A revolutionary proof of Fermat's last theorem

Hidetomo Tohmori*

*Unattached

Abstract. If the equation $A^n + B^n = C^n$ of Fermat's last theorem (hereafter, Fermat's equation) is approved in arithmetic operation, Fermat's equation is approved in surplus(modulo) operation by a prime number $p_k = 2k + 1$. But even if Fermat's equation is approved in surplus(modulo) operation by the prime number p_k, the Fermat's equation is not necessarily approved in arithmetic operation. However, if Fermat's equation is not approved in surplus(modulo) operation by the prime number p_k, the Fermat's equation is never approved in arithmetic operation. The necessary and sufficient conditions for Fermat's equation to be approved in surplus(modulo) operation by the prime number p_k without regard for (whatever) the natural number A, B and C are found. Then the natural number A, B and C include the natural number set of A_a, B_a and C_a in which Fermat's equation is approved in arithmetic operation. the Fermat's equation must be approved in surplus(modulo) operation by the prime number $p_j \neq p_k$ included in the natural number A_a. Based on this surplus(modulo) operation by the prime number $p_j \neq p_k$, it is proven that the index n is limited to only number 2. Consequently, Fermat's last theorem is proven.

1. The beginning

Fermat's last theorem is that the set of natural number A, B and C does not exist to approve Fermat's equation (1.1) with $n > 2$.

$$A^n + B^n = C^n \qquad (1.1)$$

Each of A, B and C is the product of involution of one or more prime number which are different each other. The prime number 2 is included in either of A or B. A, B and C do not share any prime factor.

Here, it is defined that $\mathrm{Re}\left(\frac{A}{p_k}\right)$ is surplus(remainder) when natural number A is surplus(modulo) operated(divided) by prime number p_k.

2. Method of proof

If the equation $A^n + B^n = C^n$ of Fermat's last theorem (hereafter, Fermat's equation) is approved in arithmetic operation, Fermat's equation is approved in surplus(modulo) operation by the prime number p_k. But even if Fermat's equation is approved in surplus(modulo) operation by the prime number p_k, the Fermat's equation is not necessarily approved in arithmetic operation. However, if Fermat's equation is not approved in surplus(modulo) operation by the prime number p_k, the Fermat's equation is never approved in arithmetic operation.

In section **3**, the necessary and sufficient conditions for Fermat's equation to be approved in surplus(modulo) operation by the prime number p_k without regard for (whatever) the natural number A, B and C are found. In section **4**, Then the natural number A, B and C include the natural number set of A_a, B_a and C_a in which Fermat's equation is approved in arithmetic operation. The Fermat's equation must be approved in surplus(modulo) operation by the prime number $p_j \neq p_k$ included in the natural number A_a. Based on this surplus(modulo) operation by the prime number $p_j \neq p_k$, it is proven that the index n is limited to only number 2. Consequently, Fermat's last theorem is proven.

3. The necessary and sufficient conditions

3.1 The necessary condition

If Fermat's equation (1.1) is surplus(modulo) operated by prime number $p_k = 2k + 1$, the following equation (3.1) is approved.

$$\mathrm{Re}\left(\frac{A^n+B^n}{p_k}\right) = \mathrm{Re}\left(\frac{A^n}{p_k}\right) + \mathrm{Re}\left(\frac{B^n}{p_k}\right) = \mathrm{Re}\left(\frac{C^n}{p_k}\right) \qquad (3.1)$$

The necessary conditions for the above equation (3.1) to be approved without regard for (whatever) natural number A, B and C are that the index n is $2mk$ (m is a positive integer) and that the prime number p_k is included in either of natural number A or B.

3.2 The sufficient condition

If the Fermat's equation (1.1) with the above necessary conditions is surplus(modulo) operated by prime number $p_k = 2k + 1$, the following equation (3.2) is approved.

$$\mathrm{Re}\left(\frac{A^{2km}+B^{2km}}{p_k}\right)=\mathrm{Re}\left(\frac{A^{2km}}{p_k}\right)+\mathrm{Re}\left(\frac{B^{2km}}{p_k}\right)=\mathrm{Re}\left(\frac{C^{2km}}{p_k}\right) \quad (3.2)$$

According to above necessary conditions, the above equation (3.2) is approved without regard for (whatever) the natural number A, B and C as shown in the following equation.

$$\mathrm{Re}\left(\frac{A^{2km}}{p_k}\right)+\mathrm{Re}\left(\frac{B^{2km}}{p_k}\right)=1=\mathrm{Re}\left(\frac{C^{2km}}{p_k}\right) \quad (3.3)$$

Then, the sufficient conditions are the same as the necessary conditions as shown above.

