Rethinking the Proof of Fermat's Last Theorem

Yadong Wang
Fushun Petrochemical Company, Beijing, 100190, China

Abstract: The proof of Fermat's last theorem, which has been recognized so far, was published by Andrew Wiles in 1995. It has been reviewed by six experts and approved by mathematicians all over the world. However, this paper from two aspects pointed out there is an intrinsically logical mistake of Wiles' proof, which means the proof of Fermat's theorem is still not completely proved. First of all, language and linguistic expression are two different things, so language does not die because of improper expression. Second, Wiles' mistake is further explained using the relationship between Galois group and automorphism group.

Keywords: Fermat's last theorem; Conjecture, Galois group; Equation non-existence, Mathematical language; Linguistic expression

1. Introduction

In 1986, German mathematician Frey gave a speech at an International Mathematics Conference in Heidelberg, Germany to state that Fermat's theorem [1] would be automatically proved when the Taniyama-Shimura conjecture (referring to conjecture) was proved. Frey assumed existing positive integers A, B, C, N to make the following formula hold:

$$A^N + B^N = C^N \ (N > 2). \tag{1}$$

And from (1) to obtain formula (2)

$$y^2 = x^3 + (A^N - B^N)x^2 - A^N B^N. \tag{2}$$

He claimed that formula (2) could not be module-formalized but without provision of exact proof. On the other hand, (2) is an elliptic equation, thus it can be module-formalized because conjecture concluded that all elliptic equations could be module-formalized. Obviously, there appears a contradiction, therefore formula (2) does not exist. As we know that formula (2) is derived from (1), so when (2) does not exist, resulting in formula (1) no existence. Thus, Fermat's theorem was proved.

Following Frey's ideas, some researchers tried to prove (2) cannot be module-formalized and some researchers focused to prove conjecture. Three years later (in 1989), Ken Ribet proved that formula (2) could not be module-formalized. Seven years later (in 1993), Andrew Wiles proved conjecture, which is the first version of the proved Fermat's theorem. Unfortunately, there were several drawbacks in the first proof edition. Andrew Wiles attempted to mend them, but the final problem is not easy to solve. He finally solved a hardest problem using the EVA Sava's theory and Krivakin Fletcher's theory. And finally, the second complete version of the proof was released in 1995. Note that the proof idea of the second version kept the same as the first version, while the description method has been mended.

However, this paper pointed out that formula (2) no need to be derived from (1) but it existed objectively. Moreover, the contradictions on (2) are from incorrect operation of module-formulation, while not caused by the existence of (2). Therefore (2) exists, and (1) exists.

2. A Set $G(A)$

We know integers 3, 4, 5 can satisfy the following formula

$$3^2 + 4^2 = 5^2. \tag{3}$$

Numbers 3, 4, 5can make formula (3) hold, also have many other applications. For example, they can

(i). Take part in many activities in markets, banks, primary pupils' arithmetic and even every corner of the society.

(ii). Construct various elliptic equations and curves, such as:

$$y^2 = x^3 + (4^2 - 3^2)x^2 - 4^2 3^2. \tag{4}$$

$$3x^2 + 4y^2 - 5z^3 = 4. \tag{5}$$

$$3x + 4y = 5. \tag{6}$$

(iii). Construct many formulas and curves where $f(3,4,5)$ is used as the coefficients or constants.

$$F[x, y, \cdots, f(3,4,5)] = 0. \tag{7}$$

$$\varphi = F[x, y, \cdots, f(3,4,5)]. \tag{8}$$

For the sake of simplicity, combining (i), (ii) and (iii) together as a set, namely $G(A)$. Obviously, it exists objectively. Numbers 3, 4 and 5 are public resources, so they can be used in both formula (3) and $G(A)$. Formula (3) and $G(A)$ are independent each other. For example, when you pay 5 yuan for spinach, and you get 3 yuan change no need the approval or deduction of (3).

For Formula (4), five conclusions without proof are given as the follows:

The following mainly discusses Formula (4) and gives five conclusions without proof:

a) As long as the numbers 3, 4 and 5 exist, there is Formula (4).

b) Formula (4) exists objectively, and it only depends on number 3, 4, 5 but no need derivation from Formula (3);

c) Due to $4^2-3^2=7$ and $4^2\cdot 3^2=144$, Formula (4) is rewritten as $y^2=x^3+7x^2-144$. Obviously, this has no any relation to Formula (3);

d) There are many operations from Formula (3) to (4) according to a certain motivation. For example, from (3) we can easily know $4^2-3^2=5^2-2\cdot 3^2$, then multiply by factor x^2 to obtain the following Formula:

$$(4^2-3^2)x^2=(5^2-2\cdot 3^2)x^2. \tag{9}$$

Let

$$y^2=x^3+(5^2-2\cdot 3^2)x^2-4^2 3^2. \tag{10}$$

Bring Formula (9) into (10), then arrives at Formula (4). There are many deduced operations from (3) to (4), and the operations don't affect the existence of (4). These operations and the existence of (4) are two different things.

e). If carrying out modular operation on formula (4), there only one result is obtained in the form of yes or not. That is to say, two contradictory results cannot exist simultaneously.

3. Isomorphic Set $G(A)'$ of Set $G(A)$

In this section, integers A,B,C,N ($N>2$) and formula (1) have similar discussion as in section 2.

(i´) Symbols A,B,C,N can join more operations and applications than number 3, 4, 5.

