The simple condition of Fermat Wiles Theorem
mainly led by Combinatorics

Junya Sebata

January 12, 2021

Abstract

This paper gives the simple and necessary condition of Fermat Wiles Theorem with mainly providing one method to analyze natural numbers and the formula \( X^n + Y^n = Z^n \) logically and geometrically, which is positioned in combinatorial design theory. The condition is \( \gcd(X, E)^n = X - E \land \gcd(Y, E)^n = Y - E \) in \(-n \mid XY\), or \( \gcd(X, E)^n/n = X - E \land \gcd(Y, E)^n = Y - E \) in \(n \mid X \land -(n \mid Y)\). Provided that \( E \) denotes \( E = X + Y - Z \), \( n \) is a prime number equal to or more than 2, and \( X, Y, Z \) are coprime numbers.

1 Introduction

Many people offer a silent prayer as if they did for victims of COVID-19 on this day morning, August 6th in Japan. In many countries, this disaster seems also man-made, if not, errors committed. To minimize the damage, the author believe that the answer is not difficult, hoping that not only a few people but as many people as possible stand on the first step of the road of seeking the truth. Most of scholars know that this attitude or principle is the basis of science too. In my past development of words automated categorizing software, just obeying the principle like a normal scientist, and doing research for computer science, foundations of mathematics, reasonable philosophy, linguistics, etc., my understanding of general thinking method was sophisticated as below. Then the author was motivated to apply the method to mathematics, especially for Fermat Wiles Theorem [1].

When we think something, we call the thing by an object. We can not think explicitly without an object. If an object is only one, our thought does not advance, therefore at least two objects are needed. We call some connection, which is not these objects and breaks each mutual independence of these objects, by a relation. If no relation exists, also our thought does not advance. Therefore, to think needs at least two objects and these relation. If we grasp our thought by the paradigm of objects and relations, we can grasp features, comparison, decomposition, abstraction, and classification of objects, or proposition and inference, or set and map, by this paradigm as well. Namely thinking and understanding mean finding objects and clarifying mutual relations. Moreover, the essence of an object is only in the relations between others, and ultimately the entity, which at least we can recognize rationally, of an object is the relations of others*, for example in mathematics, \( x = 1 - 1 \) and \( x^2 = -1 \).

At a glance, Cantor succeeded to grasp features and abstract mathematical objects to sets, but in fact sets are only the basis for describing the relations between elements or sets. Hilbert put them into the paradigm of theories. He said “We think of these points, straight lines, and planes as having certain mutual relations, which we indicate by means of such words as ‘are situated,’ ‘between,’ ‘parallel,’ ‘congruent,’ ‘continuous,’ etc. The complete and exact description of these relations follows as a consequence of the axioms of geometry.” in [2]. In this way, modern axiomatism is mostly equal to defining relations expressly, and objects become only sign or mark of joint or container for relations like pronouns or algebraic symbols.

This idea, which concentrates on the importance of relations, was also appeared in Descartes. He said “These subjects, although objects are different, think only a variety of relations, in other

2020 Mathematics Subject Classification. Primary 11D41; Secondary 05B25, 05B05, 11U99, 11A99.

Key Words and Phrases. natural numbers, Fermat Wiles theorem, combinatorics, combinatorial design theory, philosophical and relational logic.

*More details about "Relational Logic" which the author thought of are in [4], but only in Japanese.
words only proportions, which are found in these subjects", and also said “we can borrow all the advantages from geometric analysis and algebra, and all the disadvantages of either can be corrected by the other one” in [3]. It means that algebraic geometry can deepen the understanding of both geometric analysis and algebra by these mutual complementary relations.

From the philosophy above, general thinking method which is centered on relations, we consider Fermat Wiles Theorem. When we analyze natural numbers and the formula \( X^n + Y^n = Z^n \), we need to find the other objects which have strong relations with them and support our understanding on them. Once we find the objects, we just need to concentrate on seeking the relations between all of them, and repeat this thinking operation for finding new objects and relations. By this policy for seeking, as the result in this paper we see geometric structures positioned in design theory of combinatorics. “Combinatorial design theory is the study of arranging elements of a finite set into patterns (subsets, words, arrays) according to specified rules.”, cited from [5].

2 Deformation of Formula by Combinatorics

**Theorem 2.1** When \( X^n + Y^n = Z^n \) holds, decomposing each power by multinomial theorem and subtracting equal terms from both sides, then if we set \( E = X+Y-Z, X' = X-E, \) and \( Y' = Y-E, \) the left side \( X^n + Y^n \) remains \( E^n \) and the right side \( Z^n \) remains \( \sum_{r=0}^{n-2} nC_r E^r \{(X' + Y')^{n-r} - X'^{n-r} - Y'^{n-r}\} \). Therefore,

\[
E^n = \sum_{r=0}^{n-2} nC_r E^r \{(X' + Y')^{n-r} - X'^{n-r} - Y'^{n-r}\}
\]

(2.0.1)

holds.

