関数体上のペル方程式

慶應大学理工学部数理科学科　中村朝子

1　背景と概略

方程式は形によっては，その整数解がどのような構造になっているかわかりにくいことがある．また，仮に整数解が 1 つ見つかった場合でも，解が有限個か無限個かはわからない．そのなかにあってペル方程式

$$x^2 - dy^2 = 1 \quad (d \in \boldsymbol{N},\ \sqrt{d} \notin \boldsymbol{N}), \quad (x, y) \in \boldsymbol{Z}^2 \tag{1}$$

の解については，解が一元生成で無限個あること，また，$\sqrt{d}$ の連分数展開によって解を求める方法などが知られている．

ペル方程式 (1) の解 (x_1, y_1) が基本解であるとは，自明解 $(\pm 1, 0)$ 以外のすべての解 (x, y) に対して $x_1 \leq x,\ (x, x_1, y_1 > 0)$ が成り立つことと定義すると，解は次の定理のようになり，基本解がわかると無限個の解が表示できる形になっている．

定理　(x_1, y_1) を $x^2 - dy^2 = 1$ の基本解とし，X と Y を次のように定める．

$$X + Y\sqrt{d} = \pm(x_1 + y_1\sqrt{d})^n$$

このとき $x^2 - dy^2 = 1$ のすべての解は (X, Y) で与えられる ([1] (10.10) Theorem)．

本稿では整数におけるペル方程式 (1) の類似として，ペル方程式の d と解の組 (x, y) として有限体上の多項式を扱う．第 1 の主定理としてペル方程式の解が一元生成であること (定理 1) を証明した．

基本解を求める方法については，整数のペル方程式では $\sqrt{d}$ の連分数展開によって求める方法がある．

定理　m を $\sqrt{d}$ の連分数展開の周期の長さ，p_k/q_k を第 k 近似分数とする．$x > 1,\ y > 0$ なるすべての解 (x, y) は次のようにして得られる．

(a) m が偶数のとき，$(x, y) = (p_{jm-1}, q_{jm-1}) \quad (j = 1, 2, 3, \cdots)$．

(b) m が奇数のとき，$(x, y) = (p_{jm-1}, q_{jm-1}) \quad (j = 2, 4, 6, \cdots)$．　([1] (10.6) Teorem)．

系　基本解 (x_1, y_1) は次のようになる．

(a) m が偶数のとき，$(x_1, y_1) = (p_{m-1}, q_{m-1})$．

(b) m が奇数のとき，$(x_1, y_1) = (p_{2m-1}, q_{2m-1})$．　([1] (10.7) Corollary)．

そこで，この基本解を求める研究を使って，第 2 の主定理として有限体上の多項式におけるペル方程式でも，$\sqrt{d}$ の連分数展開によって基本解を求める方法 (定理 2) を証明した．

なお，有限体上の多項式における連分数については [5] などの研究があり，実 2 次体の類数に関するいくつかの応用 [3], [4] が知られている．

2　多項式におけるペル方程式

p を奇素数，$\boldsymbol{F}_p$ を p 元体，$\boldsymbol{F}_p((T^{-1})) := \{\sum_{i=-\infty}^{k} c_i T^i \mid c_i \in \boldsymbol{F}_p, k \in \boldsymbol{Z}, c_k \neq 0\}$ とする．ここではペル方程式を

$$x^2 - dy^2 = 1 \quad (d \in \boldsymbol{F}_p[T], \sqrt{d} \in \boldsymbol{F}_p((T^{-1})), d \text{ は平方因子を持たない.}) \tag{2}$$

の形とし，解の組は $(x, y) \in \boldsymbol{F}_p[T]^2$ とする．$\boldsymbol{F}_p[T]$, $\boldsymbol{F}_p((T^{-1}))$ はそれぞれ $\boldsymbol{Z}$, $\boldsymbol{R}$ の類似になる．$f(T) = \sum_{i=-\infty}^{k} c_i T^i \in \boldsymbol{F}_p((T^{-1}))$ で $c_k \neq 0$ のとき，$k = \deg f(T)$ と表す．ペル方程式 (2) の解 (x_1, y_1) が基本解であるとは，自明解 $(\pm 1, 0)$ 以外のすべての解 (x, y) に対して $\deg(x_1) \leq \deg(x)$ が成り立つことである．

