一般Lucas sequenceの素数における可除性とLaxton群について

酒井 悠帆（Yuho SAKAI）
島根大学大学院総合理工学研究科

1 はじめに

本研究は, 青木美穂氏 (島根大学) との共同研究である. 一般 Lucas sequence $\{\mathcal{G}_n\}$ を固定された整数 t, s に対して, $\mathcal{G}_0,\ \mathcal{G}_1 \in \mathbb{Z},\ \mathcal{G}_{n+2} = t\mathcal{G}_{n+1} - s\mathcal{G}_n\ (n \in \mathbb{Z})$ で定める. これ以降は簡単の為に, $\mathcal{G}_0 = a,\ \mathcal{G}_1 = b$ である一般 Lucas sequence を $\{\mathcal{G}(a,b)\}$ と表す. ここで, 2 つの有名な数列を与える. Lucas sequence $\{\mathcal{F}_n\}$ を $\mathcal{F}_0 = 0,\ \mathcal{F}_1 = 1,\ \mathcal{F}_{n+2} = t\mathcal{F}_{n+1} - s\mathcal{F}_n\ (n \in \mathbb{Z})$ を満たす数列, Companion Lucas sequence $\{\mathcal{L}_n\}$ を $\mathcal{L}_0 = 2,\ \mathcal{L}_1 = t,\ \mathcal{L}_{n+2} = t\mathcal{L}_{n+1} - s\mathcal{L}_n\ (n \in \mathbb{Z})$ 満たす数列と定める. この 2 つの数列に関しては, E. Lucas[9] や R. D. Carmichael[6] によって体系的な研究が行われた. その中に Lucas sequence の素数における可除性も考察されており, 任意の素数 p に対して, $p \mid \mathcal{F}_n$ を満たす自然数 n が存在するという結果が知られている. これは, $\mathcal{F}_0 = 0$ であることと, $\{\mathcal{F}_n\} \bmod p$ が周期的であることから得られる. しかし, Companion Lucas sequence $\{\mathcal{L}_n\}$ においては, 任意の項が割り切れないような素数 p が存在する. 例えば, 古典的なリュカ数列, つまり $t = 1, s = -1$ のときを考えると, $\{\mathcal{L}_n\} = \{\mathcal{G}(2,1)\}$ であるが, これは,$p = 5$ は任意の項を割らないことが知られている. ここで我々は, 素数 p を固定したときに, どのような一般 Lucas sequence が割り切れる項を持つか考察し, 結果を得た. 初めは, 素数 p に依存する同値関係を数列全体に導入し, その同値類の代表元を与えた. その後, C. Ballot 氏 (Caen Univ.) から素数 p に依存しない同値関係を数列全体に与えると, その商集合は群構造を持つという結果を教えて頂いた.([4], [8]) この群は定義をした B. B. Laxton の名前をとって, Laxton 群と呼ばれているが, 今回我々が定義した商集合は同様の群構造を持たなかった. しかし, 商集合の類 $\overline{\mathcal{G}}$ のうち, $\mathcal{G}$ の判別式 $\Lambda(\mathcal{G})$ が p で割り切れない類全体には同様の群構造が入ることが分かった.

2 準備

一般 Lucas sequence $\{\mathcal{G}_n\}$ の 3 項間漸化式の特性方程式を $f(X) = X^2 - tX + s \in \mathbb{Z}[X]$ と定める. 本研究では, 負の添字を持つ項に対しても整数値を取るように, $s = \pm 1$ を仮定する. さらに, $f(X)$ の根 $\theta_1,\ \theta_2$ は 1 のべき乗根でないと仮定をする. このとき, $\theta_1,\ \theta_2$ はある実 2 次体の単数である. $d := t^2 - 4s$ を $f(X)$ の判別式とする. 一般 Lucas sequence $\{\mathcal{G}_n\}$ の一般項は以下で与えられる.

$$\mathcal{G}_n = \frac{(\mathcal{G}_1 - \mathcal{G}_0\theta_2)\theta_1^n - (\mathcal{G}_1 - \mathcal{G}_0\theta_1)\theta_2^n}{\theta_1 - \theta_2} \qquad (n \in \mathbb{Z}). \tag{1}$$

また,

$$\Lambda(\mathcal{G}) := (\mathcal{G}_1 - \mathcal{G}_0\theta_1)(\mathcal{G}_1 - \mathcal{G}_0\theta_2) = \mathcal{G}_1^2 - t\mathcal{G}_0\mathcal{G}_1 + s\mathcal{G}_0^2 \quad \in \mathbb{Z}$$

を $\mathcal{G} = \{\mathcal{G}_n\}_{n\in\mathbb{Z}}$ の判別式とよぶことにする.

上記の 2 つの数列, Lucas sequence と Companion Lucas sequence は一般項が次で得られる.

$$\mathcal{F}_n = \frac{\theta_1^n - \theta_2^n}{\theta_1 - \theta_2}, \quad \mathcal{L}_n = \theta_1^n + \theta_2^n.$$

これらの数列は関係式が多く存在し, 特に重要であると考えられている.