Since above equation (3.3) is approved in surplus(modulo) operation by the prime number p_k without regard for (whatever) the natural number A, B and C. the natural number A, B and C include the natural number set of A_a, B_a and C_a in which Fermat's equation (1.1) is approved in arithmetic operation.

4. Proof of n =2

The Fermat's equation (1.1) is rewritten to the following equation (4.1) using the necessary and sufficient conditions.

$$A^{2m}+B^{2m}=C^{2m} \quad (4.1)$$

Then, above equation (4.1) is rewritten as the following transformed Fermat's equation (4.2).

$$A^{2km}=C^{2km}-B^{2km}$$

$$=(C^{2k}-B^{2k})(C^{2k(m-1)}+C^{2k(m-2)}B^{2k}+C^{2k(m-3)}B^{4k}+\cdots+C^{2k}B^{2k(m-2)}+B^{2k(m-1)})$$

$$A^{2km}=(C^{2}-B^{2})(C^{2(k-1)}+C^{2(k-2)}B^{2}+C^{2(k-3)}B^{4}+\cdots+C^{2}B^{2(k-2)}+B^{2(k-1)})(C^{2k(m-1)}+C^{2k(m-2)}B^{2k}+C^{2k(m-3)}B^{4k}+\cdots+C^{2k}B^{2k(m-2)}+B^{2k(m-1)})$$

$$A^{2km}=(C^{2}-B^{2})(\sum_{i=1}^{k}C^{2(k-i)}B^{2(i-1)})(\sum_{i=1}^{m}C^{2k(m-i)}B^{2k(i-1)}) \quad (4.2)$$

When the equation (4.2) is surplus (modulo) operated by the prime number included in natural number A, the following equation (4.3) is approved.

$$\mathrm{Re}\left(\frac{A^{2km}}{p_k}\right)=\mathrm{Re}\left(\frac{(C^{2}-B^{2})(\sum_{i=1}^{k}C^{2(k-i)}B^{2(i-1)})(\sum_{i=1}^{k}C^{2k(m-i)}B^{2k(i-1)})}{p_k}\right)$$

$$\mathrm{Re}\left(\frac{A^{2km}}{p_k}\right)=\mathrm{Re}\left(\frac{C^{2}-B^{2}}{p_k}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k}C^{2(k-i)}B^{2(i-1)}}{p_k}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k}C^{2k(m-i)}B^{2k(i-1)}}{p_k}\right) \quad (4.3)$$

If the above transformed Fermat's equation (4.2) is surplus(modulo)

operated by the prime number p_k included in A, the following equation (4.3) is approved.

$$\mathrm{Re}\left(\frac{A^{2km}}{p_k}\right) = \mathrm{Re}\left(\frac{C^2-B^2}{p_k}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k} C^{2(k-i)}B^{2(i-1)}}{p_k}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k} C^{2k(m-i)}B^{2k(i-1)}}{p_k}\right) \quad (4.3)$$

Since the prime number p_k is included in A, the left side $\mathrm{Re}\left(\frac{A^{2Km}}{p_k}\right)$ of the above equation (4.3) is 0 without regard to m, the right side must be 0 without regard to m. But the following equation is approved.

$$\mathrm{Re}\left(\frac{\sum_{i=1}^{k} C^{2k(m-i)}B^{2k(i-1)}}{p_k}\right) = \mathrm{Re}\left(\frac{m}{p_k}\right) \neq 0$$

Therefore, the following equation (4.4) must be approved.

$$\mathrm{Re}\left(\frac{C^2-B^2}{p_k}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k} C^{2(k-i)}B^{2(i-1)}}{p_k}\right) = 0 \quad (4.4)$$

As a result, the following equations are approved without regard for (whatever) C and B.

$$p_k = 3 \qquad \mathrm{Re}\left(\frac{C^2-B^2}{p_k}\right) = 0 \quad (4.5)$$

$$p_k \neq 3 \qquad \mathrm{Re}\left(\frac{\sum_{i=1}^{k} C^{2(k-i)}B^{2(i-1)}}{p_k}\right) = 0 \quad (4.6)$$

Since above equation (3.3) is approved in surplus(modulo) operation by the prime number p_k without regard for (whatever) the natural number A, B and C. the natural number A, B and C include the natural number set of A_a, B_a and C_a in which Fermat's equation (1.1) is approved in arithmetic operation.

