1　四つの平方数の和に関する Lagrange の定理

定理 1.1 (Lagrange).　任意の正の整数 n は必ず

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2, \qquad x_i \geq 0, \qquad i = 1, 2, 3, 4$$

の形に書き表すことができる．

証明.　恒等式

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = {} & (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \\ & + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ & + (x_1y_3 - x_2y_4 + x_3y_1 - x_4y_2)^2 \\ & + (x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1)^2\end{aligned}$$

によって四つの平方数の和の積もまた，四つの平方数の和として表されるから，定理を n が素数である場合に証明すれば十分である．

$n = 2$ のときは $2 = 1^2 + 1^2$ により明らかである．

p を奇素数とする．まず，p^2 より小さな p の倍数で，四つの平方数の和になっている数が存在することを示す．そのために $(p+1)/2$ 個の平方数

$$0^2, \quad 1^2, \quad 2^2, \quad \ldots, \quad \left(\frac{p-1}{2}\right)^2 \tag{1}$$

を考える．これらのどの 2 つも p を法として合同ではない．よって

$$-1, \quad -1-1^2, \quad -1-2^2, \quad \ldots, \quad -1-\left(\frac{p-1}{2}\right)^2 \tag{2}$$

も p を法として合同ではない．(1), (2) を合わせると全部で $p+1$ 個の数がある．よって部屋割り論法から p を法として考えて同じ剰余類に入る数がある．すなわち

$$x_1^2 \equiv -1 - x_2^2 \pmod{p}, \qquad 0 \leq x_i \leq \frac{p-1}{2}, \qquad i = 1, 2$$

となる整数 x_1, x_2 がある．これより，ある正の整数 h によって

$$x_1^2 + x_2^2 + 1 = ph, \qquad 0 \leq x_i \leq \frac{p-1}{2}, \qquad i = 1, 2 \tag{3}$$

と書ける．しかも

$$\begin{aligned}ph &= x_1^2 + x_2^2 + 1 \\ &\leq \frac{(p-1)^2}{4} + \frac{(p-1)^2}{4} + 1 \\ &= \frac{(p-1)^2}{2} + 1 \\ &< \frac{(p-1)^2}{2} + \frac{(p-1)^2}{2} \\ &< p^2\end{aligned}$$

であるから $1 \leq h < p$ である．

いま一般に

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = ph, \qquad 1 < h < p \tag{4}$$

とするとき，$0 < h' < h$ であるような整数 h' を適当にとって ph' が 4 つの平方数の和に分解できることを示す．これが示せれば (3) の形から，h が 1 になるまで上の操作を続けることにより，最後には p 自身の分解が得られる．

(4) における x_1, x_2, x_3, x_4 を h で割り，絶対値において最小の剰余を y_1, y_2, y_3, y_4 とおいて

$$x_1 \equiv y_1, \quad x_2 \equiv y_2, \quad x_3 \equiv y_3, \quad x_4 \equiv y_4 \pmod{h} \tag{5}$$

$$|y_i| \geq \frac{h}{2}, \qquad i = 1, 2, 3, 4 \tag{6}$$

とする．このとき

$$y_1^2 + y_2^2 + y_3^2 + y_2^4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{h}$$

よって，ある整数 $h' \geq 0$ によって

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = hh' \tag{7}$$

と書ける．これを冒頭に述べた恒等式に代入すると

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 = ph^2h'$$

ただし (5) によって

$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv \sum_{i=1}^{4} x_i^2 \equiv 0 \pmod{h},$$

$$z_2 = x_1y_1 - x_2y_2 + x_3y_4 - x_4y_3 \equiv x_1x_2 - x_2x_1 + x_3x_4 - x4x_3 = 0 \pmod{h}$$

同様に

$$z_3 = x_1y_3 - x_2y_4 + x_3y_1 - x_4y_2 \equiv 0 \pmod{h}$$

$$z_4 = x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1 \equiv 0 \pmod{h}$$

よって

$$z_1 = ht_1, \quad z_2ht_2, \quad z_3ht_3, \quad z_4ht_4$$

とおけば

$$t_1^2 + t_2^2 + t_3^2 + t_4^2 = ph'$$

となる．

さて，(6) によって

$$hh' = \sum_{i=1}^{4} y_i^2 \leq 4\left(\frac{h}{2}\right)^2 = h^2$$

ゆえに $h' \leq h$.

もし仮に等号が成り立つならば

$$y_i = \frac{h}{2}, \qquad i = 1, 2, 3, 4$$

したがって $h/2$ は整数であり，h は偶数である．また $h > 1$ より各 i について $y_i \neq 0$．よって x_i は h の倍数にはなりえない．ゆえに x_i は $h/2$ の奇数倍でなければならない．いま

$$x_i = (2m_i + 1)\frac{h}{2}$$

とおき，(3) に代入すれば

$$\frac{h}{4}\sum_{i=1}^{4}(2m_i + 1)^2 = p$$

を得る．左辺は偶数だからこれは矛盾である．したがって $h' < h$ である．

最後に $h' \neq 0$ を示す．もし $h' = 0$ とすると (7) から $y_1 = y_2 = y_3 = y_4 = 0$ となる．よって (5) から

$$x_1 = hu_1, \quad x_2 = hu_2, \quad x_3 = hu_3, \quad x_4 = hu_4$$

となる整数 u_1, u_2, u_3, u_4 が定まる．このとき (4) の両辺を h で割ると

$$h(u_1^2 + u_2^2 + u_3^2 + u_4^2) = p, \qquad 1 < h < p$$

となる．p は素数なのでこれは矛盾である．したがって $h' \neq 0$. □