

整数格子の初等幾何

前原 潤 (琉球大学)

1. 格子多角形/ピタゴラス三角形/ピックの公式
2. 平面および \mathbb{R}^{4k} の特殊な相似変換
3. 格子点のなす角
4. 格子単体の特徴づけ
5. 相似はめ込みと格子の次元
6. 対合/フェルマーの2平方和定理
7. シュタインハウスの問題/ n 個の格子点を通る円
8. n 個の格子点を通る球面

1 格子多角形/ピタゴラス三角形/ピックの公式

$\mathbb{Z}^d (\subset \mathbb{R}^d)$ を d 次元の整数格子と呼び、点 $P \in \mathbb{Z}^d$ を \mathbb{R}^d の格子点という。 \mathbb{R}^d の平行移動で1つの格子点がある他の格子点に移るなら、格子点はすべて格子点に移る。従って、平行四辺形の3頂点がある格子点なら、残りの頂点も格子点である。格子点を頂点とする多角形を格子多角形という。

② どのような $n > 0$ に対して、平面上の格子正 n 角形が存在するか？

定理 1.1. 正方形以外に \mathbb{R}^2 内の格子正多角形は存在しない。

$6 \neq n \geq 5$ の場合の格子正 n 角形の非存在については [Scherrer 1946] の素敵な証明がある。その議論は $d \geq 3$ でも通用する。 \mathbb{R}^3 内には格子正三角形、格子正六角形が存在する。

定理 1.2 (Schoenberg 1937). $d \geq 3$ のとき、 \mathbb{R}^d 内の格子正 n 角形は $n = 3, 4, 6$ の場合に限って存在する。□

系 1.1. $d \geq 3$ のとき、 \mathbb{R}^d 内の格子点を頂点とする3次元正多面体は、正四面体、立方体、正八面体に限る。□

三辺の長さが整数の直角三角形をピタゴラス三角形という。

定理 1.3. ピタゴラス三角形の1つの鋭角を θ とすると、 θ/π は無理数である。

もっと一般に次が成立する。

定理 1.4. $0 < \theta < \pi/2$ のとき $\cos \theta$ が有理数なら、 $\theta = \pi/3$ であるか、または θ/π は無理数である。[2, 11] □

定理 1.5 (ピックの公式 G. Pick 1899). 平面上の格子多角形の内部に含まれる格子点の個数を I 、周上の格子点の個数を B とすると格子多角形の面積は $I + B/2 - 1$ に等しい。

この公式の証明はいろいろある。単位平行四辺形 ($I + B = 4$ となる格子平行四辺形) の面積は 1 (極小格子三角形 ($I + B = 3$ となる格子三角形) の面積は $1/2$) であることを仮定すると、格子多角形を極小格子三角形に分割した‘平面グラフ’の三角形の個数を (オイラーの公式を用いて) 数えることによってピックの公式が導かれる。

2 平面および \mathbb{R}^{4k} の特殊な相似変換

定理 2.1 (Lagrange の 4 平方和定理). 任意の正整数は 4 つの整数の平方数の和として表すことができる。[5, 12] □

定理 2.2 (M 1995). $n = 2$ または $n = 4k$ ($k \geq 1$) とするとき、任意の $P \in \mathbb{Z}^n$ に対して \mathbb{R}^n の相似変換 $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$ で次の条件を満たすものが存在する。

$$\begin{cases} f(O) = O, f(P) = (*, 0, \dots, 0) \\ f(\mathbb{Z}^n) \subset \mathbb{Z}^n. \end{cases}$$

証明. $(a, b) \neq (0, 0)$ と $(x, y, z, w) \neq (0, 0, 0, 0)$ に対して、

$$[[a, b]] = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \quad [[x, y, z, w]] = \begin{pmatrix} x & -y & z & w \\ y & x & -w & z \\ z & -w & -x & -y \\ w & z & y & -x \end{pmatrix}$$

とおく。これらは、 $\mathbb{R}^2, \mathbb{R}^4$ の相似変換の行列である。これらの変換で $\mathbb{Z}^2 \ni P = (a, b) \mapsto (*, 0)$, $\mathbb{Z}^4 \ni (x, y, z, w) \mapsto (*, 0, 0, 0)$ となる。

$n = 8$ の場合: $P = (\dots, x, y, z, w)$ は 8×8 行列 $\begin{pmatrix} [[x, y, z, w]] & 0 \\ 0 & [[x, y, z, w]] \end{pmatrix}$ により $(p, q, r, s, m, 0, 0, 0)$