In the case of the natural number set of A_a, B_a and C_a, the following equation (4.7) must be approved in surplus(modulo) operation by the prime number $p_j \neq p_k (j \neq k)$ which is included in A_a.

$$\mathrm{Re}\left(\frac{{A_a}^{2km}}{p_j}\right) = \mathrm{Re}\left(\frac{{C_a}^2-{B_a}^2}{p_j}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k} {C_a}^{2(k-i)}{B_a}^{2(i-1)}}{p_j}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k} {C_a}^{2k(m-i)}{B_a}^{2k(i-1)}}{p_j}\right) = 0 \quad (4.7)$$

Since the prime number $p_j \neq p_k$ is included in A_a, the left side of the equation (4.7) is 0 without regard to (whatever) m. Therefore, the right side of the equation (4.7) must be 0 without regard to (whatever) m.

Therefore, the following equation must be approved.

$$\mathrm{Re}\left(\frac{C^2-B^2}{p_j}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k} C^{2(k-i)}B^{2(i-1)}}{p_j}\right) = 0$$

However, the equation (4.6) is approved in surplus(modulo) operation by the prime number p_k only without regard for (whatever) C_a and B_a in which Fermat's equation is approved in arithmetic operation. Therefore, the equation (4.6) is never approved in surplus(modulo) operation by the prime number $p_j \neq p_k (j \neq k)$.

$$\mathrm{Re}\left(\frac{\sum_{i=1}^{k} {C_a}^{2(k-i)} {B_a}^{2(i-1)}}{p_j}\right) \neq 0$$

Consequently, the following equation (4.8) must be approved in arithmetic operation.

$$\mathrm{Re}\left(\frac{{C_a}^2 - {B_a}^2}{p_j}\right) = 0 \qquad p_j \neq 3 \quad p_j \neq p_k (j \neq k) \tag{4.8}$$

The equation equation (4.8) shows $n = 2$ only.

As a result, Fermat's last theorem has been proven.

4. Conclusion

Fermat's equation with the necessary and sufficient conditions is approved in surplus(modulo) operation by the prime factor p_k without regard for the natural number A, B and C. The natural number A, B and C include the natural number set A_a, B_a and C_a in which Fermat's equation is approved in arithmetic operation. The Fermat's equation of the natural number set A_a, B_a and C_a must be approved in surplus(modulo) operation by the prime factor $p_j \neq p_k$ included in A_a. As a result, it is proven that the index n is limited to only number 2. Consequently, Fermat's last theorem has been proven.

References

There is no document nor thesis to which it refers in this thesis.

6. Supplement 1

Equation (4.4) is examined here.

$$\mathrm{Re}\left(\frac{C^{2k} - B^{2k}}{p_k}\right) = \mathrm{Re}\left(\frac{C^2 - B^2}{p_k}\right) \mathrm{Re}\left(\frac{\sum_{i=1}^{k} C^{2(k-i)} B^{2(i-1)}}{p_k}\right) = 0 \tag{4.4}$$

If $B^2 = 1$ is supposed, equation (4.4) is rewritten as follows.

$$\mathrm{Re}\left(\frac{C^2-1}{p_k}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k} C^{2(k-i)}}{p_k}\right)=0 \qquad (4.4.1)$$

$$h=\mathrm{Re}\left(\frac{C^2}{p_k}\right)$$

$$h^2=\mathrm{Re}\left(\frac{C^2}{p_k}\right)\mathrm{Re}\left(\frac{C^2}{p_k}\right)=\mathrm{Re}\left(\frac{C^{2*2}}{p_k}\right)$$

$$h^3=\mathrm{Re}\left(\frac{C^2}{p_k}\right)\mathrm{Re}\left(\frac{C^2}{p_k}\right)\mathrm{Re}\left(\frac{C^2}{p_k}\right)=\mathrm{Re}\left(\frac{C^{2*3}}{p_k}\right)$$

…

$$h^i=\mathrm{Re}\left(\frac{C^2}{p_k}\right)\mathrm{Re}\left(\frac{C^2}{p_k}\right)\ldots\mathrm{Re}\left(\frac{C^2}{p_k}\right)=\mathrm{Re}\left(\frac{C^{2i}}{p_k}\right)$$

…

$$h^k=\mathrm{Re}\left(\frac{C^{2k}}{p_k}\right)=1$$

$$\sum_{i=1}^{k} h^{k-i}=h^{k-1}+h^{k-2}+h^{k-3}+\cdots+h+1$$

As shown above, $h^i=\mathrm{Re}\left(\frac{C^{2i}}{p_k}\right)$ is an element of cyclic group $G=\langle h\rangle=\{h^k|k\in Z\}$ (k is order of cyclic group G)

$\sum_{i=1}^{k} h^{k-i}$ is the total sum of element of the cyclic group G.

the total sum is 0 in surplus (modulo) operation by prime number $p_k\neq 3$ as follows.

