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

Tae Beom Lee
join360@naver.com

Abstract: Fermat's Last Theorem(FLT) states that there is no positive integer set (a, b, c, n) which satisfies $a^n + b^n = c^n$ when $n \geq 3$. In this thesis, we related FLT to two polynomial equations. By doing so, we could analyze whether those two equations have equivalence properties in four aspects, ①irreducible factoring equivalence, ②constant term equivalence, ③ rational root factor equivalence and ④ odd-even property equivalence of a, b, c. What we found is that those two equations can not have equivalence properties in all four aspects which is enough to prove FLT.

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's relate FLT with two polynomial equations (1.2) and (1.3) as follows. Constant terms of (1.2) and (1.3) are LHS and RHS of $a^n = c^n - b^n$.

$$a^n + b^n = c^n \tag{1.1}$$

$$f(x) = x^n - a^n = 0 \tag{1.2}$$

$$g(x) = x^n - (c^n - b^n) = 0 \tag{1.3}$$

$$h(c) = c^n - b^n = 0 \tag{1.4}$$

By relating LHS and RHS of $a^n = c^n - b^n$ to constant terms of two polynomial equations (1.2) and (1.3), we can analyze whether the followings are true.

① Whether the first degree irreducible factorings [2][3][4] over the complex numbers of (1.2) and (1.3) can be identical.

② Whether $c^n - b^n$ of (1.3) can be the constant term of equation type $x^n - a^n = 0$.

③ How, by rational root theorem [5], the integer root(s) of (1.2) and (1.3) is(are) related to integer factor(s) of the constant term a^n and $c^n - b^n$.

④ Whether the odd-even property [6] of a, b, c in (1.1) causes some contradiction for odd $n \geq 3$.

Our study showed that each contradiction from ①, ②, ③ proves FLT, and a contradiction from ④ proves FLT for odd $n \geq 3$.

Equation (1.4) is a polynomial representation of the constant term of (1.3), considering c as a variable.

2. Definitions and Lemmas

2.1 Number of Roots and Root Structure

Definition 2.1.1 *n^{th} unity equation:* The n^{th} unity equation is (2.1) [2][7].

$$x^n - 1 = 0. \tag{2.1}$$

Lemma 2.1.2 The number of roots of (2.1) is as follows.

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

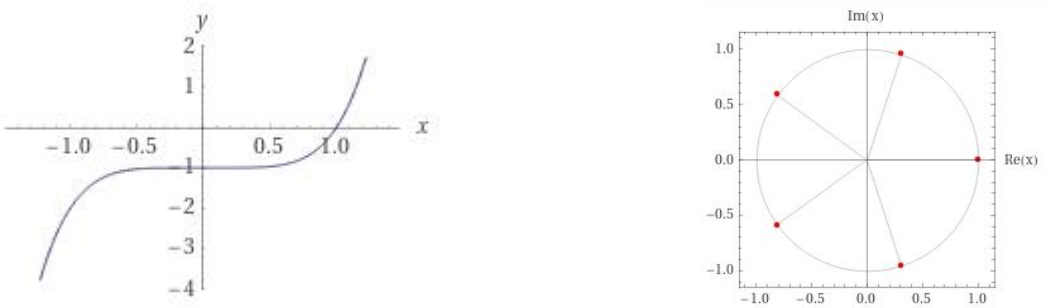
② **Even $n \geq 4$:** Two integer roots and $n-2$ complex roots.

Proof. The n roots of (2.1) are $e^{2(k-1)\pi i/n}, 1 \leq k \leq n$.

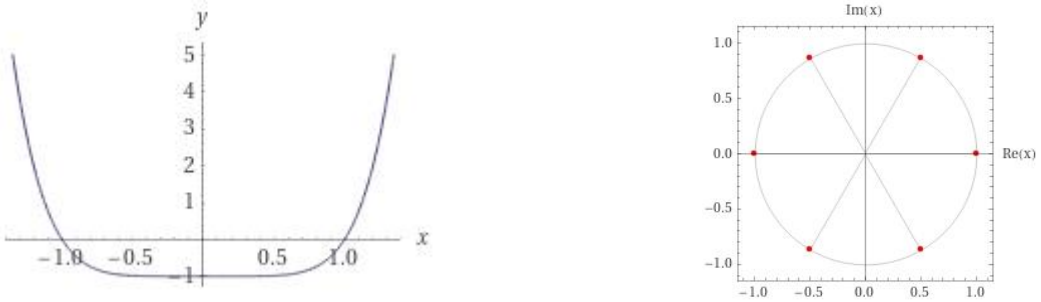
① **Odd $n \geq 3$:** The graph of $y = x^n - 1$ crosses x axis at $(1,0)$ once, so, (2.1) has one integer root and $n-1$ complex roots, as shown in Figure 1 (a).

