Lucas 数列の可除性について〜Carmichael の論文に遡る

On the divisibility of Lucas sequences, toward the source going up Carmichael

数学専攻　水落　優斗
MIZUOCHI Yuto

本論文は，Carmichael によって [1] において示された，2 階における Lucas 数列の可除性について得られた結果についてまとめた総合報告である．Lucas は Lucas 数列の可除性について研究を進め，lois de l'apparition et la répétition と彼が名付けた基本的な定理を示した．その後も次々に関連する研究がなされ続けている．最近，諏訪はこれまでに展開された議論を見直し，群スキームの理論を援用して n 階の Lucas 数列がもつ一般的な可除性を提示した．Carmichael は 2 階の場合における Lucas 数列の特殊な可除性についてを述べている．

1　n 階の Lucas 数列の一般的な可除性

初めに，先行研究で扱われている n 階における Lucas 数列の可除性について述べる．この先行研究は主に諏訪 [3]，[4]，[5] に依る．

記号 1.1. R を可換環，$P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1}t - P_n \in R[t]$ とする． このとき, $R^{\mathbb{N}}$ の部分集合 $\mathcal{L}(P,R)$ を

$$\mathcal{L}(P,R) = \{(w_k)_{k\geq 0} \in R^{\mathbb{N}} \text{ ; 各 } k \geq 0 \text{ に対して } w_{k+n} = P_1 w_{k+n-1} + \cdots + P_{n-1}w_{k+1} + P_n w_k \text{ が成立する }\}$$

によって定義する． 特に, $L_0 = \ldots = L_{n-2} = 0, L_{n-1} = 1$ によって定義される $\mathcal{L}(P,R)$ の元 $\boldsymbol{L} = (L_k)_{k\geq 0}$ を $P(t)$ に伴う Lucas 数列という．

定義 1.2. $P(t) \in \mathbb{Z}[t]$, $(L_k)_{k\geq 0}$ を $P(t)$ に伴う Lucas 数列とし, m を整数 ≥ 2 とする．

$$L_k \equiv \cdots \equiv L_{k+n-2} \equiv 0 \mod m$$

となるような最小の正の整数を，もし存在すれば，Lucas 数列 $(L_k)_{k\geq 0}$ の m を法とする rank といい，$r(m)$ で表す．

定義 1.3. $P(t) \in \mathbb{Z}[t]$，$(L_k)_{k\geq 0}$ を $P(t)$ に伴う Lucas 数列とし，m を整数 ≥ 2 とする．

$$L_k \equiv \cdots \equiv L_{k+n-2} \equiv 0 \mod m,\ L_{k+n-1} \equiv 1 \mod m$$

となるような最小の正の整数を，もし存在すれば，Lucas 数列 $(L_k)_{k\geq 0}$ の m を法とする period といい，$k(m)$ で表す．

定理 1.4. $P(t) \in \mathbb{Z}[t]$, $(L_k)_{k\geq 0}$ を $P(t)$ に伴う Lucas 数列とし，m を整数 ≥ 2 とする．このとき，$(m, P_n) = 1$ ならば，$(L_k)_{k\geq 0}$ の m を法とする rank $r(m)$ および period $k(m)$ が存在する．さらに，θ を $\mathbb{Z}[t]/(P(t))$ における t の像とすれば，次が成立する．

(1) $k(m) = [\theta$ の $G_P(\mathbb{Z}/m\mathbb{Z})$ における位数$]$

(2) $r(m) = [\theta$ の $G_{(P)}(\mathbb{Z}/m\mathbb{Z})$ における位数]

例 1.5 (Lucas の lois de l'apparition et la répétition I)**.** P, Q を整数 $\neq 0$, $(L_k)_{k\geq 0}$ を (P, Q) に伴う Lucas 数列とし，p を素数 > 2 とする．このとき，$p \nmid Q$ なら $(L_k)_{k\geq 0}$ の p を法とする rank $r(p)$ が存在する．さらに，$L_k \equiv 0 \mod p \Leftrightarrow r(p)|k$. また，$D = P^2 - 4Q$ とおくと，次が成立する．

(1) $\left(\dfrac{D}{p}\right) = 1$ なら，$r(p)|(p-1)$.
(2) $\left(\dfrac{D}{p}\right) = -1$ なら，$r(p)|(p+1)$.

