P-11

ウェアリングの問題について
Waring's problem

○山本 啓史
Hiroshi Yamamoto[1]

Abstract: In this talk, we introduce Lagrange's theorem and Waring's problem. The method of the proof of Lagrange's theorem is elementary, whereas Waring's problem is one of the most difficult problem in Number Theory and only very few facts are proven. Here we survey the proof of Lagrange's theorem, so-called theorem of four squares, namely any positive integer is represented by the sum of four squares.

1　ウェアリングの問題

平方数，立法数などのべき乗数の和として自然数を表すことに関する問題をウェアリングの問題と称する．例えば，$k,m,n\in\mathbb{N}$ に対して，$k\geq 2$ を固定して，任意の n が m 個の整数 $x_1,\cdots,x_m$ の k 乗数の和によって

$$n={x_1}^k+\cdots+{x_m}^k$$

と表現されるときの，m の最小値 s を求める問題がある．以下，断りがない限り，$k,m,n\in\mathbb{N}$ とする．
A. Wieferich (1909) が $k=3$ のとき $s=9$ であることを証明したと発表した．しかし，その証明中の誤りを A. Kempner (1912) が修正した．その後，L. E. Dickson, S. S. Pillai，I. Niven らが $k\geq 7$ の各 k に対して s を決定し，更に Pillai (1940) は $k=6$ のとき $s=73$ であること，J.-R. Chen (1964) は $k=5$ のとき $s=37$ であることを得た．$k=4$ については，R. Balasubramanian，J.-R. Deshouillers, F. Dress が $s=19$ であることを 1986 年に示した．
ここではウェアリングの問題の中でも，初等的な議論で証明される，4 平方数定理とも呼ばれるラグランジュの定理を扱うことにする．ここでいう平方数とは，非負の整数の 2 乗数のことである．

2　ラグランジュの定理

Theorem 1 (ラグランジュの定理，1770)
任意の自然数 n は 4 個の平方数の和で

$$n={x_1}^2+{x_2}^2+{x_3}^2+{x_4}^2$$

と表される．

Theorem 1 は，素数 p が 4 個の平方数の和で表されることに帰着されることを以下で説明する．

Fact 1
2 つの自然数 x,y が 4 個の平方数の和で表されているとすると，

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

より，その積も 4 個の平方数の和で表せる．

この Fact 1 と $1=1^2+0^2+0^2+0^2$ であることから Theorem 1 は次の定理から従う．

Theorem 2
任意の素数 p は 4 個の平方数の和で

$$p={x_1}^2+{x_2}^2+{x_3}^2+{x_4}^2$$

と表される．

この定理を証明するためにいくつかの Lemma を用意する．

Lemma 1
p が奇素数ならば，ある $0<m<p$ に対して

$$1+x^2+y^2=mp$$

を満たす非負の整数 x,y が存在する．

Proof of Lemma 1
$\dfrac{p+1}{2}$ 個の数

$$x^2\quad(0\leq x\leq\frac{p-1}{2}) \tag{1}$$

は p を法として互いに合同でない．更に $\dfrac{p+1}{2}$ 個の数

$$-1-y^2\quad(0\leq y\leq\frac{p-1}{2}) \tag{2}$$

もまた p を法として互いに合同でない．ここで双方の集合を合わせると，$p+1$ 個の数があるが，$(\bmod p)$ の剰余は p 個しかない．従って，(1) の中のある数は (2) の中のある数と合同でなければならず，$\dfrac{1}{2}p$ より小さい x,y で

$$x^2\equiv -1-y^2\ \text{ i.e. }\ 1+x^2+y^2=mp$$

を満たすものが存在する．また，

$$0<1+x^2+y^2<1+2\left(\frac{1}{2}p\right)^2<p^2$$

より，$0<m<p$ である．■

1: 日大理工・院 (前)・数学

Lemma 2
奇素数 p と，どれかは p で割り切れない非負の整数 x_1, x_2, x_3, x_4 に対して，正の整数 m を用いて

$$mp = {x_1}^2 + {x_2}^2 + {x_3}^2 + {x_4}^2$$

と表されたとする．このような m のうち，最小の数を m_0 とおくと m_0 は奇数である．

Proof of Lemma 2
m_0 が偶数であると仮定して矛盾を導く．
$m_0 = 2m_0'$ とすると

$$\begin{aligned} m_0 p &= {x_1}^2 + {x_2}^2 + {x_3}^2 + {x_4}^2 \\ 2m_0' p &= (x_1 + x_2 + x_3 + x_4)^2 - 2\sum_{1 \le i < j \le 4} x_i x_j \end{aligned}$$