② **Even $n \geq 4$:** The graph of $y = x^n - 1$ crosses x axis at $(1,0)$ and $(-1,0)$ twice, so, (2.1) has two integer roots and $n-2$ complex roots, as shown in Figure 1 (b). ■

Figure 1. Number of roots examples of (2.1).



(a) Number of roots for odd $n = 5$.



(b) Number of roots for even $n = 6$.

Corollary 2.1.3 The number of roots of (1.2) is as follows.

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

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

Proof. The n roots of (1.2) are $ae^{2(k-1)\pi i/n}, 1 \leq k \leq n$, so, the number of roots of (1.2) is same as lemma 2.1.2. ■

Definition 2.1.4 *Root structure:* The geometric distribution of roots of (1.2) or (2.1) on a circle with radius a or radius 1, as examples in Figure 2.

Figure 2. Root structure examples.

(a) Root structure of (1.2), $n = 5, a = 3$. (b) Root structure of (2.1), $n = 5, a = 1$.

Lemma 2.1.5 The root structure of (1.2) and (2.1) for same n differs only by the radius of circle where roots are laid.

Proof. The n roots of (1.2) are $ae^{2(k-1)\pi i/n}, 1 \leq k \leq n$ and n roots of (2.1) are $e^{2(k-1)\pi i/n}, 1 \leq k \leq n$. So, the arguments of roots are same, but the magnitude of roots, which is the radius of the circle on which roots are laid, is different. ■

For $n = 1$ or $n = 2$, the root structure is on the x axis, so, a circle on the complex plane is not required. For $n \geq 3$, the root structure on a circle is due to the existence of complex roots.

2.2 Operations on Root Structures

Definition 2.2.1 *Corresponding roots:* Roots of two n-degree root structures whose arguments are same.

Definition 2.2.2 *Root structure notation:* $R_n(a)$, where n is the degree of equation and a is the magnitude of roots.

Definition 2.2.3 *Operations on $R_n(a)$:* Operations on $R_n(a)$ are defined as follows.

① **Product:** $[R_n(a)] = \prod_{k=1}^{n} ae^{2(k-1)\pi i/n} = a^n$.

② **Addition:** $R_n(a) + R_n(b) = R_n(a+b)$.

③ **Subtraction:** $R_n(a) - R_n(b) = R_n(a-b), a \geq b$.

Lemma 2.2.4 The product operation is not closed to addition under the root structure, i.e., $[R_n(a)] + [R_n(b)] = a^n + b^n \neq [R_n(a+b)] = (a+b)^n$.

Proof.

$$[R_n(a)] + [R_n(b)] = \prod_{k=1}^{n} ae^{2(k-1)\pi i/n} + \prod_{k=1}^{n} be^{2(k-1)\pi i/n} = a^n + b^n$$

$$\neq [R_n(a+b)] = \prod_{k=1}^{n} (a+b)e^{2(k-1)\pi i/n} = (a+b)^n.$$

So, the product operation is not closed to addition under the root structure. Furthermore, note that the product operation itself is not closed under the root structure. ■

Lemma 2.2.5 The addition operation is closed, i.e., $R_n(a) + R_n(b) = R_n(a+b)$ is closed under the root structure.

Proof. The n roots of $R_n(a)$ are $ae^{2(k-1)\pi i/n}, 1 \leq k \leq n,$ and the n roots of $R_n(b)$ are $be^{2(k-1)\pi i/n}, 1 \leq k \leq n,$ so, the roots $R_n(a) + R_n(b)$ for corresponding roots are,

$$ae^{2(k-1)\pi i/n} + be^{2(k-1)\pi i/n} = (a+b)e^{2(k-1)\pi i/n}, 1 \leq k \leq n.$$

So, the addition operation is closed under the root structure. ■

Lemma 2.2.6 The subtraction operation is closed, i.e., $R_n(a) - R_n(b) = R_n(a-b), a \geq b$ is closed under the root structure.

