

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

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

上式(1)を成立させる自然数 A 、 B 及び C は、それぞれ、互いに相異な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、 $\text{Re}\left(\frac{A^n}{q_l}\right)$ 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。

$$\begin{aligned} \text{Re}\left(\frac{A^n}{q_l}\right) + \text{Re}\left(\frac{B^n}{q_l}\right) &= \text{Re}\left(\frac{C^n}{q_l}\right) \\ \text{Re}\left(\frac{B^n}{q_l}\right) &= 0 \\ \text{Re}\left(\frac{A^n}{q_l}\right) &= \text{Re}\left(\frac{C^n}{q_l}\right) = 1 \end{aligned} \quad (2)$$

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。

$$n = 2m \quad (3)$$

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。

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

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

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

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

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

ここで、上式(7)は次式(9)に書き換えられる。

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

A 及び γ, δ は共通の素因数を有さない(*2)。

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

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。

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

γ 及び δ に依存しないで上式(10)を成立させる p_k は $p_1 = 2 \times 1 + 1 = 3$ 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。

$$m = 1 \quad (11)$$

$$n = 2 \quad (12)$$

そして、式(5)及び(6)は次式(13)及び(14)に書き換えられる。

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

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

以上のとおり、 $n > 2$ 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

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

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 γ, δ 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 γ, δ 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。

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

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

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

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 $m = 1$ であり、そして、 q_l は存在しない。