Pell 方程式と縮小写像

1　研究の動機と目的

$$x^2 - Dy^2 = 1 \quad D \in \mathbb{N}\ ,\ D \text{ は平方数でない}$$

の形で表される不定方程式を Pell 方程式と言う。この方程式は因数分解をして整数解を求める解法では解を求められない。本研究ではこの Pell 方程式の解の存在性や求め方、また縮小写像との関連性について議論することを目的とする。

2　研究の方法

ここで、私たちの考え方を示す。先ず、$\sqrt{D}$ を連分数展開すると以下のようになる。

$$\sqrt{D} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots}}}}$$

このときに D=7 とおいて連分数展開を行うと、

$$\sqrt{7} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \sqrt{7} - 2}}}} \qquad \sqrt{7} = [2, \dot{1}, 1, 1, \dot{4}]$$

となり、これに対して連分数展開と逆の操作を行い戻してみると、

$$\sqrt{7} = \frac{8\sqrt{7} + 21}{3\sqrt{7} + 8}$$

と表すことができ、このとき分母の数に注目すると $3\sqrt{7} + 8$ で、上述の Pell 方程式の (x,y) に (8,3) を代入するとこの方程式を満たす x についての最小解が求まる。ここで、講義の中でこの手順を踏んだ Pell 方程式の解の導出には「行列」や「1 次分数変換」といった考え方を使えることが知られていると紹介されたので、なぜこのような方法で Pell 方程式の解が求められるのかを考えた。

3　研究内容

ここで「行列」と「1 次分数変換」を導入する。

{ **行列** }

定義 3.1. ここにおいて用いる行列を特に $[a, b, c, d \in \mathbb{R}$ を 2×2 に並べたものとする

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

また、$A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ に対して $detA=ad-bc$ を A の行列式という。

$A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$, $B=\begin{pmatrix}p & q\\ r & s\end{pmatrix}$ のとき、$AB=\begin{pmatrix}ap+br & aq+bs\\ cp+dr & cq+ds\end{pmatrix}$　この AB を A と B の積という。

3.1 より Def　1次分数変換

$$f(x)=\frac{ax+b}{cx+d}$$　ただし、ここでの x は実数の範囲でとるものとし、$ad-bc\neq 0$ である。

ここで、

Th 連続する 1 次分数変換は、行列の積で表すことができる　ということが知られている。以下にこれを示す。

proof.

$$f(x)=\frac{px+q}{rx+s}\leftarrow\begin{pmatrix}p & q\\ r & s\end{pmatrix}\quad g(x)=\frac{ax+b}{cx+d}\leftarrow\begin{pmatrix}a & b\\ c & d\end{pmatrix}$$　とおいたとき、これらを加えると

$$f(g+x)=\frac{pq(x)+q}{rq(x)+s}=\frac{p\frac{ax+b}{cx+d}+q}{r\frac{ax+b}{cx+d}+s}=\frac{p(ax+b)+q(cx+d)}{r(ax+b)+s(cx+d)}=\frac{(pa+qc)x+pb+qd}{(ra+sc)x+rb+sd}\leftrightarrow\begin{pmatrix}pa+qc & pb+qd\\ ra+sc & rb+sd\end{pmatrix}=\begin{pmatrix}p & q\\ r & s\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}$$

と表される。ここで、実際に $\sqrt{7}$ の連分数展開について考えると、

$$\sqrt{7}=\frac{a\sqrt{7}+b}{c\sqrt{7}+d}\leftrightarrow\begin{pmatrix}a & b\\ c & d\end{pmatrix}$$ ただし、detA=1 ここで式の両辺に$\sqrt{7}+d$ をかけると、$\sqrt{7}(c\sqrt{7}+d)=a\sqrt{7}+b$

Diichlet の定理

D $\in\mathbb{N}$, D は平方数でない ある $(x,y)\in\mathbb{N}\times\mathbb{N}$ と、ある $Y>0$ が存在して、

