JP Journal of Algebra, Number Theory and Applications

http://www.pphmj.com
http://dx.doi.org/10.17654/NT051010055
Volume 51, Number 1, 2021, Pages 55-75 **P-ISSN: 0972-5555**

A SIMPLE CONDITION OF FERMAT WILES THEOREM MAINLY LED BY COMBINATORICS

Junya Sebata

Momoi 4-7-12 Suginami-ku
Tokyo, Japan
e-mail: n061470@jcom.home.ne.jp

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 $\gcd(X, E)^n = X - E \wedge \gcd(Y, E)^n = Y - E$ in $\neg(n \mid XY)$, or $\gcd(X, E)^n/n = X - E \wedge \gcd(Y, E)^n = Y - E$ in $n \mid X \wedge \neg(n \mid Y)$. 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 believes that the answer is not difficult, hoping that not only a few

Received: April 30, 2021; Accepted: June 4, 2021

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

Keywords and phrases: natural numbers, Fermat Wiles Theorem, combinatorics, combinatorial design theory, philosophical and relational logic.

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 [5].

When we think something, we call the thing by an object. We cannot 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 their 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 composed of others[1], 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

[1]More details about “Relational Logic” which the author thought of is in [4], but only in Japanese.

of the axioms of geometry" in [3]. 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 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 [1]. 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 [2].

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,*

$$E^n = \sum_{r=0}^{n-2} {}_nC_r E^r \{(X' + Y')^{n-r} - X'^{n-r} - Y'^{n-r}\} \qquad (2.0.1)$$

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 e_n1 to e_nn.

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

$$S_X = \{(x_1, x_2, ..., x_X) | 0 \leq x_i \leq n \wedge x_1 + x_2 + \cdots + x_X = n\},$$

and a mapping $g_x : Q_X \mapsto S_X$ with being determined by $x_i = |f_x^{-1}(e_X i)|$. 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

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

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 $Q_X \bigcap Q_Y = \varnothing$ 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.

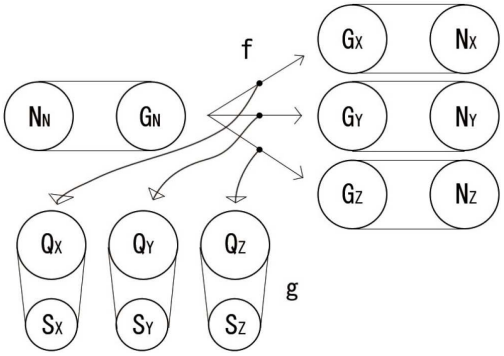

Figure 1. Related objects.

If $Z \geq X + Y$ holds, because of $Z^n \geq (X + Y)^n > X^n + Y^n$, it gives a contradiction. 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 $Y' = Y - E = Z - X > 0$.

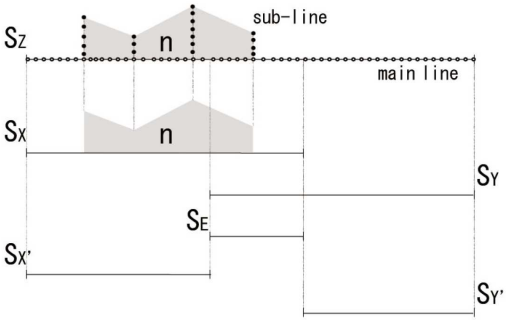

Figure 2. Correspondence relations.

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 z_1. Also, we make correspondence of S_Y and S_Z by arranging their coordinates right justified from their ends y_Y and z_Z. 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 $y'_{Y'}$ and z_Z. 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_1 and y_1, and S_E and S_X correspond by arranging their coordinates right justified from their ends e_E and x_X. We should note that S_X and $S_{X'}$, and S_Y and $S_{Y'}$ have also naturally defined correspondence by transitivity rule, S_Z mediating.