以下, p を固定された奇素数とする.

3 主結果

数列全体の集合 $G_p(f)$ を以下で定める.

$$G_p(f) := \{\mathcal{G} = \{\mathcal{G}_n\} \mid \ p \nmid \mathcal{G}_0 \text{ または } p \nmid \mathcal{G}_1 \text{ を満たす一般 Lucas sequence}\}$$

定義 1 $\mathcal{G} = \{\mathcal{G}_n\}$, $\mathcal{G}' = \{\mathcal{G}'_n\} \in G_p(f)$ に対し, 関係 $\underset{p}{\sim}$, $\underset{p}{\sim}^*$ を以下で定義する.

(i) $\mathcal{G} \underset{p}{\sim} \mathcal{G}' \iff \mathcal{G}_1\mathcal{G}'_0 \equiv \mathcal{G}'_1\mathcal{G}_0 \pmod p$.

(ii) $\mathcal{G}\underset{p}{\sim}^*\mathcal{G}' \iff {}^{\exists}m, n \in \mathbb{Z}$ $s.t.$ $\mathcal{G}_{m+1}\mathcal{G}'_n \equiv \mathcal{G}'_{n+1}\mathcal{G}_m \pmod p$.

上記 2 つの関係 $\underset{p}{\sim}$, $\underset{p}{\sim}^*$ は集合 $G_p(f)$ において同値関係である. これらの同値関係における商集合 $X_p(f)$, $X_p^*(f)$ とその部分集合 $Y_p(f)$, $Y_p^*(f)$ を以下で定める.

$$X_p(f) := G_p(f)/\underset{p}{\sim}, \qquad Y_p(f) := \{\overline{\{\mathcal{G}_n\}} \in X_p(f) \mid \text{ 任意の } n \in \mathbb{Z} \text{ に対し}, p \nmid \mathcal{G}_n\},$$
$$X_p^*(f) := G_p(f)/\underset{p}{\sim}^*, \qquad Y_p^*(f) := \{\overline{\{\mathcal{G}_n\}} \in X_p^*(f) \mid \text{ 任意の } n \in \mathbb{Z} \text{ に対し}, p \nmid \mathcal{G}_n\}.$$

このとき, $Y_p(f)$, $Y_p^*(f)$ は well-defined である. つまり, 代表元の取り方に依らないことが示せる. このとき, $X_p(f)$ と $X_p^*(f)$ に対して次が成り立つ.

補題 2

$$X_p(f) = \{\overline{\{\mathcal{G}(a,1)\}} \mid a = 0, \cdots, p-1\} \cup \{\overline{\{\mathcal{G}(1,0)\}}\},$$
$$X_p^*(f) = \{\overline{\{\mathcal{F}_n\}}\} \cup Y_p^*(f).$$

この補題から, 任意の p で割り切れる数列は Lucas sequence $\{\mathcal{F}_n\}$ と同値関係 $\underset{p}{\sim}^*$ を持つとわかる. 次に数列 $\mathcal{G} \in G_p(f)$ の 2 次数列を定義する.

定義 3 $\mathcal{G} = \{\mathcal{G}_n\} \in G_p(f)$ に対し, 2 次数列 $\{g_n\}_{n\in\mathbb{Z}}$ $(0 \le g_n \le p-1 \ or \ g_n = \infty)$ を以下で定義する.

$$g_n \begin{cases} \equiv \mathcal{G}_n\mathcal{G}_{n+1}^{-1} \pmod p & if\ p \nmid \mathcal{G}_{n+1}, \\ = \infty & otherwise. \end{cases}$$

但し, $\mathcal{G}_{n+1}^{-1}$ は $\bmod p$ における $\mathcal{G}_{n+1}$ の逆元である.

特に, Lucas sequence $\{\mathcal{F}_n\}$ の 2 次数列を $\{f_n\}$ と表す.

次に, ランク $r(p)$ を導入する.

定義 4 $p \mid \mathcal{F}_n$ をみたす最小の自然数 n を *Lucas sequence* のランクと呼び, $r(p)$ で表す.

奇素数 p に対し, $r(p)$ は $p - \left(\frac{d}{p}\right)$ の約数であることが E. Lucas ([9, §24, 25], [6, Lemma 2, Theorem 12]) によって証明されている ($(\frac{*}{*})$ は平方剰余記号を表す).

次の定理は関係 $\underset{p}{\sim}$ における同値類に関する結果である ($t = 1, s = -1$ のときは [1]).

定理 5 (Aoki-S.)

$$Y_p(f) = \{\overline{\{\mathcal{G}(a,1)\}} \mid 1 \leq a \leq p-1, a \neq f_1, \cdots, f_{r(p)-2}\},$$

$$|Y_p(f)| = p + 1 - r(p).$$

次に, 関係 $\underset{p}{\sim}^*$ における同値類に関する結果を述べる. $Y_p^*(f)$ の代表類を与えるための補足的な定理を紹介する.