例 1.6 (Lucas の lois de l'apparition et la répétition II)**.** P, Q を整数 $\neq 0$, $(S_k)_{k\geq 0}$ を (P, Q) に伴う同伴 Lucas 数列，p を素数 > 2 とし，$p \nmid Q$ と仮定する．このとき，$S_k \equiv 0 \mod p$ となるような k が存在する $\Leftrightarrow 2|r(p)$.

命題 1.7. $P(t) = t^n - P_1 t - \cdots - P_{n-1}t - P_n \in \mathbb{Z}[t]$ $(P_n \neq 0)$, p を素数 > 2, N を正の整数とし，$(p, P_n) = 1$ と仮定する．また，$\nu = \mathrm{ord}_p L_{r(p)}$ とおき，ν' を $L_{k(p)} \equiv 0 \mod p^{\nu'}$, $L_{k(p)+1} \equiv 1 \mod p^{\nu'}$ となるような最小の正の整数とする．このとき，次が成立する．

(1) $\nu = \mathrm{ord}_p L_{k(p)}$
(2) $r(p^N) = \begin{cases} r(p) & (N \leq \nu) \\ p^{N-\nu} r(p) & (N > \nu) \end{cases}$
(3) $k(p^N) = \begin{cases} k(p) & (N \leq \nu') \\ p^{N-\nu} k(p) & (N > \nu') \end{cases}$
(4) $L_{k(p)+1} \equiv 1 \mod p^{\nu}$ なら，$\nu' = \nu$

2 Carmichael の仕事

ここからは，Carmichael[1] によって示された，2 階の場合における Lucas 数列の特別な可除性について述べる．まずは 2 階の Lucas 数列の定義を再記する．

定義 2.1. $P, Q \in \mathbb{Z}$ とし，$p \neq 0,\ Q \neq 0,\ (P, Q) = 1$ と仮定する．二階線形差分方程式

$$L_0 = 0,\ L_1 = 1,\ L_{n+2} - PL_{n+1} + QL_n = 0$$

によって定義される数列 L_n を，(P, Q) に伴う Lucas 数列という．二階線形差分方程式

$$S_0 = 2,\ S_1 = P,\ S_{n+2} - PS_{n+1} + QS_n = 0$$

によって定義される数列 S_n を，(P, Q) に伴う同伴 Lucas 数列という．

公式 2.2 (Binet の公式)**.** $D = P^2 - 4Q \neq 0$ と仮定し，α, β を二次方程式 $z^2 - Pz + Q = 0$ の解とする．このとき，$n \geq 0$ に対して，次が成立する．

$$L_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \alpha^{n-1} + \alpha^{n-2}\beta + \cdots + \alpha\beta^{n-2} + \beta^{n-1}$$
$$S_n = \alpha^n + \beta^n$$

例 2.3. (1) $P = 1, Q = -1$ に伴う Lucas 数列は Fibonacci 数列に他ならない．$(F_{n+2} = F_{n+1} + F_n)$

$$F_n = \frac{1}{\sqrt{5}} \left\{ \left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n \right\}$$

(2) $P=2, Q=-1$ に伴う Lucas 数列は Pell 数列に他ならない．($P_{n+2}=2P_{n+1}+P_n$)

$$P_n=\frac{1}{2\sqrt{2}}\left\{(1+\sqrt{2})^n-(1-\sqrt{2})^n\right\}$$

以下，α,β は公式 2.2 で定義したものとする．

記号 2.4 (円分多項式)**.** n を正の整数とし，$\zeta=e^{2\pi i/n}$ とおく．$\Phi_n(X,Y)\in\mathbb{Z}$ を

$$\Phi_n(X,Y)=\prod_{\substack{1\le k\le n\\(k,n)=1}}(X-\zeta^k Y)$$

によって定義する．このとき，

$$X^n-Y^n=\prod_{d|n}\Phi_d(X,Y)$$

が，さらに，

$$\Phi_n(X,Y)=\prod_{d|n}(X^d-Y^d)^{\mu(n/d)}$$

が成立する．ここで，整数 $n\ge 1$ に対し，$\mu(n)$ は Möbius 関数

$$\mu(n)=\begin{cases}1 & n=1\\ (-1)^r & n=p_1p_2\cdots p_r\ (p_1,p_2,\cdots p_r\text{は相異なる素数})\\ 0 & n\text{が平方因子をもつ}\end{cases}$$

