A simple proof of Fermat’s last theorem

Hidetomo Tohmori*

*Unattached

Abstract. If the expression $A^n + B^n = C^n$ in Fermat's last theorem (hereafter, Fermat's expression) is approved in arithmetic operation, Fermat's expression is approved too in surplus operation. But even if Fermat's expression is approved in surplus operation, Fermat's expression is not necessarily approved in arithmetic operation. However, if Fermat's expression is not approved in surplus operation, Fermat's expression is never approved in arithmetic operation. For Fermat's expression to be approved in surplus operation, the prime factors of A and B are decided from the index n and oppositely the index n is decided from the prime factors of A and B. Moreover, the index n is limited to the number 2 because the prime factors of A and B are limited to only one of the number 3. Therefore, for Fermat's expression to be approved in arithmetic operation, the index n is limited to the number 2. Consequently, Fermat's last theorem is proven.

1. The beginning

If Fermat's expression $A^n + B^n = C^n$ in Fermat's last theorem is approved in arithmetic operation, Fermat's expression is approved too in surplus operation. But even if Fermat's expression is approved in surplus operation, Fermat's expression is not necessarily approved in arithmetic operation. However, if Fermat's expression is not approved in surplus operation, Fermat's expression is never approved in arithmetic operation. Hereinafter, Fermat's expression is examined to be approved in surplus operation.

2. Fermat’s last theorem

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

$$A^n + B^n = C^n \qquad (2.1)$$

Each of natural number A, B and C is the product of involution of one or more prime factors that 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. It is assumed that the prime factor of A except 2 is $p_k = 2k + 1$ (k is either of $k_1, k_2, \dots, k_t$) and $p_i = 2i + 1$ (i is either of $i_1, i_2, \dots, i_u$). It is assumed that the prime factor of B except 2 is $q_l = 2l + 1$ (l is either of $l_1, l_2, \dots, l_s$) and $q_j = 2j + 1$ (j is either of $j_1, j_2, \dots, j_v$).

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

3. Fermat's expression to be approved in surplus operation

3.1 The prime factors p_k and q_l decide the index $n = 2m$

It is assumed that the expressions (3.1)~(3.4) are approved when both sides of the expression (2.1) is divided by p_i, p_k, q_j and q_l.

The above assumption is reasonable because the surplus is 1 or positive integer other than 1.

$$\mathrm{Re}\left(\frac{B^n}{p_i}\right) = \mathrm{Re}\left(\frac{C^n}{p_i}\right) \neq 1 \qquad (3.1)$$

$$\mathrm{Re}\left(\frac{B^n}{p_k}\right) = \mathrm{Re}\left(\frac{C^n}{p_k}\right) = 1 \qquad (3.2)$$

$$\mathrm{Re}\left(\frac{A^n}{q_j}\right) = \mathrm{Re}\left(\frac{C^n}{q_j}\right) \neq 1 \qquad (3.3)$$

$$\mathrm{Re}\left(\frac{A^n}{q_l}\right) = \mathrm{Re}\left(\frac{C^n}{q_l}\right) = 1 \qquad (3.4)$$

Because the index n include $2k$ to approve the expression (3.2), the index n include twice number of the least common multiple of $k_1, k_2, \dots, k_t$. Because index n includes $2k$ to approve the expression (3.4), the index n includes twice number of the least common multiple of $l_1, l_2, \dots, l_s$.

Then, the following expression (3.5) is approved.

$$n = 2m \qquad (3.5)$$

m is the least common multiple of $k_1, k_2, \dots, k_t$ and $l_1, l_2, \dots, l_s$.

Namely, the prime factors p_k and q_l decide the index $n = 2m$.

3.2 The index $n = 2m$ decide the prime factors p_k and q_l

The prime factor $r_h = 2h + 1$ (h is either of $h_1, h_2, \dots, h_w$ and m is the least common multiple of $h_1, h_2, \ldots, h_w$) corresponds to p_k or q_l. Because the following illogical result occurs when r_h doesn't correspond to neither of p_k or q_l.

$$A^{2m} + B^{2m} = C^{2m}$$

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

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

In other words, p_k and q_l are the same as r_h derived from m.

Namely, the index n decide the prime factors p_k and q_l.

3.3 Proof of m =1

As shown in above, the expressions (3.6)～(3.10) are approved.

$$A^{2m} + B^{2m} = C^{2m} \tag{3.6}$$

$$\mathrm{Re}\left(\frac{B^{2m}}{p_i}\right) = \mathrm{Re}\left(\frac{C^{2m}}{p_i}\right) \neq 1 \tag{3.7}$$

$$\mathrm{Re}\left(\frac{A^{2m}}{q_j}\right) = \mathrm{Re}\left(\frac{C^{2m}}{q_j}\right) \neq 1 \tag{3.8}$$

$$\mathrm{Re}\left(\frac{B^{2\mathrm{m}}}{p_k}\right) = \mathrm{Re}\left(\frac{C^{2\mathrm{m}}}{p_k}\right) = 1 \tag{3.9}$$

$$\mathrm{Re}\left(\frac{A^{2\mathrm{m}}}{q_l}\right) = \mathrm{Re}\left(\frac{C^{2\mathrm{m}}}{q_l}\right) = 1 \tag{3.10}$$

Then, the above expression (3.8) is rewritten as the following expression (3.11).

α is positive integer including zero 0.

β, γ and δ are positive integer.

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

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

$$\mathrm{Re}\left(\frac{(\alpha A^m+\gamma)^2}{p_k}\right) = \mathrm{Re}\left(\frac{(\beta A^m+\delta)^2}{p_k}\right) = 1 \tag{3.11}$$

Even if the operational order is replaced in surplus operation, the operational result must be the same. Therefore, the following expression (3.12) must be approved constantly without depending on γ and δ.

$$\mathrm{Re}\left(\frac{\gamma^2}{p_k}\right) = \mathrm{Re}\left(\frac{\delta^2}{p_k}\right) = 1 \tag{3.12}$$

Therefore, the prime factor p_k of A is limited to only one of $p_1 = 3$.

And then, the prime factor q_l of B don’t exist.

The following expressions (3.13) and (3.14) are approved.

$$m = 1 \tag{3.13}$$

$$n = 2. \tag{3.14}$$

Also, the expressions (3.8) and (3.10) are rewritten as the following expressions (3.15) and (3.16).

$$\mathrm{Re}\left(\frac{B^2}{p_i}\right) = \mathrm{Re}\left(\frac{C^2}{p_i}\right) \tag{3.15}$$

$$\mathrm{Re}\left(\frac{A^2}{q_j}\right) = \mathrm{Re}\left(\frac{C^2}{q_j}\right) \tag{3.16}$$

As mentioned above, for Fermat's expression to be approved in surplus operation, the index n is limited to the number 2 because m is limited to the number 1.

4. Conclusion

Since the index n is limited to the number 2 for Fermat's expression to be approved in surplus operation, the index n is limited to the number 2 for Fermat's expression to be approved in arithmetic operation. Therefore, natural number A , B and C in Fermat's expression $A^n + B^n = C^n$ of $n > 2$ don't exist. Consequently, Fermat's last theorem is proven.

5. Supplement

(∗ 1) Proof of $\gamma \neq \delta$

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

Based on the expression(4), 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, $\gamma \neq \delta$

(∗ 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