定理 6 (Aoki-S.) $s(p) := \dfrac{p - (\frac{d}{p})}{r(p)}$ とおく. 以下の 2 条件をみたす $\alpha_i \in \mathbb{Z}$ $(i = 1, \cdots, s(p) + (d/p),\ 1 \leq \alpha_i \leq p-1)$ が存在する.

(i) 数列 $\{\mathcal{G}_n\} = \{\mathcal{G}(\alpha_i, 1)\}$ は任意の $n \in \mathbb{Z}$ に対し, $p \nmid \mathcal{G}_n$ を満たす.

(ii) $\mathcal{A}_i$ を $\{\mathcal{G}(\alpha_i, 1)\}$ の 2 次数列とすると, 次が成り立つ.

$$\{a \in \mathbb{Z} \mid 1 \leq a \leq p-1,\ a \neq f_1, \cdots, f_{r(p)-2}\} = \coprod_{i=1}^{s(p)+(d/p)} \mathcal{A}_i \qquad (\textit{disjoint union}).$$

この定理より, $Y_p^*(f)$ の代表元を得る.

定理 7 (Aoki-S.) α_i $(i = 1, \cdots, s(p) + (d/p))$ を 定理 *6* の $(i), (ii)$ をみたす整数の組とすると, 次が成り立つ.

$$Y_p^*(f) = \left\{ \overline{\{\mathcal{G}(\alpha_i, 1)\}} \,\middle|\, i = 1, \cdots, s(p) + \left(\frac{d}{p}\right) \right\},$$

$$|Y_p^*(f)| = s(p) + \left(\frac{d}{p}\right).$$

4 先行研究との関係

この章では, R. R. Laxton [8] によって定義された素数 p に依存しない同値類と, その同値類全体にアーベル群の構造が入ることを紹介する. また, 我々の結果との関係についても紹介する.

$$F(f) := \{\mathcal{G} = \{\mathcal{G}_n\} \mid \mathcal{G}_0 \neq 0 \text{ または } \mathcal{G}_1 \neq 0 \text{ を満たす一般 Lucas sequence}\}.$$

定義 8 $\mathcal{G} = \{\mathcal{G}_n\}, \mathcal{G}' = \{\mathcal{G}'_n\} \in F(f)$ に対し, 関係 $\sim$, $\sim^*$ を以下で定義する.

(i) $\mathcal{G} \sim \mathcal{G}' \iff {}^{\exists}\lambda,\ \mu(\neq 0) \in \mathbb{Z}\ \ s.t.\ \ \lambda\mathcal{G}_n = \mu\mathcal{G}'_n\ (n \in \mathbb{Z})$.

(ii) $\mathcal{G} \sim^* \mathcal{G}' \iff {}^{\exists}\lambda,\ \mu(\neq 0) \in \mathbb{Z},\ {}^{\exists}v \in \mathbb{Z}\ \ s.t.\ \ \lambda\mathcal{G}_{n+v} = \mu\mathcal{G}'_n\ (n \in \mathbb{Z})$.

上記の 2 つの関係 $\sim$, $\sim^*$ は集合 $F(f)$ において同値関係である．これらの同値関係における商集合を以下で定義する．

$$G(f) := F(f)/\sim, \qquad\qquad G^*(f) := F(f)/\sim^* .$$

実際には, Laxton の論文 [8] には $G(f)$ は現れないが, 我々の同値類 $X_p(f)$ に対応した集合として定義した．ここで, Laxton が数列に導入した積について述べる．まず, 2 つの数列 $\mathcal{G} = \{\mathcal{G}_n\}$, $\mathcal{G}' = \{\mathcal{G}'_n\} \in F(f)$ に対して, 一般項をそれぞれ

$$\mathcal{G}_n := \frac{A\theta_1^n - B\theta_2^n}{\theta_1 - \theta_2}, \qquad\qquad \mathcal{G}'_n := \frac{C\theta_1^n - D\theta_2^n}{\theta_1 - \theta_2},$$

で与える．但し, $A = \mathcal{G}_1 - \mathcal{G}_0\theta_2$, $B = \mathcal{G}_1 - \mathcal{G}_0\theta_1$, $C = \mathcal{G}'_1 - \mathcal{G}'_0\theta_2$, $D = \mathcal{G}'_1 - \mathcal{G}'_0\theta_1$ である．このとき, 2 つの数列 $\mathcal{G} = \{\mathcal{G}_n\}, \mathcal{G}' = \{\mathcal{G}'_n\} \in F(f)$ の積：$\mathcal{G} \times \mathcal{G}' = \mathcal{H} = \{\mathcal{H}_n\} \in F(f)$ を以下で定める．

$$\mathcal{H}_n = \frac{AC\theta_1^n - BD\theta_2^n}{\theta_1 - \theta_2} \qquad (n \in \mathbb{Z}). \tag{2}$$

定義から, この積は可換であり, 単位元は Lucas sequence $\mathcal{F} = \{\mathcal{F}_n\} = \left\{\dfrac{\theta_1^n - \theta_2^n}{\theta_1 - \theta_2}\right\}$ である．この積から自然に誘導される積において, 商集合 $G(f), G^*(f)$ はアーベル群になる．