**Proof** We think general finite set \( G \). \( G_n \) is that its number of elements is \( n \). We should note that finite is equivalent to the fact that the set has one-to-one correspondence with a subset of natural numbers, which has the max value.

For simple expression, we think \( \mathbb{N}_n \) as 1 to \( n \), a subset of natural numbers, and we take a one-to-one correspondence between \( G_n \) and \( \mathbb{N}_n \). With the correspondence, we write the elements of \( G_n \) as \( c_1 \) to \( c_n \).

We also adopt the same rule to \( X \) as \( n \). Then we think mappings \( f_x : G_n \mapsto G_X \), and a set \( Q_X \) has all \( f_x \) as its elements. We should note that \( f_x \) is what we call a duplicate permutation, or we can also say a categorized pattern of \( G_n \) by \( G_X \).

We think a coordinate set

\[
S_X = \{(x_1, x_2, \ldots, x_X) \mid 0 \leq x_i \leq n \land x_1 + x_2 + \ldots + x_X = n\},
\]

and a mapping \( g_x : Q_X \mapsto S_X \) with being determined by \( x_i = |f_x^{-1}(c_{x_i})| \). Provided that the mark \( | \) means a number of elements.

\( g_x \) is surjection. Hence for \( s \in S_X \), we think a set \( Q_{X,s} = g_x^{-1}(s) \), and

\[
|Q_{X,s}| = \frac{n!}{x_1!x_2! \cdots x_X!}
\]

holds. This is a coefficient of multinomial theorem, therefore

\[
X^n = \sum_{s \in S_X} |Q_{X,s}| = |Q_X|
\]

holds.

The discussion above can be adapted to \( Y \) and \( Z \) as well as \( X \). See Figure 1. Therefore if a simply sum set \( Q_X + Q_Y \) and \( Q_Z \) have one-to-one correspondence, \( X^n + Y^n = Z^n \) holds. Oppositely and more importantly, if \( X^n + Y^n = Z^n \) holds, because of \( Q_X \cap Q_Y = \emptyset \) and \( Q_X, Q_Y, Q_Z \) being finite sets, the numbers of elements of \( Q_X + Q_Y \) and \( Q_Z \) are equal. Therefore \( Q_X + Q_Y \) and \( Q_Z \) have one-to-one correspondence depending on their finiteness.

If \( Z \geq X+Y \) holds, because of \( Z^n \geq (X+Y)^n > X^n + Y^n \), it is contradict. Therefore \( Z < X+Y \) holds. Also \( Z > X, Y > 0 \), therefore \( 2Z > X + Y > 0 \) holds. From these inequalities, we should note \( Z > E > 0 \). We should also note \( X' = X - E = Z - Y > 0 \) and \( Y' = Y - E = Z - X > 0 \).
Next, see Figure 2. We think about the related objects of $E, X', Y'$ as well as $X, Y, Z$. Then we make correspondence of $S_X$ and $S_Z$ by arranging their coordinates left justified from their starts $x_1$ and $y_1$. Also we make correspondence of $S_Y$ and $S_Z$ by arranging their coordinates right justified from their ends $y_2$ and $z_2$. Also we make correspondence of $S_X$ and $S_Z$ by arranging their coordinates left justified from their starts $x_1$ and $z_1$. Also we make correspondence of $S_Y$ and $S_Z$ by arranging their coordinates right justified from their ends $y_2$ and $z_2$. Also we make correspondence of $S_E$ and $S_Z$ by arranging their coordinates with transitivity rule holding, as $S_E$ and $S_Y$ correspond by arranging their coordinates left justified from their starts $e$ and $x$. We should note that $S_X$ and $S_Z$, and $S_Y$ and $S_Y'$ have also naturally defined correspondence by transitivity rule, $S_Z$ mediating.

Although we can grasp this correspondence relations geometrically in multidimensional Cartesian coordinate space, it is not much helpful for us to think the relations logically. On the other hand, when we think the relations as in Figure 2, they can be seen easily as geometrical congruence or parallel translation of lattice points, and help us think logically and geometrically.

More details about Figure 2, each component corresponds to each lattice point on $S_Z, S_X, S_Y, S_X', S_Y', S_E$ main lines, and each number of the components corresponds to the same number of lattice points on each sub-line which belongs to and comes out from each lattice point on main line. As the result, $s \in S$ corresponds to $n$ lattice points on sub-lines, but not on main lines. It is no problem for us to think each $S_Z, S_X, S_Y, S_X', S_Y', S_E$ simply in two-dimensional Cartesian coordinate plane.

This geometric structures can be positioned in design theory of combinatorics, especially being related to finite geometry and block design.