に移される。これは、 8×8 行列 $\begin{pmatrix} [[p, q, r, s]] & -mI \\ mI & [[p, q, r, s]]^t \end{pmatrix}$ により $(*, 0, \dots, 0)$ に移される。これらの行列の積は \mathbb{R}^8 の相似変換の行列となる。

$n = 12$ の場合: 8×8 行列 M ($M \cdot M^t = \lambda I$) で、 P の後の方の 8 個の座標を $(*, 0, \dots, 0)$ に移す行列がある。4 平方和定理により、 $\lambda = a^2 + b^2 + c^2 + d^2$ となる $a, b, c, d \in \mathbb{Z}$ がある。すると 12×12 行列 $\begin{pmatrix} [[a, b, c, d]] & 0 \\ 0 & M \end{pmatrix}$ は相似変換の行列で、これによって、 P は $(*, *, *, *, *, 0, \dots, 0)$ に移される。この点は、同様な相似変換で $(*, 0, \dots, 0)$ に移される。これらの変換の合成を f とすればよい。 □

注 2.1. $2 < n \not\equiv 0 \pmod{4}$ については、定理 2.2 は成り立たない。

定理 2.3. 点集合 $X \subset \mathbb{Z}^{4k} \subset \mathbb{R}^{4k}$ ($k \geq 1$) が \mathbb{R}^{4k} の超平面に含まれるなら、 X は $\mathbb{Z}^{4k-1} \subset \mathbb{R}^{4k-1}$ の部分集合に相似である。

証明. X が超平面を張るとき、超平面の法線ベクトルで、成分がすべて整数のベクトル P がある。この P に対する定理 2.2 の相似変換 f で X を移せばよい。 □

系 2.1. \mathbb{R}^4 内の任意の格子三角形は \mathbb{R}^3 内の格子三角形に相似である。

系 2.2. $n = 4k - 1$ のとき、 \mathbb{R}^n 内に n 次元の格子正単体が存在する。

注 2.2. \mathbb{R}^n 内の n 次元の格子正単体の存在については [Schoenberg 1937] により、次のことが知られている。 n が偶数のときは、 $n+1$ が平方数の場合だけ。 $n \equiv 1 \pmod{4}$ のときは、 $n+1$ が 2 つの平方数の和の場合のみ。 $n \equiv 3 \pmod{4}$ のときは常に存在。

3 格子点のなす角

補題 3.1. $m \geq 0$ のとき、 $8m + 7 = \frac{b^2+c^2+d^2}{a^2}$ となる $a, b, c, d \in \mathbb{Z}$ は存在しない。

証明. このような整数 a, b, c, d があるとせよ。 a, b, c, d の最大公約数は 1 としてよい。従って a が偶数なら、 b は奇数としてよい。任意の整数 n に対して $n^2 \equiv 0, 1, 4 \pmod{8}$ だから、 a が奇数のとき、 $a^2(8m + 7) \equiv 7, b^2 + c^2 + d^2 \not\equiv 7 \pmod{8}$ 、また、 a が偶数のときは $a^2(8m + 7) \equiv 0 \pmod{4}$ 、 $b^2 + c^2 + d^2 \not\equiv 0 \pmod{4}$ で、いずれの場合も矛盾が生ずる。 \square

系 3.1. $a^2(8m + 7)$ の形の整数は 3 つの平方数の和で表すことはできない。 \square

定理 3.1 (Legendre の 3 平方和定理). 正整数 n が 3 つの平方数の和で表されるための必要十分条件は n が $4^i(8m + 7)$ ($i, m \geq 0$) の形の整数でないことである。 \square

3 点 $A, B, C \in \mathbb{Z}^n$ で決まる角 (の大きさ) $\angle ABC$ を \mathbb{Z}^n における角という。

$$\Theta_n = \{\theta \mid \theta = \angle ABC, A, B, C \in \mathbb{Z}^n\}$$

とおく。明らかに $\Theta_n \subset \Theta_{n+1}$ である。

定理 3.2 (Beeson 1992).

1. $\theta \in \Theta_2 \Leftrightarrow \theta = \pi/2$ or $\tan \theta \in \mathbb{Q}$
2. $\theta \in \Theta_4 \Leftrightarrow \theta = \pi/2$ or $\tan^2 \theta = \frac{a^2+b^2+c^2}{d^2}$ ($a, b, c, d \in \mathbb{Z}$)
3. $\theta \in \Theta_5 \Leftrightarrow \cos^2 \theta \in \mathbb{Q}$
4. $\Theta_2 \subsetneq \Theta_3 = \Theta_4 \subsetneq \Theta_5 = \Theta_6 = \dots$