この事実は, まず積が代表元の取り方に拠らないこと：$\mathcal{G}, \mathcal{H}, \mathcal{G}', \mathcal{H}' \in F(f)$ に対し,

$$\begin{aligned} \mathcal{G} \sim \mathcal{G}' \text{ かつ } \mathcal{H} \sim \mathcal{H}' \quad &\Longrightarrow \quad \mathcal{G} \times \mathcal{H} \sim \mathcal{G}' \times \mathcal{H}' \\ \mathcal{G} \sim^* \mathcal{G}' \text{ かつ } \mathcal{H} \sim^* \mathcal{H}' \quad &\Longrightarrow \quad \mathcal{G} \times \mathcal{H} \sim^* \mathcal{G}' \times \mathcal{H}' \end{aligned}$$

および, 数列 $\mathcal{G} = \{\mathcal{G}_n\} \in F(f)$, $\mathcal{G}_n = \dfrac{A\theta_1^n - B\theta_2^n}{\theta_1 - \theta_2}$, $A = \mathcal{G}_1 - \mathcal{G}_0\theta_2$, $B = \mathcal{G}_1 - \mathcal{G}_0\theta_1$ に対し, 数列 $\mathcal{H} = \{\mathcal{H}_n\}$ を $\mathcal{H}_n = \dfrac{B\theta_1^n - A\theta_2^n}{\theta_1 - \theta_2}$ で定めれば, $\mathcal{H} \in F(f)$ かつ $\mathcal{G} \times \mathcal{H} \sim \mathcal{F}$ (かつ $\sim^* \mathcal{F}$) となることから分かる．

$G^*(f)$ は Laxton 群と呼ばれる．Laxton の論文 [8] では $G^*(f)$ の部分群, $I^*(f,p)$, $G^*(f,p)$ についても考察されている．本研究との関係を見るために, $G(f)$ においても対応する部分群を $I(f,p)$, $G(f,p)$ と定める．Laxton の論文とは異なる表記を用いるが, 以下で定める．

$$\begin{aligned} I(f,p) &:= \{\mathfrak{G} \in G(f) \mid {}^{\exists}\mathcal{G} \in \mathfrak{G} \text{ s.t. } \Lambda(\mathcal{G}) \not\equiv 0 \pmod p\}, \\ G(f,p) &:= \{\mathfrak{G} \in G(f) \mid {}^{\forall}\mathcal{G} = \{\mathcal{G}_n\} \in \mathfrak{G} \text{ に対し, } p \mid \mathcal{G}_0\}, \\ I^*(f,p) &:= \{\mathfrak{G} \in G^*(f) \mid {}^{\exists}\mathcal{G} \in \mathfrak{G} \text{ s.t. } \Lambda(\mathcal{G}) \not\equiv 0 \pmod p\}, \\ G^*(f,p) &:= \{\mathfrak{G} \in G^*(f) \mid {}^{\forall}\mathcal{G} = \{\mathcal{G}_n\} \in \mathfrak{G} \text{ に対し, } {}^{\exists}n \in \mathbb{Z} \text{ s.t. } p \mid \mathcal{G}_n\}. \end{aligned}$$

これらは $G(f), G^*(f)$ の部分群であることが証明でき, 包含関係 $G(f,p) \subset I(f,p) \subset G(f)$, $G^*(f,p) \subset I^*(f,p) \subset G^*(f)$ が成り立つ．

定理 9 (R. R. Laxton) [*8, Lemma* 2.3 *and Proposition* 3.1] 群の短完全列

$$0 \longrightarrow I^*(f,p)/G^*(f,p) \longrightarrow G^*(f)/G^*(f,p) \longrightarrow G^*(f)/I^*(f,p) \longrightarrow 0,$$

に対し, 次が成り立つ．

$$I^*(f,p)/G^*(f,p) \simeq \begin{cases} \mathbb{Z}/s(p)\mathbb{Z} & \text{if } (d/p) = \pm 1, \\ 0 & \text{if } (d/p) = 0, \end{cases}$$

$$G^*(f)/I^*(f,p) \simeq \begin{cases} \mathbb{Z}^{\frac{1+(d/p)}{2}} & \text{if } (d/p) = \pm 1, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } (d/p) = 0, \end{cases}$$

ここで, $s(p) = \dfrac{p-(d/p)}{r(p)}$ である.