Proof. The n roots of $R_n(a)$ are $ae^{2(k-1)\pi i/n}, 1 \leq k \leq n,$ and the n roots of $R_n(b)$ are $be^{2(k-1)\pi i/n}, 1 \leq k \leq n,$ so, the roots $R_n(a) - R_n(b)$ for corresponding roots are,

$$ae^{2(k-1)\pi i/n} - be^{2(k-1)\pi i/n} = (a-b)e^{2(k-1)\pi i/n}, 1 \leq k \leq n.$$

So, the subtraction operation is closed under the root structure. ■

In view of operations on root structure, FLT implies whether $a^n + b^n = c^n$ can have solutions which are not closed under the root structure.

2.3 Irreducible Factorings

Lemma 2.3.1 The following (2.3.1) is the unique irreducible factoring of (2.1) over the complex numbers.

$$x^n - 1 = \prod_{k=1}^{n} (x - e^{2(k-1)\pi i/n}). \qquad (2.3.1)$$

Proof. The n roots of (2.1) are $e^{2(k-1)\pi i/n}, 1 \leq k \leq n$, and (2.3.1) is the degree 1 factoring of (2.1) over the complex numbers. So, (2.3.1) is the unique irreducible factoring of (2.1) over the complex numbers. ■

Corollary 2.3.2 The following (2.3.2) is the unique irreducible factoring of (1.2) over the complex numbers.

$$f(x) = x^n - a^n = \prod_{k=1}^{n}(x - ae^{2(k-1)\pi i/n}). \quad (2.3.2)$$

Proof. The n roots of (1.2) are $ae^{2(k-1)\pi i/n}, 1 \le k \le n$, and (2.3.2) is the degree 1 factoring of (1.2) over the complex numbers. So, (2.3.2) is the unique irreducible factoring of (1.2) over the complex numbers. ■

Corollary 2.3.3 The following (2.3.3) is the unique irreducible factoring of (1.4) over the complex numbers.

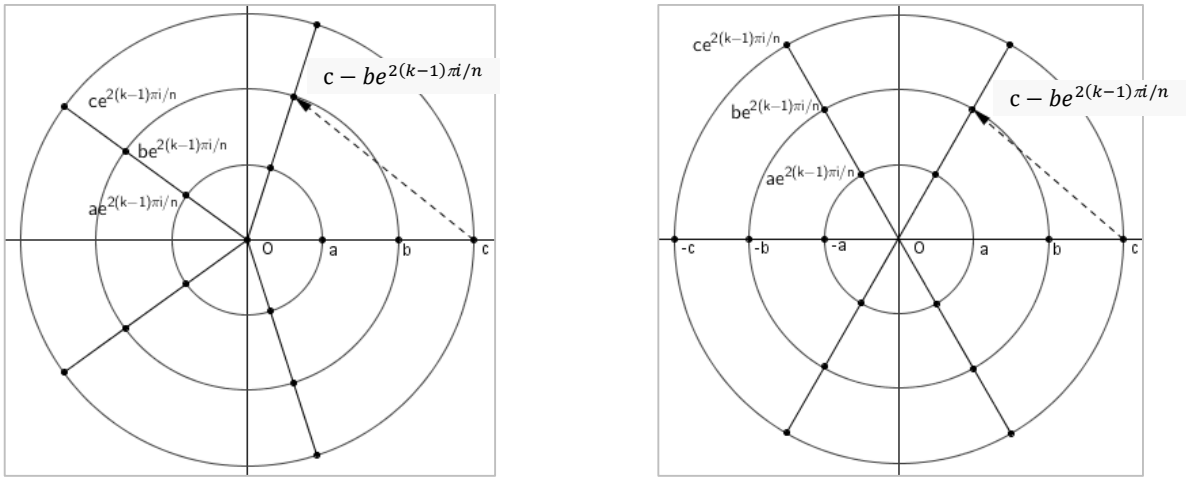
$$h(c) = c^n - b^n = \prod_{k=1}^{n}(c - be^{2(k-1)\pi i/n}) \quad (2.3.3)$$

Proof. The n roots of (1.4) are $c = be^{2(k-1)\pi i/n}, 1 \le k \le n$, and (2.3.3) is the degree 1 factoring of (1.4) over the complex numbers. So, (2.3.3) is the unique irreducible factoring of (1.4) over the complex numbers. ■

Lemma 2.3.4 All factors of (2.3.3) can not have the same magnitude.