We think the elements of $S_Z$ which have at least one component having equal to or more than 1 both in $z_1$ to $z_X$ and $z_{X+1}$ to $z_Z$, and call them a set $S_{X,Y'}\in S_Z$. Also we think the elements of $S_Z$ which do not correspond to the elements of $S_X$, and call them a set $S_{(Z-X)\in S_Z}$. Also we think the elements of $S_Z$ which do not correspond to the elements of $S_Y$, and call them a set $S_{(Z-Y)\in S_Z}$. Then $S_{(Z-X)\in S_Z} = S_{X,Y'}\in S_Z$, and $S_{(Z-Y)\in S_Z} = S_{X,Y'}\in S_Z$ holds.

We think the elements of $S_Z$ which have at least one component having equal to or more than 1 both in $z_1$ to $z_X$ and $z_{X+1}$ to $z_Z$, and call them a set $S_{X,Y'}\in S_Z$. We should note that the elements of $S_{X,Y'}\in S_Z$ can have components having equal to or more than 1 in $z_{X+1}$ to $z_X$.

From the above,

\[
S_{(Z-X)\in S_Z} = S_{(Z-X)\in S_Z} \cap S_{(Z-Y)\in S_Z} = (S_{X,Y'}\in S_Z) \cap (S_{X,Y'}\in S_Z).
\]

Since $S_{X,Y'}\in S_Z$ holds.

\[
(S_{X,Y'}\in S_Z) \cap (S_{X,Y'}\in S_Z) = S_{X,Y'}\in S_Z \cap S_{X,Y'}\in S_Z
\]

holds.

---

**Figure 1: Related Objects**

![Related Objects Diagram](image-url)
Correspondence Relations

If \( s \in S_X; Y \in Z \), \( s \in S_X, Y \in Z \) and \( s \in S_X, Y' \in Z \), therefore \( S_X, Y \in Z \subset S_X, Y' \in Z \). Oppositely, if \( s \in S_X, Y \in Z \cap S_X, Y' \in Z \), \( s \) has at least one component having equal to or more than 1 both in \( z_1 \) to \( z_X' \) and \( z_{X+1} \) to \( z_Z \), therefore \( S_X, Y \in Z \cap S_X, Y' \in Z \subset S_X, Y' \in Z \). Hence \( S_X, Y \in Z \cap S_X, Y' \in Z = S_X, Y' \in Z \) holds. From this, \( S(z - X, Y) \in Z = S_X, Y' \in Z \) holds.

Next we think the elements of \( S_Z \) which correspond to the elements of \( S_X \), and call them a set \( S_X \in Z \). As well as this, \( S_Y \in Z \) and \( S \in Z \) are defined. In addition to these sets, we define \( S([X \cup Y]) = S_X \cup Z \) and \( S([X \cap Y]) = S_X \cap Z \).

Then \( S(z - X, Y) \in Z = S_Z - (S_X \cup Z + (S_X \cap Z)) \) holds. Since \( S(z - X, Y) \in Z = S \cup Z, S(z - X, Y) \in Z = S\in Z - (S_X \cup Z + (S_X \cap Z)) \) holds. Therefore \( S_X, Y \in Z = S_Z - (S_X \cup Z + (S_X \cap Z)) \).

By the reverse mapping \( g_z^{-1} \) from \( S_Z \) to \( Q_Z \), we think the reverse images of \( S_X, Y \in Z, S \in Z \), and \( S_X, Y \in Z \), and call them \( Q_X, Y \in Z, Q \in Z \), \( Q_X, Y \in Z \). Since \( g_x^{-1} \) is a mapping, \( X, Y \in Z = g_x^{-1}(S_X, Y \in Z) = g_x^{-1}(S_Z - (S_X \cup Z + (S_X \cap Z))) = Q_Z - (Q_X \cup Z + (Q \in Z - Q \in Z)) \) holds. Therefore \( Q_X, Y \in Z = Q_Z - (Q_X \cup Z + (Q \in Z - Q \in Z)) \) holds, and then \( |Q_X, Y \in Z| = |Q_Z| \).

\( n \) should recall that \( X \in Z = Z \), and \( Q_X \cup Y \in Z \) and \( Q_Z \) have one-to-one correspondence, therefore \( |Q_X, Y \in Z| = |Q_X| + |Q_Y| - |Q_X \in Z| + |Q \in Z| \) holds. We should note that \( Q_X \) and \( Q \in Z \) are different sets. Also \( Q_Y \) and \( Q \in Z \) are different sets. Also \( Q_E \) and \( Q \in Z \) are different sets. But each pair of sets has the same number of elements.