ここで, 我々の研究と Laxton の研究との関係について述べる. 第 3 章で定めた同値類全体 $X_p(f) := G_p(f)/\underset{p}{\sim}$, $X_p^*(f) := G_p(f)/\underset{p}{\sim}^*$ は, Laxton 群と同様の群構造を持たない. 例として, $1+s-t \equiv 0 \pmod p$ のときを考える. 2 つの $\mathcal{G} = \{\mathcal{G}_n\}, \mathcal{G}' = \{\mathcal{G}'_n\} \in G_p(f)$ を $\mathcal{G}_0 \equiv \mathcal{G}_1 \not\equiv 0 \pmod p$ かつ $\mathcal{G}'_0 \equiv \mathcal{G}'_1 \not\equiv 0 \pmod p$ を満たす数列とする. このとき, $\mathcal{W} = \{\mathcal{W}_n\} = \mathcal{G} \times \mathcal{G}'$ とおくと, $p \mid \mathcal{W}_0,\ \mathcal{W}_1$ となる. よって, $\mathcal{W} \notin G_p(f)$ となり, 積で閉じていない. しかし, ここで次の $X_p(f),\ X_p^*(f)$ の部分集合を考える.

$$Z_p(f) := \{\overline{\mathcal{G}} \in X_p(f) \mid \Lambda(\mathcal{G}) \not\equiv 0 \pmod p\}, \quad Z_p^*(f) := \{\overline{\mathcal{G}} \in X_p^*(f) \mid \Lambda(\mathcal{G}) \not\equiv 0 \pmod p\}$$

これらの集合は, well-defined である. すなわち, $\mathcal{G} = \{\mathcal{G}_n\} \in G_p(f)$ が $\Lambda(\mathcal{G}) \not\equiv 0 \pmod p$ を満たすとすると, $\mathcal{G} \underset{p}{\sim} \mathcal{G}'$ (または $\mathcal{G} \underset{p}{\sim}^* \mathcal{G}'$) を満たす $\mathcal{G}' = \{\mathcal{G}'_n\} \in G_p(f)$ も, $\Lambda(\mathcal{G}') \not\equiv 0 \pmod p$ を満たす. さらに, Laxton が導入した積によって, $Z_p(f), Z_p^*(f)$ はアーベル群になる. このとき, mod p した同値類の集合 $Z_p(f),\ Z_p^*(f)$ と, mod p しない同値類の集合 $I(f,p), G(f,p), I^*(f,p), G^*(f,p)$ に関し, 以下の群の同型が成り立つ.

定理 10 (Aoki-S.)

$$I(f,p)/G(f,p) \simeq Z_p(f), \qquad I^*(f,p)/G^*(f,p) \simeq Z_p^*(f).$$

定理 10 の同型写像は, 全射準同型写像 :

$$\psi_p : I(f,p) \to Z_p(f), \qquad \psi_p(\mathfrak{G}) = \mathfrak{G}_p,$$
$$\psi_p^* : I^*(f,p) \to Z_p^*(f), \qquad \psi_p^*(\mathfrak{G}) = \mathfrak{G}_p,$$

$\mathfrak{G}_p := \{\mathcal{G} = \{\mathcal{G}_n\} \in \mathfrak{G} \mid p \nmid \mathcal{G}_0$ または $p \nmid \mathcal{G}_1\}$ に準同型定理を用いることで得られる.

$F = \mathbb{Q}(\theta_1)$ とおき, $\mathcal{O}_F$ を F の整数環とする. F は実 2 次体である. p の上にある F の素イデアル $\mathfrak{p}$ に対し, $K_1 := \mathcal{O}_F/\mathfrak{p}$, $K_2 := \mathbb{Z}/p\mathbb{Z}$ とおく. 上記の写像 ψ_p, ψ_p^* と Laxton [8, Theorem 3.7 and its proof] による考察から, 以下の可換図式を得る. 図式の各行は短完全列である.

(I) $\left(\dfrac{d}{p}\right) = 1$ のとき.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Ker}(\iota) & \longrightarrow & I(f,p)/G(f,p) & \xrightarrow{\iota} & I^*(f,p)/G^*(f,p) & \longrightarrow & 0 \\
 & & \downarrow\uparrow & & \psi_p \downarrow\uparrow & & \psi_p^* \downarrow\uparrow & & \\
0 & \longrightarrow & \{\overline{\{\mathcal{G}(f_i,1)\}} \mid i = 0, \cdots, r(p)-2\} \cup \{\overline{\{\mathcal{G}(1,0)\}}\} & \longrightarrow & Z_p(f) & \longrightarrow & Z_p^*(f) & \longrightarrow & 0 \\
 & & \downarrow\uparrow & & \varphi_p^+ \downarrow\uparrow & & \downarrow\uparrow & & \\
0 & \longrightarrow & \langle\theta_2/\theta_1\rangle & \longrightarrow & K_1^* & \longrightarrow & K_1^*/\langle\theta_2/\theta_1\rangle & \longrightarrow & 0
\end{array}$$

ここで ι は自然な全射であり, 写像 φ_p^+ は $\varphi_p^+(\overline{\mathcal{G}}) = (\mathcal{G}_1 - \mathcal{G}_0\theta_1)/(\mathcal{G}_1 - \mathcal{G}_0\theta_2)$ で与えられる.