Proof. The n factors of (2.3.3) are $c - be^{2(k-1)\pi i/n}, 1 \le k \le n$. Each factor can be considered as the difference vector between $(c, 0)$ and $(bcos\frac{2(k-1)\pi i}{n}, bsin\frac{2(k-1)\pi i}{n})$, as shown in Figure 3.

Figure 3. Vector factor examples of (2.3.3).



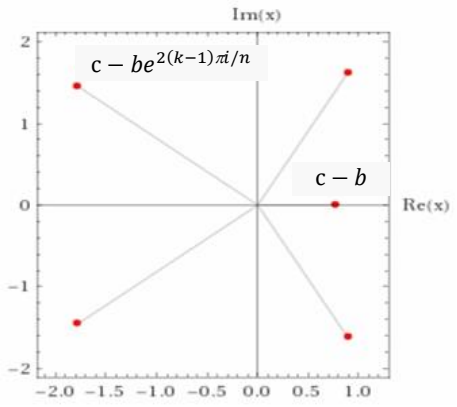
(a) n = 5 example. (b) n = 6 example.

Because $|be^{2(k-1)\pi i/n}| = b$ and $c > b > 0$, $|c - be^{2(k-1)\pi i/n}|$ is same only when two $be^{2(k-1)\pi i/n}$ are complex conjugates. So, $|c - be^{2(k-1)\pi i/n}|$ can not be same for all k. ■

Lemma 2.3.5 A polynomial equation of n roots, whose magnitudes are not all same, can not be the roots of polynomial equation type $f(x) = x^n - a^n = 0$.

Proof. The n roots of $x^n - a^n = 0$ lies on the circle with radius a, so, a polynomial equation of n roots whose magnitudes are not all a can not be the roots of any polynomial equation type $f(x) = x^n - a^n = 0$, as shown in Figure 4. ■

Figure 4. Example factors of $c^n - b^n$.



2.4 Root-coefficient Relationships

Let the n roots of a monic polynomial $p(x)$ be $x_1, x_2, \ldots, x_n$, then,

$$p(x) = (x - x_1)(x - x_2) \ldots (x - x_n)$$

$$= x^n + c_1 x^{n-1} + c_2 x^{n-2} + \cdots + c_{n-1} x + c_n \qquad (2.4.1)$$

$$c_1 = (-1) \sum_{k=1}^{n} x_k$$

$$c_2 = (-1)^2 \sum_{k,l=1,k<l}^{n} x_k x_l$$

$$\ldots..$$

$$c_n = (-1)^n \prod_{k=1}^{n} x_k$$

Definition 2.4.1 *Context:* The situation where a number, a coefficient or a variable is used in a monic polynomial equation with degree n.

Definition 2.4.2 *Context structure:* The root structure of a monic polynomial equation.

Definition 2.4.3 *Variable degree:* The degree of x of each term in (2.4.1).

Definition 2.4.4 *Coefficient degree:* The number of roots that is multiplied to generate a coefficient c_i. Table 1 shows the relationship between coefficient and variable degree.

Definition 2.4.5 *Context free:* The situation where a number, a coefficient or a variable is used in a constant function.

In view of context, variables a, b, c in $a^n + b^n = c^n$ are not context free. They have a context structure which we called *root structure* in definiftion 2.1.4. So, the simple algebraic

solution $c = \sqrt[n]{a^n + b^n}$ may not give a right solution within the context concept, because, as in lemma 2.2.4, the product operation is not closed to addition.

If we consider a^n or $c^n - b^n$ as the parametrized products of n roots, and also considering the degree of variable and coefficient in Table 1, the degree n of a^n or $c^n - b^n$ is the number of roots to generate a^n or $c^n - b^n$. Likewise, the degree of factored constant terms, like $c - b$, also is the number of roots to generate that factor.

Table 1. Relationship between variable and coefficient degree.

