ディオファントス近似とペル方程式

学籍番号：
名前：
指導教員：越智　禎宏

1　はじめに

この卒研概要では，鳩ノ巣原理がどのようにディオファントス近似定理とペル方程式の解の存在定理に持ちられるかに焦点を当てて見ていく．なおこの論考では，自然数は 0 は含まないとする．

無理数 α があったとき，それを有理数で近似していくことは自然である．例えば π は $\dfrac{22}{7}$ で十分良く近似できる．最初に，無理数の有理数による近似に関するディリクレの定理を証明する．次に，それを用いてペル方程式の解の存在定理を紹介する．最後に，シルバーマンの「初めての数論」にある問題を解く．

2　鳩ノ巣原理

ディリクレ (Dirichlet) が巧妙に使用した「鳩ノ巣原理 (The Pigeonhole Principle)」は以下のようなものである：

「いま n 個の鳩ノ巣があるとする．$n+1$ 以上の鳩がそれらの巣のどれかに入るとすると，必ず 2 羽以上鳩の入っている巣がある．」

以下，この簡単な原理がどのように数学の証明で使われるかを見ていく．

3　ディリクレのディオファントス近似定理

無理数とは実数で，整数 x, y を用いて $\dfrac{x}{y}$ の形に表されない実数である．例えば $\sqrt{2}, \pi, e$ や $\log_2 3$ は無理数であり，ほとんどの実数が無理数である．

定理（ディリクレのディオファントス近似定理）$\alpha > 0$ を任意の無理数とする．このとき，不等式

$$|x - y\alpha| < \frac{1}{y}$$

をみたす整数の組 (x, y) が無数に存在する．言い換えると，

$$\left|\frac{x}{y} - \alpha\right| < \frac{1}{y^2}$$

をみたす有理数 $\dfrac{x}{y}$ が無数に存在する．

証明： いま $M > 0$ を自然数とし，開区間 $(0,1)$ を M 等分する．$k = 0,1,2,\cdots,M-1$ に対して M 個の開区間 $I_k = \left(\dfrac{k}{M}, \dfrac{k+1}{M}\right)$ を考える．

$N > M$ として自然数の N 個の組 $(x_1,y_1),(x_2,y_2),\cdots,(x_N,y_N)$ を与える．ここで，$y_1 < y_2 < \cdots < y_N$ とし，$k = 1,2,\cdots,N-1$ に対して $y_{k+1} - y_k > M$ となるようにとる．x_i も同様にとる．

$x_i - y_i\alpha$ の整数部分を m_i，小数部分を ξ_i とする（で $m_i \in \mathbf{Z}$, $0 < \xi_i < 1$）．すると，各 ξ_i は I_k の1つに入る．$N > M$ だから鳩ノ巣原理よりある区間 I_ℓ があって2つ以上の ξ_j, ξ_k がそこに入る．$x_j - y_j\alpha = m_j + \xi_j$，$x_k - y_k\alpha = m_k + \xi_k$ とすると，$|(x_j - x_k) - (m_j - m_k) - (y_j - y_k)\alpha)| = |\xi_j - \xi_k| < \dfrac{1}{M}$ であるので，$x = (x_j - x_k) - (m_j - m_k), y = y_j - y_k$ とおけば，$|x - y\alpha| < \dfrac{1}{M}$ である．y_i の取りかたから，$y = y_j - y_k > M$ なので，$|x - y\alpha| < \dfrac{1}{y}$ である．

もし $|x - y\alpha| < \dfrac{1}{y}$ をみたす整数の組 (x,y) が有限個ならば，それらを $(x_1,y_1),(x_2,y_2),\cdots,(x_s,y_s)$ とすると，どんな $i = 1,2,\cdots,s$ に対しても $|x_i - y_i\alpha| > A$ となる定数 A がある（α は無理数なので）．しかし，$M = \dfrac{1}{A}$ として上の議論を実行すれば，$|x - y\alpha| < \dfrac{1}{y}$ で $|x - y\alpha| < \dfrac{1}{M} = A$ である整数の組が作れるので，矛盾する．□

4　ペル方程式の解の存在

D は平方数でない自然数とするとき，方程式 $x^2 - Dy^2 = 1$ を伝統的に「ペル方程式」という．その自然数解は最小の解 x_1, y_1 をとって（最小とは x_1 について言う），

$$(x_1 + y_1\sqrt{D})^k = x_k + y_k\sqrt{D}$$

とするとき，(x_k, y_k) で与えられる．例えば，$x^2 - 2y^2 = 1$ の最小の解は $(x,y) = (3,2)$ である．その他の解は $(x,y) =$ などである．