Equation (4.4.1) is rewritten as follows.

$$\mathrm{Re}\left(\frac{C^2-1}{p_k}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k} C^{2(k-i)}}{p_k}\right)=\left(\mathrm{Re}\left(\frac{C^2}{p_k}\right)-\mathrm{Re}\left(\frac{1}{p_k}\right)\right)\left(\sum_{i=1}^{k}\mathrm{Re}\left(\frac{C^{2(k-i)}}{p_k}\right)\right)=0$$

$$\left(\mathrm{Re}\left(\frac{C^2}{p_k}\right)-\mathrm{Re}\left(\frac{1}{p_k}\right)\right)=\mathrm{Re}\left(\frac{C^2}{p_k}\right)-1=h-1=0 \qquad (4.4.1.1)$$

Above equation (4.4.1.1) is approved in surplus (modulo) operation by prime number $p_k=3$ only.

$$\sum_{i=1}^{k}\mathrm{Re}\left(\frac{C^{2(k-i)}}{p_k}\right)=\mathrm{Re}\left(\frac{\sum_{i=1}^{k} h^{k-i}}{p_k}\right)=0 \qquad (4.4.1.2)$$

Above equation (4.4.1.2) is approved in surplus (modulo) operation by prime number $p_k\neq 3$.

The same applies to $g=\mathrm{Re}\left(\frac{B^2}{p_k}\right)$.

Then, equation (4.4.1) is rewritten as follows.

$$\sum_{i=1}^{k} \mathrm{Re}\left(\frac{C^{2(k-i)}B^{2(i-1)}}{p_k}\right) = \mathrm{Re}\left(\frac{\sum_{i=1}^{k} h^{(k-i)}g^{(i-1)}}{p_k}\right) = \sum_{i=1}^{k} \mathrm{Re}\left(\frac{h^{(k-i)}g^{(i-1)}}{p_k}\right) = 0 \qquad (4.4.1.3)$$

Direct product $f^i = h^{(k-i)}g^{(i-1)}$ of h and g is also an element of cyclic group $G = \langle h \rangle = \{h^k | k \in Z\}$ (k is order of cyclic group G)

6. Supplement 2

$$\mathrm{Re}\left(\frac{C^{2km}-B^{2km}}{p_k}\right) = \mathrm{Re}\left(\frac{B^{2km}\left(\left(\frac{C^{2km}}{B^{2km}}\right)-1\right)}{p_k}\right) = \mathrm{Re}\left(\frac{B^{2km}}{p_k}\right)\mathrm{Re}\left(\frac{(C/B)^{2km}-1}{p_k}\right) = 0$$

$$\mathrm{Re}\left(\frac{B^{2km}}{p_k}\right) = 1$$

$$\mathrm{Re}\left(\frac{C^{2km}-B^{2km}}{p_k}\right) = \mathrm{Re}\left(\frac{(C/B)^{2km}-1}{p_k}\right) = \mathrm{Re}\left(\frac{(\frac{C}{B})^{2}-1}{p_k}\right)\mathrm{Re}\left(\frac{\sum_{i=1}^{k}(\frac{C}{B})^{2(k-i)}}{p_k}\right) = 0$$

$$\mathrm{Re}\left(\frac{(\frac{C}{B})^{2}-1}{p_k}\right) = 0 \qquad (6.1)$$

Or

$$\mathrm{Re}\left(\frac{\sum_{i=1}^{k}(\frac{C}{B})^{2(k-i)}}{p_k}\right) = 0 \qquad (6.2)$$

Above equation (6.1) is examined.

Since natural number C and B don't share any prime number, C/B is rational number.

Therefore, Above equation (6.1) shows that surplus (modulo) operation by prime number is approved for rational number.

What about complex number?

Hidetomo Tohmori (non member) 〒302-0110 Moriya 3-2661-9 Ibaraki Japan
Electric Engineering Section of Department of Engineering at Tohoku University graduate
Unattached at present after Examiner & Hearing Examiner in Japan Patent Office and Patent attorney in Yamakawa International Patent Office