証明. 1. と 2. は定理 2.2 を用いる。3. $\theta \in \Theta_n$ なら、余弦定理により $\cos^2 \theta \in \mathbb{Q}$ 。逆に $\cos^2 \theta \in \mathbb{Q}$ なら、 $\tan^2 \theta \in \mathbb{Q}$ であるから、4 平方和定理により、 $\theta \in \Theta_5$ となる。4. $\pi/3 \in \Theta_3 \setminus \Theta_2$, $\arctan \sqrt{7} \in \Theta_5 \setminus \Theta_4$ 。系 2.1 により $\Theta_3 = \Theta_4$ 。 $\theta \in \Theta_n \Rightarrow \cos^2 \theta \in \mathbb{Q} \Rightarrow \theta \in \Theta_5$ 。 \square

4 格子単体の特徴づけ

格子点を頂点とする単体を格子単体と呼ぶ。単体 T が格子単体と合同なら、 T の辺の長さの 2 乗はすべて整数である。逆は正しくない。例えば、辺の長さが $1, \sqrt{7}, \sqrt{7}$ の三角形は格子三角形と合同にはならない。

定理 4.1. 単体 T が格子単体に相似であるための必要十分条件は、 T の 3 つの頂点で作られる角 θ がすべて Θ_5 に属する ($\cos^2 \theta \in \mathbb{Q}$ となる) ことである。

すべての角が Θ_5 に属することが必要条件であるのは明らかである。これ十分条件であることを示すため 2 つの補題を準備する。座標がすべて有理数の点を有理点と呼ぶ。

補題 4.1. ベクトル $\vec{v}_1, \dots, \vec{v}_k$ が線形独立のとき、 $a_{ij} = \vec{v}_i \cdot \vec{v}_j$ (内積) を要素とする行列式 $\det(a_{ij})$ の値は、 $\vec{v}_1, \dots, \vec{v}_k$ の張る平行体の体積の 2 乗に等しい。(この行列式は $\vec{v}_1, \dots, \vec{v}_k$ の Gram 行列式と呼ばれている。) \square

補題 4.2. $S = A_1 \dots A_k$ を格子単体とし、点 F を S の張るフラット上の点とする。このとき、 $|A_i F|^2 \in \mathbb{Q}$ ($i = 1, \dots, k$) ならば、 F は有理点である。

証明. $\overrightarrow{A_1 F} = x_2 \overrightarrow{A_1 A_2} + \dots + x_k \overrightarrow{A_1 A_k}$ とする。各 $\overrightarrow{A_1 A_i}$ と $\overrightarrow{A_1 F}$ の内積をとると、

$$x_2 \overrightarrow{A_1 A_2} \cdot \overrightarrow{A_1 A_i} + \dots + x_k \overrightarrow{A_1 A_k} \cdot \overrightarrow{A_1 A_i} = \overrightarrow{A_1 F} \cdot \overrightarrow{A_1 A_i} \quad (i = 2, \dots, k) \quad (1)$$

となる。 $\overrightarrow{A_1 F} \cdot \overrightarrow{A_1 A_i} = (|A_1 F|^2 + |A_1 A_i|^2 - |F A_i|^2)/2 \in \mathbb{Q}$ 、同様に $\overrightarrow{A_1 A_i} \cdot \overrightarrow{A_1 A_j} \in \mathbb{Q}$ であるから、(1) を有理数係数の連立方程式と見ると、係数行列は正則で、(1) の解はすべて有理数となる。従って $x_2, \dots, x_k \in \mathbb{Q}$ で、 F は有理点である。 \square

定理 4.1 の証明 (十分性). 単体 T の次元 d に関する帰納法。 $d \leq 1$ の場合は定理は明らかに正しい。 $d < k$ の場合は正しいとして、 $d = k$ の場合を考える。 $T = A_0 A_1 \dots A_k$ とする。 $T \subset \mathbb{R}^{n+4}$ ($n > k$) で、 A_1, \dots, A_k は $\mathbb{R}^n \times \{(0, 0, 0, 0)\}$ 内の格子点と仮定してよい。すると、正弦定理により、 $|A_0 A_i|^2 \in \mathbb{Q}$ ($i = 1, 2, \dots, k$) であることがわかる。 A_0 から $S := A_1 \dots A_k$ の張るフラットに下ろした垂線の足を F とし、 $h = |A_0 F|$ とおく。 T の体積の平方 $|T|^2$ 、および、 S の $(k-1)$ 次元の体積の平方 $|S|^2$ は有理数で、 $|T| = \frac{1}{k} |S| \cdot h$ であるから、 $h^2 = |A_0 F|^2 \in \mathbb{Q}$ である。ゆえに、ピタゴラスの定理により、すべての i に対して、 $|A_i F|^2 \in \mathbb{Q}$ である。補題 4.2 により、 $F \in \mathbb{Q}^n \times \{(0, 0, 0, 0)\}$ となる。さらに、 T を平行移動して $F = (0, \dots, 0) \in \mathbb{Q}^{n+4}$ としてよい。 h^2 は有理数だから、4 平方定理によって、 $h^2 = \frac{a^2 + b^2 + c^2 + d^2}{e^2}$ となる $a, b, c, d, e \in \mathbb{Z}$ が存在する。 $A'_0 = (0, \dots, 0, \frac{a}{e}, \frac{b}{e}, \frac{c}{e}, \frac{d}{e}) \in \mathbb{Q}^{n+4}$ とおくと、 A'_0, A_1, \dots, A_k はすべて有理点で T と合同な単体を張る。この単体を相似拡大して T と相似な格子単体が得られる。 \square

