MOD p EQUIVALENCE CLASSES OF LINEAR RECURRENCE SEQUENCES OF DEGREE TWO

MIHO AOKI AND YUHO SAKAI

ABSTRACT. Laxton introduced a group structure on the set of equivalence classes of linear recurrence sequences of degree two. This result yields much information on the divisibilities of such sequences. In this paper, we introduce other equivalence relations for the set of linear recurrence sequences (G_n) which are defined by $G_0, G_1 \in \mathbb{Z}$ and $G_n = TG_{n-1} - NG_{n-2}$ for fixed integers T and $N = \pm 1$. The relations are given by certain congruences modulo p for a fixed prime number p which are different from Laxton's without modulo p equivalence relations. We determine the initial terms G_0, G_1 of all the representatives of the equivalence classes $\overline{(G_n)}$ satisfying $p \nmid G_n$ for any integer n, and give the number of the equivalence classes. Furthermore, we determine the representatives of Laxton's without modulo p classes from our modulo p classes.

1. Introduction. Let $f(X) = X^2 - TX + N \in \mathbb{Z}[X],\ N = \pm 1$ be a polynomial whose roots θ_1 and θ_2 are not roots of unity. Then θ_1 and θ_2 are units of a certain real quadratic field. Let $d := T^2 - 4N$ be the discriminant of $f(X)$. We consider linear recurrence sequences $\mathcal{G} = (G_n)_{n\in\mathbb{Z}}$ defined by

$$G_0, G_1 \in \mathbb{Z}, \quad G_n = TG_{n-1} - NG_{n-2}. \tag{1.1}$$

If $G_0 = a, G_1 = b$, then we denote it by $\mathcal{G} = (G(a,b))$. We call $\mathcal{F} = (\mathcal{F}_n) = (G(0,1))$ and $\mathcal{L} = (\mathcal{L}_n) = (G(2,T))$ the Lucas sequence and the companion Lucas sequence, respectively. We fix a prime number p. It is well-known that the sequence $(G_n \bmod p)$ is periodic for any $\mathcal{G} = (G_n)$ defined by (1.1). Let $r(p)$ be the rank of the Lucas sequence $\mathcal{F} = (\mathcal{F}_n)$. Namely, it is the smallest positive integer n satisfying $p|\mathcal{F}_n$. We can easily check $r(2) = 2$ if T is even, and $r(2) = 3$ if T is odd. If $p \neq 2$, then E. Lucas ([**7,** §24, 25] or [**5,** Lemma 2, Theorem 12]) showed that $r(p)$ divides $p - \left(\frac{d}{p}\right)$ where $\left(\frac{*}{*}\right)$ is the Legendre symbol.

We define two relations $\underset{p}{\sim}$ and $\underset{p}{\sim}^*$ for the set of linear recurrence sequences.

Definition. Let $\mathcal{G} = (G_n)$ and $\mathcal{G}' = (G'_n)$ be linear recurrence sequences defined by (1.1).

(1) If the congruence $G_1G'_0 \equiv G'_1G_0 \pmod p$ holds, then we write $\mathcal{G} \underset{p}{\sim} \mathcal{G}'$.

(2) If there are some integers m and n satisfying $G_{m+1}G'_n \equiv G'_{n+1}G_m \pmod p$, then we write $\mathcal{G} \underset{p}{\sim}^* \mathcal{G}'$.

Define a set $\mathscr{X}_p(f)$ of linear recurrence sequences by

$$\mathscr{X}_p(f) := \{\mathcal{G} \mid \text{linear recurrence sequences defined by (1.1) with } p \nmid G_0 \text{ or } p \nmid G_1\}.$$

We can easily show that the first relation $\underset{p}{\sim}$ is an equivalence relation for the set $\mathscr{X}_p(f)$. Furthermore, we can show that the second relation $\underset{p}{\sim}^*$ is also an equivalence relation for the set $\mathscr{X}_p(f)$ (cf. [**2,** Lemma 9]) by using the following lemmas.

Lemma 1. *Let $\mathcal{G} = (G_n)$ and $\mathcal{G}' = (G'_n)$ be linear recurrence sequences defined by* (1.1). *If $G_{m+1}G'_n \equiv G'_{n+1}G_m \pmod p$, then we have the following congruences.*

$$G_{m+2}G'_{n+1} \equiv G'_{n+2}G_{m+1} \pmod p \quad \textit{and} \quad G_mG'_{n-1} \equiv G'_nG_{m-1} \pmod p.$$

1991 AMS *Mathematics subject classification.* 11B37, 11B39.
Keywords and phrases. linear recurrence sequences, the rank of appearance of Lucas sequences, the Laxton group.
Received by the editors October, 8, 2016.