Although we can grasp these 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 lines. 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 structure 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 do not correspond to the elements of S_X or S_Y, and call them a set $S_{(Z-X\cup Y)inZ}$. Also, we think the elements of S_Z which do not correspond to the elements of S_X, and call them a set $S_{(Z-X)inZ}$. Also, we think the elements of S_Z which do not correspond to the elements of S_Y, and call them a set $S_{(Z-Y)inZ}$. Then $S_{(Z-X\cup Y)inZ} = S_{(Z-X)inZ} \cap S_{(Z-Y)\text{in } Z}$ 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 $S_{X,Y'inZ}$. Also, we think the elements of S_Z which correspond to the elements of $S_{Y'}$, and call them a set $S_{Y'inZ}$. Then $S_{(Z-X)inZ} = S_{Y'inZ} + S_{X,Y'\text{in } Z}$ holds. As well as this, $S_{(Z-Y)inZ} = S_{X'inZ} + S_{Y,X'inZ}$ also 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 $S_{X',Y'inZ}$. We should note that the elements of $S_{X',Y'inZ}$ can have components having equal to or more than 1 in $z_{X'+1}$ to z_X.

From the above,

$$S_{(Z-X\cup Y)inZ} = S_{(Z-X)inZ} \cap S_{(Z-Y)inZ}$$

$$= (S_{Y'inZ} + S_{X,Y'inZ}) \cap (S_{X'inZ} + S_{Y,X'inZ}).$$

Since $S_{Y'inZ} \cap (S_{X'inZ} + S_{Y,X'inZ}) = (S_{Y'inZ} + S_{X,Y'inZ}) \cap S_{X'inZ} = \varnothing$,

$$(S_{Y'inZ} + S_{X,Y'inZ}) \cap (S_{X'inZ} + S_{Y,X'inZ}) = S_{X,Y'inZ} \cap S_{Y,X'inZ}$$

holds.

If $s \in S_{X',Y'inZ}$, $s \in S_{X,Y'inZ}$ and $s \in S_{Y,X'inZ}$, therefore $S_{X',Y'inZ} \subset S_{X,Y'inZ} \cap S_{Y,X'inZ}$. Oppositely, if $s \in S_{X,Y'inZ} \cap S_{Y,X'inZ}$, 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 $S_{X,Y'inZ} \bigcap S_{Y,X'inZ} \subset S_{X',Y'inZ}$. Hence $S_{X,Y'inZ} \bigcap S_{Y,X'inZ} = S_{X',Y'inZ}$ holds. From this, $S_{(Z-X\bigcup Y)inZ} = S_{X',Y'inZ}$ holds.

Next we think the elements of S_Z which correspond to the elements of S_X, and call them a set S_{XinZ}. As well as this, S_{YinZ} and S_{EinZ} are defined. In addition to these sets, we define $S_{(X\bigcup Y)inZ} = S_{XinZ} \bigcup S_{YinZ}$ and $S_{(X\bigcap Y)inZ} = S_{XinZ} \bigcap S_{YinZ}$.

Then

$$S_{(Z-X\bigcup Y)inZ} = S_Z - S_{(X\bigcup Y)inZ} = S_Z - (S_{XinZ} + (S_{YinZ} - S_{(X\bigcap Y)inZ}))$$

holds. Since $S_{(X\bigcap Y)in\,Z} = S_{E\,in\,Z}$,

$$S_{(Z-X\bigcup Y)inZ} = S_Z - (S_{XinZ} + (S_{YinZ} - S_{EinZ}))$$

holds. Therefore $S_{X',Y'inZ} = S_Z - (S_{XinZ} + (S_{YinZ} - S_{EinZ}))$ holds.

By the reverse mapping g_z^{-1} from S_Z to Q_Z, we think the reverse images of S_{XinZ}, S_{YinZ}, S_{EinZ}, $S_{X',Y'inZ}$, and call them Q_{XinZ}, Q_{YinZ}, Q_{EinZ}, $Q_{X',Y'inZ}$. Since g_z is a mapping,

$$\begin{aligned} Q_{X',Y'inZ} &= g_z^{-1}(S_{X',Y'inZ}) = g_z^{-1}(S_Z - (S_{XinZ} + (S_{YinZ} - S_{EinZ}))) \\ &= Q_Z - (Q_{XinZ} + (Q_{YinZ} - Q_{EinZ})) \end{aligned}$$

holds. Therefore, $Q_{X',Y'inZ} = Q_Z - (Q_{XinZ} + (Q_{YinZ} - Q_{EinZ}))$ holds, and then $|Q_{X',Y'inZ}| = |Q_Z| - |Q_{XinZ}| - |Q_{YinZ}| + |Q_{EinZ}|$ holds.