定理 4.2 (M 1995). 1 直線上にない有限個の点の集合 X について、次の 3 つは同値である。

- (1) X は格子点の集合に相似である。
- (2) 任意の $A, B, C \in X$ に対して、 $\left(\frac{|AB|}{|BC|}\right)^2 \in \mathbb{Q}$.
- (3) 任意の $A, B, C \in X$ に対して、 $\angle ABC \in \Theta_5$.

証明. (1) \Rightarrow (2) \Rightarrow (3) は明らか。(3) \Rightarrow (1): X の凸包の次元を k とすると、 $k \geq 2$ で、 X は k 次元単体 T の頂点集合を含み、残りの点は T の張るフラット上にある。後は定理 4.1 と補題 4.2 を用いる。 \square

注 4.1. 有限個の点の集合 X が 1 直線上にある場合でも、(1) と (2) は同値である。この場合、(2) は条件「 X の任意の 3 点 A, B, C に対して、 $\frac{|AB|}{|BC|} \in \mathbb{Q}$ 」と同値になる。

問題 4.1. 1 直線上にない無限個の点の集合 Y の 2 点間の距離の平方がすべて整数なら、 Y は格子点の集合に相似か。

1 次元単体が \mathbb{R}^1 内の格子単体に相似であることに注意して、定理 4.1 の十分性の証明をたどると、三角形については次の結果が得られる。

定理 4.3. 三角形 ABC の 3 つの内角が Θ_5 に属し、 $\angle A = \alpha \neq \frac{\pi}{2}$ とせよ。このとき、

- (1) ABC は \mathbb{R}^5 内の格子三角形に相似である。
- (2) $\alpha \in \Theta_3$ なら ABC は \mathbb{R}^3 の格子三角形に相似である。
- (3) $\alpha \in \Theta_2$ なら ABC は \mathbb{R}^2 の格子三角形に相似である。

系 4.1. $k = 2, 3$ に対して、格子三角形の 1 つの内角 ($\neq \frac{\pi}{2}$) が Θ_k に属するなら、3 つの内角はすべて Θ_k に属する。

5 相似はめ込みと格子の次元

単体 T の頂点集合と相似な点集合を \mathbb{Z}^d 内にとることを、 T の \mathbb{Z}^d への相似はめ込みという。

② 任意の n 次元格子単体 (つまり単体の次元が n) が相似はめ込み出来るような \mathbb{Z}^d の次元 d の最小値 $\delta(n)$ はいくらか。

定理 4.2 と次の定理により、 $\delta(n) \leq n + 3$ である。

定理 5.1 (熊田敏宏 1998). n 次元単体 T の各辺の長さの 2 乗が有理数なら、 T の頂点集合は $\mathbb{Q}^{n+3} (\subset \mathbb{R}^{n+3})$ の部分集合に 合同 である。(一般に次元を $n + 3$ より小さくすることはできない。) □

この定理は、定理 4.1 の証明を、Lagrange の 4 平方和定理の代わりに次の命題を用いて、修正することによって証明できる。命題：正の有理数 a, b, c, d, e に対して $ax^2 = by^2 + cz^2 + du^2 + ev^2$ が自明でない実数解 (x, y, z, u, v) を持つならば、自明でない有理数解をもつ。(この命題は [Meyer 1884] の「有理数係数の $\text{rank} \geq 5$ の 2 次形式が \mathbb{R} 上で自明でない零点を持つなら、 \mathbb{Q} 上でも自明でない零点をもつ」という定理の特別な場合である。)

