幾何的視点から観たLucas数列～3階の場合

齊藤 暢 (中央大学)

序

本稿ではLucas数列を幾何的視点から考察する方法について, 特に3階の場合を取り上げて説明する. 線型漸化式

$$w_{k+n} = P_1 w_{k+n-1} + \cdots + P_{n-1} w_{k+1} + P_n w_k \ (P_1, \ldots, P_{n-1}, P_n \in \mathbb{Z},\ w_0, w_1, \ldots, w_{n-1} \in \mathbb{Z})$$

によって定義される数列 $(w_k)_{k\geq 0}$ は様々な観点から, 例えば整数論や組み合わせ論において興味深い対象であり, 膨大な結果が蓄積されている. 特に, $n = 2$, $P_1 = 1$, $P_2 = 1$, $w_0 = 0$, $w_1 = 1$ の場合, $(w_k)_{k\geq 0}$ はFibonacci数列に他ならならず, 広くその名が知られている.

$n = 2$, $w_0 = 0$, $w_1 = 1$ の場合, 数列 $(w_k)_{k\geq 0}$ はLucas数列と呼ばれているが, これは19世紀後半に発表されたLucas [5] の仕事に由来する. 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. 20世紀初めにCarmichaelは [2] においてLucasの方法を整備して証明を簡略化し, また結果を付け加えた. この後も次々に関連する研究がなされ続けている.

諏訪は Ward [11], Laxton [3][4], 青木-酒井 [1] で展開された議論を見直し, 群スキームの理論を援用してLucas数列を幾何的に観る方法を提示した. 2階の場合は [7][8] に詳述されており, 一般の場合は [9] に概略が述べられている. 本論の第1節と第2節で [9] の概略を紹介する. 第1節では線型漸化式

$$w_{k+n} = P_1 w_{k+n-1} + \cdots + P_{n-1} w_{k+1} + P_n w_k \ (P_1, \ldots, P_{n-1}, P_n \in \mathbb{Z},\ w_0, w_1, \ldots, w_{n-1} \in \mathbb{Z})$$

によって定義される数列 $(w_k)_{k\geq 0}$ を剰余環 $\mathbb{Z}[t]/(t^n - P_1 t^{n-1} - \cdots - P_{n-1} t - P_n)$ において解釈する方法を一般の可換環の上で述べる. この方法は Ward [10] に遡る. 第2節ではLucas数列の記述に必要な群スキームを定義し, 既約剰余類群 $(\mathbb{Z}/p^N\mathbb{Z})^\times$ の構造に関するよく知られた定理を p 進指数函数を援用して一般化する. また, Lucas数列以外の線型漸化式を幾何的視点から観る方法について述べる. 第3節では3階の場合に例を示して観察を幾つか述べる.

中央大学のカリキュラムでは2年次から3年次にかけて代数学の基礎を学ぶ. 「代数学1」で群論を学び, 「代数学2」では環論を, そして「代数学3」ではガロア理論を学んだ. また, 「幾何学序論」という科目では群作用について学習した. 本稿の第1節は「代数学2」で学んだ環の準同型定理が核をなし, また, 第2節については「代数学1」で学んだ群の位数に関する定理や「幾何学序論」で得た群作用や軌道の知識が議論の理解に繋がった. Lucas数列の現地調査員として例を作り観察をした第3節では「代数学3」で得た体の拡大とガロア理論の知識によって計算の根拠が得られた. 今回の講演と本稿の作成を通して大学で学んだ代数学の知識と幾何学の知識を改めて理解をする機会を得た.

福岡数論研究集会で講演する機会を与えてくださった世話人の先生方に, また, 研究集会で有益な助言をくださった方々にこの場を借りてお礼申し上げます.

1 Lucas sequence

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

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

によって定義すれば, $\mathcal{L}(P,R)$ は $R^{\mathbb{N}}$ の部分 R 加群. $\mathcal{L}(P,R)$ の元は多項式 $P(t)$ を特性多項式にもつ線型漸化式に他ならない. さらに, $(w_k)_{k\geq 0} \mapsto (w_0, w_1, \ldots, w_{n-1})$ によって R 同型 $\mathcal{L}(P,R) \xrightarrow{\sim} R^n$ が与えられる.

定義 1.2. $\tilde{R} = R[t]/(P(t))$ とし, $\tilde{R} = R[t]/(P(t))$ において $\theta \equiv t \mod P(t)$ とおく. また, D を多項式 $P(t)$ の判別式とする. このとき $\{1, \theta, \ldots, \theta^{n-1}\}$ は $\tilde{R}$ の R 上の基底をなす. したがって, $\tilde{R}$ は R の上に有限 flat. さらに D が R において巾零でなければ, $\tilde{R} \otimes_R R[1/D]$ は $R[1/D]$ の上に有限 étale である.

$\rho : \tilde{R} \to M(n,R)$ を R 上の基底 $\{1, \theta, \ldots, \theta^{n-1}\}$ に関する R 代数 $\tilde{R}$ の正則表現とする. $\eta \in \tilde{R}$ のノルム $\mathrm{Nr}\,\eta$ を $\mathrm{Nr}\,\eta = \det \rho(\eta)$ によって定義する. このとき, 「η が $\tilde{R}$ において可逆 $\Leftrightarrow$ $\mathrm{Nr}\,\eta$ が R において可逆」が成り立つ.

R 準同型 $\omega : \tilde{R} \to R$ を

$$\omega(a_0 + a_1\theta + \cdots + a_{n-2}\theta^{n-2} + a_{n-1}\theta^{n-1}) = a_{n-1}$$

によって定義する. さらに, R 準同型 $\tilde{\omega} : \tilde{R} \to R^{\mathbb{N}}$ を

$$\tilde{\omega}(\eta) = (\omega(\theta^k \eta))_{k\geq 0}$$

によって定義する.

R の元の列 $(w_k)_{k\geq 0} = (\omega(\theta^k\eta))_{k\geq 0}$ は線型漸化式 $w_{k+n} = P_1 w_{k+n-1} + \cdots + P_{n-1}w_{k+1} + P_n w_k$ を満たすが, 次の命題によって R 加群 $\mathcal{L}(P,R)$ と剰余環 $\tilde{R} = R[t]/(P(t))$ とが完全に関係付けられる.