を表す．

Carmichael は 2 階の Lucas 数列がこの円分多項式を用いて表すことができることを発見し，様々な可除性を見出してきた．

公式 2.5.

$$L_n=\prod_{\substack{d|n\\ d\neq 1}}\Phi_d(\alpha,\beta)$$

$$S_n=\prod_{\substack{d|2n\\ d\nmid n}}\Phi_d(\alpha,\beta)$$

定理 2.6. ν が n の約数のとき，$L_\nu|L_n$ で，

$$\frac{L_n}{L_\nu}=\prod_{\substack{d|n\\ d\nmid\nu}}\Phi_d(\alpha,\beta)$$

さらに，$\dfrac{n}{\nu}$ が奇数ならば，$S_\nu|S_n$ で，$r=\mathrm{ord}_2 n$ とおくと，

$$\frac{S_n}{S_\nu}=\prod_{\substack{d|n\\ d\nmid\nu}}\Phi_{2^{r+1}d}(\alpha,\beta)$$

が成り立つ．

定理 2.7.

$$(L_m,L_n)=L_{(m,n)}$$

さらに，$\dfrac{m}{(m,n)}$ と $\dfrac{n}{(m,n)}$ がともに奇数ならば，

$$(S_m,S_n)=S_{(m,n)}$$

3 primitive factor

素数による Lucas 数列の可除性について，Carmichael は characteristic factor というものを定義して議論をした．この characteristic factor を新たに primitive factor として読み換えて得られた結果を述べていく．

定理 3.1. n を整数 ≥ 2，p を素数とし，$(p, Q) = 1$ と仮定する．このとき，次の条件は同値．

(a) $r(p) = n$.
(b) $p|L_n$，また，$1 \leq k < n$ に対して $p \nmid L_k$.
(c) $p|\Phi_n(\alpha, \beta)$ で $r(p) = n$.
(d) $p|\Phi_n(\alpha, \beta)$，また，$2 \leq k < n$ に対して $p \nmid \Phi_k(\alpha, \beta)$.

系 3.2. n を整数 ≥ 2，p を素数とし，$(p, Q) = 1$ と仮定する．このとき，次の条件は同値．

(a) $r(p) = 2n$.
(b) $p|S_n$，また，$1 \leq k < n$ に対して $p \nmid S_k$.
(c) $p|\Phi_{2n}(\alpha, \beta)$ で $r(p) = 2n$.

定義 3.3. n を整数 ≥ 2，p を素数とする．定理 3.1 の同値な条件が成立するとき，p は $L_n, \Phi_n(\alpha, \beta)$ の primitive factor であるという．系 3.2 の同値な条件が成立するとき，p は S_n の primitive factor であるという．

定理 3.4. (1) $\Phi_n(\alpha, \beta)$ の primitive factor は L_n の primitive factor.
(2) $\Phi_{2n}(\alpha, \beta)$ の primitive factor は S_n の primitive factor.

定理 3.5. $\alpha, \beta \in \mathbb{R}$, $n \neq 1, 2, 6$ のとき，$n = 12, P = \pm 1, Q = -1$ の場合を除いて L_n は少なくとも 1 つの primitive factor をもつ．

定理 3.6. $\alpha, \beta \in \mathbb{R}$，$n \neq 1, 3$ のとき，$n = 6, P = \pm 1, Q = -1$ の場合を除いて，S_n は少なくとも 1 つの primitive factor をもつ．

参考文献

[1] E. Lucas, Théorie des fonctions numériques simplement périodiques. Amer. J. Math. 1 (1878) 184–240.
[2] R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. Ann. of Math. 15 (1913) 30–70
[3] 諏訪紀幸，Geometric aspects of Lucas sequences, I. Tokyo J. Math. 43 (2020) 75–136
[4] 諏訪紀幸，Geometric aspects of Lucas sequences, II. Tokyo J. Math. 43 (2020) 383–454
[5] 諏訪紀幸，Geometric aspects of Lucas sequences, a survey. RIMS Kôkyûroku Bessatsu B86 (2020) 149–176
[6] 齊藤暢，幾何的視点から観た Lucas 数列〜3 階の場合，中央大学，2020