多項式における連分数を考える．$\alpha = \sum_{i=-\infty}^{k} c_i T^i \in \boldsymbol{F}_p((T^{-1}))$　$(c_i \in \boldsymbol{F}_p,\ k \in \boldsymbol{Z},\ c_k \neq 0)$ とする．ガウス記号 [ ] を $[\alpha] := \sum_{i=0}^{k} c_i T^i$ と定義する．$a_0 = [\alpha]$, $\alpha_1 = 1/(\alpha - a_0)$ とする．$a_i = [\alpha_i]$, $\alpha_{i+1} = 1/(\alpha_i - a_i)$ とおく．すると，α は次の形で書き表される．

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{\alpha_n}}}}}$$

略して $\alpha = \langle a_0, a_1, a_2 \cdots, a_{n-1}, \alpha_n \rangle$ と書く．

$\alpha \in \boldsymbol{F}_p((T^{-1}))$ の連分数展開における近似分数を考える．α の連分数展開を $\alpha = \langle a_0, a_1, \cdots \rangle$ とする．

定義 1　$a_0, a_1, a_2, \cdots$ $(a_i \in \boldsymbol{F}_p[T])$ に対して，$p_k, q_k \in \boldsymbol{F}_p[T]$ $(k \geq 1)$ を次のように定義する．

$$p_{-1} = 1, \quad p_0 = a_0, \quad p_k = a_k p_{k-1} + p_{k-2},$$
$$q_{-1} = 0, \quad q_0 = 1, \quad q_k = a_k q_{k-1} + q_{k-2}.$$

このとき $\langle a_0, a_1, \cdots, a_k \rangle = p_k/q_k$ となる (証明は実数の連分数の場合 [1] (9.4) Theorem と同様)．p_k/q_k を α の第 k 近似分数という．

3　主結果

補題 1　$x^2 - dy^2 = 1$ には基本解が存在する．

補題 2　(a_1, b_1) と (a_2, b_2) を $x^2 - dy^2 = 1$ の解とする．X と Y を次のように定める．

$$X + Y\sqrt{d} = (a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}).$$

このとき (X, Y) は $x^2 - dy^2 = 1$ の解となる．

定理 1　(x_1, y_1) を $x^2 - dy^2 = 1$ の基本解とする．X と Y を次のように定める．

$$X + Y\sqrt{d} = \pm(x_1 + y_1\sqrt{d})^n \quad (n \in \boldsymbol{Z}).$$

このとき $x^2 - dy^2 = 1$ のすべての解は (X, Y) で与えられる．また，(x_1, y_1) のかわりに $(-x_1, -y_1)$，$(x_1, -y_1)$，$(-x_1, y_1)$ を基本解としてもよい．

定理 2　p_k/q_k を $\sqrt{d}$ の第 k 近似分数とし $(p_k, q_k$の値は定義 1 より求める$)$，$p_k^2 - dq_k^2 = r_k$ とおく．$r_k \in \boldsymbol{F}_p$, $\left(\dfrac{r_k}{p}\right) = 1$ となる最小の k に対し $(r_k^{-\frac{1}{2}} p_k,\ r_k^{-\frac{1}{2}} q_k)$ が $x^2 - dy^2 = 1$ の基本解である．

4　証明

補題 1 の証明． $x^2 - dy^2 = 1$ が自明解 $(\pm 1, 0)$ 以外の解を持てば，基本解が存在する．自明解以外の解を持つことを示す．$x^2 - dy^2 = 1$ は $(x + y\sqrt{d})(x - y\sqrt{d}) = 1$ と書きかえることができる．$\epsilon = x + y\sqrt{d}$, $\epsilon' = x - y\sqrt{d}$ とおくと，ペル方程式の解を求めることは，$\epsilon\epsilon' = 1$ を満たす ϵ を求めることと同値になる．このような ϵ は $\boldsymbol{F}_p[T, \sqrt{d}]$ の単数である．2 次体の単数群の構造定理 ([6] Chapter IV, §4, Theorem 9) より，単数が無限個存在する．$\boldsymbol{F}_p[T, \sqrt{d}]$ の単数 $\epsilon = r + s\sqrt{d}$ $(s \neq 0)$ を 1 つとる．単数の定義より

$$\frac{1}{\epsilon} = \frac{1}{r + s\sqrt{d}} = \frac{r - s\sqrt{d}}{r^2 - ds^2} \in \boldsymbol{F}_p[T, \sqrt{d}]$$