命題 1.3. R 準同型 $\tilde{\omega} : \tilde{R} \to R^{\mathbb{N}}$ は R 同型 $\tilde{\omega} : \tilde{R} \to \mathcal{L}(P,R)$ を誘導する. $\tilde{\omega} : \tilde{R} \to \mathcal{L}(P,R)$ の逆写像は

$$(w_0, w_1, \ldots, w_{n-1}, \ldots) \mapsto$$
$$w_0\theta^{n-1} + (w_1 - P_1 w_0)\theta^{n-2} + \cdots + (w_{n-1} - P_1 w_{n-2} - \cdots - P_{n-2}w_1 - P_{n-1}w_0)$$

によって与えられる.

系 1.4. I を R のイデアルとし, $\eta, \eta' \in \tilde{R}$ とする. このとき, $\eta \equiv \eta' \mod I \Leftrightarrow \mathcal{L}(P,R)$ において $\tilde{\omega}(\eta) \equiv \tilde{\omega}(\eta') \mod I$.

R 加群の同型 $\tilde{\omega} : \tilde{R} \xrightarrow{\sim} \mathcal{L}(P,R)$ によって Binet の公式に縛られずに線型漸化式を扱うことができる.

例 1.5. $(L_k)_{k\geq 0} = \tilde{\omega}(1) \in \mathcal{L}(P,R)$ を $P(t)$ に伴う Lucas 数列と呼ぶことにする. 言い換えれば, $(L_k)_{k\geq 0}$ は, 線型漸化式 $w_{k+n} = P_1 w_{k+n-1} + \cdots + P_{n-1}w_{k+1} + P_n w_k$ と初項 $L_0 = \ldots = L_{n-2} = 0$, $L_{n-1} = 1$ によって定義される R の元の列である.

観察 1.6. R 加群の同型 $\tilde{\omega}:\tilde{R}\xrightarrow{\sim}\mathcal{L}(P,R)$ によって $\mathcal{L}(P,R)$ に R 代数の構造を定義する．このとき, Lucas 数列 $(L_k)_{k\geq 0}=\tilde{\omega}(1)$ は環 $\mathcal{L}(P,R)$ の単位元である．さらに, R 同型 $\tilde{\omega}:\tilde{R}\xrightarrow{\sim}\mathcal{L}(P,R)$ は $\tilde{R}$ での θ による乗法を $\mathcal{L}(P,R)$ における項をずらす操作 $(w_k)_{k\geq 0}\mapsto(w_{k+1})_{k\geq 0}$ に移す．

$\eta\in\tilde{R}$ とし, $\boldsymbol{w}=\tilde{\omega}(\eta)\in\mathcal{L}(P,R)$ とおく．さらに $\Delta(\boldsymbol{w})$ を $\Delta(\boldsymbol{w})=\mathrm{Nr}\,\eta$ と定義する．このとき, 「$\boldsymbol{w}$ が $\mathcal{L}(P,R)$ において可逆 $\Leftrightarrow$ $\Delta(\boldsymbol{w})$ が R において可逆」が成り立つ．

以上の議論を $R=\mathbb{Z}$ の場合に適用して, Lucas 数列の可除性に関する幾つかの結果を捉え直せる．

定義 1.7. $(L_k)_{k\geq 0}$ を $P(t)=t^n-P_1t^{n-1}-\cdots-P_{n-1}t-P_n\in\mathbb{Z}[t]$ に伴う Lucas 数列とする．Lucas 数列 $(L_k)_{k\geq 0}\mod m$ の rank (あるいは, period) を, $L_k\equiv 0\mod m,\ldots,L_{k+n-2}\equiv 0\mod m$ (あるいは, $L_k\equiv 0\mod m,\ldots,L_{k+n-2}\equiv 0\mod m, L_{k+n-1}\equiv 1\mod m$) を満たす正の整数 k が存在するとき, その最小値として定義する．また, Lucas 数列 $(L_k)_{k\geq 0}\mod m$ の rank (あるいは, period) を $r(m)$ (あるいは, $k(m)$) と書く．

同型 $\tilde{\omega}:\tilde{R}\xrightarrow{\sim}\mathcal{L}(P,\mathbb{Z})$ によって $\theta^n\in\tilde{R}=\mathbb{Z}[t]/(P(t))$ は数列 $(L_{n+k})_{k\geq 0}$ に移される．したがって, 系 1.4 を $R=\mathbb{Z}$, $I=m\mathbb{Z}$ に適用することによって次の定理を得る．

定理 1.8. m を整数 ≥ 2 とし, $(m,P_n)=1$ と仮定する．このとき, 次が成立する．
(1) $k(m)$ は $\mathcal{L}(P,\mathbb{Z}/m\mathbb{Z})^\times=(\mathbb{Z}[t]/(m,P(t)))^\times$ における θ の位数と等しい．
(2) $r(m)$ は $\mathcal{L}(P,\mathbb{Z}/m\mathbb{Z})^\times/(\mathbb{Z}/m\mathbb{Z})^\times=(\mathbb{Z}[t]/(m,P(t)))^\times/(\mathbb{Z}/m\mathbb{Z})^\times$ における θ の位数と等しい．

系 1.9. m を整数 ≥ 2 とし, $(m,P_n)=1$ と仮定する．このとき,
(1) 正の整数 k に対して $L_k\equiv 0\mod m,\ldots,L_{k+n-2}\equiv 0\mod m$ が成立するなら, k は $r(m)$ によって割り切れる．
(2) 正の整数 k に対して $L_k\equiv 0\mod m,\ldots,L_{k+n-2}\equiv 0\mod m, L_{k+n-1}\equiv 1\mod m$ が成立するなら, k は $k(m)$ によって割り切れる．
(3) $r(m)$ は $(\mathbb{Z}[t]/(m,P(t)))^\times/(\mathbb{Z}/m\mathbb{Z})^\times$ の位数を割り切る．
(4) $k(m)$ は $(\mathbb{Z}[t]/(m,P(t)))^\times$ の位数を割り切る．
(5) $r(m)$ は $k(m)$ を割り切る．

系 1.10. p を奇素数とする．このとき, $k(p)/r(p)$ は $p-1$ を割り切る．

$n=2$ で m が素数であるとき, 系 1.9(2)(3) は Lucas の lois de l'apparition et la répétition に他ならない．

2 Lucas 数列の幾何学的視点

定理 1.8 で現れた乗法群 $((\mathbb{Z}[t]/(m,P(t)))^\times$ や $((\mathbb{Z}[t]/(m,P(t)))^\times/(\mathbb{Z}/m\mathbb{Z})^\times)$ は群スキームの視点から観ることができる．[10] に従って, 議論の展開に必要な群スキームを定義した後に, p 巾を法とする Lucas 数列の rank と period の記述に必要な事項を述べる．