1 つの頂点から出る辺がすべて直交しているような単体を直交単体という。任意の単体 $T = A_0A_1A_2 \dots A_n$ に対して、ベクトル $\vec{v}_i := \overrightarrow{A_0A_i}$ ($i = 1, 2, \dots, n$) を Schmidt の方法で (正規化はせずに) 直交化する：

$$\vec{u}_1 = \vec{v}_1, \quad \vec{u}_2 = \vec{v}_2 - \frac{\vec{v}_2 \cdot \vec{u}_1}{\vec{u}_1 \cdot \vec{u}_1} \vec{u}_1, \quad \vec{u}_3 = \vec{v}_3 - \frac{\vec{v}_3 \cdot \vec{u}_1}{\vec{u}_1 \cdot \vec{u}_1} \vec{u}_1 - \frac{\vec{v}_3 \cdot \vec{u}_2}{\vec{u}_2 \cdot \vec{u}_2} \vec{u}_2, \quad \dots$$

すると、 $B_0 = A_0$, $\overrightarrow{B_0B_i} = \vec{u}_i$ ($i = 1, 2, \dots, n$) となる直交単体 $B_0B_1B_2 \dots B_n$ が得られる。得られる直交単体は、要の頂点 A_0 の選び方、直交化する順序によって異なる。補題 4.2 を用いて次の補題が証明できる。

補題 5.1. 単体 T が \mathbb{Z}^d に相似はめ込み出来るための必要十分条件は、 T から直交化して得られる直交単体 (の 1 つ) が \mathbb{Z}^d に相似はめ込みできることである。 □

補題 5.2. 格子直交四面体の 3 つの直角三角形の 1 つは Θ_4 に属する鋭角をもつ。

証明. 直交する3辺の長さを ξ, η, ζ とする。 $(\xi\eta)^2$ が3つの平方数の和で表されるなら、 $(\xi/\eta)^2 = (\xi\eta)^2/\eta^4$ より、 ξ, η を2辺とする直角三角形の鋭角は Θ_4 に属する。 $(\xi\eta)^2, (\eta\zeta)^2$ のいずれも3つの平方数の和で表せないなら、これらは $4^i(8k+7)$ の形の整数で、 $7^2 \equiv 1 \pmod{8}$ より、 $(\xi\eta^2\zeta)^2$ は3つの平方数の和で表される。従って $(\xi/\zeta)^2$ は $(b^2 + c^2 + d^2)/a^2$ ($a, b, c, d \in \mathbb{Z}$) の形に表され、長さ ξ, ζ の2辺を含む直角三角形の鋭角は Θ_4 に属する。□

注 5.1. 格子四面体が Θ_4 に属する角をもつとは限らない。例えば、1対の対辺の長さが2で残りの4つの辺の長さが $\sqrt{8}$ の格子四面体は Θ_4 に属する角を持たない。

定理 5.2 (M 1998). 任意の格子直交四面体は (従って、任意の格子四面体は) \mathbb{Z}^5 に相似はめ込み可能である。□

証明. 格子直交四面体と相似な直交四面体を $OABC$ とし、3辺 OA, OB, OC が直交するとする。補題 5.2 により、 OAB, OBC, OCA の1つは \mathbb{Z}^4 に相似はめ込みできる。従って、 $O, A, B \in \mathbb{Z}^4$, $O = (0, 0, 0, 0)$ としてよい。 $|OC| = \eta$ とおく。4平方和定理により、 $\eta^2 = x^2 + y^2 + z^2 + w^2$ なる $x, y, z, w \in \mathbb{Z}$ がある。相似変換 $[[x, y, z, w]]$ で三角形 OAB は η 倍された三角形 $OA'B'$ に移る。 $O, A', B' \in \mathbb{Z}^4$ を $\mathbb{Z}^4 \times \{0\} \subset \mathbb{Z}^5$ の点とみなし、 $C' = (0, 0, 0, 0, \eta^2)$ とすると、三角形 $OA'B'C'$ は三角形 $OABC$ に相似で \mathbb{Z}^5 にはめ込まれている。□

従って、 $\delta(1) = 1, \delta(2) = \delta(3) = 5$ である。

問題 5.1. $n \geq 3$ なら $\delta(n) \leq n + 2$ か。

問題 5.2. \mathbb{Z}^4 に (従って、 \mathbb{Z}^3 に) 相似はめ込み可能な四面体の特徴づけよ。3頂点のなす角がすべて Θ_3 に属するような四面体は \mathbb{Z}^4 にはめ込み可能か。