As the result, we can know that

\[
|Q_E| = |Q_X, Y \in Z| \tag{2.0.2}
\]

is a necessary condition. We should note that \( |Q_E| \) is derived from \( X \in Z + Y \) and \( |Q_X, Y \in Z| \) is derived from \( Z \). In other words, by thinking \( S([X \cup Y]) \) as a standard, the overlapped elements of \( X \) and \( Y \) are \( E \), namely \( E \), and the exceeded elements of \( S_Z \) are \( S_X, Y \in Z \), namely \( S_X, Y \in Z \).

Now \( |Q_E| = E \). Next we think \( |Q_X, Y \in Z| \). For \( s \in S_X, Y \in Z \), \( |g_x^{-1}(s)| = \frac{n!}{z_1 \cdots z_2 \cdots \cdots z_2} \) holds.

Provided that we call the sum of components of \( S \in Z \) as \( r \), in other words, \( r = z_X + 1 + \cdots + z_X \)

Now \( S_X, Y \in Z \) can be divided into the cases of \( 0 \leq r \leq n - 2 \) in \( S \in Z \). We should note that an element \( s \) of \( S_X, Y \in Z \) has at least one component having equal to or more than 1 both in \( z_1 \) to \( z_X \), and \( z_X + 1 \) to \( z_Z \), therefore \( r \) can not be \( n - 1 \) and \( n \). For each case of \( r \), it is equivalent to the case that the sum of components of \( S_X \in Z \) and \( S \in Z \) has \( n - r \), however being excluded the two cases that only \( S_X \in Z \) has \( n - r \) and only \( S \in Z \) has \( n - r \).

Figure 2: Correspondence Relations

\[
\begin{align*}
S_Z & \quad \text{sub-line} \\
S_X & \quad \text{main line} \\
S_Y & \\
S_X' & \\
S_Y' & \\
S_E & \\
\end{align*}
\]
Therefore, about $|Q_{X',Y'}in Z| = \sum |g^{-1}(s)|$, we can first take the sum by $r = z_{X'+1} + \cdots + z_X$,

$$\sum \frac{r(r-1) \cdots 2 \cdot 1}{z_{X'+1} \cdots z_X!} = E'$$

holds. Next we can take the sum by $n-r = z_1 + \cdots + z_{X'} + z_{X'+1} + \cdots + z_Z$,

$$\sum \frac{(n-r)(n-r-1) \cdots 2 \cdot 1}{z_1! \cdots z_{X'}! \cdot z_{X'+1}! \cdots z_Z!} = (Z - E)^{n-r} - (X - E)^{n-r} - (Y - E)^{n-r}$$

holds.

It is clear that \( \frac{n(n-1) \cdots (r+1)}{(n-r)(n-r-1) \cdots 2 \cdot 1} = n C_r \), therefore

$$|Q_{X',Y'}in Z| = \sum_{r=0}^{n-2} n C_r E' \{(Z - E)^{n-r} - (X - E)^{n-r} - (Y - E)^{n-r}\}$$

holds. From the above, $E^n = \sum_{r=0}^{n-2} n C_r E' \{(X' + Y')^{n-r} - X'^{n-r} - Y'^{n-r}\}$ holds.

\[\Box\]

The equivalence between two formulas is easy to be proved by elementary deformation with binomial theorem as the following, however it is difficult to understand the meaning or the value of the formula without demonstration of THEOREM 2.1. This is the complementary effectiveness of the logical operations in the geometric structures. It gives us strong motivation and hints for additional seeking on the formula.

**Theorem 2.2** When we set $E = X + Y - Z$, $X' = X - E$, $Y' = Y - E$,

$$X^n + Y^n = Z^n \iff E^n = \sum_{r=0}^{n-2} n C_r E' \{(X' + Y')^{n-r} - X'^{n-r} - Y'^{n-r}\}$$

**Proof**

\[E^n = \sum_{r=0}^{n-2} n C_r E' \{(X' + Y')^{n-r} - X'^{n-r} - Y'^{n-r}\}.\]

\[\Box\]

**3 Preparations for Analysis**

**Lemma 3.1** When $n$ is a prime number equal to or more than 2, $E \equiv 0 (mod \ n)$ holds.

**Proof** If $E \not\equiv 0 (mod \ n)$ holds, $E^n \equiv E \equiv \sum_{r=0}^{n-2} n C_r E' \{(X' + Y')^{n-r} - X'^{n-r} - Y'^{n-r}\} (mod \ n)$.

When $1 \leq r \leq n-2$, $n C_r \equiv 0 (mod \ n)$ holds. Therefore $E \equiv (X' + Y')^{n-r} - X'^{n-r} - Y'^{n-r} (mod \ n)$ holds. Regardless of whether $(X' + Y')$, $X'$, $Y'$ can be divided by $n$ or not, $E \equiv X' + Y' - X' - Y' \equiv 0 (mod \ n)$ holds. This contradicts the assumption $E \not\equiv 0 (mod \ n)$, hence $E \equiv 0 (mod \ n)$ holds.

\[\Box\]
Definition 3.2 For a natural number $n$, when we call the index by $s \geq 0$ on the prime factor $p \geq 2$ in prime factorization of $n$, we define the function $f_p(n) = s$.

