Proof by small theorem of Fermat's last theorem

Hidetomo Tohmori 2016.11.07

$$A^n + B^n = C^n \qquad (1)$$

A, B and C are respectively factorized by the product of the involution of a mutually different prime factor.

Number 2 must be contained in either of A or B.

Therefore, A, B and C don't contain any common prime factor.

Prime factors of A except for 2 are assumed to be $p_k = 2k + 1$ (k is either of $k_1, k_2, \dots, k_t$) and p_i (i is either of $i_1, i_2, \dots, i_u$).

Prime factors of B except for 2 are assumed to be $q_l = 2l + 1$ (l is either of $l_1, l_2, \dots, l_s$) and q_j (j is either of $j_1, j_2, \dots, j_v$).

Here, it is defined that $\mathrm{Re}\left(\frac{A^n}{q_l}\right)$ is the surplus when A^n is surplus operated by the prime factor q_l.

It is assumed that the following expressions (2)~(5) are formed.

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

$$\mathrm{Re}\left(\frac{A^n}{q_j}\right) = \mathrm{Re}\left(\frac{C^n}{q_j}\right) \qquad (3)$$

$$\mathrm{Re}\left(\frac{B^n}{p_k}\right) = \mathrm{Re}\left(\frac{C^n}{p_k}\right) = 1 \qquad (4)$$

$$\mathrm{Re}\left(\frac{A^n}{q_l}\right) = \mathrm{Re}\left(\frac{C^n}{q_l}\right) = 1 \qquad (5)$$

Then, since the number n must contain $2k$ as a factor for the expression (4) to be formed, the number n must contain two times of the least common multiple of $k_1, k_2, \dots, k_t$ as a factor.

Since the same thing is approved for the expression (5), the number n must contain two times of the least common multiple of $l_1, l_2, \dots, l_s$ as a factor.

Therefore, the following expression (6) is formed.

$$n = 2m \qquad (6)$$

m is the least common multiple of $k_1, k_2, \dots, k_t$ and $l_1, l_2, \dots, l_s$(*3).

Then, the expressions (1)~(5) are rewritten as the following expressions (7)~(11).

$$A^{2m} + B^{2m} = C^{2m} \quad (7)$$

$$\mathrm{Re}\left(\frac{B^{2m}}{p_i}\right) = \mathrm{Re}\left(\frac{C^{2m}}{p_i}\right) \quad (8)$$

$$\mathrm{Re}\left(\frac{A^{2m}}{q_j}\right) = \mathrm{Re}\left(\frac{C^{2m}}{q_j}\right) \quad (9)$$

$$\mathrm{Re}\left(\frac{B^{2\mathrm{m}}}{p_k}\right) = \mathrm{Re}\left(\frac{C^{2\mathrm{m}}}{p_k}\right) = 1 \quad (10)$$

$$\mathrm{Re}\left(\frac{A^{2\mathrm{m}}}{q_l}\right) = \mathrm{Re}\left(\frac{C^{2\mathrm{m}}}{q_l}\right) = 1 \quad (11)$$

Then, the above expression (10) is rewritten as following expression (12).

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

A and γ, δ do not contain any common prime factor (∗ 2).

$$\mathrm{Re}\left(\frac{(\alpha A^m+\gamma)^2}{p_k}\right) = \mathrm{Re}\left(\frac{(\beta A^m+\delta)^2}{p_k}\right) = 1 \quad (12)$$

Even if the operational order is replaced, the operational result must be the same. Therefore, the following expression (13) must be formed constantly without depending on γ and δ.

$$\mathrm{Re}\left(\frac{\gamma^2}{p_k}\right) = \mathrm{Re}\left(\frac{\delta^2}{p_k}\right) = 1 \quad (13)$$

Therefore, the prime factor p_k of A must be only one of $p_1 = 3$ for the expression (10) to be formed constantly without depending on γ and δ. And the prime factor q_l of B don't exist.

Then, the following expressions (14) and (15) must be formed.

$$m = 1 \quad (14)$$

$$n = 2. \quad (15)$$

And also, the expressions (8) and (9) are rewritten as the following expressions (16) and (17).

$$\mathrm{Re}\left(\frac{B^2}{p_i}\right) = \mathrm{Re}\left(\frac{C^2}{p_i}\right) \quad (16)$$

$$\mathrm{Re}\left(\frac{A^2}{q_j}\right) = \mathrm{Re}\left(\frac{C^2}{q_j}\right) \quad (17)$$

Natural number A, B and C for the expression (1) of $\mathrm{n} > 2$ to be formed don't exist as mentioned above.

(∗ 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.

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

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

When $\gamma = \delta$, 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 common prime factor, A and B, C must share the common prime factor. However A and B, C don't share any common prime factor. Therefore, A and γ, δ don't share any common prime factor.

(∗ 3) 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 $h_1, h_2, \dots, h_w$) 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.

$$A^{2m} + B^{2m} = C^{2m} \qquad (4)$$

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

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

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

However, as mentioned above, p_k is only one of $p_1 = 3$, $m = 1$, $n = 2$ and q_l doesn't exist.