定義 2.1. R を環, $P(t)=t^n-P_1t^{n-1}-\cdots-P_{n-1}t-P_n\in R[t]$ とし, $\tilde{R}=R[t]/(P(t))$ とおく．また, D を多項式 $P(t)$ の判別式とする．$G_P=\prod_{\tilde{R}/R}\mathbb{G}_{m,\tilde{R}}$ (乗法群スキームの環の拡大 $\tilde{R}/R$ に関する Weil 制限) とおく．このとき, Weil 制限の定義から, R 代数 S に対して $G_P(S)=(\tilde{R}\otimes_R S)^\times$ が成立する．

標準単射 $R^\times \to \tilde{R}^\times$ は群スキームの準同型

$$i : \mathbb{G}_{m,R} \to G_P = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}$$

によって表現される. 一方, ノルム写像 $\mathrm{Nr} : \tilde{R}^\times \to R^\times$ は群スキームの準同型は

$$\mathrm{Nr} : G_P = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} \to \mathbb{G}_{m,R}$$

によって表現される. さらに, 次が示せる.
(1) $G_P = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}$ は R 上 smooth である.
(2) $i : \mathbb{G}_{m,R} \to G_P$ は closed immersion である.
(3) $\mathrm{Nr} : G_P \to \mathbb{G}_{m,R}$ は faithfully flat である.
(4) $\mathrm{Nr} \circ i : \mathbb{G}_{m,R} \to \mathbb{G}_{m,R}$ は n 乗写像である.

ここで,

$$U_P = \mathrm{Ker}[\mathrm{Nr} : G_P = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} \to \mathbb{G}_{m,R}],\ G_{(P)} = \mathrm{Coker}[i : \mathbb{G}_{m,R} \to G_P = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}]$$

とおく. このとき $G_{(P)}$ は R 上 smooth である. さらに, D が R において巾零でなければ, $G_P \otimes_R R[1/D]$, $U_P \otimes_R R[1/D]$, $G_{(P)} \otimes_R R[1/D]$ は $R[1/D]$ 上のトーラスである.

$$\beta : G_P = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} \to G_{(P)} = \Big(\prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}\Big)/\mathbb{G}_{m,R}$$

を標準全射とする.

注意 2.2. 正則表現 $\rho_R : G_P(R) = \tilde{R}^\times \to GL(n,R)$ は群スキームの準同型 $\rho : G_P \to GL_{n,R}$ によって表現される. さらに, $\rho : G_P \to GL_{n,R}$ は closed immersion.

さらに, 次の完全列の可換図式を得る:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{G}_{m,R} & \longrightarrow & G_P & \xrightarrow{\beta} & G_{(P)} & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \rho} & & \\
1 & \longrightarrow & \mathbb{G}_{m,R} & \longrightarrow & GL_{n,R} & \longrightarrow & PGL_{n,R} & \longrightarrow & 1
\end{array}$$

準同型 $\rho : G_{(P)} \to PGL_{n,R}$ は closed immersion である. また, $G_{(P)}$ は準同型 $\rho : G_{(P)} \to PGL_{n,R}$ を通して $\mathbb{P}^{n-1}_R$ に作用する.

注意 2.3. $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}[t]$ とし, p を素数とする.
(1) 群スキームの完全列

$$0 \longrightarrow \mathbb{G}_{m,\mathbb{Z}} \xrightarrow{i} G_P \xrightarrow{\beta} G_{(P)} \longrightarrow 0$$

から次の完全列の可換図式を得る:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Q}^\times & \xrightarrow{i} & G_P(\mathbb{Q}) & \xrightarrow{\beta} & G_{(P)}(\mathbb{Q}) & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \mathbb{Z}^\times_{(p)} & \xrightarrow{i} & G_P(\mathbb{Z}_{(p)}) & \xrightarrow{\beta} & G_{(P)}(\mathbb{Z}_{(p)}) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & (\mathbb{Z}/p^N\mathbb{Z})^\times & \xrightarrow{i} & G_P(\mathbb{Z}/p^N\mathbb{Z}) & \xrightarrow{\beta} & G_{(P)}(\mathbb{Z}/p^N\mathbb{Z}) & \longrightarrow & 0
\end{array}$$

(2) reduction map $G_P(\mathbb{Z}_{(p)}) \to G_P(\mathbb{Z}/p^N\mathbb{Z})$, $G_{(P)}(\mathbb{Z}_{(p)}) \to G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})$ は全射である.

さらに, R を環とする. 群スキームの完全列

$$0 \longrightarrow \mathbb{G}_{m,\mathbb{Z}} \xrightarrow{i} G_P \xrightarrow{\beta} G_{(P)} \longrightarrow 0$$

は次の完全列を与える:

$$0 \longrightarrow R^\times \xrightarrow{i} G_P(R) \xrightarrow{\beta} G_{(P)}(R) \longrightarrow H^1(R, \mathbb{G}_{m,R})$$

従って, $H^1(R, \mathbb{G}_{m,R}) = \mathrm{Pic}(R) = 0$ のとき完全列

$$0 \longrightarrow R^\times \xrightarrow{i} G_P(R) \xrightarrow{\beta} G_{(P)}(R) \longrightarrow 0$$

を得る. この完全列は $R = \mathbb{Q}$, $\mathbb{Z}_{(p)}$ or $\mathbb{Z}/p^n\mathbb{Z}$ の時に与えられる.

さらに, $\eta \in \mathbb{Z}[\theta]$ が可逆 $\Leftrightarrow \mathrm{Nr}\,\eta \not\equiv 0 \mod p$ であるので, reduction map $G_P(\mathbb{Z}_{(p)}) \to G_P(\mathbb{Z}/p^N\mathbb{Z})$, $G_{(P)}(\mathbb{Z}_{(p)}) \to G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})$ は全射である.

記号 2.4. p を素数とし, $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}_p[t]$ とおく. また, $|\ |_p$ を $\mathbb{Q}_p$ の p 進絶対値とする. $\mathbb{Q}_p$ 線型空間 $\tilde{R} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \mathbb{Q}_p \cdot 1 + \mathbb{Q}_p \cdot \theta + \cdots + \mathbb{Q}_p \cdot \theta^{n-1}$ の上の実数値関数 $||\ ||_p$ を

$$||a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}||_p = \max(|a_0|_p, |a_1|_p, \cdots, |a_{n-1}|_p)$$

によって定義する. $||\ ||_p$ に対しては次のことが分かる.

(a) $||\eta||_p = 0 \Leftrightarrow \eta = 0$.