Lemma 3.3 For natural numbers $a, b, c$, when $c$ can be decomposed by summation of $a$ and $b$, in other words, $c = a + b$ holds, if $f_p(a) = 0$ and $f_p(b) \geq 1$ hold, $f_p(c) = 0$ holds.

Proof If $f_p(c) \geq 1$ holds, since $a = c - b$, $0 = f_p(a) = f_p(c - b) \geq 1$ holds. This is contradiction, therefore $f_p(c) = 0$ holds.

Lemma 3.4 For natural numbers $a, b, c$, when $c$ can be decomposed by summation of $a$ and $b$, in other words, $c = a + b$ holds, $f_p(c) \geq \min(f_p(a), f_p(b))$ holds.

In addition to it, if $f_p(c) = \min(f_p(a), f_p(b))$ holds, $\max(f_p(a), f_p(b)) \geq f_p(c)$ holds. If $f_p(c) > \min(f_p(a), f_p(b))$ holds, $f_p(a) = f_p(b)$ holds.

Proof If $f_p(c) < \min(f_p(a), f_p(b))$ holds, $f_p(a + b) \geq \min(f_p(a), f_p(b)) > f_p(c)$ holds. This contradicts $f_p(a + b) = f_p(c)$, therefore $f_p(c) \geq \min(f_p(a), f_p(b))$ holds.

If $f_p(c) = \min(f_p(a), f_p(b))$ holds, $\max(f_p(a), f_p(b)) \geq \min(f_p(a), f_p(b)) = f_p(c)$ holds. Therefore $\max(f_p(a), f_p(b)) \geq f_p(c)$ holds.

If $f_p(c) > \min(f_p(a), f_p(b))$ and $f_p(a) \neq f_p(b)$ hold, especially $f_p(a) \neq f_p(b)$ and because of LEMMA 3.3,

$$f_p\left(\frac{a}{\min(f_p(a), f_p(b))} + \frac{b}{\min(f_p(a), f_p(b))}\right) = 0$$

holds. Now

$$c = a + b = \min(f_p(a), f_p(b)) \cdot \left(\frac{a}{\min(f_p(a), f_p(b))} + \frac{b}{\min(f_p(a), f_p(b))}\right)$$

holds, therefore

$$f_p(c) = f_p\left(\min(f_p(a), f_p(b))\right) + f_p\left(\min(f_p(a), f_p(b)) + \frac{a}{\min(f_p(a), f_p(b))} + \frac{b}{\min(f_p(a), f_p(b))}\right) = \min(f_p(a), f_p(b))$$

holds. This contradicts $f_p(c) > \min(f_p(a), f_p(b))$. Therefore if $f_p(c) > \min(f_p(a), f_p(b))$ holds, $f_p(a) = f_p(b)$ holds.

□

Lemma 3.5 For natural numbers $a, b, c$, when $c$ can be decomposed by summation of $a$ and $b$, in other words, $c = a + b$ holds, if $f_p(a) \neq f_p(b)$ holds, $f_p(c) = \min(f_p(a), f_p(b))$ holds.

Proof From LEMMA 3.4, $f_p(c) \geq \min(f_p(a), f_p(b))$ holds. If $f_p(c) > \min(f_p(a), f_p(b))$ holds, $f_p(a) = f_p(b)$ holds, however this contradicts $f_p(a) \neq f_p(b)$. Therefore $f_p(c) = \min(f_p(a), f_p(b))$ holds.

□

Theorem 3.6 For any decomposition of a natural number $a$ by addition, if $x$ denotes its each term, in other words, $a = \sum x$ holds, and then

$$f_p(a) = f_p\left(\sum_{f_p(x) \geq f_p(a)} x\right)$$

holds.

Proof First we set a natural number $x'$ and a term $y$ of the decomposition as

$$x' = \sum_{f_p(x) \geq f_p(a)} x$$

and $f_p(a) < f_p(y)$.

Next we assume $f_p(a) \neq f_p(x')$. Since LEMMA 3.5, in the case $f_p(x') \neq f_p(y)$ holds, $f_p(x' + y) = \min(f_p(x'), f_p(y))$ holds. Since $f_p(a) \neq f_p(x')$ and $f_p(a) < f_p(y)$, $f_p(a) \neq \min(f_p(x'), f_p(y))$ holds. Therefore $f_p(a) \neq f_p(x' + y)$ holds.
On the other hand, in the case \( f_p(x') = f_p(y) \) holds, \( f_p(a) < f_p(y) = \min(f_p(x'), f_p(y)) \) and because of LEMMA 3.4 \( \min(f_p(x'), f_p(y)) \leq f_p(x' + y) \) holds. Therefore \( f_p(a) \neq f_p(x' + y) \) also holds. In short, if \( f_p(a) \neq f_p(x') \) holds, \( f_p(a) \neq f_p(x' + y) \) holds.