Terms	x^n	c_1x^{n-1}	c_2x^{n-2}	…	$c_{n-1}x$	c_n
Degree of variable x	n	$n-1$	$n-2$	…	1	0
Degree of coefficient c_i	0	1	2	…	$n-1$	n
Degree of terms	n	n	n	…	n	n

Here, we focus on $x^n - a^n = 0$ type equation where all roots are on a circle of radius a. So, the root-coefficient relationships are restricted only to the constant term a^n or $c^n - b^n$.

$$a^n = a \cdot a^2 \text{ ..., odd } n \geq 3. \tag{2.4.2}$$

$$a^n = a^2 \cdot a^2 \text{ ..., even } n \geq 4. \tag{2.4.3}$$

$$c^n - b^n = (c-b)(c^{n-1} + bc^{n-2} + \cdots + b^{n-2}c + b^{n-1}) \text{ , odd } n \geq 3. \tag{2.4.4}$$

$$c^n - b^n = (c^2 - b^2)(c^{n-2} + bc^{n-3} + \cdots + b^{n-3}c + b^{n-3}) \text{ , even } n \geq 4. \tag{2.4.5}$$

If the degree of a in (2.4.2) or (2.4.3) is 1, then, 1 root is required to generate it. If the degree of a is 2, then, 2 roots are required to generate it, whether they are 2 complex conjugate roots or 2 integer roots. Likewise, in (2.4.4) or (2.4.5), the degree of $c - b$ is 1, so, 1 root is required to generate it, and so on.

Definition 2.4.6 *Integer part:* The part of the constant term where only integer root(s) exist(s). For odd $n \geq 3$, if x_1 is 1 integer root,

$$x_1 = a \text{ or}$$

$$x_1 = c - b.$$

For even $n \geq 4$, if x_1, x_2 are 2 integer roots,

$$x_1x_2 = -a^2 \text{ or}$$

$$x_1x_2 = c^2 - b^2.$$

Definition 2.4.7 *Complex part:* The part of the constant term where only complex roots exist. For odd $n \geq 3$, it is the product of $n - 1$ complex roots.

$$x_2x_3 \dots x_n = \prod_{k=2}^{n} ae^{\frac{2(k-1)\pi i}{n}} = a^{n-1} \text{ or}$$

$$x_2x_3 \dots x_n = c^{n-1} + bc^{n-2} + \cdots + b^{n-2}c + b^{n-1}.$$

For even $n \geq 4$, it is the product of $n-2$ complex roots.

$$x_3x_4 \dots x_n = \prod_{k=3}^{n} ae^{2(k-1)\pi i/n} = a^{n-2} \text{ or}$$

$$x_3x_4 \dots x_n = c^{n-2} + bc^{n-3} + \cdots + b^{n-3}c + b^{n-2}.$$

Definition 2.4.8 *Factor moving:* A moving of any integer factor d between integer and complex part.

Lemma 2.4.9 A factor moving causes some root structure change.

Proof. Suppose d is any integer factor of $x_1x_2 \dots x_n$, which belongs to integer or complex part. Then, moving d between integer and complex part will cause some changes to at least two or more roots, at least one in integer part and at least one in complex part. Let x_k' be roots after moving of d, then,

$$x_1'x_2' \dots x_n' = a^n.$$

There exist at least two $x_k' \neq x_k,\ k = 1, 2, \dots, n$, so,

$$x^n - a^n = (x - x_1)(x - x_2) \dots (x - x_n) \neq (x - x_1')(x - x_2') \dots (x - x_n').$$

So, any factor moving causes some root structure change. ■

2.5 Odd-even Relationships

Lemma 2.5.1. In equation (1.1), a or b must be even, and others are odd.

Proof. Table 2 shows all odd-even cases of a, b, c.

Table 2. Odd-even cases of a, b, c.

Case	a	b	c	LHS	RHS	Remarks	ox
1	odd	odd	odd	even	odd	odd-even mismatch	x
2	odd	odd	even	even	even	$a^n + b^n \pmod 4 \neq c^n \pmod 4$	x
3	odd	even	odd	odd	odd		o
4	odd	even	even	odd	even	odd-even mismatch	x
5	even	odd	odd	odd	odd		o
6	even	odd	even	odd	even	odd-even mismatch	x
7	even	even	odd	even	odd	odd-even mismatch	x
8	even	even	even	even	even	not pairwise coprime	x

Only cases 3 and 4 are permitted, where a or b is even, and others are odd. ■

3. Proof of FLT

Lemma 3.1. Each contradiction from ①, ②, ③ proves FLT, and a contradiction from ④ proves FLT for odd $n \geq 3$.

① The contradiction on the first degree irreducible factoring of (1.2) and (1.3) over the complex numbers.

② $c^n - b^n$ can not be the constant term of equation type $x^n - a^n = 0$.