$|x-y\sqrt{D}|<\frac{1}{Y}\leqq\frac{1}{y}$

$0,\sqrt{D}-[\sqrt{D}],2\sqrt{D}-[2\sqrt{D}],\cdots,Y\sqrt{D}-[Y\sqrt{D}]\in[0,1)$

区間 [0,1) を Y 等分する $[0,1)=[0,\frac{1}{Y})\cup[\frac{1}{Y},\frac{2}{Y})\cup\cdots\cup[\frac{Y-1}{Y},1)$ ここで鳩の巣原理という考え方を使う。鳩を $0,\sqrt{D}-[\sqrt{D}],2\sqrt{D}-[2\sqrt{D}],\cdots,Y\sqrt{D}-[Y\sqrt{D}]$、鳩の巣を $[0,\frac{1}{Y})\cup[\frac{1}{Y},\frac{2}{Y})\cup\cdots\cup[\frac{Y-1}{Y},1)$ とすると鳩は $(Y+1)$ 羽、鳩の巣は Y 個となるため、鳩が 2 羽以上入る巣が必ず現れる。このとき、ある $m,n\in0,1,2,\cdots,Y(m<n)$ が存在して、

$|(m\sqrt{D}-[m\sqrt{D}]-(n\sqrt{D}-[n\sqrt{D}])|<\frac{1}{Y}\therefore|[n\sqrt{D}]-[m\sqrt{D}]-(n-m)\sqrt{D}|<\frac{1}{Y}$

$x=[n\sqrt{D}]-[m\sqrt{D}],y=n-m$ とおくと、$|x-y\sqrt{D}|<\frac{1}{Y}$

ここで、$0\leqq m<n\leqq Y$

$y=n-m\leqq n\leqq Y$

$\frac{1}{y}\geqq\frac{1}{Y}\therefore|x-y\sqrt{D}|<\frac{1}{Y}\leqq\frac{1}{y}$ また、このとき (x,y) は無数に存在する。

Pell 方程式の別証明 $x+y\sqrt{D}$ において D が平方数でない正の整数

$$x^2+Dy^2=1\cdots(P)$$

はいつでも正の整数解を持つ。さらに、（x_1,y_1）を最小解とした時、(P) の解 (x_k,y_k) は

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

$k\in\mathbb{N}$ で得られる (P) は少なくとも 1 つの解を持つので、$Dirichlet$ の定理より、$|x-y\sqrt{D}|<\frac{1}{y}\cdots(5.1)$ を満たす $(x,y)\in\mathbb{N}\times\mathbb{N}$ が無数にある。(5.1) を満たす (x,y) を 1 つとる

$$|x^2-Dy^2|=|x+y\sqrt{D}||x-y\sqrt{D}|$$

右辺の第二因数について (5.1) より、

$$\frac{-1}{y}<x-y\sqrt{D}<\frac{1}{y}\cdots\times x<y\sqrt{D}+\frac{1}{y}x+y\sqrt{D}<y\sqrt{D}+\frac{1}{y}+y\sqrt{D}=2y\sqrt{D}+\frac{1}{y}$$

ここで、$D,y\in\mathbb{N}$ より、$\frac{1}{y}\leqq1\leqq y\sqrt{D}$

$$x+y\sqrt{D}<2y\sqrt{D}+\frac{1}{y}<3y\sqrt{D}x+y\sqrt{D}<3y\sqrt{D}\cdots(5.2)$$