であるので，$r^2 - ds^2 \in \boldsymbol{F}_p$ である．$r^2 - ds^2 = a \in \boldsymbol{F}_p$ とおく．ϵ の共役を $\epsilon' = r - s\sqrt{d}$ とすると，

$$\epsilon\epsilon' = (r + s\sqrt{d})(r - s\sqrt{d}) = r^2 - ds^2 = a.$$

$\epsilon_1\epsilon_1' = 1$ となる ϵ_1 が存在することを示す．$\epsilon_1 = a^{-1}\epsilon^2$ とおく．

$$\begin{aligned} \epsilon_1\epsilon_1' &= (a^{-1}\epsilon^2)(a^{-1}\epsilon^2)' = a^{-1}\epsilon^2 a^{-1}(\epsilon')^2 \\ &= (a^{-1})^2(\epsilon\epsilon')^2 = (a^{-1})^2 a^2 = 1. \end{aligned}$$

$\epsilon \notin \boldsymbol{F}_p$ より，$\epsilon_1 \notin \boldsymbol{F}_p$. よって自明でない．

補題 2 の証明． $X^2 - dY^2 = 1$ となることを示せばよい．X, Y の決め方より，$X = a_1a_2 + b_1b_2d$, $Y = a_1b_2 + a_2b_1$．また，$(a_1 - b_1\sqrt{d})(a_2 - b_2\sqrt{d}) = X - Y\sqrt{d}$ であるから，

$$\begin{aligned} X^2 - dY^2 &= (X + Y\sqrt{d})(X - Y\sqrt{d}) = (a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d})(a_1 - b_1\sqrt{d})(a_2 - b_2\sqrt{d}) \\ &= (a_1^2 - db_1^2)(a_2^2 - db_2^2) = 1. \end{aligned}$$

定理 1 の証明. 補題 2 より，$x^2 - dy^2 = 1$ の解からつくられる ϵ は単数群の無限部分群をなす．よって，(一元生成)×(有限部分) になり，あとは (有限部分)$= \pm 1$ を示せばよい．単数の定義より $a \in \boldsymbol{F}_p$ に対して $a\epsilon, (a\epsilon)'$ も $\boldsymbol{F}_p[T, \sqrt{d}]$ の単数である．$a\epsilon \times (a\epsilon)' = 1$ より $a^2 = 1$，よって $a = \pm 1$. したがって，有限部分は ± 1 となる．

注. 定理 1 は $\boldsymbol{F}_p$ を一般の体としても成り立つことが以下のようにしてわかる．一般の体 k に対し，環 $k[T, \sqrt{d}] \quad (d \in k[T], \sqrt{d} \in k((T^{-1}))$，$d$ は平方因子を持たない．) の単数群を U とする．体 $k(T, \sqrt{d})$ は $k(T)$ の"実"2 次拡大であり，2 つの無限素点 v_1, v_2 を持つ．準同型 $\varphi : U \ni f(T) \longmapsto (v_1(f), v_2(f)) \in \boldsymbol{Z} \times \boldsymbol{Z}$ を考えると，$\mathrm{Ker}(\varphi) = k^\times$，$\mathrm{Im}(\varphi) = \{(x, y) \mid x + y = 0\} \cong \boldsymbol{Z}$ であるから，$U/k^\times \cong \boldsymbol{Z}$．よって U は一元生成となり，単数定理が環 $k[T, \sqrt{d}]$ においても成り立つことがわかる．これを用いると，上記定理 1 の証明と同様にして $a = \pm 1$ がいえる．

