P-2

球面上の格子点に関する問題について
Lattice points on spheres

○栗本 裕太
Yuta Kurimoto[1]

Abstract

Let n be a positive integer. In 1958, A. Schinzel proved the existence of a circle in $\mathbb{R}^2$ which has exactly n lattice points on its circumference, using Fermat's lemma on the number of the integer solutions of a quadratic equation. In this talk, we show how to generalize Schinzel's theorem to a higher dimensional sphere.

1　はじめに

m を 2 以上の整数とする．本稿では全ての座標が整数である $\mathbb{R}^m$ 上の点を格子点と呼ぶ.「任意の正整数 n に対して，円周上にちょうど n 個の格子点をもつ円は存在するか」という問題を考える．この問題を $\mathbb{R}^m$ 内の球面に対して考えた T. Kulikowski の定理と，その元となる $\mathbb{R}^2$ の円における A. Schinzel の定理を紹介する [2].

Definition
中心 $(a_1, a_2, \cdots, a_m) \in \mathbb{R}^m$，半径 r の球面を

$$S_{m-1} = \left\{ (x_1, x_2, \cdots, x_m) \in \mathbb{R}^m | \sum_{k=1}^{m} (x_k - a_k)^2 = r^2 \right\}$$

で定める．

$m = 2$ のとき S_1 は平面 $\mathbb{R}^2$ 内の円である．まずは一般次元の定理を述べよう．

Theorem 1 (T. Kulikowski [3])
n を任意の正整数とする．このとき，ちょうど n 個の格子点をもつ $S_{m-1} \subset \mathbb{R}^m$ が存在する．

特に $m = 2$ の場合は円の方程式が具体的に与えられているが，この方程式が一意的という訳ではない．

Theorem 2 (A. Schinzel [5])
n を任意の正整数とする．このとき円周上にちょうど n 個の格子点をもつ円が存在する．その円は次の方程式で与えられる．
$n = 2k$ のとき (k は 1 以上の整数)

$$\left(x - \frac{1}{2}\right)^2 + y^2 = \frac{5^{k-1}}{4},$$

$n = 2k + 1$ のとき (k は 0 以上の整数)

$$\left(x - \frac{1}{3}\right)^2 + y^2 = \frac{5^{2k}}{9}.$$

この証明に本質的な役割を担うのは，次の Lemma 1 であり，2 次体の整数論による証明を次節で概説する．

[1]日大理工・院 (前)・数学

Lemma 1 (P. Fermat [4])
n を任意の正整数とする．n の約数で　mod 4 で 1，mod 4 で 3 を満たすものの個数をそれぞれ d_1，d_3 と定める．このとき，方程式 $x^2 + y^2 = n$ の整数解 $(x,\ y) \in \mathbb{Z}^2$ の個数 $r(n)$ は，次の式で与えられる．

$$r(n) = 4(d_1 - d_3).$$

2　Kulikowski の定理の証明

まず Schinzel の定理成立を仮定する．$\mathbb{R}^m$ 内の x_1-x_2 平面において円周上に格子点を n 個もつ円の方程式を

$$(x_1 - a_1)^2 + (x_2 - a_2)^2 = c, \quad x_3 = 0, \cdots, x_m = 0 \qquad (1)$$

とおく ($a_1, a_2, c \in \mathbb{Q}, c > 0$). つまり円 (1) に n 個の格子点 $(X_1, X_2, 0, \cdots, 0) \in \mathbb{Z}^m$ が乗っている．

今 $a_3, a_4, \cdots, a_m \in \mathbb{R}$ を $1, a_3, a_4, \cdots, a_m$ が $\mathbb{Q}$ 上 1 次独立になるようにとる．そして $\mathbb{R}^m$ の S_{m-1} として方程式

$$(x_1 - a_1)^2 + (x_2 - a_2)^2 + \sum_{k=3}^{m} (x_k - a_k)^2 = c + \sum_{k=3}^{m} {a_k}^2 \qquad (2)$$

で定まるものを考える．$x_3 = 0, \cdots, x_m = 0$ ならば (1) 式と (2) 式は等しい．従ってこの球面上に $(X_1, X_2, 0, \cdots, 0)$ の形の格子点が n 個ある．一方 $(X_3, X_4, \cdots, X_m) \neq (0, 0, \cdots, 0)$ を満たす格子点 $(X_1, X_2, X_3, \cdots, X_m) \in \mathbb{Z}^m$ が S_{m-1} 上に存在したと仮定する．(2) 式より

$$(X_1 - a_1)^2 + (X_2 - a_2)^2 + \sum_{k=3}^{m} {X_k}^2 - c = 2 \sum_{k=3}^{m} a_k X_k$$