(ii´) Construct various elliptic equations and curves such as:

$$y^2=x^3+(A^N-B^N)x^2-A^N B^N. \tag{11}$$

$$A^N x^2+B^N y^2-C^N z^3=B^N. \tag{12}$$

$$A^N x+B^N y=C^N. \tag{13}$$

Note that, formula $y^2=x^3+(A^N-B^N)x^2-A^N B^N$ in here is as the same as formula (2) in section 1. but is numbered as (11) again only for symmetrical description to section 2.

(iii´) Construct many formulas and curves where $f(A,B,C,N)$ is used as the coefficients or constants:

$$F[x,y,\cdots,f(A,B,C,N)]=0. \tag{14}$$

$$\varphi=F[x,y,\cdots,f(A,B,C,N)]. \tag{15}$$

Again, combining (i´), (ii´) and (iii´) together as a set, namely $G(A)'$. Obviously, it also exists objectively, and is isomorphic with $G(A)$. Integers A,B,C,N are public resources, so they can be used in both formula (11) and $G(A)'$. Formula (11) and $G(A)'$ are independent each other.

Accordingly, for Formula (11), five conclusions without proof are given as the follows:

a´). Formula (11) exists as long as symbols A,B,C,N exist.

b´). Formula (11) exists objectively, and it only depends on A,B,C,N but no need derivation from formula (1).

c´). Let $A^N-B^N=m$ and $A^N B^N=n$, then formula (11) is rewritten as $y^2=x^3+mx^2-n$. Obviously, this has no any relation to formula (1).

d´). There are many operations from (1) to (11) according to a certain motivation. For example, from (1) we can easily obtain $A^N-B^N=C^N-2B^N$, then multiply by factor x^2 to obtain the following formula:

$$(A^N-B^N)x^2=(C^N-2B^N)x^2. \tag{16}$$

Let

$$y^2=x^3+(C^N-2B^N)x^2-A^N B^N. \tag{17}$$

Note that, formula (17) is from (13) according to the properties of $G(A)'$. Bring formula (16) into (17), then get formula (11). Obviously, formula (4) is isomorphic with (11). There are many deduced operations from (1) to (11), and the operations don't affect the existence of formula (11).

e´). If carry out modular operation on formula (11), there only one result is obtained in the form of yes or not. That is to say, two contradictory results cannot exist simultaneously.

Proposition 1 Equation $y^2=x^3+(A^N-B^N)x^2-A^N B^N$ exists objectively. It is independent of equation $A^N+B^N=C^N$, and no need to be derived from $A^N+B^N=C^N$.

In a conclusion, formula (11) is an equation where symbols m,n are given parameters and symbols x,y are unknown variables. While (11) is a basis of the proof of the Fermat's last theorem.

4. Galois Group in Rational Field

Few people really understand Galois group because it is as abstruse as theory of relativity in physics. That is the reason why several mistakes in conjecture have been found but not in application of Galois group. For Galois groups, there are two kinds of description as follows [2]:

Algebraic equation description

The initial definition of Galois group means that Galois group is the permutation group of the roots of the algebraic equation with rational coefficient. Galois group is produced and developed in the process of solving the roots of algebraic equations of degree 5 and above.

Expansion domain description

Galois group is a kind of automorphism group of the extension field of rational number field. This automorphism group has a fixed "rational number field". This description is consistent with the first description to definitely reveal the essence of Galois group.

Galois group belongs to the algebraic equation with rational coefficient. The famous German mathematician E. Aden called "Galois group of algebraic equation" [3]. Wiles' study is elliptic equation, so Galois group cannot be applied, which is found obviously according to the first description. When the first description cannot be applied, hence the second description cannot be applied. However, Galois group is easy to be confused with many other automorphism groups in the second description. There is a module-P integer field. This field can also have an extension field. This extension field can also have an automorphism group. This automorphism group can also have a fixed field. However, this fixed field is not a rational number field, and the automorphism group is not a Galois group. This tiny conclusion has been ignored by Wiles. That is to means the Galois group applied by Wiles is a "pseudo Galois group" of non-Galois group. The conjecture proved by the "pseudo Galois group" must be wrong. In fact, Ken Ribet has proved that formula (11) cannot be module-formalized, then we can deduce that the conjecture not hold.

So far, this paper gave the reasons from two aspects why the conjecture did not hold, which showed that the proof of Fermat's last theorem did not completed.

5. Conclusion

Equation is a kind of natural language, which can express different mathematical ideas. For example, $y^2 = x^3 + (A^N - B^N)x^2 - A^N B^N$ can represent a solution set on the rational number field, or a solution set on the real number field, a curve on the plane, even a surface in the three-dimensional space.

It's not the same thing that an equation doesn't exist and it doesn't have a solution. Equation is a kind of language which exists forever, and an equation without solution is a linguistic expression. Some people think that Wiles' proof is not like a proof but can't deny it. Furthermore, Wiles was not awarded the Newton prize in mathematics by the Royal Society of England, whilst some mathematicians claimed that Wiles gave out effective proof [4].

Overall, equations $y^2 = x^3 + (A^N - B^N)x^2 - A^N B^N$ and $A^N + B^N = C^N$ are mathematical languages. There has no logical relationship between languages. Thus, $y^2 = x^3 + (A^N - B^N)x^2 - A^N B^N$ can have non-positive integer solution, but it always exists in there.

References

[1] Singh Simon. Fermat's Last Theorem. Shanghai: Shanghai Translation Publishing House. 2005.

[2] Sun Benwang. Galois Theory. Shanghai: Shanghai Education Press. 1980.

[3] Artin E. Galois Theory. Shanghai: Shanghai Science and Technology Press. 1979.

[4] Clausen C. Calvin. Mathematical Sorcery. Hunan Science & Technology Press. 2010.