Lemma 2. *Assume $\mathcal{G} = (G_n) \in \mathscr{X}_p(f)$. If $p|G_n$, then we have $p \nmid G_{n-1}$ and $p \nmid G_{n+1}$.*

These two lemmas follow from the recurrence formula in (1.1). Now, we consider the quotient sets using these relations. We put

$$X_p(f) := \mathscr{X}_p(f)/\underset{p}{\sim}, \qquad Y_p(f) := \{\overline{(G_n)} \in X_p(f) \mid p \nmid G_n \text{ for any } n \in \mathbb{Z}\},$$
$$X_p^*(f) := \mathscr{X}_p(f)/\underset{p}{\sim}^*, \qquad Y_p^*(f) := \{\overline{(G_n)} \in X_p^*(f) \mid p \nmid G_n \text{ for any } n \in \mathbb{Z}\},$$

where $\overline{(G_n)}$ is the equivalence class which includes (G_n). The sets Y_p and Y_p^* are well-defined, that is, we will show in §2, Lemma 4 that if $(G_n) \underset{p}{\sim} (G'_n)$ (or $(G_n)\underset{p}{\sim}^*(G'_n)$) and $p \nmid G_n$ for any $n \in \mathbb{Z}$, then we have $p \nmid G'_n$ for any $n \in \mathbb{Z}$. For any $\mathcal{G} = (G_n) \in \mathscr{X}_p(f)$ satisfying $p|G_\nu$ for some $\nu \in \mathbb{Z}$, we have $\mathcal{F}_1 G_\nu \equiv 0 \equiv G_{\nu+1}\mathcal{F}_0 \pmod p$. Therefore, we have $\mathcal{G}\underset{p}{\sim}^*\mathcal{F} = (G(0,1))$ (the Lucas sequence) and get the following lemma.

Lemma 3. *We have $X_p(f) = \{\overline{(G(a,1))} \mid a = 0, \dots, p-1\} \cup \{\overline{(G(1,0))}\}$ and $X_p^*(f) = \overline{\mathcal{F}} \cup Y_p^*(f)$.*

For any integer G that is not divisible by p, we denote an inverse element modulo p by G^{-1} $(\in \mathbb{Z})$ (i.e., $GG^{-1} \equiv 1 \pmod p$).

Definition. Assume $\mathcal{G} = (G_n) \in \mathscr{X}_p(f)$. We define the sequence $(g_n)_{n\in\mathbb{Z}}$ $(0 \le g_n \le p-1$ or $g_n = \infty)$ by

$$g_n \begin{cases} \equiv G_n G_{n+1}^{-1} \pmod p & \text{if } p \nmid G_{n+1}, \\ = \infty & \text{otherwise.} \end{cases}$$

We call the sequence (g_n) the second sequence of $\mathcal{G}$. In particular, we denote the second sequence of the Lucas sequence $\mathcal{F}$ by $(\mathfrak{f}_n)$.

We will show in §2, the second sequences (g_n) have the periods which divide $r(p)$ (Proposition 1). In §3, we will show the following theorems by using Proposition 1. These theorems are generalizations of our previous results in the case $T = 1, N = -1$ ([**1**], [**2**]).

Theorem 1. *We have*

$$Y_p(f) = \{\overline{(G(a,1))} \mid 1 \le a \le p-1, a \ne \mathfrak{f}_1, \cdots, \mathfrak{f}_{r(p)-2}\}$$

and

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

Theorem 2. *Assume $p \ne 2$ and put $s(p) := \dfrac{p - (\frac{d}{p})}{r(p)}$. There exist integers α_i $(i = 1, \dots, s(p) + (d/p),\ 1 \le \alpha_i \le p-1)$ satisfying the following conditions.*

1. *For the sequence $(G_n) = (G(\alpha_i, 1))$, we have $p \nmid G_n$ for any $n \in \mathbb{Z}$.*
2. *Let $\mathcal{A}_i$ be the second sequence of $(G(\alpha_i, 1))$. Then we have*

$$\{a \in \mathbb{Z} \mid 1 \le a \le p-1,\ a \ne \mathfrak{f}_1, \cdots, \mathfrak{f}_{r(p)-2}\} = \coprod_{i=1}^{s(p)+(d/p)} \mathcal{A}_i \qquad (\textit{disjoint union}).$$