において左辺は有理数である．これは $1, a_3, a_4, \cdots, a_m$ が $\mathbb{Q}$ 上 1 次独立であることに矛盾する．従って $(X_3, X_4, \cdots, X_m) \neq (0, 0, \cdots, 0)$ となる格子点は存在しない．以上より，(2) 式は球面上にちょうど n 個の格子点をもつ S_{m-1} の方程式である．　□

3　Schinzel の定理の証明

(i) $n = 2k$ $(k = 1, 2, 3, \cdots)$ のとき
方程式 $X^2 + Y^2 = 5^{k-1}$ を考える．このとき後述の Lemma 1 よりこの方程式は $4k$ 個の整数解をもつ．また，X, Y の対称式であることから整数解 $(X_1, Y_1), (Y_1, X_1)$ をまとめてひとつの組と考えると $X^2 + Y^2 = 5^{k-1}$ の整数解は $2k$ 組である．さらに 5^{k-1} は奇数であることから整数解は (奇数，偶数) と (偶数, 奇数) の場合がそれぞれ

$2k$ 個ずつ存在する．従って $X=2x-1$，$Y=2y$ と置換して整数解 (X,Y) を (奇数, 偶数) のみに制限することで $2k$ 個の整数解をもつ円の方程式を得ることができる．即ち方程式 $(2x-1)^2+(2y)^2=5^{k-1}$ つまり下記がちょうど $2k$ 個の格子点を円周上にもつ円の方程式となる．

$$\left(x-\frac{1}{2}\right)^2+y^2=\frac{5^{k-1}}{4}.$$

(ii) $n=2k+1$ $(k=0,1,2,\cdots)$ のとき

方程式 $X^2+Y^2=5^{2k}$ を考える．このとき，Lemma 1 よりこの方程式は $8k+4$ 個の整数解をもち，その内訳は，

$$(\pm X_2,\pm Y_2),(\pm X_2,\mp Y_2),(\pm Y_2,\pm X_2),(\pm Y_2,\mp X_2)$$

の 8 個の整数解を 1 組としたものが k 組であり，残りの 4 つの整数解は $(0,5^k),(0,-5^k),(5^k,0),(-5^k,0)$ である．さらに $5^{2k}=25^k\equiv 1^k\equiv 1(\mathrm{mod}\,3)$ より，$(X,Y)\equiv(-1,0)(\mathrm{mod}\,3)$ という条件を満たす整数解 (X,Y) を考えると，8 個の解からなる組では $(X,Y),(X,-Y)$ または $(-X,Y),(-X,-Y)$ のどちらか一方のみ条件を満たす．また，4 個の解からなる組では $(5^k,0),(-5^k,0)$ のどちらか一方のみ条件を満たす．従って，この条件を満たす $X^2+Y^2=5^{2k}$ の整数解は $2k+1$ 個である．よって，$X=3x-1,Y=3y$ と置き換えると，ちょうど $2k+1$ 個の整数解をもつ円の方程式 $(3x-1)^2+(3y)^2=5^{2k}$ を得る．即ち $2k+1$ 個の格子点を円周上にもつ円の方程式は

$$\left(x-\frac{1}{3}\right)^2+y^2=\frac{5^{2k}}{9}.$$

で与えられる．　□

Proof of Lemma 1

正整数 m に対して，写像 $\chi:\mathbb{N}\to\mathbb{Z}$，$\delta:\mathbb{N}\to\mathbb{Z}$，$d:\mathbb{N}\to\mathbb{Z}$ を次のように定める．

$$\chi(m) := \begin{cases} 0 & (m=2k) \\ (-1)^{\frac{1}{2}(m-1)} & (m=2k-1) \end{cases} \quad (k=1,2,\cdots)$$

$$\delta(m) := \sum_{d|m}\chi(d) \qquad (d \text{ は } m \text{ の正の約数})$$

$$d(m) := \sum_{d|m} \qquad (d \text{ は } m \text{ の正の約数})$$

$0<n_1,n_2\in\mathbb{Z}$ に対し $\chi(n_1n_2)=\chi(n_1)\chi(n_2)$ が定義より成り立つ．また，n の約数のうち偶数であるものの個数を d_2 とすると，χ の作り方から次が得られる．