(b) $||c\eta||_p = |c|_p||\eta||_p$ $(c \in \mathbb{Q}_p,\ \eta \in \tilde{R} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$.

(c) $||\eta + \xi||_p \le \max(||\eta||_p, ||\xi||_p)$ $(\eta, \xi \in \tilde{R} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$.

(d) $||\eta\xi||_p \le ||\eta||_p||\xi||_p$ $(\eta, \xi \in \tilde{R} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$.

$\mathbb{Q}_p$ 線型空間 $\tilde{R} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ はノルム $||\ ||_p$ に対して完備である.

定義 2.5. p を素数とし, $\eta \in \tilde{R}$ とする. このとき,

$$\exp \eta = \sum_{k=0}^{\infty} \frac{\eta^k}{k!}$$

は $p > 2$ かつ $\eta \in p\tilde{R}$, または, $p = 2$ かつ $\eta \in 4\tilde{R}$ のとき収束する. また, $p > 2$ かつ $N \ge 1$, または, $p = 2$ かつ $N \ge 2$ のとき, 写像 $\exp : p^N\tilde{R} \to \tilde{R}$ は加法群 $p^N\tilde{R}$ から乗法群 $1 + p^N\tilde{R}$ への同型写像を与える. $\exp : p^N\tilde{R} \to 1 + p^N\tilde{R}$ の逆写像は

$$1 + \eta \mapsto \log(1 + \eta) = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k}\eta^k$$

により与えられる.

以降は exp が収束する範囲で考える. 既約剰余類群 $(\mathbb{Z}/p^N\mathbb{Z})^\times$ の構造に関する定理の一般化として系 2.9 および系 2.12 を得る.

命題 2.6. 写像 $\exp : p^N\tilde{R} \to G_p(\mathbb{Z}_p)$ は同型写像

$$\exp : p^N\tilde{R} \to \mathrm{Ker}[G_P(\mathbb{Z}_p) \to G_P(\mathbb{Z}/p^N\mathbb{Z})]$$

を与える. したがって, $\mathrm{Ker}[G_P(\mathbb{Z}_p) \to G_P(\mathbb{Z}/p^N\mathbb{Z})]$ は階数 n の自由 $\mathbb{Z}_p$ 加群. さらに, 次の完全列を得る:

$$0 \to p^N\tilde{R} \xrightarrow{\exp} G_P(\mathbb{Z}_p) \to G_P(\mathbb{Z}/p^N\mathbb{Z}) \to 0$$

系 2.7. $\eta \in G_P(\mathbb{Z}_p)$ とする. また,

$$\eta \in \mathrm{Ker}[G_P(\mathbb{Z}_p) \to G_P(\mathbb{Z}/p^N\mathbb{Z})]\ ,\ \eta \notin \mathrm{Ker}[G_P(\mathbb{Z}_p) \to G_P(\mathbb{Z}/p^{N+1}\mathbb{Z})]$$

を仮定する. このとき,

$$\eta^p \in \mathrm{Ker}[G_P(\mathbb{Z}_p) \to G_P(\mathbb{Z}/p^{N+1}\mathbb{Z})]\ ,\ \eta^p \notin \mathrm{Ker}[G_P(\mathbb{Z}_p) \to G_P(\mathbb{Z}/p^{N+2}\mathbb{Z})]$$

が成り立つ.

注意 2.8. $p > 2$ かつ $N \geq 1$, または, $p = 2$ かつ $N \geq 2$ のとき, 次の合同式を使うことで, 系 3.7 を示すことも出来る:

$$(1 + p^N\xi)^p \equiv 1 + p^{N+1}\xi \mod p^{N+2}.$$

系 2.9. $p > 2$ なら, 次の完全列を得る:

$$0 \to (\mathbb{Z}/p^{N-1}\mathbb{Z})^n \to G_P(\mathbb{Z}/p^N\mathbb{Z}) \to G_P(\mathbb{Z}/p\mathbb{Z}) \to 0$$

一方で, $p = 2$ なら, 次の完全列を得る:

$$0 \to (\mathbb{Z}/2^{N-2}\mathbb{Z})^n \to G_P(\mathbb{Z}/2^N\mathbb{Z}) \to G_P(\mathbb{Z}/4\mathbb{Z}) \to 0$$

系 2.10. reduction map $G_{(P)}(\mathbb{Z}_p) \to G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})$ は全射. また, $\mathrm{Ker}[G_{(P)}(\mathbb{Z}_p) \to G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})]$ は階数 $n-1$ の自由 $\mathbb{Z}_p$ 加群.

系 2.11. $\eta \in G_P(\mathbb{Z}_p)$ とする. また,

$$\eta \in \mathrm{Ker}[G_{(P)}(\mathbb{Z}_p) \to G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})]\ ,\ \eta \notin \mathrm{Ker}[G_{(P)}(\mathbb{Z}_p) \to G_{(P)}(\mathbb{Z}/p^{N+1}\mathbb{Z})]$$

を仮定する. このとき,

$$\eta^p \in \mathrm{Ker}[G_{(P)}(\mathbb{Z}_p) \to G_{(P)}(\mathbb{Z}/p^{N+1}\mathbb{Z})]\ ,\ \eta^p \notin \mathrm{Ker}[G_{(P)}(\mathbb{Z}_p) \to G_{(P)}(\mathbb{Z}/p^{N+2}\mathbb{Z})]$$

が成り立つ.

系 2.12. $p > 2$ なら, 次の完全列を得る:

$$0 \to (\mathbb{Z}/p^{N-1}\mathbb{Z})^{n-1} \to G_{(P)}(\mathbb{Z}/p^N\mathbb{Z}) \to G_{(P)}(\mathbb{Z}/p\mathbb{Z}) \to 0$$

一方, $p = 2$ なら, 次の完全列を得る:

$$0 \to (\mathbb{Z}/2^{N-2}\mathbb{Z})^{n-1} \to G_{(P)}(\mathbb{Z}/2^N\mathbb{Z}) \to G_{(P)}(\mathbb{Z}/4\mathbb{Z}) \to 0$$

系 2.7 と系 2.11 から次の公式が導ける.