Theorem 3. *Assume $p \neq 2$. Let α_i $(i = 1, \dots, s(p) + (d/p))$ be the integers in Theorem 2. We have*

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

and

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

In the case $p = 2$, we have

$$X_2(f) = \{\overline{(G(0,1))}(= \overline{\mathcal{F}}), \overline{(G(1,1))}, \overline{(G(1,0))}\}, \qquad Y_2(f) = \begin{cases} \emptyset & \text{if } T \text{ is odd },\\ \overline{(G(1,1))} & \text{otherwise }, \end{cases}$$

$$X_2^*(f) = \begin{cases} \overline{(G(0,1))} & \text{if } T \text{ is odd },\\ \overline{(G(0,1))}, \overline{(G(1,1))} & \text{otherwise }, \end{cases} \qquad Y_2^*(f) = \begin{cases} \emptyset & \text{if } T \text{ is odd },\\ \overline{(G(1,1))} & \text{otherwise }. \end{cases}$$

In §4, we will explain the relation between our "modulo p" equivalence classes and Laxton's "without modulo p" equivalence classes **[6]**. He introduced a commutative group structure on certain sets of equivalence classes $G(f)$ and $G^*(f)$. We will show that the certain subsets of $X_p(f)$ and $X_p^*(f)$ have the same group structures and isomorphic to finite quotient groups of $G(f)$ and $G^*(f)$ (Theorem 4). From these facts, by using our theorems, we can give the representatives of Laxton's quotient groups. In §5, we give some examples.

2. Mod p Equivalence Classes.

Lemma 4. *Assume $\mathcal{G} = (G_n), \mathcal{G}' = (G'_n) \in \mathscr{X}_p(f)$. If $\mathcal{G} \underset{p}{\sim} \mathcal{G}'$ (or $\mathcal{G} \underset{p}{\sim}^* \mathcal{G}'$) and $p \nmid G_n$ for any $n \in \mathbb{Z}$. Then we have $p \nmid G'_n$ for any $n \in \mathbb{Z}$.*

Proof. If $\mathcal{G} \underset{p}{\sim} \mathcal{G}'$, then we have $G_1 G'_0 \equiv G'_1 G_0 \pmod p$. Assume that there exists an integer ℓ such that $p \mid G'_\ell$. Using Lemma 1, we have $G_{\ell+1} G'_\ell \equiv G'_{\ell+1} G_\ell \pmod p$. Since p divides G'_ℓ and does not divide $G'_{\ell+1}$ by Lemma 2, we get $p \mid G_\ell$. This contradicts the assumption. We can show similarly the assertion for the case $\mathcal{G} \underset{p}{\sim}^* \mathcal{G}'$. □

From the above lemma, we know that the set Y_p and Y_p^* in §1 are well-defined. Next, we will show that any second sequence has the period dividing $r(p)$. Let $\mathcal{G} = (G_n)$ be a linear recurrence sequence defined by (1.1). Then we have

$$G_n = \frac{(G_1 - G_0\theta_1)\theta_2^n - (G_1 - G_0\theta_2)\theta_1^n}{\theta_2 - \theta_1} \qquad (n \in \mathbb{Z}). \tag{2.1}$$

Put

$$\Lambda(\mathcal{G}) := (G_1 - G_0\theta_1)(G_1 - G_0\theta_2) = G_1^2 - TG_0G_1 + NG_0^2.$$

From (2.1), we can show the following lemma.

Lemma 5. *Let $\mathcal{G} = (G_n)$ be a linear recurrence sequence defined by (1.1). For any $n, m \in \mathbb{Z}$, we have*

$$G_{n+m} = \mathcal{F}_m G_{n+1} - N\mathcal{F}_{m-1} G_n.$$

Proof. Put $B = G_1 - G_0\theta_1$ and $A = G_1 - G_0\theta_2$. Then, we have

$$\begin{aligned}
&\mathcal{F}_m G_{n+1} - N\mathcal{F}_{m-1}G_n \\
&= \frac{(\theta_2^m - \theta_1^m)(B\theta_2^{n+1} - A\theta_1^{n+1}) - N(\theta_2^{m-1} - \theta_1^{m-1})(B\theta_2^n - A\theta_1^n)}{(\theta_2 - \theta_1)^2} \\
&= \frac{1}{(\theta_2 - \theta_1)^2}\big(B(\theta_2^{m+n+1} - N\theta_2^{m+n-1}) + A(-\theta_1^{n+1}\theta_2^m + N\theta_1^n\theta_2^{m-1}) \\
&\qquad + B(-\theta_1^m\theta_2^{n+1} + N\theta_1^{m-1}\theta_2^n) + A(\theta_1^{m+n+1} - N\theta_1^{m+n-1})\big).
\end{aligned}$$