6 対合/フェルマーの2平方和定理

写像 $f: S \rightarrow S$ が $f \circ f = id$ を満たすとき、 f を S の対合 (involution) という。

補題 6.1. 有限集合 S の任意の対合 $f: S \rightarrow S$ に対して、次が成立する。

$$[f \text{ の不動点の個数}] \equiv |S| \pmod{2}. \quad \square$$

例 6.1. $n \in \mathbb{N}$ に対して n の約数の個数 = $\begin{cases} \text{奇数} & n \text{ が平方数のとき} \\ \text{偶数} & n \text{ が非平方数のとき} \end{cases}$
 (対合 $\{n \text{ の約数の集合}\} \ni a \mapsto n/a \in \{n \text{ の約数の集合}\}$ を考える。)

定理 6.1 (フェルマーの2平方和定理). 素数 $p = 4k + 1$ は2つの平方数の和として $p = a^2 + b^2$ ($a, b \in \mathbb{N}$) と表すことができる。

証明. (D. Zagier) $5 = 4 \cdot 1 + 1 = 2^2 + 1^2$ で、 $4 \cdot 2 + 1 = 9$ は素数ではないから、 $k > 2$ の場合を考える。

$$\begin{aligned} S &= \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\} \\ A &= \{(x, y, z) \in S \mid x < y - z\} \\ B &= \{(x, y, z) \in S \mid y - z < x < 2y\} \\ C &= \{(x, y, z) \in S \mid 2y < x\} \end{aligned}$$

とおく。(< が = になる場合は生じない。) $(1, k, 1) \in A, (1, 1, k) \in B, (3, 1, k-2) \in C$ であるから、 A, B, C は空集合ではない。また、 $S = A \cup B \cup C$ (disjoint union) となっている。 $A \ni (x, y, z) \mapsto (x+2z, z, y-x-z) \in C$ が全単射になるから、 $|A| = |C|$ である。また、 $B \ni (x, y, z) \mapsto (2y-x, y, x-y+z) \in B$ は B の対合で、その不動点は $(1, 1, k)$ のみだから $|B|$ は奇数である。ゆえに $|S|$ も奇数である。従って S の対合 $S \ni (x, y, z) \mapsto (x, z, y) \in S$ は (奇数個の) 不動点 (x, y, y) をもつ。よって、 $p = x^2 + 4y^2 = x^2 + (2y)^2$ を満たす $x, y \in \mathbb{N}$ がある。 \square

7 シュタインハウスの問題/ n 個の格子点を通る円

②(シュタインハウス 1957) どんな $n > 0$ についても、ちょうど n 個の格子点を内部に含むような平面上の円が存在するか。

補題 7.1 (Sierpinski). 点 $(\sqrt{2}, \frac{1}{3}) \in \mathbb{R}^2$ を中心とする円の周上の格子点の個数は 1 個以下である。従って、内部にちょうど n 個の格子点を含むような円が存在する。

②任意の $n \in \mathbb{N}$ に対して、ちょうど n 個の格子点を通るような円が存在するか。

補題 7.2. 素数 $p \equiv 1 \pmod{4}$ に対して、 $w\bar{w} = p^k$ を満たすような $w \in \mathbb{Z}[i]$ の個数は $4(k+1)$ 個である。

証明. フェルマーの 2 平方和定理により、 $p = a^2 + b^2$ と書けるから、 $p = (a+bi)(a-bi)$ となり、 $w\bar{w} = p^k = (a+bi)^k(a-bi)^k$ となる。(注意: $a+bi, a-bi$ は $\mathbb{Z}[i]$ の既約元。) 従って、 w は

$$u(a+bi)^s(a-bi)^{k-s} \quad (s = 0, 1, 2, \dots, k, u = \pm 1, \pm i)$$

のいずれかであり、 $w\bar{w} = p^k$ を満たすような $w \in \mathbb{Z}[i]$ の個数は $4(k+1)$ 個である。 \square

定理 7.1 (M+松本眞 1998). 素数 p が $p \equiv 1 \pmod{4}$, $p^k \equiv 1 \pmod{8}$ を満たすとき、円 $(4x-1)^2 + (4y)^2 = p^k$ の周上にはちょうど $k+1$ 個の格子点がある。