③ The rational root theorem requires the following identities, which contradicts.

$$a = c - b, \text{ odd } n \geq 3. \tag{3.1}$$

$$a^2 = c^2 - b^2, \text{ even } n \geq 4. \tag{3.2}$$

④ For odd $n \geq 3$, constant term factoring of a^n and $c^n - b^n$ introduces a contradiction.

Proof. Let's expand (2.3.3) as follows, where integer and imaginary parts are divided.

$$\prod_{k=1}^{n}(c - be^{2(k-1)\pi i/n}) = (c-b)\prod_{k=2}^{n}(c - be^{2(k-1)\pi i/n}) \text{ , odd } n \geq 3$$

$$= (c-b)(c^{n-1} + bc^{n-2} + \cdots + b^{n-2}c + b^{n-1}). \tag{3.3}$$

$$\prod_{k=1}^{n}(c - be^{2(k-1)\pi i/n}) = (c^2-b^2)\prod_{k=3}^{n}(c - be^{2(k-1)\pi i/n}) \text{ , even } n \geq 4$$

$$= (c^2-b^2)(c^{n-2} + bc^{n-3} + \cdots + b^{n-3}c + b^{n-3}). \tag{3.4}$$

① (1.2) and (1.3) can not have identical irreducible factoring, because, by lemma 2.3.4, the magnitude of roots of (1.3) can not be all same.

② Lemma 2.3.5 states that $c^n - b^n$ can not be the constant term of a polynomial equation type $x^n - a^n = 0$.

③ By lemma 2.4.9, factor moving is prohibited.

- In (3.3), the only integer part is $c - b$, so, it should be the only integer root of (1.3) for odd $n \geq 3$.
- In (3.4), the only integer part is $c^2 - b^2$, so, it should be the product of two integer roots a and $-a$ of (1.3) for even $n \geq 4$.

④ By lemma 2.5.1, one of a or b is even, and others are odd. Let a be even, then,

$$a = 2^{t0}p_1^{t1}p_2^{t2}\ldots p_k^{tk}, \; t_i \geq 0 \text{ integer}, \; t_0 \geq 1, \; p_k \text{ prime} \tag{3.5}$$

$$a^n = (2^{t0}p_1^{t1}p_2^{t2}\ldots p_k^{tk})^n \tag{3.6}$$

In (3.3), $c-b$ is even because b,c are odd, and $c^{n-1}+bc^{n-2}+\cdots+b^{n-2}c+b^{n-1}$ is odd because $b,$c are odd and the number of terms in $c^{n-1}+bc^{n-2}+\cdots+b^{n-2}c+b^{n-1}$ is n which is odd $n\geq 3$. So, in (3.6), the factor $(2^{t0})^n$ must belong to $c-b$, i.e., $(2^{t0})^n \mid (c-b)$. But, (1.2) and (1.3) should be identical equations, so, the complex part of (1.3), $\prod_{k=2}^{n}(c-be^{2(k-1)\pi i/n})$, must be same as the complex part of (1.2), $\prod_{k=2}^{n} ae^{2(k-1)\pi i/n}$, which must contain at least one $a^2=(2^{t0}p_1^{t1}p_2^{t2}\ldots p_k^{tk})^2$ factor. But, because the factor $(2^{t0})^n$ belongs to $c-b$, a^2 can not exist in $\prod_{k=2}^{n}(c-be^{2(k-1)\pi i/n})=c^{n-1}+bc^{n-2}+\cdots+b^{n-2}c+b^{n-1}$. ■

4. Conclusion

In this thesis, we related FLT to two polynomial equations to compare whether those two equations have equivalence properties in four aspects, ① irreducible factoring equivalence, ② constant term equivalence, ③ rational root factor equivalence and ④ odd-even property equivalence of a,b,c. We found that each contradiction from ①, ②, ③ proves FLT, and a contradiction from ④ proves FLT for odd $n\geq 3$.

References

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

[2] W. Keith Nicholson, Introduction to Abstract Algebra, Fourth Edition, Wiley, 2012.

[3] S. A. Park, Modern Algebra, 9th Edition, Kyung Moon Sa, 2019 (Korean Language).

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

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

[6] Vinay Kumar, Proof of Fermat Last Theorem based on Odd Even Classification of Integers, Int. J. Open Problems Compt. Math., Vol. 7, No. 4, December 2014 ISSN 1998-6262.

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

List of Figures

List of Tables