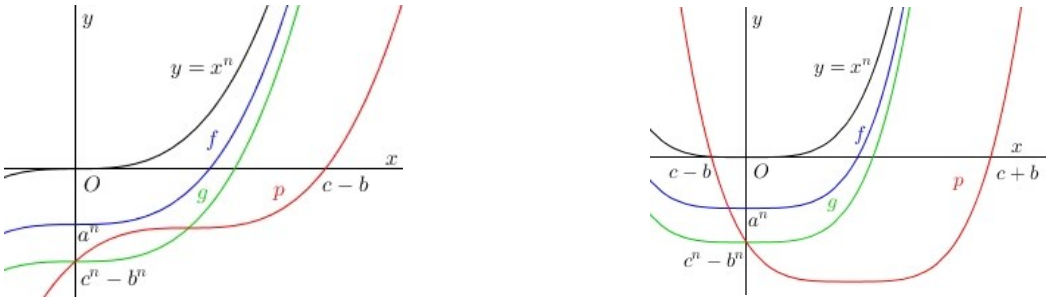
Following three graphs are results of parallel movement of the graph x^n, as in Figure 3.

$$f(x) = x^n - a^n.$$

$$g(x) = x^n - (c^n - b^n).$$

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

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



(a) Odd *n* graphs. (b) Even *n* graphs.

Two graphs $f(x)$ and $g(x)$ are generated by vertically moving the graph x^n, but graph $p(x)$ requires, in addition, horizontal movement by c. That is to say,

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

$$\prod_{k=1}^{n}\{(x - c) - (-b)e^{\frac{2k\pi i}{n}})\} =$$

$$\prod_{k=1}^{n}\{X - (-b)e^{\frac{2k\pi i}{n}})\}, X = x - c. \qquad (2.2.1)$$

Lemma 2.2.1. To make $p(x)$ overlap $f(x)$, which satisfies $a^n + b^n = c^n$, c should be zero.

Proof. Two graphs $f(x) = x^n - a^n$ and $g(x) = x^n - (c^n - b^n)$ must exactly overlap to satisfy $a^n + b^n = c^n$. One x-intercept of $p(x)$ always is $c - b$, whether n is odd or even, which is an integer-root-factor of the constant term $c^n - b^n = (c - b)(c^{n-1} + c^{n-2}b + \cdots + b^n)$. Moving $p(x)$ to overlap $f(x)$ by *integer steps,* the following two operations must be taken.

① In (2.2.1), $X = x - c$ should be x, i.e., $c = 0$.

② Vertically move to make the constant term to be $-a^n$.

Only *integer-step-moving* is permitted to keep the x-intercept $c-b$ be an integer. So, to make $p(x)$ overlap $f(x)$, which satisfies $a^n+b^n=c^n$, c should be zero. ■

3. Proofs of FLT

Lemma 3.1. Lemma 2.1.5 is a proving Lemma.

Proof. Because n factors of (2.1.2) can't lie on the circle with radius a, so, a polynomial form $x^n-(c^n-b^n)$ can't be identical to a polynomial form x^n-a^n. So, FLT is true. ■

Lemma 3.2. Lemma 2.2.1 is a proving Lemma.

Proof. When there can't be any parallel graph movements that make $p(x)$ and $f(x)$ overlap, without making $c=0$, any non-trivial solutions $c^n=a^n+b^n$ can't be generated. So, FLT is true. ■

5. Conclusion

In this thesis, by relating FLT to monic polynomial properties, we could see the structural aspects of FLT. Each a^n, b^n and c^n has its own internal structure, and c^n-b^n can't be a constant term of a polynomial form x^n-a^n. We also graphically showed that $p(x)$ can't overlap $f(x)$ unless $c=0$. The parallel movements of a graph are equivalent to algebraic operations. So, if there can't be possible graphic movement operations to make $p(x)$ and $f(x)$ overlap, without making $c=0$, a non-trivial solution $c^n=a^n+b^n$ can't be achieved.

As for the solutions of $a^n+b^n=c^n$, $a+b=c$ is the first and the last solution for odd n, and $a^2+b^2=c^2$ for even n. When $n\geq 3$, the advent of pairwise complex conjugate roots latches all further possible solutions. Anyway, we proved FLT using ordinary methods, which many people waited for so long time. But, we think Fermat was wrong, because our proofs can be summed up on the margin of a page.

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

List of Figures

1 Number of roots examples of $x^n - 1$ 2

2 Vector factor examples of (2.1.2) 2

3 Example graphs of $f(x), g(x)$ and $p(x)$ 3