Since $N = \theta_1\theta_2$, we have $A(-\theta_1^{n+1}\theta_2^m + N\theta_1^n\theta_2^{m-1}) = 0$. In the same way, we get $B(-\theta_1^m\theta_2^{n+1} + N\theta_1^{m-1}\theta_2^n) = 0$. Furthermore, the equalities $B(\theta_2^{m+n+1} - N\theta_2^{m+n-1}) = B\theta_2^{m+n}(\theta_2 - N\theta_2^{-1}) = B\theta_2^{m+n}(\theta_2 - \theta_1)$ and $A(\theta_1^{m+n+1} - N\theta_1^{m+n-1}) = A\theta_1^{m+n}(\theta_1 - N\theta_1^{-1}) = A\theta_1^{m+n}(\theta_1 - \theta_2)$ hold. Therefore, we have

$$\begin{aligned}
\mathcal{F}_m G_{n+1} - N\mathcal{F}_{m-1}G_n &= \frac{B\theta_2^{m+n}(\theta_2 - \theta_1) + A\theta_1^{m+n}(\theta_1 - \theta_2)}{(\theta_2 - \theta_1)^2} \\
&= \frac{B\theta_2^{m+n} - A\theta_1^{m+n}}{\theta_2 - \theta_1} \\
&= G_{m+n}.
\end{aligned}$$

□

We can show the following lemma by induction on n.

Lemma 6. *Let $\mathcal{G} = (G_n)$ be a linear recurrence sequence defined by (1.1). For any $n \in \mathbb{Z}$, we have*

$$G_n^2 - TG_{n-1}G_n + NG_{n-1}^2 = N(G_{n+1}^2 - TG_nG_{n+1} + NG_n^2).$$

Assume that $\mathcal{G} = (G_n) \in \mathscr{X}_p(f)$ satisfies $p|G_\nu$ for some $\nu \in \mathbb{Z}$. Since the sequence $(G_n \bmod p)$ is periodic, there exists the integer $r(\mathcal{G}, p)$ such that $p|G_n$ if and only if $r(\mathcal{G}, p)|n - \nu$. We have the following lemma easily.

Lemma 7. *Let $\mathcal{G} = (G_n) \in \mathscr{X}_p(f)$ which satisfies $p|G_\nu$ for some $\nu \in \mathbb{Z}$. Then we have $r(\mathcal{G}, p) = r(p)$.*

Lemma 8. *Let $\mathcal{G} = (G_n) \in \mathscr{X}_p(f)$ and assume that $\Lambda(\mathcal{G}) \equiv 0 \pmod p$. Then we have $p \nmid G_n$ for any $n \in \mathbb{Z}$.*

Proof. The assertion follows from the fact that $p \nmid G_0$ or $p \nmid G_1$ and Lemma 2, Lemma 6. □

The next proposition asserts that the second sequences (g_n) have the periods which divide $r(p)$.

Proposition 1. *Let $\mathcal{G} = (G_n) \in \mathscr{X}_p(f)$ and (g_n) be the second sequence of $\mathcal{G}$.*

(1) *If $\Lambda(\mathcal{G}) \not\equiv 0 \pmod p$, then we have $g_m = g_n$ if and only if $m \equiv n \pmod{r(p)}$.*
(2) *If $\Lambda(\mathcal{G}) \equiv 0 \pmod p$, then we have $g_n = g_0$ for any $n \in \mathbb{Z}$.*