定理 2 の証明. $A := \{(\pm x, \pm y) \mid x^2 - dy^2 = 1\}$，$B := \{(\pm r_k^{-\frac{1}{2}} p_k, \pm r_k^{-\frac{1}{2}} q_k) \mid r_k \in \boldsymbol{F}_p, \left(\frac{r_k}{p}\right) = 1\}$ とする．$A = B$ を示す．

$A \subset B$: 補題 1 より，$A \neq \emptyset$. 任意の解 $(t, u) \in A$ に対し，t/u が $\sqrt{d}$ の連分数展開における近似分数となることを示す．

(t, u) を与えるとき，t/u の $\deg \geq 0$ の部分が $\sqrt{d}$ と同一になるように $(\pm t, \pm u)$ の中から 1 つ決める．同一のものが存在することを示す．$(\pm t, \pm u)$ が解であることから，$t^2 - du^2 = 1$ が成り立ち

$$\begin{aligned} &(t - u\sqrt{d})(t + u\sqrt{d}) = 1, \\ &\deg(t - u\sqrt{d}) + \deg(t + u\sqrt{d}) = \deg 0. \end{aligned}$$

$\deg(t - u\sqrt{d}), \deg(t + u\sqrt{d})$ のうち一方が負，または両方 0 である．$\deg(t - u\sqrt{d}) < 0$ とすると

$$\deg(t/u - \sqrt{d}) < -\deg(u) \leq 0.$$

よって t/u と $\sqrt{d}$ の $\deg \geq 0$ の部分が同一である．$\deg(t + u\sqrt{d}) < 0$ の場合も同様に考え，$-t/u$ と $\sqrt{d}$ の $\deg \geq 0$ の部分が同一である．また，$\deg(t - u\sqrt{d}) = 0, \deg(t + u\sqrt{d}) = 0$ とすると

$$\deg((t - u\sqrt{d}) + (t + u\sqrt{d})) \leq 0$$

が成り立ち $\deg(t) \leq 0$．これは $\deg(t) > 0$ であることに反する．よって $\deg(t - u\sqrt{d}) = 0, \deg(t + u\sqrt{d}) = 0$ の場合はない．以上より t/u の $\deg \geq 0$ の部分が $\sqrt{d}$ と同一になるように $(\pm t, \pm u)$ の中から 1 つ決めることができる．

t/u の連分数展開を

$$\frac{t}{u} = \langle b_0, b_1, \cdots, b_{k-2}, b_{k-1} \rangle \quad (k \geq 0) \tag{3}$$

とし，

$$\frac{t'}{u'} := \langle b_0, b_1, \cdots, b_{k-2} \rangle \quad (t', u' \text{の値は定義 1 より求める.})$$

とする．$\langle b_0, b_1, \cdots, b_{k-2}, b_{k-1}, \omega \rangle = \sqrt{d}$ となる $\omega \in \boldsymbol{F}_p((T^{-1})), \deg(\omega) > 0$ が存在することを示せばよい．$\alpha \in \boldsymbol{F}_p((T^{-1}))$ の連分数展開を $\alpha = \langle a_0, a_1, \cdots, a_{n-1}, \omega \rangle$ とすると，$\alpha = (\omega p_{n-1} + p_{n-2})/(\omega q_{n-1} + q_{n-2})$ が成り立つことから (実数の場合 [1] (9.4) Theorem と同様の証明)

$$\sqrt{d} = \frac{t\omega + t'}{u\omega + u'} \tag{4}$$

より ω を求める (t, u の定数倍のずれは ω で調整する)．t', u' を $c \in \boldsymbol{F}_p, t, u, b_0$ を使って表わす．$p_{k-1}q_{k-2} - p_{k-2}q_{k-1} = (-1)^k \quad (k \geq 1)$ が成り立つことから (実数の場合 [1] (9.7) Theorem と同様の方法で証明)

