1　$n = 4$ の場合におけるフェルマの定理の証明

命題 1.1.　方程式

(1) $$x^2 + y^2 = z^2$$

の原始解，すなわち x, y, z の最大公約数が 1 であるような正の整数解はすべて

(2) $$x = a^2 - b^2, \qquad y = 2ab, \qquad z = a^2 + b^2$$

あるいは

(3) $$x = 2ab, \qquad y = a^2 - b^2, \qquad z = a^2 + b^2$$

なる形で書き表すことができる．ただし a, b は正の整数で

(4) $$a > b, \qquad (a, b) = 1, \qquad a \not\equiv b \pmod 2$$

を満たす．

証明．　x, y, z を方程式 (1) の原始解とする．x, y, z のどれか 2 つに 1 でない公約数 d があるとすると，残りの 1 つも d を約数とする．よって x, y, z はどの 2 つも互いに素である．特に x, y の両方ともが偶数になることはない．また，x と y とが奇数であるとすると

$$x \equiv 1, \qquad y \equiv 1 \pmod 2$$

より

$$x^2 \equiv 1, \qquad y^2 \equiv 1 \pmod 4$$

となるから，(1) より

$$z^2 = x^2 + y^2 \equiv 2 \pmod 4$$

となる．これは z を奇数としても偶数としても成り立たない．よって $x \not\equiv y \pmod 2$ である．

x を奇数，y を偶数とする．このとき z は奇数である．(1) を変形すると

(5) $$y^2 = (z - x)(z + x)$$

となる．y^2 は偶数かつ正なので，$z + x$, $z - x$ はともに偶数かつ正である．よって正の整数 m, n によって

(6) $$z + x = 2m, \qquad z - x = 2n$$

とおくことができ

(7) $$x = m - n, \qquad z = m + n$$

となる．x, z は互いに素なので

(8) $$m > n, \qquad (m, n) = 1, \qquad m \not\equiv n \pmod 2$$

である．

(6) を (5) に代入すれば

$$y^2 = 4mn \tag{9}$$

y は偶数であるから，$y = 2y'$ とおけば ${y'}^2 = mn$ となる．m, n は互いに素だから m, n は別々に完全平方数にならなければならない．したがって正の整数 a, b によって

$$m = a^2, \qquad n = b^2$$

とおくことができる．したがって (7)，(9) により原始解 x, y, z は (2) の形で書け，(8) により a, b は (4) を満たす.

x が偶数，y が奇数のときも同様にして原始解 x, y, z が (3) の形で書けて，a, b が (4) を満たすことがいえる. □

定理 1.2 ($n = 4$ の場合における Fermat の定理)．方程式

$$x^4 + y^4 = z^4 \tag{10}$$

は正の整数解をもたない.

証明. Euler による証明．方程式 (10) の正の整数解 x, y, z が存在するとして矛盾を導く.

$u = z^2$ とおくことにより

$$x^4 + y^4 = u^2 \tag{11}$$

も正の整数解 x, y, z をもたなければならない．u の値が最小になるような解を x_1, y_1, u_1 とする．このとき $(x_1, y_1, u_1) = 1$ と考えてよい．なぜならこれら 3 つの数が共通因数をもてば u_1 よりも小さい u の値があるからである．そうすれば x_1, y_1, u_1 は方程式

$$x^2 + y^2 = u^2$$

の原始解である．命題 1.1 により，正の整数 a, b によって

$$x_1^2 = a^2 - b^2, \tag{12}$$

$$y_1^2 = 2ab, \tag{13}$$

$$u_1 = a^2 + b^2 \tag{14}$$

と表すことができる．ただし

$$a > b, \qquad (a, b) = 1, \qquad a \not\equiv b \pmod 2$$

である．しかもこの場合は a が奇数で b が偶数である．なぜなら，もし a が偶数，b が奇数とすれば，(12) より

$$x_1^2 = a^2 - b^2 \equiv -1 \,(\mathrm{mod}\, 4)$$

となり，一方，これは x_1 が偶数，奇数のいずれであっても成り立たないからである.

さて，a, b が互いに素で，a が奇数，b が偶数ならば，(13) より互いに素な a と $2b$ との積が完全平方数であるから，正の整数 u_2, v によって

$$a = u_2^2, \qquad 2b = 4v^2 \tag{15}$$

となる．また (12) により

$$x_1^2+b^2=a^2, \qquad (a,\, b,\, x_1)=1$$

であるから，再び命題 1.1 によって

$$x_1^2=a_1^2-b_1^2, \tag{16}$$

$$b=2a_1b_1, \tag{17}$$

$$a=a_1^2+b_1^2 \tag{18}$$

と表され

$$a_1>b_1, \qquad (a_1,\, b_1)=1, \qquad a_1 \not\equiv b_1 \pmod 2$$

でなれけばならない．(15)，(17) より

$$v^2=a_1b_1$$

これより，また $a_1,\, b_1$ は完全平方数となり

$$a_1=x_2^2, \qquad b_1=y_2^2$$

とおくことができる．したがって (15)，(18) により

$$x_2^4+y_2^4=u_2^2$$

これは (11) と同じ形の方程式で，$x_2,\, y_2,\, u_2$ は (11) の解であり，(14)，(15) より明らかに

$$u_2 \le a < u_1$$

となる．これは u_1 の最小性に反する．したがって (10) は正の整数解をもたない． □