Proof. (1) We will show the assertion for two cases. First, we assume that $p \nmid G_n$ for any $n \in \mathbb{Z}$. By the definition of the second sequence, we have $g_n = g_m$ if and only if $G_mG_{n+1} \equiv G_{m+1}G_n \pmod p$. Since $G_{n+1} = \mathcal{F}_{n-m+1}G_{m+1} - N\mathcal{F}_{n-m}G_m$ and $G_n = \mathcal{F}_{n-m}G_{m+1} - N\mathcal{F}_{n-m-1}G_m$ from Lemma 5, we have $g_m = g_n$ if and only if

$$G_{m+1}^2\mathcal{F}_{n-m} - G_mG_{m+1}(\mathcal{F}_{n-m+1} + N\mathcal{F}_{n-m-1}) + NG_m^2\mathcal{F}_{n-m} \equiv 0 \pmod p. \tag{2.2}$$

By the recurrence formula (1.1) and Lemma 6, we have

$$\begin{aligned}&G_{m+1}^2\mathcal{F}_{n-m}-G_mG_{m+1}(\mathcal{F}_{n-m+1}+N\mathcal{F}_{n-m-1})+NG_m^2\mathcal{F}_{n-m}\\ &\equiv \mathcal{F}_{n-m}(G_{m+1}^2-TG_mG_{m+1}+NG_m^2)\\ &\equiv \mathcal{F}_{n-m}N^m\Lambda(\mathcal{G}) \pmod p.\end{aligned}$$

By the assumption $\Lambda(\mathcal{G})\not\equiv 0 \pmod p$, we conclude that $g_m\equiv g_n$ if and only if $m\equiv n \pmod{r(p)}$. We get the proof of the case.

Secondly, we consider the case that $p|G_\nu$ for some $\nu\in\mathbb{Z}$. We assume that $g_m=\infty$ (that is, $p|G_{m+1}$). Then we have $g_n=\infty$ if and only if $m\equiv n \pmod{r(\mathcal{G},p)}$. From now on, we assume that $g_m\neq\infty$ (that is, $p\nmid G_{m+1}$). We consider two subsequences of $(G_n \bmod p)$:

$$\begin{aligned}&G_{m+1},\, G_m\equiv g_mG_{m+1},\, G_{m-1}\equiv(Tg_m-1)NG_{m+1},\, G_{m-2}\equiv(T^2g_m-T-g_m)N^2G_{m+1},\,\cdots\\ &G_{n+1},\ G_n\equiv g_nG_{n+1},\quad G_{n-1}\equiv(Tg_n-1)NG_{n+1},\quad G_{n-2}\equiv(T^2g_n-T-g_n)N^2G_{n+1},\quad\cdots\end{aligned}\tag{2.3}$$

Assume that $g_m=g_n$. Since $g_n\neq\infty$, we have $p\nmid G_{n+1}$. Therefore, from (2.3), we have $G_{m-k}\equiv 0 \pmod p$ if and only if $G_{n-k}\equiv 0 \pmod p$. We conclude that $m\equiv n \pmod{r(\mathcal{G},p)}$.

Conversely, we assume that $m\equiv n \pmod{r(\mathcal{G},p)}$. Since $p\nmid G_{m+1}$, we have $p\nmid G_{n+1}$. Let $\mathcal{I}=(I_n)$ and $\mathcal{J}=(J_n)$ be the linear recurrence sequences defined by (1.1) with $I_0=g_m$, $J_0=g_n$ and $I_1=J_1=1$. We can denote the above two subsequences (2.3) by

$$\begin{aligned}&I_1G_{m+1},\, G_m\equiv I_0G_{m+1},\, G_{m-1}\equiv I_{-1}G_{m+1},\, G_{m-2}\equiv I_{-2}G_{m+1},\,\cdots\\ &J_1G_{n+1},\ G_n\equiv J_0G_{n+1},\ G_{n-1}\equiv J_{-1}G_{n+1},\ G_{n-2}\equiv J_{-2}G_{n+1},\ \cdots\end{aligned}\tag{2.4}$$

For an integer $k\geq 0$, by the assumption $m\equiv n \pmod{r(\mathcal{G},p)}$, we have $p|G_{m-k}$ if and only if $p|G_{n-k}$. Hence the subsequences (2.4) imply $p|I_{-k}$ if and only if $p|J_{-k}$. By Lemma 5, we have

$$I_{-k}=\mathcal{F}_{-k}I_1-N\mathcal{F}_{-k-1}I_0\equiv\mathcal{F}_{-k}-N\mathcal{F}_{-k-1}g_m \pmod p$$

and

$$J_{-k}=\mathcal{F}_{-k}J_1-N\mathcal{F}_{-k-1}J_0\equiv\mathcal{F}_{-k}-N\mathcal{F}_{-k-1}g_n \pmod p.$$