$$\delta(n)=\sum_{d|m}\chi(d)=1\cdot d_1+0\cdot d_2+(-1)\cdot d_3=d_1-d_3.$$

さらに，素数 p,q が $p\equiv 1(\mathrm{mod}\,4)$，$q\equiv 3(\mathrm{mod}\,4)$ を満たすと仮定すると，$\alpha,r,s\in\mathbb{Z}$ を用いて $n=2^\alpha\prod p^r\prod q^s$ と表すことができる．p と q に関する上記の積は以後同様のものを意味することとする．$N=\prod p^r\prod q^s$ とおくと，$\delta(n)=\delta(N)$ である．また，N の約数全体は積

$$\prod(1+p+p^2+\cdots+p^r)\prod(1+q+q^2+\cdots+q^s) \quad (3)$$

の展開に現れる項全体に一致することより，各項 $\prod p^i\prod q^j$ を $\chi(\prod p^i\prod q^j)=\prod(\chi(p))^i\prod(\chi(q))^j=\prod 1^i\prod(-1)^j$ に置き換えたものが $\delta(N)$ の値となる．

ゆえに χ の $\delta(N)$ は (3) の p を 1，q を -1 に置き換えた値となるので，次の式が得られる．

$$\delta(n) = \begin{cases} 0 & (s \text{ の少なくとも 1 つが奇数}) \\ d(\prod p^r) & (s \text{ がすべて偶数}) \end{cases}$$

ここで次の (i),(ii) を示そう．

(i) $\prod q^s$ が平方数 $\Rightarrow r(n)=4d(\prod p^r)$

(ii) $\prod q^s$ が平方数でない $\Rightarrow r(n)=0$

さて，n を $\mathbb{Z}[i]$ の素元の積で表すと，次のようになる．

$$n=\{(1+i)(1-i)\}^\alpha\prod\{(a+bi)(a-bi)\}^r\prod q^s\ (a,b\in\mathbb{Z}).$$

いま $r(n)>0$，すなわち $n=A^2+B^2$ となるような $A,B\in\mathbb{Z}$ が存在すると仮定する．
$A+Bi$ と $A-Bi$ は複素共役であることから $\mathbb{Z}[i]$ の素元を用いて次のように表すことができる．

$$A+Bi=i^t(1+i)^{\alpha_1}(1-i)^{\alpha_2}\prod\{(a+bi)^{r_1}(a-bi)^{r_2}\}\prod q^{s_1}$$

$$A-Bi=(-i)^t(1-i)^{\alpha_1}(1+i)^{\alpha_2}\prod\{(a-bi)^{r_1}(a+bi)^{r_2}\}\prod q^{s_1}$$

ただし $t=0,1,2,3$.

このとき $(A+Bi)(A-Bi)=A^2+B^2$ 及び $\mathbb{Z}[i]$ が一意分解整域であることから $s=2s_1$ となるため，$\prod q^s=(\prod q^{s_1})^2$ となる．従って，「$r(n)>0\Rightarrow\prod q^s$ は平方数」が成り立ち，対偶から (ii) が成り立つ．
一方，$A+Bi$ と $A-Bi$ に因数 q を分ける方法は上の議論からただ 1 通りである．さらに，$1+i=i(1-i)$ であるので $(1+i)^{\alpha_1}(1-i)^{\alpha_2}=i^{\alpha_1}(1-i)^\alpha$ となり，結局 α_1 と α_2 の値のとりかたは t の取り方に置き換えることができる．これより，因数の分け方の場合の数は $4\prod(r+1)=4d(\prod p^r)$ 通り．また，$a+bi,a-bi$ は $\mathbb{Z}[i]$ の素元であるため，(r_1,r_2) の組み合わせの分だけ (A,B) は異なる組となる．即ち $r(n)=4\prod(r+1)=4d(\prod p^r)$ となり，(i) が成り立つ．
以上より，$r(n)=4(d_1-d_3)$ が成り立つ．　□

References

[1] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, 1st ed., (1938), 6th ed., (2008), 313–317.

[2] R. Honsberger, *Mathematical Gems I*, Dolciani Math. Expositions Math. Association of America, (1973), 117–127.

[3] T. Kulikowski, *Sur l'existence d'une sphère passant par un nombre donné aux coordonnées entières*, L'Enseignement Math., Sér. 2, **5**, (1960), 89–90.

[4] I. Niven H. S. Zuckerman and H. L. Montgomery, *An introduction to the theory of numbers*, 1st ed., (1960), 5th ed., (1991), Wiley, 54–56.

[5] A. Schinzel, *Sur l'existence d'un cercle passant par un nombre donné de points aux coordonnées entières*, L'Enseignement Math., Sér. 2, **4**, (1958), 71–72.