フェルマー最終定理の小定理による証明

東森秀朋　2016.11.07

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

上式(1)を成立させる自然数A、B及びC は、それぞれ、互いに相異する素因数の累乗の積に分解される。

素因数2はAまたはBに含まれる。A、B及びCは共通の素因数を有さない。

自然数Aの素因数2を除く素因数を$p_k = 2k + 1$（kは$k_1, k_2, \dots, k_t$のいずれか)及びp_i（i は$i_1, i_2, \dots, i_u$のいずれか)とする。 同様に、自然数Bの素因数2を除く素因数を$q_l = 2l + 1$（lは$l_1, l_2, \dots, l_s$のいずれか)及びq_j（jは$j_1, j_2, \dots, j_v$のいずれか）とする。

ここでは、$\mathrm{Re}\left(\frac{A^n}{q_l}\right)$は$A^n$を$q_l$で剰余演算したときの剰余であると定義する。

式(1)の両辺を$q_l = 2l + 1$で剰余演算すると、式(2)が成立すると仮定する。

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

$$\mathrm{Re}\left(\frac{B^n}{q_l}\right) = 0$$

$$\mathrm{Re}\left(\frac{A^n}{q_l}\right) = \mathrm{Re}\left(\frac{C^n}{q_l}\right) = 1 \qquad (2)$$

式(2)を成立させるためにnは$2l$を因子として含むから、nは$l_1, l_2, \dots, l_s$の最小公倍数の倍数を因子として含む。同じことは、Aの$p_k = 2k + 1$についても成立するから、nは$k_1, k_2, \dots, k_t$の最小公倍数の倍数を因子として含む。

それ故、次式(3)が成立する。

$$n = 2m \tag{3}$$

mは$k_1, k_2, \dots, k_t$及び$l_1, l_2, \dots, l_s$の最小公倍数である$(*3)$。

そのとき、式(1)は式(4)に書き換えられる。そして、次の式(5)～(8)が成立する。

$$A^{2m} + B^{2m} = C^{2m} \tag{4}$$

$$\mathrm{Re}\left(\frac{B^{2m}}{p_i}\right) = \mathrm{Re}\left(\frac{C^{2m}}{p_i}\right) \tag{5}$$

$$\mathrm{Re}\left(\frac{A^{2m}}{q_j}\right) = \mathrm{Re}\left(\frac{C^{2m}}{q_j}\right) \tag{6}$$

$$\mathrm{Re}\left(\frac{B^{2\mathrm{m}}}{p_k}\right) = \mathrm{Re}\left(\frac{C^{2\mathrm{m}}}{p_k}\right) = 1 \tag{7}$$

$$\mathrm{Re}\left(\frac{A^{2\mathrm{m}}}{q_l}\right) = \mathrm{Re}\left(\frac{C^{2\mathrm{m}}}{q_l}\right) = 1 \tag{8}$$

ここで、上式(7)は次式(9)に書き換えられる。

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

A 及び $\gamma,\ \delta$ は共通の素因数を有さない$(*2)$。

$$\mathrm{Re}\left(\frac{(\alpha A^m+\gamma)^2}{p_k}\right) = \mathrm{Re}\left(\frac{(\beta A^m+\delta)^2}{p_k}\right) = 1 \tag{9}$$

剰余演算において、その順序を入れ換えても、その結果は同じである。それ故、次式(10)はγ及びδに依存しないで成立する。

$$\mathrm{Re}\left(\frac{\gamma^2}{p_k}\right) = \mathrm{Re}\left(\frac{\delta^2}{p_k}\right) = 1 \qquad (10)$$

γ及びδに依存しないで上式(10)を成立させるp_kは $p_1 = 2\times1 + 1 = 3$のみである。そして、q_lは存在しない。

そのとき、次の式(11)及び(12)が成立する。

$$m = 1 \qquad (11)$$
$$n = 2 \qquad (12)$$

そして、式(5)及び(6)は次式(13)及び(14)に書き換えられる。

$$\mathrm{Re}\left(\frac{B^2}{p_k}\right) = \mathrm{Re}\left(\frac{C^2}{p_k}\right) \qquad (13)$$

$$\mathrm{Re}\left(\frac{A^2}{q_l}\right) = \mathrm{Re}\left(\frac{C^2}{q_l}\right) \qquad (14)$$

以上のとおり、$\mathrm{n} > 2$の式(1)を成立させる自然数A、B及びC は存在しない。

$(*1)$ $\gamma \neq \delta$の証明

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

式(4)から次の不等式が成立する。

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

ここで、$\gamma = \delta$であるならば、次の不等式が成立する。

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

しかしながら、このような整数βは存在し得ない。

それ故、$\gamma \neq \delta$である。

$(*2)$ もしAと$\gamma,\ \delta$ がある素因子を共有するならば、Aと$B,\ C$ もその素因子を共有することになる。しかしながら、Aと$B,\ C$ はいかなる素因子も共有することはない。 それ故、A と $\gamma,\ \delta$ は素因子を共有できない。

$(*3)$ 素因数$r_h = 2h+1$（hは$h_1, h_2, \dots, h_w$のいずれかであって、$h_1, h_2, \dots, h_w$の最小公倍数はmである。)はp_k又はq_lのいずれかに一致する。何故ならば、もしr_hがp_k又はq_lのいずれかにも一致しないとき、次のように不合理を生じるからである。

$$A^{2m} + B^{2m} = C^{2m} \tag{4}$$

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

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

言い換えれば、p_k及びq_lは最小公倍数mから得られる素因数r_hと同一である。

しかしながら、既に証明されているように、$p_k = p_1 = 3$のみであり、最小公倍数$\mathrm{m} = 1$であり、そして、q_lは存在しない。