命題 2.13. $P(t) = t^n - P_1t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}[t]$, p を素数とし, $(p, P_n) = 1$ と仮定する. さらに,

$$\nu = \begin{cases} \max\{N\ ;\ \beta(\theta)^{r(p)} \in \mathrm{Ker}[G_{(P)}(\mathbb{Z}_{(p)}) \to G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})] & (p > 2) \\ \max\{N\ ;\ \beta(\theta)^{r(4)} \in \mathrm{Ker}[G_{(P)}(\mathbb{Z}_{(2)}) \to G_{(P)}(\mathbb{Z}/2^N\mathbb{Z})] & (p = 2), \end{cases}$$

また

$$\nu' = \begin{cases} \max\{N\ ;\ \theta^{k(p)} \in \mathrm{Ker}[G_P(\mathbb{Z}_{(p)}) \to G_P(\mathbb{Z}/p^N\mathbb{Z})] & (p>2) \\ \max\{N\ ;\ \theta^{k(4)} \in \mathrm{Ker}[G_P(\mathbb{Z}_{(2)}) \to G_P(\mathbb{Z}/2^N\mathbb{Z})] & (p=2) \end{cases}$$

とおく. このとき, $N > \nu$ に対して

$$r(p^N) = \begin{cases} p^{N-\nu} r(p) & (p>2) \\ 2^{N-\nu} r(4) & (p=2) \end{cases}$$

が成立する. また, $N > \nu'$ に対して

$$k(p^N) = \begin{cases} p^{N-\nu'} k(p) & (p>2) \\ 2^{N-\nu'} k(4) & (p=2) \end{cases}$$

が成立する.

$n = 2$ の場合は Lucas [5] と Carmichael [2] に遡る.
以下, Lucas 数列以外の線型漸化式の周期性について考察する.

記号 2.14. R を環, $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1}t - P_n \in R[t]$ とする. また, P_n は R において可逆と仮定する. このとき,

$$\Theta = [\theta\text{によって生成される } G_P(R) \text{ の部分群}]$$

と定義する.

Laxton [3][4] は $G_{(P)}(\mathbb{Q})$, $G_{(P)}(\mathbb{Z}_{(p)})$, $G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})$ における Θ 軌道分解について考察していると解釈できる. 青木-酒井 [1] は $G_P(\mathbb{Z}_{(p)})$ に属さない線型漸化式に対しても Laxton の議論を適用する方法を提示した. 以上の先行研究の群スキームの理論を援用した定式化については, 2 階の場合は [7][8] において徹底して議論されていて, さらに [9] では一般の階数の場合に定式が及んでいる. 以下, その概略を説明する.

観察 2.15. $G_P(R)$ の部分群 Θ は群の同型 $\tilde{\omega} : G_P(R) \xrightarrow{\sim} \mathcal{L}(P,R)^\times$ を通して乗法によって $\mathcal{L}(P,R)$ の上に左から作用する. このとき, 観察 1.6 で見たように, $(w_k)_{k\geq 0} \in \mathcal{L}(P,R)$ の Θ 軌道は $\{(w_{k+l})_{k\geq 0}\ ;\ l \in \mathbb{Z}\}$ によって与えられる.

また, $\mathcal{L}(P,R)$ の上への Θ の左作用は $\mathcal{L}(P,R)/R^\times$ の上への Θ の左作用を誘導する. $[(w_k)_{k\geq 0}] \in \mathcal{L}(P,R)/R^\times$ の Θ 軌道は $\{[(w_{k+l})_{k\geq 0}]\ ;\ l \in \mathbb{Z}\}$ によって与えられる.

観察 2.16. $\mathrm{Pic}\, R = 0$ と仮定する. $\mathcal{L}(P,R)^\circ = \{(w_k)_{k\geq 0} \in \mathcal{L}(P,R)\ ;\ (w_0, w_1, \ldots, w_{n-1}) = R\}$ とおく. このとき, $\mathcal{L}(P,R)^\circ$ は $G_P(R) = \mathcal{L}(P,R)^\times$ の $\mathcal{L}(P,R)$ の上への作用に対して安定. したがって, 乗法群 $R^\times \subset G_P(R)$ の $\mathcal{L}(P,R)$ の上への作用に対しても安定. $\mathrm{Pic}\, R = 0$ なので, $\mathbb{P}^{n-1}(R) = \mathcal{L}(P,R)^\circ/R^\times$ を得る. このとき, $G_P(R)$ の $\mathcal{L}(P,R)^\circ$ の上への作用は $G_{(P)}(R) = G_P(R)/R^\times$ の $\mathcal{L}(P,R)^\circ/R^\times = \mathbb{P}^{n-1}(R)$ への作用を誘導する.

$\boldsymbol{w} = (w_k)_{k\geq 0}$ の $\mathcal{L}(P,R)^\circ/R^\times = \mathbb{P}^{n-1}(R)$ における類を $[\boldsymbol{w}] = (w_0 : w_1 : \cdots : w_{n-1})$ で表わす. $(w_0 : w_1 : \cdots : w_{n-1}) \in \mathbb{P}^{n-1}(R) = \mathcal{L}(P,R)^\circ/R^\times$ の Θ 軌道は $\{(w_l : w_{l+1} : \cdots : w_{l+n-1})\ ;\ l \in \mathbb{Z}\}$ によって与えられる.

例 2.17. $P(t)=t^n-P_1t^{n-1}-\cdots-P_{n-1}t-P_n\in\mathbb{Z}[t]$, $(L_k)_{k\geq 0}$ を $P(t)$ に伴う Lucas 数列とする. また, m を整数 ≥ 2 とし, $(m,P_n)=1$ と仮定する. このとき, $\mathcal{L}(P,\mathbb{Z}/m\mathbb{Z})$ における $\tilde{\omega}(1)$ の Θ 軌道は乗法群

$$G_P(\mathbb{Z}/m\mathbb{Z})=\mathcal{L}(P,\mathbb{Z}/m\mathbb{Z})^\times\subset\mathcal{L}(P,\mathbb{Z}/m\mathbb{Z})$$

の θ によって生成される部分群に他ならない. したがって, $\mathcal{L}(P,\mathbb{Z}/m\mathbb{Z})$ における $\tilde{\omega}(1)$ の Θ 軌道の長さは Lucas 数列 $(L_k)_{k\geq 0}$ の period mod m に一致する. また, $\mathcal{L}(P,\mathbb{Z}/m\mathbb{Z})/(\mathbb{Z}/m\mathbb{Z})^\times$ における $\tilde{\omega}(1)$ の Θ 軌道は

$$G_{(P)}(\mathbb{Z}/m\mathbb{Z})=\mathcal{L}(P,\mathbb{Z}/m\mathbb{Z})^\times/(\mathbb{Z}/m\mathbb{Z})^\times\subset\mathcal{L}(P,\mathbb{Z}/m\mathbb{Z})/(\mathbb{Z}/m\mathbb{Z})^\times$$

の θ によって生成される部分群に他ならない. したがって, $\mathcal{L}(P,\mathbb{Z}/m\mathbb{Z})/(\mathbb{Z}/m\mathbb{Z})^\times$ における $\tilde{\omega}(1)$ の Θ 軌道の長さは Lucas 数列 $(L_k)_{k\geq 0}$ の rank mod m に一致する.