Hence we get

$$\mathcal{F}_{-k-1}g_m\equiv\mathcal{F}_{-k-1}g_n \pmod p\tag{2.5}$$

for any integer $k\geq 0$ such that $I_{-k}\equiv J_{-k}\equiv 0 \pmod p$. Let ν be an integer satisfying $p|G_\nu$. Since $G_{m-k}\equiv I_{-k}G_{m+1}\equiv 0 \pmod p$, we have $m-k\equiv\nu \pmod{r(\mathcal{G},p)}$. On the other hand, we know that $m+1\not\equiv\nu \pmod{r(\mathcal{G},p)}$ since $p\nmid G_{m+1}$. Therefore, we get $k\not\equiv -1 \pmod{r(\mathcal{G},p)}$, and hence $k\not\equiv -1 \pmod{r(p)}$ since $r(\mathcal{G},p)=r(p)$. The congruence (2.5) implies $g_m\equiv g_n \pmod p$, and hence $g_m=g_n$ since $0\leq g_m,g_n\leq p-1$. By using lemma 7, we can prove the case.

(2) In this case, we have $p\nmid G_n$ for any $n\in\mathbb{Z}$ from Lemma 8. Due to the periodicity of $(G_n \bmod p)$, it is sufficient to consider $n\geq 0$. First, we will show that $g_1\equiv g_0 \pmod p$. We have

$$\begin{aligned}g_1&\equiv G_1G_2^{-1}\\ &\equiv G_1(TG_1-NG_0)^{-1}\\ &\equiv (T-NG_0G_1^{-1})^{-1}\\ &\equiv (T-Ng_0)^{-1} \pmod p.\end{aligned}$$

On the other hand, since $\Lambda(\mathcal{G}) \equiv 0 \pmod{p}$, we have

$$\begin{aligned}0 &\equiv G_1^2 - TG_1G_0 + NG_0^2 \\ &\equiv G_1^2(1 - TG_0G_1^{-1} + NG_0^2G_1^{-2}) \\ &\equiv G_1^2(1 - Tg_0 + Ng_0^2) \pmod{p},\end{aligned}$$

and hence $g_0 \equiv (T - Ng_0)^{-1} \pmod{p}$. We get $g_1 \equiv g_0 \pmod{p}$. Next, we assume that $g_k = g_0$ holds for any positive integers k less than $n+1$. Then we have

$$\begin{aligned}g_{n+1} &\equiv G_{n+1}G_{n+2}^{-1} \\ &\equiv (TG_n - NG_{n-1})(TG_{n+1} - NG_n)^{-1} \\ &\equiv (T - NG_{n-1}G_n^{-1})(TG_{n+1}G_n^{-1} - N)^{-1} \\ &\equiv (T - Ng_{n-1})(Tg_n^{-1} - N)^{-1} \\ &\equiv (T - Ng_0)(Tg_0^{-1} - N)^{-1} \\ &\equiv g_0 \pmod{p}.\end{aligned}$$

Since $1 \leq g_0, g_{n+1} \leq p-1$, we have $g_{n+1} = g_0$. □

Definition. Let $\mathcal{G} \in \mathscr{X}_p(f)$ and (g_n) be the second sequence of $\mathcal{G}$. We call the period $\overline{r}(\mathcal{G})$ of (g_n) the second period of $\mathcal{G}$.

By Proposition 1, we have the following corollary.

Corollary 1. *For $\mathcal{G} \in \mathscr{X}_p(f)$, let $\overline{r}(\mathcal{G})$ be the second period of $\mathcal{G}$. Then we have*

$$\overline{r}(\mathcal{G}) = \begin{cases} r(p) & \text{if } \Lambda(\mathcal{G}) \not\equiv 0 \pmod{p}, \\ 1 & \text{if } \Lambda(\mathcal{G}) \equiv 0 \pmod{p}. \end{cases}$$

3. Proofs of theorems. In this section, we prove theorems in §1. First, the following lemma follows from Lemma 5.

Lemma 9. *Let $\mathcal{G} = (G_n) \in \mathscr{X}_p(f)$ with $p \nmid G_0, G_1$. We have $p|G_n$ for some $n \in \mathbb{Z}$ if and only if $NG_1G_0^{-1} \equiv \mathfrak{f}_m \pmod{p}$ for some $m \in \mathbb{Z}$ satisfying $1 \leq m \leq r(p) - 2$.*