証明. 補題 7.2 により、 $X^2 + Y^2 = p^k$ を満たすような整数の組 (X, Y) の個数は $4(k+1)$ 個ある。(整数) $^2 \equiv 0, 1, 4 \pmod{8}$ だから、 $X^2 + Y^2 \equiv 1 \pmod{8}$ なら、 $X^2 \equiv 1, Y^2 \equiv 0 \pmod{8}$ または $X^2 \equiv 0, Y^2 \equiv 1 \pmod{8}$ である。ゆえに、 $X^2 + Y^2 = p^k$ なら $X \equiv \pm 1; Y \equiv 0 \pmod{4}$ または $X \equiv 0; Y \equiv \pm 1 \pmod{4}$ である。よって、 $(4x-1)^2 + (4y)^2 = p^k$ を満たす格子点 (x, y) の個数は

$$X^2 + Y^2 = p^k, X \equiv -1 \pmod{4} \tag{2}$$

を満たす (X, Y) の個数に等しい。 $X^2 + Y^2 = p^k$ の各 4 組の整数解 $(\pm A, B), (B, \pm A)$ ($B \equiv 0 \pmod{4}$) のうちただ 1 つだけが (2) を満たす。従って、円 $(4x-1)^2 + (4y)^2 = p^k$ の周上の格子点の個数は $4(k+1)/4 = k+1$ である。 \square

系 7.1. 任意の正整数 n に対して、ちょうど n 個の格子点を通る平面上の円が存在する。 \square

定理 7.2. 素数 $p \equiv 1 \pmod{4}$ に対して、円 $(2x-1)^2 + (2y)^2 = p^k$ の周上には $2k+2$ 個の格子点がある。 \square

問題 7.1. $n = 3, 4, 5, \dots, 10$ に対して、ちょうど n 個の格子点を通る円の最小半径を決定せよ。(最小半径の上界は定理 7.1, 7.2 によって与えられるから、計算機で調べられると思う。)

8 n 個の格子点を通る球面

例 8.1. \mathbb{R}^3 の球面で、与えられた個数の格子点を通るものがある。例えば、球面

$$(4x - 1)^2 + (4y)^2 + (4z - \sqrt{2})^2 = 17^k + 2$$

はちょうど $k + 1$ 個の格子点を通る。しかしこの場合、これらの格子点はすべて平面 $z = 0$ 上にあり、平面上の円の場合と本質的な違いはない。

② 任意の $n \geq 4$ に対して、 \mathbb{R}^3 の球面で、次の条件 (*) を満たすものが存在するか。

$$(*) \begin{cases} \text{球面上にはちょうど } n \text{ 個の格子点があり、} \\ \text{これらの格子点の凸包は 3 次元凸体をなす。} \end{cases}$$

定理 8.1 (M 2006). 任意の $n > d \geq 2$ に対して、ちょうど n 個の格子点を通る \mathbb{R}^d の球面が存在し、しかもこれらの n 個の格子点は d 次元のポリトープを張る。

補題 8.1. M_1, M_2, \dots, M_s を相異なる素数とし、 $a_1, a_2, \dots, a_s \in \mathbb{Z}$ とする。このとき、

$$\sum_{i=1}^s \frac{a_i}{M_i} \in \mathbb{Z} \iff \frac{a_i}{M_i} \in \mathbb{Z}, i = 1, 2, \dots, s.$$

証明. 通分して見る。 □

定理 8.1 の証明. ($d = 5$ の場合) $k_0 + k_1 + k_2 + k_3 + 4 = n$, $k_0 \geq 2$ となる非負整数 k_i をとり、相異なる素数 $p_0, p_1, p_2, p_3, M_1, M_2, M_3$ を $p_0 \equiv p_1 \equiv p_2 \equiv p_3 \equiv 1 \pmod{8}$ で $p_1^{k_1} + p_2^{k_2} + p_3^{k_3} < p_0^{k_0} < M_1 < M_2 < M_3$ となるように選ぶ。(これは、Dirichlet の定理により可能。) さらに、 $\tau_i = 2M_i + \frac{p_i^{k_i} - p_0^{k_0}}{8M_i}$ ($i = 1, 2, 3$) とおく。 \mathbb{R}^5 の座標を (x, y, z_1, z_2, z_3) とし、次の式で定義される球面を Σ とする。

$$(4x - 1)^2 + (4y)^2 + (4z_1 - \tau_1)^2 + (4z_2 - \tau_2)^2 + (4z_3 - \tau_3)^2 = p_0^{k_0} + \tau_1^2 + \tau_2^2 + \tau_3^2.$$

この球面がちょうど n 個の格子点を通ることを見るため、 (x, y, j_1, j_2, j_3) を Σ 上の格子点とすると、

$$\begin{aligned} (4x - 1)^2 + (4y)^2 &= p_0^{k_0} + \sum_{i=1}^3 \tau_i^2 - \sum_{i=1}^3 (4j_i - \tau_i)^2 = p_0^{k_0} - \sum_{i=1}^3 (16j_i^2 - 8j_i\tau_i) \\ &= p_0^{k_0} - 16 \sum_{i=1}^3 (j_i^2 - j_i M_i) + \sum_{i=1}^3 \frac{j_i(p_i^{k_i} - p_0^{k_0})}{M_i} \end{aligned}$$