Now we unite \( x' + y \) and reset \( x' \) to denote the united term, and also reset \( y \) to another term which satisfies \( f_p(a) < f_p(y) \). Since \( f_p(a) \neq f_p(x') \) and \( f_p(a) < f_p(y) \) still hold from the above, we can rethink the same operation as well. This operation can be repeated until \( y \) becomes empty. Therefore \( f_p(a) \neq f_p(\sum x) \) holds. However this contradicts \( a = \sum x \). Therefore

\[
    f_p(a) = f_p(\sum_{f_p(a) \geq f_p(z)} x)
\]

holds.

\[ \square \]

**Lemma 3.7** For any decomposition of a natural number \( a \) by addition, if \( z \) is the only one term which has the minimum index \( f_p(z) \) for the prime factor \( p \),

\[
    f_p(a) = f_p(z)
\]

holds.

**Proof** First we set a term \( y \) of the decomposition as \( y \) is the different term from \( z \). Since LEMMA 3.5 holds, \( f_p(y + z) = \min(f_p(y), f_p(z)) = f_p(z) \) holds.

Now we unite \( y + z \) and reset \( z \) to denote the united term, and also reset \( y \) to another term which is the different term from \( z \). Since \( f_p(z) \) is still the minimum index from the above, we can rethink the same operation as well. This operation can be repeated until \( y \) becomes empty. Therefore \( f_p(a) = f_p(z) \) holds.

\[ \square \]

We should note that, in LEMMA 3.7, for all the term \( y \) which are the different terms from the term \( z \), \( f_p(y) > f_p(z) = f_p(a) \) holds. We do not use THEOREM 3.6 in this paper, but the theorem will help us understand LEMMA 3.7, because LEMMA 3.7 is the special case of THEOREM 3.6. LEMMA 3.7 is the very important proposition in this paper, when it applies to the formula (2.0.1) in the next theorem. We will feel that the difficulty of finding solution of Fermat Wiles Theorem comes from this LEMMA 3.7, which is derived from the fundamental proposition LEMMA 3.3.

## 4 Leading the Condition

**Theorem 4.1** When \( n \) is a prime number equal to or more than 2, for any prime factor \( \forall p | X' \),

\[
    n \neq p \quad \Rightarrow \quad nf_p(E) = f_p(X')
\]

\[
    n = p \quad \Rightarrow \quad nf_p(E) = f_p(X') + 1
\]

hold.

**Proof** Since

\[
    (X' + Y')^{n-r} - X'^{n-r} - Y'^{n-r} = \sum_{r'=0}^{n-r} n-rC_{r'} X'^{n-r-r'}Y'^{r'} - X'^{n-r} - Y'^{n-r}
\]

\[
    = \sum_{r'=1}^{n-r-1} n-r-1C_{r'} X'^{n-r-r'}Y'^{r'}
\]

holds, with putting this formula into the formula (2.0.1),

\[
    E^n = \sum_{r=0}^{n-2} nC_r E^r \left( \sum_{r'=1}^{n-r-1} n-r-1C_{r'} X'^{n-r-r'}Y'^{r'} \right)
\]

(4.0.3)

holds. Therefore \( X'Y'|E^n \) holds. Since \( p | X' \), \( p | E^n \) and then \( p | E \) holds.
Now if \( X^n + Y^n = Z^n \) has the set of the solution \((X, Y, Z)\) and \(X, Y\) have a common prime factor \(q\), \(Z\) also has a prime factor \(q\). Therefore even if each term of the formula has been divided by \(q^n\), the formula \((X/q)^n + (Y/q)^n = (Z/q)^n\) holds again. Repeating this operation until \((X, Y, Z)\) have no common prime factor, we can find the set of the solution \((X, Y, Z)\) which are coprime numbers. Therefore for seeking the existence of the solution \(X^n + Y^n = Z^n\), it is enough to discuss about only the case that the solution \((X, Y, Z)\) are coprime numbers. From now on, we state this condition in this paper.

Next for \(\forall p|X', p|E\) and \(X = X' + E\) hold, therefore \(p|X\) holds. It is also said that for \(\forall p'|Y', p'|E\) and \(Y = Y' + E\) hold, therefore \(p'|Y\) holds. In addition, \(X, Y\) are coprime numbers, therefore \(p \neq p'\) and \(X, Y'\) are also coprime numbers. Hence \(f_p(Y') = 0\) holds.