Now we should recall that $X^n + Y^n = Z^n$, and $Q_X + Q_Y$ and Q_Z have one-to-one correspondence, therefore

$$|Q_{X',Y'inZ}| = |Q_X| + |Q_Y| - |Q_{XinZ}| - |Q_{YinZ}| + |Q_{EinZ}|$$

holds. We should note that Q_X and Q_{XinZ} are different sets. Also, Q_Y and Q_{YinZ} are different sets. Also, Q_E and Q_{EinZ} are different sets. But each pair of sets has the same number of elements.

As the result, we can know that

$$|Q_E| = |Q_{X',Y'inZ}| \tag{2.0.2}$$

is a necessary condition. We should note that $|Q_E|$ is derived from $X^n + Y^n$ and $|Q_{X',Y'inZ}|$ is derived from Z^n. In other words, by thinking $S_{(X\cup Y)inZ}$ as a standard, the overlapped elements of S_X and S_Y are S_E, namely Q_E, and the exceeded elements of S_Z are $S_{X',Y'inZ}$, namely $Q_{X',Y'inZ}$.

Now $|Q_E| = E^n$. Next, we think $|Q_{X',Y'inZ}|$. For $s \in S_{X',Y'inZ}$, $|g_z^{-1}(s)| = \dfrac{n!}{z_1!z_2!\cdot\cdots\cdot z_z!}$ holds. And then it can be divided into three parts:

$$\frac{n!}{z_1!z_2!\cdots z_z!}$$

$$= \frac{n(n-1)\cdots(r+1)}{(n-r)(n-r-1)\cdots 2\cdot 1}\cdot\frac{(n-r)(n-r-1)\cdots 2\cdot 1}{z_1!\cdots z_{X'}!\cdot z_{X+1}!\cdots z_Z!}\cdot\frac{r(r-1)\cdots 2\cdot 1}{z_{X'+1}!\cdots z_X!}.$$

Provided that we call the sum of components of S_{EinZ} as r, in other words, $r = z_{X'+1} + \cdots + z_X$.

Now $S_{X',Y'inZ}$ can be divided into the cases of $0 \le r \le n-2$ in S_{EinZ}. We should note that an element s of $S_{X',Y'inZ}$ 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 cannot be $n-1$ and n. For each case of r, it is equivalent to the case that the sum of components of $S_{X'inZ}$ and $S_{Y'inZ}$ has $n-r$, however, being excluded the two cases that only $S_{X'inZ}$ has $n-r$ and only $S_{Y'inZ}$ has $n-r$.

Therefore, about $|Q_{X',Y'inZ}| = \sum |g_z^{-1}(s)|$, we can first take the sum by $r = z_{X'+1} + \cdots + z_X$,

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

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 $\frac{n(n-1)\cdots(r+1)}{(n-r)(n-r-1)\cdots 2\cdot 1} = {}_nC_r$, therefore

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

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

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* $E = X + Y - Z$, $X' = X - E$, $Y' = Y - E$,

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

Proof.

$$0 = Z^n - X^n - Y^n = (Z-E+E)^n - (X-E+E)^n - (Y-E+E)^n$$

$$= \sum_{r=0}^{n} {}_nC_r E^r \{(Z-E)^{n-r} - (X-E)^{n-r} - (Y-E)^{n-r}\}$$

$$= {}_nC_n E^n(-1) + {}_nC_{n-1} E^{n-1}\{(Z-E) - (X-E) - (Y-E)\}$$

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

$$= -E^n + nE^{n-1}(Z+E-X-Y)$$

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

holds. Therefore, $E^n = \sum_{r=0}^{n-2} {}_nC_r E^r \{(X'+Y')^{n-r} - X'^{n-r} - Y'^{n-r}\}$. □

3. Preparations for Analysis

Lemma 3.1. *When n is a prime number equal to or more than 2, $E \equiv 0 \pmod{n}$ holds.*

Proof. If $E \not\equiv 0 \pmod{n}$ holds, then

$$E^n \equiv E \equiv \sum_{r=0}^{n-2} {}_nC_r E^r \{(X'+Y')^{n-r} - X'^{n-r} - Y'^{n-r}\} \pmod{n}.$$

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

Definition 3.2. For a natural number n, when we call the index by $s \ge 0$ on the prime factor $p \ge 2$ 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 a 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, then $f_p(a) = f_p(b)$ holds.