両辺に $|x-y\sqrt{D}|$ をかける

$$|x^2-y^2D|<3y\sqrt{D}|x-y\sqrt{D}| \text{ より } |x^2-y^2D|<3y\sqrt{D}|x-y\sqrt{D}|<3y\sqrt{D}\times\frac{1}{y}=3\sqrt{D}\cdots(5.3)$$

$$\therefore -3\sqrt{D}<x^2-Dy^2<3\sqrt{D}$$

鳩の巣：$-3\sqrt{D}$と$3\sqrt{D}$の間にある有限の整数　鳩：(5.1) を満たす $(x,y)\in\mathbb{N}\times\mathbb{N}$ でこの (x,y) 無数に存在するある整数 M $(-3\sqrt{D}<M<3\sqrt{D})$ が存在して、$x^2-Dy^2=M\cdots(5.4)$ は無数の解をもつ。(5.4) の解 $(X_1,Y_1),(X_2,Y_2)\cdots$に対して M の剰余類、すなわち、$X_1,X_2\cdots$は次の $\subset[0],\subset[1],\cdots.\subset[M-1]$ の M 個の部分集合に分けられる。$\subset[0]:=X_i:X_i\equiv 0(modM)\subset[1]:=X_i:X_i\equiv 1(modM)\cdots\subset[M-1]:=X_i:X_i\equiv M-1(modM)Y_1,Y_2$も同様。したがって、$(X,Y)$ は $\subset[0,0]:=(X_i,Y_i):X_i\equiv 0,Y_i\equiv 0(modM)\subset[0,1]:=(X_i,Y_i):X_i\equiv 0,Y_i\equiv 1(modM)\cdots\subset[M-1,M-1]:=(X_i,Y_i):X_i\equiv M-1,Y_i\equiv M-1(modM)(X_i,Y_i)$ は無数ある $(X_j,Y_j)(X_k,Y_k)$ とある $A,B=0,1,\cdots M-1(j\neq k)$ が存在して $(X_j,Y_j)(X_k,Y_k)\in\subset[A,B]$

$$X_j\equiv X_k\equiv A(modM)Y_j\equiv Y_k\equiv B(modM)$$

(5.4) より

$$X_j^2-DY_j^2=MX_k^2-DY_k^2=M$$

を満たすここで、Lemma を用意する

{nakada}

補題 3.2. $(a,b)(c,d)\in\mathbb{N}\times\mathbb{N},x^2-Dy^2=l$ の解 ($l\in\mathbb{Z}$ ここで、$a\equiv c(mod\ l)b\equiv d(mod\ l)\dfrac{c-d\sqrt{D}}{a-b\sqrt{D}}=X+Y\sqrt{D}$ を満たす (X,Y) は $x^2-Dy^2=1$ の整数解

{nakada}

Proof

$$\begin{aligned}X+Y\sqrt{D}&=\frac{c-d\sqrt{D}}{a-b\sqrt{D}}\times\frac{a+b\sqrt{D}}{a+b\sqrt{D}}\\&=\frac{(ac-bdD)+(bc-ad)\sqrt{D}}{a^2-b^2D}\\&=\frac{(ac-bdD)+(bc-ad)\sqrt{D}}{l}\end{aligned}$$

$$X=\frac{ac-bdD}{l}\qquad Y=\frac{bc-ad}{l}$$

$$\begin{aligned}X^2-DY^2&=(\frac{ac-bdD}{l})^2-D(\frac{bc-ad}{l})^2\\&=\frac{a^2c^2-2acbdD+b^2d^2D^2}{l^2}-\frac{D(b^2c^2-2bcad+a^2d^2}{l^2}\\&=\frac{a^2c^2-(b^2c^2-a^2d^2)D+b^2d^2D^2}{l^2}\\&=\frac{(a^2-Db^2)(c^2-Dd^2)}{l^2}\\&=1\end{aligned}$$

(X,Y) は $X^2-DY^2=1$ を満たす X , Y が整数であることを示す

$$ac-bdD\equiv a^2-b^2D\equiv l\equiv 0\ (mod\ l)\qquad bc-ad\equiv ab-ab=0\ (mod\ l)$$