Now from the formula (4.0.3),

\[
E^n = \sum_{r=0}^{n-2} \sum_{r'=1}^{n-r-1} n C_{r-n} E_{n-r} E_{r} X^{n-r} Y^{n-r-r'}^{m-r'} \tag{4.0.4}
\]

holds. When we think about all the terms \(n C_{r-n} E_{n-r} E_{r} X^{n-r} Y^{n-r-r'}^{m-r'}\) of the formula above, we can notice that the term \(nX'Y'^{-m-1}\), which is the term of \((r, r') = (0, 1)\), has the special value. Here \(D\) denotes the other term of \(n C_{r-n} E_{n-r} E_{r} X^{n-r} Y^{n-r-r'}^{m-r'}\), but not \(nX'Y'^{-m-1}\).

In the case of \(n \neq p\), since \(f_p(Y') = 0\) holds, \(f_p(X') = f_p(nX'Y'^{-m-1})\) holds. \(D\) always includes \(EX' (r \geq 1)\) or \(X'^2 (r' \geq 2)\), therefore

\[
f_p(D) \geq f_p(EX') \quad \text{or} \quad f_p(D) \geq f_p(X'^2)
\]

hold. Since \(p|E\),

\[
f_p(EX') > f_p(X') \quad \text{and} \quad f_p(X'^2) > f_p(X')
\]

hold. From all of the above, \(f_p(D) > f_p(nX'Y'^{-m-1})\) holds. Therefore, for the right side of the formula (4.0.4), which is the decomposition of the natural number \(E^n\) by addition, the term \(nX'Y'^{-m-1}\) is the only term which has the minimum index \(f_p(nX'Y'^{-m-1})\) for the prime factor \(p\). Since \(\text{LEMMA } 3.7\),

\[
n f_p(E) = f_p(E^n) = f_p(nX'Y'^{-m-1}) = f_p(X')
\]

holds.

In the case of \(n = p\), since \(f_p(Y') = 0\) holds, \(f_p(nX') = f_p(nX'Y'^{-m-1})\) holds. \(D\) always includes \(nEX' (r \geq 1)\) or \(nX'^2 (r = 0 \land r' \geq 2)\), therefore

\[
f_p(D) \geq f_p(nEX') \quad \text{or} \quad f_p(D) \geq f_p(nX'^2)
\]

hold. Since \(p|E\),

\[
f_p(nEX') > f_p(nX') \quad \text{and} \quad f_p(nX'^2) > f_p(nX')
\]

hold. From all of the above, \(f_p(D) > f_p(nX'Y'^{-m-1})\) holds. Therefore, for the right side of the formula (4.0.4), which is the decomposition of the natural number \(E^n\) by addition, the term \(nX'Y'^{-m-1}\) is the only term which has the minimum index \(f_p(nX'Y'^{-m-1})\) for the prime factor \(p\). Since \(\text{LEMMA } 3.7\),

\[
n f_p(E) = f_p(E^n) = f_p(nX'Y'^{-m-1}) = f_p(nX') = f_p(X') + 1
\]

holds.

We should note that in the case of \(n = 2\), \(D\) denotes no term, but from the formula (4.0.4) \(E^2 = 2X'Y'\) holds. Therefore

\[
2 \neq p \quad \Rightarrow \quad 2f_p(E) = f_p(E^2) = f_p(2X'Y') = f_p(X') \quad 2 = p \quad \Rightarrow \quad 2f_p(E) = f_p(E^2) = f_p(2X'Y') = f_p(X') + 1
\]

also hold.

\[
\square
\]

Figure 3 is the space which displays the relations between the prime factorizations of \(X, Y, X', Y'\), \(E, E^n\). Primes are arranged in ‘a right way’ on its plane, and the vertical axis shows their indexes. Provided that the case of \(n = p\), and especially \(n = 2 \land f_2(E) = 1\), is excluded from the figure.
Theorem 4.2 When $n$ is a prime number equal to or more than 2,
\[ \neg(n|X) \Rightarrow \gcd(X, E)^n = X - E \]
\[ n|X \Rightarrow \frac{\gcd(X, E)^n}{n} = X - E \]
hold. These also hold for $Y$.

Proof For any prime factor $\forall p|X'$, as referred in the proof of THEOREM 4.1, $p|E$ holds. Since $X = X' + E$, $p|X$ also holds. Therefore $p|\gcd(X, E)$ holds.

Since $X' = X - E$, $\gcd(X, E)|X'$ holds. Therefore for any prime factor $\forall q|\gcd(X, E)$, $q|X'$ holds. Now we define a radical of a natural number by
\[ \text{rad}(X') := \prod_{p|X'} p. \]

From the above, we have known that $\text{rad}(X') = \text{rad}(\gcd(X, E))$ holds.