3 実例

この節では, $P(t)$ が 3 次多項式の場合を考察する. 初めに $G_P(\mathbb{F}_p)$ の構造について考察し, 幾つかの多項式に対する計算例を示す.

3.1 $G_P(\mathbb{F}_p)$ の構造

乗法群 $G_P(\mathbb{F}_p)=(\mathbb{F}_p[t]/(P(t)))^\times$ および $G_{(P)}(\mathbb{F}_p)=(\mathbb{F}_p[t]/(P(t)))^\times/\mathbb{F}_p^\times$ の構造は $\mathbb{F}_p[t]$ における $P(t)$ の既約分解によって決定される. $P(t)$ が 3 次多項式であるとき, 以下のように場合分けされる.

命題 3.2. $P(t)=t^3-P_1t^2-P_2t-P_3\in\mathbb{F}_p[t]$ とする. このとき,
(1) $P(t)=(t-\alpha)(t-\beta)(t-\gamma)$ (α, β, γ は相異なる $\mathbb{F}_p$ の元) なら, $G_P(\mathbb{F}_p)\simeq\mathbb{F}_p^\times\times\mathbb{F}_p^\times\times\mathbb{F}_p^\times$.
(2) $P(t)=(t-\alpha)^2(t-\beta)$ (α, β は相異なる $\mathbb{F}_p$ の元) なら, $G_P(\mathbb{F}_p)\simeq\mathbb{F}_p^\times\times\mathbb{F}_p\times\mathbb{F}_p^\times$.
(3) $P(t)=(t-\alpha)^3$ ($\alpha\in\mathbb{F}_p$ の元) なら, $G_P(\mathbb{F}_p)\simeq\begin{cases}\mathbb{Z}/4\mathbb{Z} & (p=2)\\ \mathbb{F}_p^\times\times\mathbb{F}_p\times\mathbb{F}_p & (p>2).\end{cases}$
(4) $P(t)=$(既約 2 次多項式)$(t-\alpha)$ ($\alpha\in\mathbb{F}_p$ の元) なら, $G_P(\mathbb{F}_p)\simeq\mathbb{F}_{p^2}^\times\times\mathbb{F}_p^\times$.
(5) $P(t)=$(既約 3 次多項式) なら, $G_P(\mathbb{F}_p)\simeq\mathbb{F}_{p^3}^\times$.

証明. (4)(5) は「素数巾 q を位数に持つ有限体の一意性」から従う. 以下, (2)(3) の場合を考える.
(2) 剰余環 $\mathbb{F}_p[u]/(u^2)$ における u の類を ε で表わせば, $\mathbb{F}_p[\varepsilon]^\times=\{a+b\varepsilon\ ;\ a\in\mathbb{F}_p^\times,\ b\in\mathbb{F}_p\}$. さらに, 対応 $a+b\varepsilon\mapsto(a,b/a)$ は群の同型 $\mathbb{F}_p[\varepsilon]^\times\xrightarrow{\sim}\mathbb{F}_p^\times\times\mathbb{F}_p^\times$ を与える.
(3) 剰余環 $\mathbb{F}_p[u]/(u^3)$ における u の類を ε で表わす. $p=2$ の場合, $\mathbb{F}_2[\varepsilon]^\times=\{1,1+\varepsilon,1+\varepsilon^2,1+\varepsilon+\varepsilon^2\}$. ここで, $(1+\varepsilon)^2=1+\varepsilon^2$ なので, $\mathbb{F}_2[\varepsilon]^\times$ は $1+\varepsilon$ によって生成される位数 4 の巡回群. $p>2$ の場合, $\mathbb{F}_p[\varepsilon]^\times=\{a+b\varepsilon+c\varepsilon^2\ ;\ a\in\mathbb{F}_p^\times,\ b,c\in\mathbb{F}_p\}$. ここで,

$$(1+\varepsilon)^k=1+k\varepsilon+\frac{k(k-1)}{2}\varepsilon^2,\ (1+\varepsilon^2)^k=1+k\varepsilon^2$$

なので, $1+\varepsilon$, $1+\varepsilon^2$ の位数は p. さらに, $1\leq k<p$ に対して $(1+\varepsilon)^k\neq 1+\varepsilon^2$. したがって, $\mathbb{F}_p[\varepsilon]^\times$ の元は $a(1+\varepsilon)^k(1+\varepsilon^2)^l$ ($a\in\mathbb{F}_p^\times$, $0\leq k<p$, $0\leq l<p$) の形に一意的に表わせる. □

系 3.3. $P(t)=t^3-P_1t^2-P_2t-P_3\in\mathbb{F}_p[t]$ とする. このとき,
(1) $P(t)=(t-\alpha)(t-\beta)(t-\gamma)$ (α, β, γ は相異なる $\mathbb{F}_p$ の元) なら, $G_{(P)}(\mathbb{F}_p)\simeq\mathbb{F}_p^\times\times\mathbb{F}_p^\times$.
(2) $P(t)=(t-\alpha)^2(t-\beta)\mod p$ (α, β は相異なる $\mathbb{F}_p$ の元) なら, $G_{(P)}(\mathbb{F}_p)\simeq\mathbb{F}_p\times\mathbb{F}_p^\times$.
(3) $P(t)=(t-\alpha)^3$ ($\alpha\in\mathbb{F}_p$ の元) なら, $G_{(P)}(\mathbb{F}_p)\simeq\begin{cases}\mathbb{Z}/4\mathbb{Z} & (p=2)\\ \mathbb{F}_p\times\mathbb{F}_p & (p>2).\end{cases}$
(4) $P(t)=$(既約 2 次多項式)$(t-\alpha)$ ($\alpha\in\mathbb{F}_p$ の元) なら, $G_{(P)}(\mathbb{F}_p)\simeq\mathbb{F}_{p^2}^\times$.
(5) $P(t)=$(既約 3 次多項式) なら, $G_{(P)}(\mathbb{F}_p)$ は位数 p^2+p+1 の巡回群.

以下, 幾つかの 3 階の Lucas 数列に対して, 特性方程式の mod p における多項式の分解, rank, period, また, 乗法群 $G_P(\mathbb{F}_p), G_{(P)}(\mathbb{F}_p), G_{(P)}(\mathbb{F}_p)/\Theta$ の位数を表にして示す.