ここでは，ディリクレのディオファントス近似定理を用いて，解の存在を示す．鳩ノ巣原理が巧妙に用いられる．

定理：　D は平方数でない自然数とするとき，ペル方程式 $x^2 - Dy^2 = 1$ の解 (x,y) が必ず存在する．

証明： この証明では，$|x - y\sqrt{D}| < \dfrac{1}{y}$ をみたす整数の組 (x,y) のみを考える．ディオファントス近似定理よりそのような整数の組は無数にある．そのような (x,y) に対しては，$x < y\sqrt{D} + \dfrac{1}{y}$ だから，$x + y\sqrt{D} < 2y\sqrt{D} + \dfrac{1}{y} < 3y\sqrt{D}$ である．したがって，$|(x - y\sqrt{D})(x + y\sqrt{D})| < 3\sqrt{D}$ である．

今，K を $3\sqrt{D}$ 以下の最大の自然数とする．$|x-y\sqrt{D}|<\dfrac{1}{y}$ をみたす整数の組 (x,y) に対して，$|(x-y\sqrt{D})(x+y\sqrt{D})|<3\sqrt{D}$ だから，x^2-Dy^2 は $-K,-K+1,-K+2,\cdots,-1,1,2,\cdots,K$ のうちのどれかに一致する．ディオファントス近似定理より $|x-y\sqrt{D}|<\dfrac{1}{y}$ となるような整数の組は無数にあるので，鳩ノ巣原理より，ある自然数 M があって，$-K\le M\le K$ で $|x-y\sqrt{D}|<\dfrac{1}{y}$ で $x^2-Dy^2=M$ となる整数の組 (x,y) が無限個あるようなできる．簡単のため，$M>0$ とする．

そのような整数の組 (x,y) の 2 つをとって，それらを $(x_j,y_j),(x_k,y_k)$ とする．このとき，

$$\frac{x_j+y_j\sqrt{D}}{x_k+y_k\sqrt{D}}=\frac{(x_jx_k-y_jy_kD)+(x_ky_j-x_jy_k)\sqrt{D}}{x_k^2-y_j^2D}$$

$$=\frac{(x_jx_k-y_jy_kD)+(x_ky_j-x_jy_k)\sqrt{D}}{M}=\frac{x_jx_k-y_jy_kD}{M}+\frac{x_ky_j-x_jy_k}{M}\sqrt{D}$$

を考えると，$(x,y)=\left(\dfrac{x_jx_k-y_jy_kD}{M},\dfrac{x_ky_j-x_jy_k}{M}\right)$ は $x^2-Dy^2=1$ の有理数解である（整数解とは限らない）．実際，

$$\frac{(x_j+y_j\sqrt{D})((x_j-y_j\sqrt{D})}{(x_k+y_k\sqrt{D})(x_k-y_k\sqrt{D})}=\frac{M}{M}=1$$

だが，この左辺を計算すると，$\left(\dfrac{x_jx_k-y_jy_kD}{M}\right)^2-D\left(\dfrac{x_ky_j-x_jy_k}{M}\right)^2$ になる．

あとは，$x_jx_k-y_jy_kD$ と $x_ky_j-x_jy_k$ が M の倍数になるように $(x_j,y_j),(x_k,y_k)$ が取れることを言えばよい．$|x-y\sqrt{D}|<\dfrac{1}{y},x^2-Dy^2=M$ をみたす整数の組 (x,y) は無限個あるので，それらを $(A,B)\pmod{M}$ の M^2 個の箱の中に入れていくと $(A,B=0,1,2,\cdots,M-1)$，鳩ノ巣原理より，ある箱 (A,B) に無限個はいっている，そこから 2 つ $(x_j,y_j),(x_k,y_k)$ 取り出すと，$x_j\equiv x_k\pmod{M}$ と $y_j\equiv y_k\pmod{M}$ を満たしている．このとき，$x_jx_k-y_jy_kD$ と $x_ky_j-x_jy_k$ が M の倍数である．実際簡単な合同式の計算より，$x_jx_k-y_jy_kD\equiv x_jx_j-y_jy_jD=x_j^2-Dy_j^2=M\equiv 0\pmod{M}$ であり，$x_ky_j-x_jy_k\equiv x_ky_j-x_ky_j=0\pmod{M}$ だから．

したがって，上のように $(x_j,y_j),(x_k,y_k)$ を取れば，

$$\frac{x_jx_k-y_jy_kD}{M}\in\mathbf{Z},\frac{x_ky_j-x_jy_k}{M}\in\mathbf{Z}$$

である．□

5　問題とその解

このセクションでは，シルバーマンの「初めての数論」第 31, 32 章の問題の解を与えていく.（適当に問題を選んでもよい.）

（＊問の内容も書くようにする.）

問 1.

解.

問 2.

（＊最後に参考文献を挙げる．複数でも OK.or rather better)

参考文献:

J. シルバーマン「初めての数論」