In the case $\neg(n|X)$, since $p|X$, $n \neq p$ holds. Therefore from THEOREM 4.1, $n f_p(E) = f_p(X')$ holds. Since $n \geq 2$ and $f_p(E) \geq 1$, $f_p(E) < f_p(X')$ holds. Therefore we can apply LEMMA 3.7 to $X = X' + E$, and then $f_p(X) = f_p(E)$ holds. Therefore
\[ f_p(\gcd(X, E)) = f_p(p^{\min(f_p(X), f_p(E))}) = f_p(p^{f_p(E)}) = f_p(E) = \frac{f_p(X')}{n} \]
\[ n f_p(\gcd(X, E)) = f_p(X') \]
holds. Since $\text{rad}(\gcd(X, E)) = \text{rad}(X')$ and the above, when $X' \neq 1$, $\gcd(X, E)^n = X' = X - E$ holds. Even if $X' = 1$, obviously it also holds.

In the case $n|X$, we can apply the same discussion to $n \neq p$. It means that $n f_p(\gcd(X, E)) = f_p(X')$ holds. Therefore we need to think about only the case $n = p$. We should note that since LEMMA 3.1 and $X' = X - E$, $n|X'$ holds. Therefore there inevitably exists $\exists p|X'$ which satisfies $n = p$. From THEOREM 4.1, $n f_p(E) = f_p(X') + 1$ holds.

When $n \geq 3$, because of $f_p(E) \geq 1$, $f_p(E) < n f_p(E) - 1 = f_p(X')$ holds. When $n = 2$ and $f_2(E) \geq 2, f_2(E) < 2 f_2(E) - 1 = f_2(X')$ holds. Therefore, in the two cases, we can apply LEMMA 3.7 to $X = X' + E$, and then $f_p(X) = f_p(E)$ holds. Therefore
\[ f_p(\gcd(X, E)) = f_p(p^{\min(f_p(X), f_p(E))}) = f_p(p^{f_p(E)}) = f_p(E) = \frac{f_p(X') + 1}{n} \]
\[ n f_p(\gcd(X, E)) - 1 = f_p(X') \]
holds.

When $n = 2$ and $f_2(E) = 1, f_2(X') = 2 f_2(E) - 1 = 1$ holds. Since $X = X' + E$, $f_2(X) = f_2(X' + E) \geq 1$ holds, and then $f_2(X) \geq f_2(E)$ holds. Therefore
\[ f_2(\gcd(X, E)) = f_2(2^{\min(f_2(X), f_2(E))}) = f_2(2 f_2(E)) = f_2(E) = \frac{f_2(X') + 1}{2} \]
\[ 2 f_2(\gcd(X, E)) - 1 = f_2(X') \]
also holds.

Since \( \text{rad}(\gcd(X, E)) = \text{rad}(X') \) and the above,

\[
\frac{\gcd(X, E)^n}{n} = X' = X - E
\]

holds. Provided that \( X' \neq 1 \) holds, because of \( X > E, n | X \), and LEMMA 3.1. The same discussion applies to \( Y \).

\[
\square
\]

5 Conclusions

Putting two conditions of \( X \) and \( Y \) to one, from this paper we have a new question whether there exist the solutions for natural numbers \( (X, Y, E) \), which satisfy that \( X \) and \( Y \) are relatively prime, \( E \) is a multiple of \( n \), and

\[
\gcd(X, E)^n = X - E \quad \land \quad \gcd(Y, E)^n = Y - E \quad \text{(Provided \( \neg(n \mid XY) \))}
\]

or

\[
\frac{\gcd(X, E)^n}{n} = X - E \quad \land \quad \gcd(Y, E)^n = Y - E \quad \text{(Provided \( (n \mid X) \land \neg(n \mid Y) \)).}
\]

At least \( (n, X, Y, E) = (3, 335, 553, 210) \) satisfies the condition above. At the last, when we put the condition into \( X^n + Y^n = Z^n \),

\[
(gcd(X, E)^n + E)^n + (gcd(Y, E)^n + E)^n = (gcd(X, E)^n + gcd(Y, E)^n + E)^n
\]

(Provided \( \neg(n \mid XY) \))

or

\[
\frac{gcd(X, E)^n}{n} + E)^n + (gcd(Y, E)^n + E)^n = \frac{gcd(X, E)^n}{n} + gcd(Y, E)^n + E)^n
\]

(Provided \( (n \mid X) \land \neg(n \mid Y) \))

holds. It means that we can make \( X^n + Y^n = Z^n \), the formula of Fermat Wiles Theorem, to the more strict one in this paper. In addition, it is interesting that this condition can be satisfied at least in simple \( n = 2 \) with Pythagorean triples. However Pythagorean triples seem to need \( (2 \mid X) \).

References


Junya Sebata
Sebata & CO.,LLC
n061470@jcom.home.ne.jp

10