A simple proof of Fermat's last theorem

Hidetomo Tohmori*

*Unattached

Abstract. If the expression $A^n + B^n = C^n$ of Fermat's last theorem (hereafter, Fermat's expression) is approved by arithmetic operation of A, B and C, the Fermat's expression is approved too by surplus operation of prime factor p_k. But even if the Fermat's expression is approved by surplus operation of prime factor p_k, the Fermat's expression is not necessarily approved by arithmetic operation. However, if the Fermat's expression is not approved by surplus operation of prime factor p_k, the Fermat's expression is never approved by arithmetic operation. The necessary and sufficient condition for the Fermat's expression to be approved by surplus operation of the prime factor p_k without depending on A, B and C is that the index n include factor $2k$ and the prime factor p_k is included in A or B. The prime factor p_k is limited to number 3, because the Fermat's expression with the necessary and sufficient condition must be approved by arithmetic operation. As the result, the index n is limited to number 2. Consequently, Fermat's last theorem is proven.

1. The beginning

Fermat's last theorem is that natural number A, B and C do not exist to approve Fermat's expression (1.1) of the index n larger than the number 2.

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

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

Here, $\mathrm{Re}\left(\frac{A^n}{p_k}\right)$ is the surplus when A^n is divided by p_k.

2. Proof method of Fermat's last theorem

If the expression $A^n + B^n = C^n$ of Fermat's last theorem (hereafter, Fermat's expression) is approved by arithmetic operation, the Fermat's expression is approved too by surplus operation of prime factor p_k. But even if the Fermat's expression is approved by surplus operation of prime factor p_k, the Fermat's expression is not necessarily approved by arithmetic operation. However, if the Fermat's expression is not approved by surplus operation of prime factor p_k, the Fermat's expression is never approved by arithmetic operation. In section **3**, the necessary and sufficient condition for the Fermat's expression to be approved by surplus operation of the prime factor p_k without depending on A, B and C is derived. In section **4**, it is proven that the prime factor p_k is limited to number 3 and the index n is limited to number 2 for the Fermat's expression with the necessary and sufficient condition to be approved by arithmetic operation.

3. The necessary and sufficient condition for Fermat's expression to be approved by surplus operation of prime factor p_k

3.1 Necessary condition

If both side of Fermat's expression (1.1) is surplus operated by the prime factor $p_k = 2k + 1$ (k is either of $k_1, k_2, \dots, k_t$), the following expression (3.1) is approved.

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

The necessary condition for above expression (3.1) to be approved without depending on A, B and C is that the index n include factor $2k$ and the prime factor p_k is included in A or B.

3.2 Sufficient condition

Fermat's expression (1.1) is rewritten as the following expression (3.2) with above necessary condition.

$$A^{2m} + B^{2m} = C^{2m} \qquad (3.2)$$

If both side of above expression are surplus operated by the prime factor p_k, the following expression (3.3) is approved.

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

Because the index n is $2m$ (m is the least common multiple of

$k_1, k_2, \ldots, k_t$) and the prime factor p_k is included in A or B, the above expression (3.3) is approved without depending on A, B and C as shown in following expression.

$$\mathrm{Re}\left(\frac{A^{2m}}{p_k}\right) + \mathrm{Re}\left(\frac{B^{2m}}{p_k}\right) = 1 = \mathrm{Re}\left(\frac{C^{2m}}{p_k}\right) \qquad (3.4)$$

Necessary condition is sufficient condition too as shown in above.

3.3 Proof of m =1

If the expression (3.2) is approved by arithmetic operation of A, B and C, the expression (3.2) is rewritten as the following expression (3.5).

α is positive integer including zero 0.

β, γ and δ are positive integer.

$B^m = \alpha A^m + \gamma \qquad C^m = \beta A^m + \delta \qquad A^m > \gamma \neq \delta \qquad (*1)$

A and γ, δ do not share any prime factor $(*2)$.

$$A^{2m} + (\alpha A^m + \gamma)^{2m} = (\beta A^m + \delta)^{2m} \qquad (3.5)$$

If both side of above expression are surplus operated by the prime factor p_k, the following expression (3.6) is approved.

$$\mathrm{Re}\left(\frac{(\alpha A^m + \gamma)^2}{p_k}\right) = \mathrm{Re}\left(\frac{(\beta A^m + \delta)^2}{p_k}\right) = 1$$

$$\mathrm{Re}\left(\frac{\gamma^2}{p_k}\right) = \mathrm{Re}\left(\frac{\delta^2}{p_k}\right) = 1 \qquad (3.6)$$

The above expression (3.6) must be approved constantly without depending on γ and δ. Therefore, prime factor p_k is only one of $p_1 = 3$. Then, $m = 1$ and $n = 2$.

4. Conclusion

Fermat's expression $A^n + B^n = C^n$ is limited to the expression $A^{2m} + B^{2m} = C^{2m}$ to be approved by surplus operation of prime factor p_k. Then, for the expression $A^{2m} + B^{2m} = C^{2m}$ to be approved in arithmetic operation of A, B and C, prime factor p_k is only one of $p_1 = 3$, m is 1 and n is 2. Therefore, natural number A, B and C of Fermat's expression $A^n + B^n = C^n$ with $\mathrm{n} > 2$ don't exist. Consequently, Fermat's last theorem has been proven.

5. Supplement

$(*\mathbf{1})$ Proof of $\gamma \neq \delta$

$B^m = \alpha A^m + \gamma \qquad C^m = \beta A^m + \delta$

Based on the expression (3.5), the following inequality is formed.

$B^m < C^m < A^m + B^m$

$\alpha A^m + \gamma < \beta A^m + \delta < A^m + \alpha A^m + \gamma$

If $\gamma = \delta$, the above inequality is rewritten as the following.

$\alpha A^m < \beta A^m < (\alpha + 1)A^m$

$\alpha < \beta < (\alpha + 1)$

However, such integer β could not exist.

Therefore, $\gamma \neq \delta$

$(*\mathbf{2})$ If A and γ, δ share a prime factor, A and B, C must share the prime factor. However, A and B, C don't share any prime factor. Therefore, A and γ, δ don't share any prime factor.

References

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

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