(II) $\left(\dfrac{d}{p}\right) = -1$ のとき.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Ker}(\iota) & \longrightarrow & I(f,p)/G(f,p) & \xrightarrow{\iota} & I^*(f,p)/G^*(f,p) & \longrightarrow & 0 \\
 & & \downarrow\uparrow & & \psi_p \downarrow\uparrow & & \psi_p^* \downarrow\uparrow & & \\
0 & \longrightarrow & \{\overline{\{\mathcal{G}(f_i,1)\}} \mid i=0,\cdots, & \longrightarrow & Z_p(f) & \longrightarrow & Z_p^*(f) & \longrightarrow & 0 \\
 & & r(p)-2\} \cup \{\overline{\{\mathcal{G}(1,0)\}}\} & & & & & & \\
 & & \downarrow\uparrow & & \varphi_p^- \downarrow\uparrow & & \downarrow\uparrow & & \\
0 & \longrightarrow & K_2^*\langle\theta_1\rangle/K_2^* & \longrightarrow & K_1^*/K_2^* & \longrightarrow & K_1^*/K_2^*\langle\theta_1\rangle & \longrightarrow & 0
\end{array}$$

ここで ι は自然な全射であり, 写像 φ_p^- は $\varphi_p^-(\overline{\mathcal{G}}) = \mathcal{G}_1 - \mathcal{G}_0\theta_2$ で与えられる.

(III) $\left(\dfrac{d}{p}\right) = 0$ のとき.

$$I^*(f,p)/G^*(f,p) \overset{\psi_p^*}{\simeq} Z_p^*(f) \simeq 0$$

and

$$\begin{aligned}
Z_p(f) &= \{\overline{\{\mathcal{G}(f_i,1)\}} \mid i=0,\cdots,r(p)-2\} \cup \{\overline{\{\mathcal{G}(1,0)\}}\} \\
&= \{\overline{\{\mathcal{G}(\mathcal{F}_i,\mathcal{F}_{i+1}\}} \mid i=0,\cdots,r(p)-1\} \overset{\sim}{\underset{\varphi_p^0}{\to}} \mathbb{Z}/p\mathbb{Z}
\end{aligned}$$

ここで写像 φ_p^0 は $\varphi_p^0(\overline{\{\mathcal{G}(\mathcal{F}_i,\mathcal{F}_{i+1}\}}) = i$ で与えられる.

補題 2, 定理 5, 定理 7, 定理 10 から, アーベル群 $Z_p(f), Z_p^*(f), I(f,p)/G(f,p), I^*(f,p)/G^*(f,p)$ の代表系が以下のように分かる.

系 11 (1) $Z_p(f)$ と $I(f,p)/G(f,p)$ の全ての元は以下で与えられる.

$$\{\overline{\{\mathcal{G}(a,1)\}} \mid 0 \le a \le p-1,\ f(a^{-1}) \not\equiv 0 \pmod p\} \cup \{\overline{\{\mathcal{G}(1,0)\}}\}.$$

(2) α_i $(i = 1,\cdots,s(p)+(d/p))$ を 定理 6 の $(i),(ii)$ をみたす整数の組とする. $Z_p^*(f)$ と $I^*(f,p)/G^*(f,p)$ の全ての元は以下で与えられる.

$$\{\overline{\{\mathcal{G}(\alpha_i,1)\}} \mid i=1,\cdots,s(p)+(d/p),\ f(\alpha_i^{-1}) \not\equiv 0 \pmod p\} \cup \{\overline{\mathcal{F}}\}.$$

5 Examples

最後に代表元の計算例を挙げる. 表 1 は $t=1, s=-1$ の場合で, このとき漸化式は古典的なフィボナッチ数やリュカ数と同じ式になる. 特に $\{\mathcal{G}(0,1)\}$ はフィボナッチ数であり, $\{\mathcal{G}(2,1)\}$ はリュカ数である. 表 2 は $t=6, s=1$ の場合で, $\{\mathcal{G}(0,1)\}$ は Balancing numbers, $\{\mathcal{G}(1,3)\}$ は Lucas Balancing numbers と呼ばれている. Balancing numbers は, ラマヌジャンの有名な家の問題の解となる数列である ([5]). 表の数字に付いたアスタリスク a^* は a が $f(a^{-1}) \equiv 0 \pmod p$ の根であることを表す.