となる。これは整数だから $j_i = s_i M_i$ ($s_i \in \mathbb{Z}$) でなければならない。従って、 $(4x - 1)^2 + (4y)^2 = p_0^{k_0} - 16 \sum_{i=1}^3 M_i^2 (s_i^2 - s_i) + \sum_{i=1}^3 s_i (p_i^{k_i} - p_0^{k_0})$ となる。左辺は非負であるから、 $s_i = 0, 1$ で、

$$\begin{aligned} (4x - 1)^2 + (4y)^2 &= p_0^{k_0} + \sum_{i=1}^3 s_i (p_i^{k_i} - p_0^{k_0}) = p_0^{k_0} + \sum_{i=1}^3 s_i p_i^{k_i} - (s_1 + s_2 + s_3) p_0^{k_0} \\ &< 2p_0^{k_0} - (s_1 + s_2 + s_3) p_0^{k_0} \end{aligned}$$

となる。従って $s_1 + s_2 + s_3 \leq 1$ であり、 (s_1, s_2, s_3) の可能な値は $(0, 0, 0), (1, 0, 0), (0, 1, 0), (0, 0, 1)$ の 4 通りで、これらに対応して、4 つの方程式 $(4x - 1)^2 + (4y)^2 = p_i^{k_i}$ ($i = 0, 1, 2, 3$) が得られる。各方程式は $k_i + 1$ 個の整数解をもつ。従って、 Σ はちょうど n 個の格子点を通る。これらの n 個の格子点は $(*, *, 0, 0, 0), (*, *, 0, 0, 0), (*, *, 0, 0, 0), (*, *, M_1, 0, 0), (*, *, 0, M_2, 0), (*, *, 0, 0, M_3)$ の形の 6 点を含むから、5 次元のポリトープを張る。 □

系 8.1. 任意の $n \geq 4$ に対して、 \mathbb{R}^3 の球面で、条件 (*) を満たすものが存在する。

問題 8.1. 任意の $n \geq 4$ に対して、 \mathbb{R}^3 の球面で、ちょうど n 個の格子点を通り、しかもこれら n 個の格子点は一般の位置にある、というものが存在するか。

参考文献

- [1] M. J. Beeson, Triangles with vertices on lattice points, *Amer. Math. Monthly* 99(1992) 243–252.
- [2] P. Frankl・前原潤：「幾何学の散歩道」共立出版 1991.
- [3] W. W. Funkenbusch, From Euler’s formula to Pick’s formula using an edge theorem, *Amer. Math. Monthly*, 81(1974) 647–648.
- [4] H. Hadwiger and H. Debrunner (Translated by Victor Klee), *Combinatorial Geometry in the Plane*, Holt, Rinehart and Winston, New York 1964.
- [5] A. Y. Khinchin (蟹江幸博 訳・解説)：「数論の 3 つの真珠」日本評論社 2000.
- [6] T. Kumada, Isometric embedding of metric \mathbb{Q} -vector space into \mathbb{Q}^N , *Europ. J. Combin.* 19(1998) 701–709.
- [7] H. Maehara, Embedding a polytope in a lattice, *Discrete Comput Geom* 13(1995) 585–592.
- [8] H. Maehara, Embedding a set of rational points in lower dimensions, *Discrete Math.* 192(1998) 273–279.
- [9] H. Maehara and M. Matsumoto, Is there a circle that passes through a given number of lattice points?, *European J. Combin.* 19(1998) 591–592.
- [10] H. Maehara, On a sphere that passes through n lattice points, *to appear*.
- [11] I. Niven, *Numbers: Rational and Irrational*, MAA, 1961.
- [12] I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, Wiley, New York 1972.
- [13] W. Scherrer, Die Einlagerung eines regulären Vielecks in ein Gitter, *Elemente der Math.* 1(1946) 97–98.
- [14] I. J. Schoenberg, Regular simplices and quadratic forms, *J. London Math. Soc.* 12(1937) 48–55.
- [15] I. J. シェーンベルグ (三村護 訳)「数学点描」近代科学社 1989.
- [16] ジョセフ・H・シルヴァーマン (鈴木治郎 訳)：「はじめての数論」ピアソン・エデュケーション 2007.
- [17] H. Steinhaus, *One Hundred Problems in Elementary Mathematics*, Dover Publications, Inc. New York 1964.
- [18] 渡辺敬一・草場公邦「代数の世界」朝倉書店 1994.
- [19] D. Zagier, A one sentence proof that every prime $p \equiv 1 \pmod{4}$ is a sum of two squares, *Amer. Math. Monthly* 97(1990), 144.