$ac-bdD=ml$, $bc-ad=nl$ となる $m,n\in\mathbb{Z}$ が存在する。

よって、$X=\dfrac{ml}{l}=m\in\mathbb{Z}$, $Y=\dfrac{nl}{l}=n\in\mathbb{Z}\therefore(X,Y)$ は $x^2-Dy^2=1$ の整数解より $x+y\sqrt{D}=\dfrac{X_j-Y_j\sqrt{D}}{X_k-Y_k\sqrt{D}}$で 3より求める (x,y) は $x^2-Dy^2=1$ の整数解 ($x\geqq 0,y\geqq$ としてよい)(x,y) は自明な解すなわち $x=\dfrac{X_jX_k-Y_jY_kD}{M}y=$

$\frac{X_jY_k - X_kY_jD}{M} \cdots (5.5)(x,y) = (\pm 1, 0)$ とならないことを示す $y = 0$ とする (5.5) より　$X_jY_k = X_kY_j \cdots (5.6)$

$Y_k^2M = Y_k^2(X_j^2 - DY_j^2) = (X_jY_k)^2 - D(X_jY_k)^2 = (X_kY_j)^2 - D(Y_jY_k)^2 = Y_j^2(X_k^2 - DY_k^2) = Y_j^2M$

$Y_j, Y_k > 0 Y_j = Y_k$矛盾 $y \neq 0 x^2 - Dy^2 = 1$ は非自明な自然数解をもつ (x_1, y_1): 最小任意の $(x_k, y_k), X^2 - DY^2 = 1$ の解　$k = 1$ として $x_k - \sqrt{D}y_k = (x_1 - \sqrt{D}y_1)^k, k \in \mathbb{N}$ 任意の $(u, v) : x^2 - Dy^2 = 1$ の自然数解を一つ固定するある k が存在して、$u + vsqrtD = (x + \sqrt{D}y)^k$ を示せばよい $z = x_1 + y_1\sqrt{D}r = u + v\sqrt{D}$ とおく $z > 1$

ある整数 k が存在して、

$z^k \leqq r \leqq z^k + 1 \cdots (5.7)$

$logz^k \leqq logr \leqq logz^k + 1$

$klogz \leqq logr \leqq (k+1)logz$

$z > 1$ より、$logz > 0$

$k \leqq \frac{logr}{logz} < k + 1$

k = $[\frac{logr}{logz}]$ ととればよい

z の最小性より、$[\frac{logr}{logz}] \geqq 1 \quad \therefore k \geqq 1$

$1 \leqq z^k r \leqq z \cdots (5.8)$

(x_k, y_k) を $x_k + sqrtDy_k = (x_1 + sqrtDy_1)^k$ から求められるとする

$z^-k = \frac{1}{z^k} = \frac{1}{(x_1+y_1sqrtD)^k} = \frac{1}{x_k+y_ksqrtD} * \frac{(x_k-y_ksqrtD)}{(x_k-y_k\sqrt{D})} = x_k - y_k\sqrt{D}$

$z^-kr = (x_k - y_k\sqrt{D}) * (u + v\sqrt{D}) = (x_ku - y_kvD) + (x_kv - y_ku)\sqrt{D}$

$x_ku - y_kvD = s, x_kv - y_ku = t$ とおく

s , t は次のことが言える

$(1)s^2 - Dt^2 = 1 \quad (2)s + t\sqrt{D} \geqq 1 \quad (3)s + t\sqrt{D} < z \quad (4)s \leqq 0, t \leqq 0$