Proof. If $f_p(c) < \min(f_p(a), f_p(b))$ holds, then $f_p(a + b) \geq \min(f_p(a), f_p(b)) > f_p(c)$ 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, then

$$\max(f_p(a), f_p(b)) \geq \min(f_p(a), f_p(b)) = f_p(c)$$

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,

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

holds. Now

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

holds. Therefore,

$$f_p(c) = f_p(p^{\min(f_p(a), f_p(b))})$$

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

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*

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

holds.

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

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

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

Next, we assume $f_p(a) \neq f_p(x')$. Since by 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, then $f_p(a) \neq f_p(x'+y)$ 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, $f_p(a) \neq f_p\left(\sum x\right)$ holds. However, this contradicts $a = \sum x$. Therefore,

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

holds. □

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. □

We should note that, in Lemma 3.7, for all the terms y which are different 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 $\forall p \mid X'$,*

$$n \neq p \Rightarrow nf_p(E) = f_p(X'),$$
$$n = p \Rightarrow nf_p(E) = f_p(X') + 1$$

hold.

Proof. Since

$$(X'+Y')^{n-r} - X'^{n-r} - Y'^{n-r} = \sum_{r'=0}^{n-r} {}_{n-r}C_{r'} X'^{r'} Y'^{n-r-r'} - X'^{n-r} - Y'^{n-r}$$
$$= \sum_{r'=1}^{n-r-1} {}_{n-r}C_{r'} X'^{r'} Y'^{n-r-r'}$$

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

$$E^n = \sum_{r=0}^{n-2} {}_nC_r E^r \left\{ \sum_{r'=1}^{n-r-1} {}_{n-r}C_{r'} X'^{r'} Y'^{n-r-r'} \right\} \tag{4.0.3}$$

holds. Therefore, $X'Y' | E^n$ holds. Since $p | X'$, $p | E^n$, $p | E$ holds.

Now if $X^n + Y^n = Z^n$ has the set of the solutions (X, Y, Z) and X, Y have a common prime factor q, then 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) has no common prime factor, we can find the set of the solution (X, Y, Z) entries which are coprime numbers. Therefore, for seeking the existence of the solution of $X^n + Y^n = Z^n$, it is enough to discuss about only the case of the solution (X, Y, Z) with coprime components. From now, we postulate 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),

$$E^n = \sum_{r=0}^{n-2} \sum_{r'=1}^{n-r-1} {}_nC_r E^r {}_{n-r}C_{r'} X'^{r'} Y'^{n-r-r'} \tag{4.0.4}$$

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

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

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

holds. Since $p \mid E$,

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

hold. From all of the above, $f_p(D) > f_p(nX'Y'^{n-1})$ 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 $nX'Y'^{n-1}$ is the only one term which has the minimum index $f_p(nX'Y'^{n-1})$ for the prime factor p. By Lemma 3.7,

$$nf_p(E) = f_p(E^n) = f_p(nX'Y'^{n-1}) = f_p(X')$$

holds.

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

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

holds. Since $p \mid E$,

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

hold. From all of the above, $f_p(D) > f_p(nX'Y'^{n-1})$ 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 $nX'Y'^{n-1}$ is the only one term which has the minimum index $f_p(nX'Y'^{n-1})$ for the prime factor p. By Lemma 3.7,

$$nf_p(E) = f_p(E^n) = f_p(nX'Y'^{n-1}) = f_p(nX') = f_p(X') + 1$$

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,

$$2 \neq p \Rightarrow 2f_p(E) = f_p(E^2) = f_p(2X'Y') = f_p(X'),$$

$$2 = p \Rightarrow 2f_p(E) = f_p(E^2) = f_p(2X'Y') = f_p(X') + 1$$

also hold.

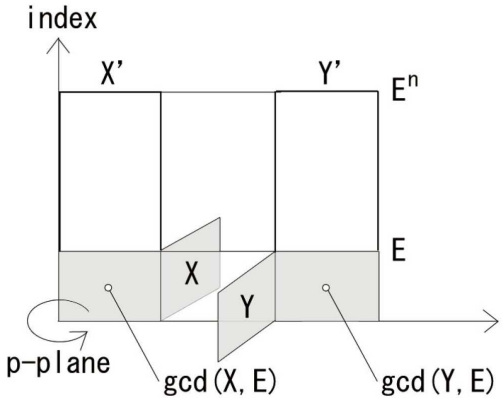

Figure 3. Primes' space.