より $x_1 + x_2 + x_3 + x_4$ は偶数であるので
(i) x_1, x_2, x_3, x_4 はすべて偶数
(ii) x_1, x_2, x_3, x_4 はすべて奇数
(iii) x_1, x_2, x_3, x_4 のうち，2 個が偶数で 2 個が奇数
のいずれかが成り立つ．(iii) のとき x_1, x_2 を偶数，x_3, x_4 を奇数とすると，(i)，(ii)，(iii) のどの場合においても

$$x_1 + x_2\ ,\ x_1 - x_2\ ,\ x_3 + x_4\ ,\ x_3 - x_4$$

はすべて偶数になるので

$$\begin{aligned} \frac{1}{2} m_0 p &= \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 \\ &\quad + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 \end{aligned}$$

は 4 個の平方数の和である．x_1, x_2, x_3, x_4 のどれかは p で割り切れないので，これらの平方数のどれかは p で割り切れない．しかし，これは m_0 の最小性に反する．従って m_0 は奇数である．■

Proof of Theorem 2
まず，$2 = 1^2 + 1^2 + 0^2 + 0^2$ より $p > 2$ をとることができる．このとき Lemma 1 より，どれかは p で割り切れない x_1, x_2, x_3, x_4 に対して

$$mp = {x_1}^2 + {x_2}^2 + {x_3}^2 + {x_4}^2$$

を満たす自然数 m が存在する．このような m のうち，最小の数を m_0 とする．このとき，$m_0 = 1$ であることを示す．
$m_0 > 1$ とする．Lemma 1 より $m_0 < p$ である．更に Lemma 2 より，m_0 が奇数であることが分かる．
次に x_1, x_2, x_3, x_4 のすべてが m_0 で割り切れるとする．このとき

$$\begin{aligned} {m_0}^2 \mid {x_1}^2 + {x_2}^2 + {x_3}^2 + {x_4}^2 &\Rightarrow {m_0}^2 \mid m_0 p \\ &\Rightarrow m_0 \mid p \end{aligned}$$

となるが，p は素数なので矛盾する．よって，x_1, x_2, x_3, x_4 のどれかは m_0 で割り切れない．今，m_0 は奇数なので $m_0 \ge 3$ である．従って

$$y_i = x_i - b_i m_0 \quad (i = 1, 2, 3, 4)$$

が

$$|y_i| < \frac{1}{2} m_0 \ ,\ {y_1}^2 + {y_2}^2 + {y_3}^2 + {y_4}^2 > 0$$

を満たすように非負の整数 b_i を選ぶことができる．このとき $y_i \in \mathbb{Z}$ で，

$$0 < {y_1}^2 + {y_2}^2 + {y_3}^2 + {y_4}^2 < 4\left(\frac{1}{2} m_0\right)^2 = {m_0}^2 \qquad (3)$$

であり，また

$$\begin{aligned} {y_1}^2 + {y_2}^2 + {y_3}^2 + {y_4}^2 &= {x_1}^2 + {x_2}^2 + {x_3}^2 + {x_4}^2 \\ &\quad - 2(b_1 x_1 + b_2 x_2 + b_3 x_3 + b_4 x_4) m_0 \\ &\quad + ({b_1}^2 + {b_2}^2 + {b_3}^2 + {b_4}^2) {m_0}^2 \\ &\equiv 0 \pmod{m_0} \end{aligned}$$

が成り立つ．よって，ある自然数 m_1 を用いて

$$ {y_1}^2 + {y_2}^2 + {y_3}^2 + {y_4}^2 = m_0 m_1$$

が成り立ち，(3) より $0 < m_1 < m_0$ がわかる．また，

$$ {x_1}^2 + {x_2}^2 + {x_3}^2 + {x_4}^2 = m_0 p \quad (m_0 < p)$$

であったので，Fact 1 より，

$$ {m_0}^2 m_1 p = {z_1}^2 + {z_2}^2 + {z_3}^2 + {z_4}^2 \qquad (4)$$

とかける．ここで z_1, z_2, z_3, z_4 は Fact 1 の計算の右辺に現れる 4 個の数である．しかし

$$z_1 = \sum x_i y_i = \sum x_i (x_i - b_i m_0) \equiv \sum {x_i}^2 \equiv 0 \pmod{m_0}$$

であり，同様に z_2, z_3, z_4 も m_0 で割り切れる．
従って $t_i \in \mathbb{Z},\ i = 1, 2, 3, 4$ に対して，

$$z_i = m_0 t_i$$

が成り立ち，(4) は

$$ m_1 p = {t_1}^2 + {t_2}^2 + {t_3}^2 + {t_4}^2$$

となるが $m_1 < m_0$ より m_0 の最小性に反する．以上より $m_0 = 1$ がわかり，任意の素数 p は 4 個の平方数の和である．■

3　参考文献

[1] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford, Oxford University Press, 1st edition, 1938, 6th edition, 2008.

[2] 日本数学会編，数学辞典第 4 版，岩波書店，2007.

[3] 川田浩一，Waring 問題の研究における技術の進展について，数学第 57 巻 1 号，(2005)，21–49.