p	$r(p)$	$s(p)$	$(\frac{d}{p})$	$\mathcal{A}_i$ $(i=1,\cdots,s(p)+(\frac{d}{p}))$	$Y_p^*(f)$	$Z_p^*(f)$ $(I^*(f,p)/G^*(f,p))$
3	4	1	-1	$\emptyset$	$\emptyset$	$\overline{\mathcal{F}}$
5	5	1	0	$\{2^*\}$	$\overline{\{\mathcal{G}(2,1)\}}$	$\overline{\mathcal{F}}$
7	8	1	-1	$\emptyset$	$\emptyset$	$\overline{\mathcal{F}}$
11	10	1	1	$\{3^*\},\{7^*\}$	$\overline{\{\mathcal{G}(3,1)\}}$, $\overline{\{\mathcal{G}(7,1)\}}$	$\overline{\mathcal{F}}$
13	7	2	-1	$\{2,3,4,6,8,9,10\}$	$\overline{\{\mathcal{G}(2,1)\}}$	$\overline{\mathcal{F}},\overline{\{\mathcal{G}(2,1)\}}$
17	9	2	-1	$\{2,3,5,6,8,10,11,13,14\}$	$\overline{\{\mathcal{G}(2,1)\}}$	$\overline{\mathcal{F}},\overline{\{\mathcal{G}(2,1)\}}$
19	18	1	1	$\{4^*\},\{14^*\}$	$\overline{\{\mathcal{G}(4,1)\}}$, $\overline{\{\mathcal{G}(14,1)\}}$	$\overline{\mathcal{F}}$
23	24	1	-1	$\emptyset$	$\emptyset$	$\overline{\mathcal{F}}$
29	14	2	1	$\{5^*\},\{23^*\},\{3,4,6,7,9,11,12,16,17,19,21,22,24,25\}$	$\overline{\{\mathcal{G}(3,1)\}}$, $\overline{\{\mathcal{G}(5,1)\}}$, $\overline{\{\mathcal{G}(23,1)\}}$	$\overline{\mathcal{F}},\overline{\{\mathcal{G}(3,1)\}}$
31	30	1	1	$\{12^*\},\{18^*\}$	$\overline{\{\mathcal{G}(12,1)\}}$, $\overline{\{\mathcal{G}(18,1)\}}$	$\overline{\mathcal{F}}$
37	19	2	-1	$\{2,4,5,7,9,10,11,14,15,18,21,22,25,26,27,29,31,32,34\}$	$\overline{\{\mathcal{G}(2,1)\}}$	$\overline{\mathcal{F}},\overline{\{\mathcal{G}(2,1)\}}$
41	20	2	1	$\{6^*\},\{34^*\},\{3,4,5,7,8,9,10,13,15,18,22,25,27,30,31,32,33,35,36,37\}$	$\overline{\{\mathcal{G}(3,1)\}}$, $\overline{\{\mathcal{G}(6,1)\}}$, $\overline{\{\mathcal{G}(34,1)\}}$	$\overline{\mathcal{F}},\overline{\{\mathcal{G}(3,1)\}}$
43	44	1	-1	$\emptyset$	$\emptyset$	$\overline{\mathcal{F}}$
47	16	3	-1	$\{3,4,5,8,9,11,12,15,18,19,20,21,29,33,39,40\}$, $\{6,7,13,17,25,26,27,28,31,34,35,37,38,41,42,43\}$	$\overline{\{\mathcal{G}(3,1)\}}$, $\overline{\{\mathcal{G}(6,1)\}}$	$\overline{\mathcal{F}},\overline{\{\mathcal{G}(3,1)\}}$, $\overline{\{\mathcal{G}(6,1)\}}$