3.4 $P(t)=t^3-t^2-t-1$ に伴う Lucas 数列 (OEIS A000073)

$P(t)=t^3-t^2-t-1$ に伴う Lucas 数列 $(L_k)_{k\geq0}$ のはじめの項は以下のようになる:

$L_0=0,\ L_1=0,\ L_2=1,\ L_3=1,\ L_4=2,\ L_5=4,\ L_6=7,\ L_7=13,\ L_8=24,$
$L_9=44,\ L_{10}=81,\ L_{11}=149,\ L_{12}=274,\ L_{13}=504,\ L_{14}=927,$
$L_{15}=1705,\ L_{16}=3136,\ L_{17}=5768,\ L_{18}=10609,\ L_{19}=19513,\ L_{20}=35890,\ldots$

また, 多項式 $P(t)=t^3-t^2-t-1$ の判別式 D は $D=-44$ である.

p	$P(t) \mod p$	period	rank	$\lvert G_P(\mathbb{F}_p)\rvert$	$\lvert G_{(P)}(\mathbb{F}_p)\rvert$	$\lvert G_{(P)}(\mathbb{F}_p)/\Theta\rvert$
2	$(t+1)^3$	4	4	4	4	1
3	既約	13	13	26	13	1
5	既約	31	31	124	31	1
7	$(t-3)(t^2+2t-2)$	48	16	6×48	48	3
11	$(t+2)(t+4)^2$	110	110	10×110	110	1
13	$(t+6)(t^2+6t+2)$	168	56	12×168	168	3
17	$(t+3)(t^2-4t-6)$	96	96	16×288	288	4
19	$(t+6)(t^2-7t+3)$	360	120	18×360	360	3
23	既約	553	553	12166	553	1
29	$(t-9)(t^2+8t+13)$	140	140	28×840	840	6
31	既約	331	331	29790	993	3
37	既約	469	469	50652	1407	3
41	$(t-19)(t^2+18t+13)$	560	560	40×1680	1680	3
43	$(t-4)(t^2+3t+11)$	308	308	42×1848	1848	6
47	$(t+21)(t-5)(t-17)$	46	46	$46\times46\times46$	46×46	46
53	$(t-13)(t-20)(t-21)$	52	52	$52\times52\times52$	52×52	52
59	既約	3541	3541	205378	3541	1
61	$(t+25)(t^2-26t-22)$	1860	620	60×3720	3720	6
67	既約	1519	1519	300762	4557	3
71	既約	5113	5113	357910	5113	1
73	$(t+5)(t^2-6t+29)$	5328	1776	72×5328	5328	3
79	$(t-19)(t^2+18t+25)$	3120	1040	78×6240	6240	6
83	$(t-21)(t^2+20t+4)$	287	287	82×6888	6888	24
89	既約	8011	8011	704968	8011	1
97	既約	3169	3169	912672	9507	3
101	$(t+39)(t^2-40t+44)$	680	680	100×10200	10200	15
103	$(t+21)(t+11)(t-33)$	51	17	$102\times102\times102$	102×102	612
107	$(t+13)(t^2-14t-33)$	1272	1272	106×11448	11448	9
109	$(t+43)(t^2-44t+38)$	990	330	108×11880	11880	36
113	既約	12883	12883	1442896	12883	1

3.5 $P(t) = t^3 - t^2 - 2t + 1$ に伴う Lucas 数列 (OEIS A006053)

$P(t) = t^3 - t^2 - 2t + 1$ に伴う Lucas 数列 $(L_k)_{k\geq 0}$ のはじめの項は以下のようになる:

$$L_0 = 0,\ L_1 = 0,\ L_2 = 1,\ L_3 = 1,\ L_4 = 3,\ L_5 = 4,\ L_6 = 9,\ L_7 = 14,\ L_8 = 28,$$
$$L_9 = 47,\ L_{10} = 89,\ L_{11} = 155,\ L_{12} = 286,\ L_{13} = 507,\ L_{14} = 924,$$
$$L_{15} = 1652,\ L_{16} = 2993,\ L_{17} = 5373,\ L_{18} = 9707,\ L_{19} = 17460,\ L_{20} = 31501, \ldots$$

また, 多項式 $P(t) = t^3 - t^2 - 2t + 1$ の判別式 D は $D = 49$ である.

p	$P(t) \mod p$	period	rank	$\lvert G_P(\mathbb{F}_p)\rvert$	$\lvert G_{(P)}(\mathbb{F}_p)\rvert$	$\lvert G_{(P)}(\mathbb{F}_p)/\Theta\rvert$
2	既約	7	7	7	7	1
3	既約	26	13	26	13	1
5	既約	62	31	124	31	1
7	$(t+2)^3$	42	7	42×7	7×7	7
11	既約	266	133	1330	133	1
13	$(t-3)(t-5)(t-6)$	12	12	$12 \times 12 \times 12$	12×12	12
17	既約	614	307	4912	307	1
19	既約	254	127	6858	381	3
23	既約	1106	553	12166	553	1
29	$(t+7)(t+3)(t-11)$	28	28	$28 \times 28 \times 28$	28×28	28
31	既約	1986	331	29790	993	3
37	既約	2814	469	50652	1407	3
41	$(t+14)(t-4)(t-11)$	40	40	$40 \times 40 \times 40$	40×40	40
43	$(t+19)(t+15)(t+8)$	42	42	$42 \times 42 \times 42$	42×42	42
47	既約	4514	2257	103822	2257	1
53	既約	5726	2863	148876	2863	1
59	既約	7082	3541	205378	3541	1
61	既約	582	97	226980	3783	39
67	既約	9114	1519	300762	4557	3
71	$(t+14)(t+4)(t-19)$	70	70	$70 \times 70 \times 70$	70×70	70
73	既約	3602	1801	389016	5403	3
79	既約	12642	2107	493038	6321	3
83	$(t+15)(t+10)(t-25)$	82	82	$82 \times 82 \times 82$	82×82	82
89	既約	16022	8011	704968	8011	1
97	$(t+41)(t+30)(t+25)$	96	96	$96 \times 96 \times 96$	96×96	96
101	既約	20606	10303	1030300	10303	1
103	既約	21426	3571	1092726	10713	3
107	既約	23114	11557	1225042	11557	1
109	既約	23982	3997	1295028	11991	3
113	$(t+24)(t+9)(t-34)$	112	112	$112 \times 112 \times 112$	112×112	112