$$tu' - ut' = c \in \boldsymbol{F}_p^{\times}. \tag{5}$$

(t, u) は $x^2 - dy^2 = 1$ の解であることから

$$t^2 - du^2 = 1 \tag{6}$$

が成り立つ．$(5) \times c^{-1} - (6)$ より

$$t(c^{-1}u' - t) = u(c^{-1}t' - du). \tag{7}$$

(3) より $\deg(t/u - b_0) < 0$ であるから

$$\deg(t - b_0 u) < \deg(u). \tag{8}$$

$(t, u) = 1$ であるから，(7) よりある $l \in \boldsymbol{F}_p[T]$ に対して

$$c^{-1}u' - t = lu, \tag{9}$$

$$c^{-1}t' - du = lt. \tag{10}$$

(9) の両辺に $b_0 u$ をたして

$$c^{-1}u' - (t - b_0 u) = (l + b_0)u. \tag{11}$$

$\deg(u') < \deg(u)$ より $\deg(c^{-1}u') < \deg(u)$ が成り立ち，これと (8) より $\deg(c^{-1}u' - (t - b_0 u)) < \deg(u)$．(11) より $\deg((l + b_0)u) < \deg(u)$，よって $l = -b_0$．(9)，(10) に $l = -b_0$ を代入して

$u' = c(t - b_0 u)$，$t' = c(du - b_0 t)$ となる．t', u' を (4) に代入して，$\omega = c(b_0 + \sqrt{d})$ を得る．$\deg(\omega) > 0$ であることを確かめる．$\sqrt{d},\ t/u,\ b_0$ の $\deg \geq 0$ の部分は同一であるから

$$\deg(\omega) = \deg(c(b_0 + \sqrt{d})) = \deg(b_0) > 0.$$

よって，任意の解 (t, u) に対し，t/u が $\sqrt{d}$ が連分数展開における近似分数となる．

すなわちこれは，任意の解 (t, u) に対し，ある $k \geq 0$ と $a \in \boldsymbol{F}_p$ が存在して，$t = ap_k, u = aq_k$ が成り立つことであるから

$$r_k = p_k^2 - dq_k^2 = (a^{-1}t)^2 - d(a^{-1}u)^2 = a^{-2}(t^2 - du^2) = a^{-2}.$$

よって，$r_k \in \boldsymbol{F}_p,\ \left(\dfrac{r_k}{p}\right) = 1$ が成り立ち，$A \subset B$ が示せた．

$A \supset B$: $\emptyset \neq A \subset B$ より $B \neq \emptyset$．任意の $(\pm r_k^{-\frac{1}{2}} p_k,\ \pm r_k^{-\frac{1}{2}} q_k) \in B$ が $x^2 - dy^2 = 1$ の解であることを示せばよい．

$$(\pm r_k^{-\frac{1}{2}} p_k)^2 - d(\pm r_k^{-\frac{1}{2}} q_k)^2 = r_k^{-1}(p_k^2 - dq_k^2) = r_k^{-1} \cdot r_k = 1.$$

以上より $A = B$ が示せた．また，「最小の k」が基本解となることは，定義 1 より $\deg(p_k) < \deg(p_{k+1}) \quad (k \geq 1)$ であることからわかる．

注． $\deg(t - u\sqrt{d}) = \deg(t + u\sqrt{d}) = 0$ はあり得ないことが分かると $|t/u - \sqrt{d}| < |1/u^2|$ $(|x| := p^{\deg(x)})$ となる．これは t/u が $\sqrt{d}$ の非常に良い近似分数であることを示している．このことから直接 t/u が $\sqrt{d}$ の連分数展開における近似分数であることを証明することも可能である ([2] Lemma1.7)．

注． $\sqrt{d}$ の連分数展開が循環することは，上西千春さん [7] Theorem4.3.3 によって証明されている．

5 例

定理 2 を用い，$\sqrt{d}$ の連分数展開の近似分数から基本解を求める．

例 1 $p = 5,\ d = T^4 + T^3 + 3T^2 + 2$ とする．$\sqrt{d} = \langle T^2 + 3T + 2,\ \overline{4T + 3,\ 2T^2 + T + 4} \rangle$ ($\overline{\quad}$ は循環節) となる．定義 1 より (p_k, q_k) の値を求める．$(p_0, q_0) = (T^2 + 3T + 2, 1)$ より $r_0 = 2T + 2 \notin \boldsymbol{F}_p$．$(p_1, q_1) = (4T^3 + 2T + 2, 4T + 3)$ より $r_1 = 1$．よって基本解は $(p_1, q_1) = (4T^3 + 2T + 2, 4T + 3)$ となる．