表 1: $t=1,\ s=-1$

p	$r(p)$	$s(p)$	$(\frac{d}{p})$	$\mathcal{A}_i$ $(i=1,\cdots,s(p)+(\frac{d}{p}))$	$Y_p^*(f)$	$Z_p^*(f)$ $(I^*(f,p)/G^*(f,p))$
3	2	2	-1	$\{1,2\}$	$\overline{\{\mathcal{G}(1,1)\}}$	$\overline{\mathcal{F}},\overline{\{\mathcal{G}(1,1)\}}$
5	3	2	-1	$\{2,3,4\}$	$\overline{\{\mathcal{G}(2,1)\}}$	$\overline{\mathcal{F}},\overline{\{\mathcal{G}(2,1)\}}$
7	3	2	1	$\{2^*\},\{4^*\},\{1,3,5\}$	$\overline{\{\mathcal{G}(1,1)\}}$, $\overline{\{\mathcal{G}(2,1)\}}$, $\overline{\{\mathcal{G}(4,1)\}}$	$\overline{\mathcal{F}},\overline{\{\mathcal{G}(1,1)\}}$
11	6	2	-1	$\{1,5,7,8,9,10\}$	$\overline{\{\mathcal{G}(1,1)\}}$	$\overline{\mathcal{F}},\overline{\{\mathcal{G}(1,1)\}}$
13	7	2	-1	$\{2,3,4,7,9,10,12\}$	$\overline{\{\mathcal{G}(2,1)\}}$	$\overline{\mathcal{F}},\overline{\{\mathcal{G}(2,1)\}}$
17	4	4	1	$\{8^*\},\{15^*\},\{1,5,7,16\}$ $\{2,12,13,14\},\{4,9,10,11\}$	$\overline{\{\mathcal{G}(1,1)\}}$, $\overline{\{\mathcal{G}(2,1)\}}$ $\overline{\{\mathcal{G}(4,1)\}}$, $\overline{\{\mathcal{G}(8,1)\}}$, $\overline{\{\mathcal{G}(15,1)\}}$	$\overline{\mathcal{F}},\overline{\{\mathcal{G}(1,1)\}}$ $\overline{\{\mathcal{G}(2,1)\}},\overline{\{\mathcal{G}(4,1)\}}$
19	10	2	-1	$\{1,2,4,5,7,10,11,14,15,18\}$	$\overline{\{\mathcal{G}(1,1)\}}$	$\overline{\mathcal{F}},\overline{\{\mathcal{G}(1,1)\}}$
23	11	2	1	$\{13^*\},\{16^*\},\{1,3,5,8,9,$ $11,14,15,18,20,21\}$	$\overline{\{\mathcal{G}(1,1)\}}$, $\overline{\{\mathcal{G}(13,1)\}}$, $\overline{\{\mathcal{G}(16,1)\}}$	$\overline{\mathcal{F}},\overline{\{\mathcal{G}(1,1)\}}$
29	5	6	-1	$\{2,9,19,20,22\},\{3,7,10,$ $25,28\},\{4,13,15,16,26\},$ $\{8,12,14,18,24\},\{11,17,$ $21,23,27\}$	$\overline{\{\mathcal{G}(2,1)\}}$, $\overline{\{\mathcal{G}(3,1)\}}$, $\overline{\{\mathcal{G}(4,1)\}}$, $\overline{\{\mathcal{G}(8,1)\}}$, $\overline{\{\mathcal{G}(11,1)\}}$	$\overline{\mathcal{F}},\overline{\{\mathcal{G}(2,1)\}}$, $\overline{\{\mathcal{G}(3,1)\}},\overline{\{\mathcal{G}(4,1)\}}$, $\overline{\{\mathcal{G}(8,1)\}},\overline{\{\mathcal{G}(11,1)\}}$
31	15	2	1	$\{18^*\},\{19^*\},\{1,2,3,4,5,$ $8,12,13,15,16,21,22,24,$ $25,29\}$	$\overline{\{\mathcal{G}(1,1)\}}$, $\overline{\{\mathcal{G}(18,1)\}}$, $\overline{\{\mathcal{G}(19,1)\}}$	$\overline{\mathcal{F}},\overline{\{\mathcal{G}(1,1)\}}$
37	19	2	-1	$\{3,7,8,11,13,14,16,18,$ $20,21,22,23,25,27,29,$ $30,32,35,36\}$	$\overline{\{\mathcal{G}(3,1)\}}$	$\overline{\mathcal{F}},\overline{\{\mathcal{G}(3,1)\}}$
41	5	8	1	$\{10^*\},\{37^*\},\{1,3,5,14,33\},$ $\{2,17,18,26,31\},\{4,16,21,$ $29,30\},\{8,11,20,32,38\},$ $\{12,19,22,23,34\},\{9,15,27,$ $36,39\},\{13,24,25,28,35\}$	$\overline{\{\mathcal{G}(1,1)\}}$, $\overline{\{\mathcal{G}(2,1)\}}$, $\overline{\{\mathcal{G}(4,1)\}}$, $\overline{\{\mathcal{G}(8,1)\}}$, $\overline{\{\mathcal{G}(9,1)\}}$, $\overline{\{\mathcal{G}(10,1)\}}$, $\overline{\{\mathcal{G}(12,1)\}}$, $\overline{\{\mathcal{G}(13,1)\}}$, $\overline{\{\mathcal{G}(37,1)\}}$	$\overline{\mathcal{F}},\overline{\{\mathcal{G}(1,1)\}}$, $\overline{\{\mathcal{G}(2,1)\}},\overline{\{\mathcal{G}(4,1)\}}$, $\overline{\{\mathcal{G}(8,1)\}},\overline{\{\mathcal{G}(9,1)\}}$, $\overline{\{\mathcal{G}(12,1)\}},\overline{\{\mathcal{G}(13,1)\}}$

表 2: $t=6,\ s=1$

参考文献

[1] M. Aoki and Y. Sakai, On divisibility of generalized Fibonacci numbers, Integers, vol.15, Paper No. A31 (2015).

[2] M. Aoki and Y. Sakai, On Equivalence Classes of Generalized Fibonacci sequences, Journal of Integer Sequences, volume19, Article 16.2.6 (2016).

[3] M. Aoki and Y. Sakai, Mod p Equivalence Classes of Recurrence Sequences of Degree Two, submitted.

[4] C. Ballot, Density of prime divisors of linear recurrences, Mem. Amer. Math. Soc. **115**, no. 551, 1995.

[5] A. Behera and G. K. Panda, On the square roots of triangular numbers, Fibonacci Quart. **37**, no. 2, 98–105, (1999).

[6] R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. Annals of Math., 15, 30-70 (1913).

[7] T. Koshy, Fibonacci and Lucas numbers with applications, Pure and Applied Mathematics, New York (2001).

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

[9] E. Lucas, Théorie des fonctions numériques simplement périodiques, Amer. J. Math., 1, 184-240 and 289-321 (1878).

[10] M. Kôzaki and T. Nakahara, On Arithmetric Properties of Generalized Fibonacci Sequences, Reports of the Faculty of Science and Engineering, Saga University Vol.28 no.1 p.1 -17 (1999).

[11] 中村 滋, フィボナッチ数の小宇宙, 日本評論社, 2002.

[12] A. Schinzel, Abelian binomials, power residues and exponential congruences. Acta Arith. 32, no. 3, 245–274 (1977).