$s, t > 0$ のとき、(x, y) の最小性から $x_1 \leqq s$

さらに、$x^2 - Dy^2 = 1 \quad y^2 = \frac{x^2-1}{D}$

$(s, t), (x_1, y_1) : x^2 - Dy^2 = 1$ の解は

$t^2 = \frac{s^2-1}{D} \geqq \frac{x_1^2-1}{D} = y_1^2$

$t > 0, y_1 > 0$ より、$t \geqq y_1$

$\therefore s + t\sqrt{D} \geqq x_1 + y_1\sqrt{D} = z$

これは (3) に矛盾

$\therefore s > 0, t = 0$ または $s = 0, t > 0$

$s > 0, t = 0$ とする

$s^2 - Dt^2 \leqq 1$ より、$s^2 = 1$

$s^2 = 1, t = 0$

$z^-kr = s + t\sqrt{D} = 1$

$\therefore r = z^k$

$\therefore u + vsqrtD = (x_1 + y_1sqrtD)^k$

まとめると、$(x_1, y_1) : x^2 - Dy^2 = 1$ の最小解とする

どんな $x^2 - Dy^2 = 1$ の解 (u, v) に対し、

$k = [\frac{log(u+v\sqrt{D})}{log(x_1+y_1\sqrt{D})}] \in \mathbb{N}$　ととれば、

$u + v\sqrt{D} = (x_1 + y_1\sqrt{D})^k \ |x - y\sqrt{D}| < \frac{1}{Y} \leqq \frac{1}{y}$ をみたす $(x, y) \in \mathbb{N} \times \mathbb{N}$ が有限個しかないとする。それらを $(x_1, y_1), (x_2, y_2), \cdots, (x_N, y_N)$ とすると、$|x_n - y_n\sqrt{D}| (n = 1, 2, \cdots, N)$ の最小値があることになる。その最小値を ρ とおく。Dirichlet の定理より、$Y > \frac{1}{\rho}$となる $Y \in N$ が存在する。この Y に対して、ある $(x, y) \in \mathbb{N} \times \mathbb{N}$ が存在して、$|x - y\sqrt{D} < \frac{1}{Y} < \rho$ よって ρ より小さい (x, y) があるので、Dirichlet の定理の $(x, y) \in \mathbb{N} \times \mathbb{N}$ は無数にある。宇野君↓ $x^2 - Dy^2 = 1$ の最小解を（a,b) とし任意の解を (x_k, y_k) とする。

ある自然数 k があって

$x_k + y_k\sqrt{D} = (a + b\sqrt{D})^k$

$x_k + \sqrt{D} = (a + b\sqrt{D})(c + d\sqrt{D})$ を満たす (c,d) を求める。

$x_k + y_k\sqrt{D} = ac + bdD + (ad + bc)\sqrt{D}$

$$\begin{cases} ac + bdD = x_k \\ ad + bc = y_k \end{cases}$$

この連立方程式を解くと $c = ax_k - bDy_k \quad d = ay_K - bx_k$

$c^2 - Dd^2 = (ax_k - bDy_k)^2 - D(ay_k - bx_k)^2 = (a^2 - Db^2)(x_k^2 - Dy_k^2) = 1$

また $(x_k + \sqrt{D}y_k)(x_k - \sqrt{D}y_k) = 1$

$x_k + \sqrt{D}y_k > 0$ より $x_k - \sqrt{D}y_k > 0$ したがって $x_k > \sqrt{D}y_k > 0$

同様にして $a > \sqrt{D}y_k > 0$

ゆえに $ax_k > bDy_k$, $ax_k - bDy_k > 0$

したがって $c > 0$

また $x_k > a$

$x_k^2 > a^2$

$a^2x_k^2 > a^2 + (a^2 - 1)x_k^2$

$x_k^2 - 1 > \frac{a^2-1}{a^2}x_k^2$

$Dy_k^2 > \frac{a^2-1}{a^2}x_k^2$

$y_k > \sqrt{\frac{a^2-1}{a^2D}}x_k$

$d = ay_k - bx_k > a\sqrt{\frac{a^2-1}{a^2D}}x_k - bx_k = \sqrt{\frac{a^2-1}{D}}x_k - bx_k = 0 \quad d > 0$

以上から $x_k + y_k\sqrt{D} = (a + b\sqrt{D})(c + d\sqrt{D})$ を満たす

ペル方程式の解 (c,d) があり $c > 0$,$d > 0$ を満たす。