例 2 $p = 3,\ d = T^2 + 1$ とする．$\sqrt{d} = \langle T,\ \overline{2T} \rangle$ となる．$(p_0, q_0) = (T, 1)$ より $r_0 = -1 \in \boldsymbol{F}_p$，$(\frac{-1}{3}) \neq 1$．$(p_1, q_1) = (2T^2 + 1, 2T)$ より $r_1 = 1$．よって基本解は $(p_1, q_1) = (2T^2 + 1, 2T)$ となる．

例 3 $p = 7,\ d = T^2 + T$ とする．$\sqrt{d} = \langle T + 4,\ \overline{6T + 3,\ 2T + 1} \rangle$ となる．$(p_0, q_0) = (T + 4, 1)$ より $r_0 = 2 \in \boldsymbol{F}_p$．$(\frac{2}{7}) = 1,\ r_0^{-\frac{1}{2}} = \pm 2$．よって基本解は $(r_0^{-\frac{1}{2}} p_0,\ r_0^{-\frac{1}{2}} q_0) = (\pm 2(T + 4),\ \pm 2)$ となる．

例4　$p=5$, $d=T^4+T^3+T^2+2T+3$ とする．$\sqrt{d}=\langle T^2+3T+1,\ \overline{2T+2,\ 2T+2,\ 2T^2+T+2}\rangle$ となる．$(p_0,q_0)=(T^2+3T+1,1)$ より $r_0=4T+3\notin \boldsymbol{F}_p$．$(p_1,q_1)=(2T^3+3T^2+3T+3,2T+2)$ より $r_1=T+2\notin \boldsymbol{F}_p$．$(p_2,q_2)=(4T^4+3T^2+2,4T^2+3T)$ より $r_2=4\in \boldsymbol{F}_p$．$(\frac{4}{5})=1$, $r_2^{-\frac{1}{2}}=\pm 2$．よって基本解は $(r_2^{-\frac{1}{2}}p_2,\ r_2^{-\frac{1}{2}}q_2)=(\pm 2(4T^4+3T^2+2),\ \pm 2(4T^2+3T))$ となる．

注． C.Friesen の学位論文 [2] Lemma2.0 により $\sqrt{d}\in \boldsymbol{F}_p((T^{-1}))$ の連分数展開は

$$\sqrt{d}=\langle [\sqrt{d}],\overline{a_1,\cdots,a_{m-1},2[\sqrt{d}]/c,a_{m-1},\cdots,a_1,2[\sqrt{d}]}\rangle,$$

$$(a_i\neq [\sqrt{d}]c'\ (1\leq i\leq m-1),\quad c,c'\in \boldsymbol{F}_p)$$

となることが知られている．この結果を用いると $\sqrt{d}$ の連分数展開の形から定理 2 の「最小の k」と基本解を求めることができる．

参考文献

[1] A.Adler and J.E.Coury, "The Theory of Numbers: A text and source book of problem", Jones and Bartlett Publishers, Boston, 1995.

[2] C.Friesen, "Continued fractions and real quadratic function fields", Doctoral Thesis, Brown University (1989).

[3] C.Friesen, "Class numbers divisibility in real quadratic function fields", Canada. Math. Bull. 35 (1992), no3, 367-370.

[4] C.Friesen and P. Van Wamelen, "Class numbers of real quadratic function fields", Acta Arith. 81 (1997), no1, 45-55.

[5] D.Thakur, "Continued fraction for the exponential for $\boldsymbol{F}_q[T]$", J. Number Theory 41 (1992), 150-155.

[6] A.Weil, "Basic Number Theory", Springer-Verlag, New York, 1973.

[7] 上西千春「2 次の無理多項式における連分数展開」数学研究法セミナー報告集 1999 年度, 66-77, 慶應義塾大学理工学部.