3.6 $P(t) = t^3 - 4t^2 + t + 1$ に伴う Lucas 数列

$P(t) = t^3 - 4t^2 + t + 1$ に伴う Lucas 数列 $(L_k)_{k\geq 0}$ のはじめの項は以下のようになる:

$$L_0 = 0,\ L_1 = 0,\ L_2 = 1,\ L_3 = 4,\ L_4 = 15,\ L_5 = 55,\ L_6 = 201,\ L_7 = 734,\ L_8 = 2680,$$
$$L_9 = 9785,\ L_{10} = 35726,\ L_{11} = 130439,\ L_{12} = 476245,\ L_{13} = 1738815,$$
$$L_{14} = 6348576,\ L_{15} = 23179244,\ L_{16} = 84629585,\ L_{17} = 308990520,\ L_{18} = 1128153251,$$
$$L_{19} = 4118992899,\ L_{20} = 15038827825, \ldots$$

また, 多項式 $P(t) = t^3 - 4t^2 + t + 1$ の判別式 D は $D = 169$ である.

p	$P(t) \mod p$	period	rank	$\lvert G_P(\mathbb{F}_p)\rvert$	$\lvert G_{(P)}(\mathbb{F}_p)\rvert$	$\lvert G_{(P)}(\mathbb{F}_p)/\Theta\rvert$
2	既約	7	7	7	7	1
3	既約	13	13	26	13	1
5	$(t+2)(t+1)(t-2)$	4	4	$4\times4\times4$	4×4	4
7	既約	19	19	342	57	3
11	既約	133	133	1330	133	1
13	$(t+3)^3$	39	13	156×13	13×13	13
17	既約	307	307	4912	307	1
19	既約	381	127	6858	381	3
23	既約	553	553	12166	553	1
29	既約	871	871	24388	871	1
31	$(t+8)(t-5)(t-7)$	30	30	$30\times30\times30$	30×30	30
37	既約	1407	469	50652	1407	3
41	既約	1723	1723	68920	1723	1
43	既約	1893	631	79506	1893	3
47	$(t+21)(t-10)(t-15)$	23	23	$23\times23\times23$	23×23	23
53	$(t+19)(t-8)(t-15)$	52	52	$52\times52\times52$	52×52	52
59	既約	3541	3541	205378	3541	1
61	既約	3783	1261	226980	3783	3
67	既約	4557	1519	300762	4557	3
71	既約	5113	5113	357910	5113	1
73	$(t+11)(t+6)(t-21)$	72	72	$72\times72\times72$	72×72	72
79	$(t+16)(t-6)(t-14)$	39	39	$78\times78\times78$	78×78	156
83	$(t+36)(t-9)(t-31)$	82	82	$82\times82\times82$	82×82	82
89	既約	8011	8011	704968	8011	1
97	既約	9507	3169	912672	9507	3
101	既約	10303	10303	1030300	10303	1
103	$(t-21)(t-36)(t-50)$	102	34	$102\times102\times102$	102×102	306
107	既約	11557	11557	1225042	11557	1
109	$(t+30)(t+7)(t-41)$	108	108	$108\times108\times108$	108×108	108
113	既約	12883	12883	1442896	12883	1

4　今後の課題

(1) 特性多項式 $P(t)$ の mod p における既約分解について　$n=2$ の場合は $P(t)$ の判別式 D によって記述ができるが, $n>2$ の場合は記述が難しい. 渋川 [6] で研究されているように, $P(t)$ の最小分解体がアーベル体である場合例えば 3 階の場合は simplest cubic polynomial $P_a(t) := t^3 - at^2 + (a-3)t + 1$ (3.4 $P_1(t)$, 3.5 $P_4(t)$) 等に的を絞るべきか.

(2) $G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})/\Theta$ の位数について　r を $P(t)$ を特性多項式に持つ Lucas 数列の rank mod p とし,

$$\nu = \max\{N\ ;\ \theta^r \in \mathrm{Ker}[G_{(P)}(\mathbb{Z}_{(p)}) \to G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})]\}$$

とおく. $n=2$ の場合,

$$|G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})/\Theta| = |G_{(P)}(\mathbb{Z}/p^\nu\mathbb{Z})/\Theta|\ (N \geq \nu)$$

が成立し, これは Laxton の仕事で鍵となる事実であった. 一方, $n>2$ の場合は

$$|G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})/\Theta| = p^{(N-\nu)(n-2)}|G_{(P)}(\mathbb{Z}/p^\nu\mathbb{Z})/\Theta|\ (N \geq \nu)$$

が成立し, したがって, $|G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})/\Theta|$ は有界ではない. Laxton の結果をどのように解釈すべきなのか.

(3) $G_{(P)}(\mathbb{Q})/G_{(P)}(\mathbb{Z}_{(p)})$ **の解析について**　$n=2$ の場合, Laxton は二次体の整数論を援用して, Laxton 群の枠組で研究した. さらに, 諏訪は群スキームを援用して Laxton の仕事を補足した. そこでは Waterhouse-Weisfeler による $G_{(P)}$ の具体的な記述があることが決定的であった. しかし, $n>2$ の場合, $G_{(P)}$ の具体的な記述は難しいし, 具体的な記述に頼れそうもない.

参考文献

[1] M. Aoki and Y. Sakai, Mod p equivalence classes of linear recurrence sequences of degree 2, Rocky Mountain J. Math. **47** (2017), 2513–2533.

[2] R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, Ann. of Math. (2) **15** (1913/14), 30–48.

[3] R. R. Laxton, On groups of linear recurrences. I, Duke Math. J. **36** (1969), 721–736.

[4] R. R. Laxton, On groups of linear recurrences. II, Elements of finite order, Pacific J. Math. **32** (1970), 173–179.

[5] E. Lucas, Théorie des fonctions numériques simplement périodiques, Amer. J. Math. **1** (1878), 184–196.

[6] 渋川元樹, abenacci 数と abelucas 数, 日本フィボナッチ協会第 14 回研究集会報告書, 99–121, 2016.

[7] N. Suwa, Geometric aspects of Lucas sequences. I, Preprint series No.122, Chuo Universtiy, 2018.

[8] N. Suwa, Geometric aspects of Lucas sequences. II, Preprint series No.125, Chuo Universtiy, 2018.

[9] N. Suwa, Geometric aspects of Lucas sequences. A survey, Preprint series No.127, Chuo University, 2019.

[10] M. Ward, The arithmetical theory of linear recurring series, Trans. Amer. Math. Soc. **35** (1933), 600–628.

[11] M. Ward, The linear p-adic recurrences of order two, Illinois J. Math. **6** (1962), 40–52.