□

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 $n = 2 \wedge f_2(E) = 1$, is excluded from the figure.

Theorem 4.2. *When n is a prime number equal to or more than* 2,

$$\neg(n \mid X) \Rightarrow \gcd(X, E)^n = X - E,$$

$$n \mid X \Rightarrow \frac{\gcd(X, E)^n}{n} = X - E$$

hold. These also hold for Y.

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

Since $X' = X - E$, $\gcd(X, E) \mid X'$ holds. Therefore, for any prime factor $\forall q \mid \gcd(X, E)$, $q \mid X'$ holds. Now we define a radical of a natural number by

$$rad(X') := \prod_{p \mid X'} p.$$

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

In the case $\neg(n \mid X)$, since $p \mid X$, $n \neq p$ holds. Therefore, from Theorem 4.1, $nf_p(E) = f_p(X')$ 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,

$$f_p(\gcd(X, E)) = f_p(p^{\min(f_p(X), f_p(E))}) = f_p(p^{f_p(E)}) = f_p(E) = \frac{f_p(X')}{n},$$

$$nf_p(\gcd(X, E)) = f_p(X')$$

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

When $n \geq 3$, because of $f_p(E) \geq 1$, $f_p(E) < nf_p(E) - 1 = f_p(X')$ holds. When $n = 2$ and $f_2(E) \geq 2$, $f_2(E) < 2f_2(E) - 1 = f_2(X')$ 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,

$$f_p(\gcd(X, E)) = f_p(p^{\min(f_p(X), f_p(E))}) = f_p(p^{f_p(E)}) = f_p(E) = \frac{f_p(X')+1}{n},$$

$$nf_p(\gcd(X, E)) - 1 = f_p(X')$$

hold.

When $n = 2$ and $f_2(E) = 1$, $f_2(X') = 2f_2(E) - 1 = 1$ 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,

$$f_2(\gcd(X, E)) = f_2(2^{\min(f_2(X), f_2(E))}) = f_2(2^{f_2(E)}) = f_2(E) = \frac{f_2(X')+1}{2},$$

$$2f_2(\gcd(X, E)) - 1 = f_2(X')$$

also hold.

Since $rad(\gcd(X, E)) = rad(X')$, from the above

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

holds. Provided that $X' \neq 1$ holds, because of $X > E$, $n \mid X$, and Lemma 3.1. The same discussion applies to Y. □

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

$$\gcd(X, E)^n = X - E \wedge \gcd(Y, E)^n = Y - E \ (Provided \ \neg(n \mid XY))$$

or

$$\frac{\gcd(X, E)^n}{n} = X - E \wedge \gcd(Y, E)^n = Y - E \ (Provided (n \mid X) \wedge \neg (n \mid Y)).$$

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

$$\left(\frac{\gcd(X, E)^n}{n} + E\right)^n + (\gcd(Y, E)^n + E)^n = \left(\frac{\gcd(X, E)^n}{n} + \gcd(Y, E)^n + E\right)^n$$

$$(Provided (n \mid X) \wedge \neg (n \mid Y))$$

holds. It means that we can make $X^n + Y^n = Z^n$, the formula of Fermat Wiles Theorem be 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

[1] R. Descartes, Discourse on the Method, T. Tanigawa (trans.), 33rd ed., Iwanami Shoten, Tokyo, 2017 (in Japanese).

[2] P. Dukes, E. Lamken and R. Wilson, Combinatorial Design Theory, Banff International Research Station for Mathematical Innovation and Discovery, 2008, https://www.birs.ca/workshops/2008/08w5098/report08w5098.pdf (accessed 2020-11-02).

[3] D. Hilbert, The Foundations of Geometry, E. J. Townsend (trans.), Reprint ed., The Open Court Publishing Company, Illinois, 1950.

[4] J. Sebata, Object and Relation, Relational Logic, Why What How Learn [serial online], http://www.linktracktool.com/what-why-study/object-relation.html (accessed 2020-09-29) (in Japanese).

[5] A. J. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. (2) 141(3) (1995), 443-551.