We put

$$X_p'(f) := \{\overline{(G_n)} \in X_p(f) \mid p \nmid G_0, G_1\}.$$

This set is well-defined, that is, if $(G_n) \underset{p}{\sim} (G_n')$ and $p \nmid G_0, G_1$, then we have $p \nmid G_0', G_1'$. Clearly, $Y_p(f) \subset X_p'(f) \subset X_p(f)$ and

$$X_p'(f) = \{\overline{(G(a,1))} \mid a = 1, \ldots, p-1\}.$$

Proof of Theorem 1. By Lemma 5, we have

$$0 \equiv \mathcal{F}_{r(p)} = \mathcal{F}_{n+(r(p)-n)} = \mathcal{F}_{r(p)-n}\mathcal{F}_{n+1} - N\mathcal{F}_{r(p)-n-1}\mathcal{F}_n \pmod{p}.$$

Therefore, we have $\mathfrak{f}_n \equiv N\mathfrak{f}_{r(p)-n-1}^{-1} \pmod{p}$. From this congruence and Lemma 9, we have

$$\begin{aligned}&\{\overline{(G_n)} \in X'_p(f) \mid p|G_n \text{ for some } n \in \mathbb{Z}\}\\ =&\{\overline{(G(a,1))} \mid 1 \le a \le p-1,\ Na^{-1} \equiv \mathfrak{f}_n \pmod{p} \text{ for some } n\ (1 \le n \le r(p)-2)\}\\ =&\{\overline{(G(a,1))} \mid 1 \le a \le p-1,\ a \equiv \mathfrak{f}_{r(p)-n-1} \pmod{p} \text{ for some } n\ (1 \le n \le r(p)-2)\}\\ =&\{\overline{(G(a,1))} \mid a = \mathfrak{f}_1, \dots, \mathfrak{f}_{r(p)-2}\}\end{aligned}$$

Hence we conclude that

$$Y_p(f) = X'_p(f) - \{\overline{(G(a,1))} \mid a = \mathfrak{f}_1, \dots, \mathfrak{f}_{r(p)-2}\} = \{\overline{(G(a,1))} \mid 1 \le a \le p-1, a \ne \mathfrak{f}_1, \dots, \mathfrak{f}_{r(p)-2}\}.$$

The equality $|Y_p(f)| = p + 1 - r(p)$ follows from the first assertion and Proposition 1. □

Next, we will give the proof of Theorem 2. We get the following lemma by the definition of the Legendre symbol.

Lemma 10. *Let $f(X) = X^2 - TX + N \in \mathbb{Z}[X]$, and $d = T^2 - 4N$. For any prime number p $(\ne 2)$, we have*

$$|\{\beta \in \mathbb{Z} \mid 1 \le \beta \le p-1, f(\beta^{-1}) \equiv 0 \pmod{p}\}| = \left(\frac{d}{p}\right) + 1.$$

Lemma 11. *Let $\mathcal{G} = (G_n), \mathcal{G}' = (G'_n) \in \mathscr{X}_p(f)$, and $(g_n), (g'_n)$ be the second sequences respectively. Assume that $p \nmid G_n, G'_n$ for any $n \in \mathbb{Z}$, and let $\overline{r}(\mathcal{G})$ be the second period of $\mathcal{G}$. Then we have $\mathcal{G} \underset{p}{\sim}^* \mathcal{G}'$ if and only if $g'_0 = g_n$ for some $n \in \mathbb{Z}$ satisfying $1 \le n \le \overline{r}(\mathcal{G})$.*

Proof. By the definition of the second sequence, the equality $g'_0 = g_n$ for some $n \in \mathbb{Z}$ implies $\mathcal{G} \underset{p}{\sim}^* \mathcal{G}'$. Conversely, if $\mathcal{G} \underset{p}{\sim}^* \mathcal{G}'$, then there exist integers m and n such that $G_{m+1}G'_n \equiv G'_{n+1}G_m \pmod{p}$. By Lemma 1, we have $G_{m-n+1}G'_0 \equiv G'_1 G_{m-n} \pmod{p}$. Therefore, we have $g'_0 \equiv g_{m-n} \pmod{p}$ and hence $g'_0 = g_{m-n}$. Since the second period of $\mathcal{G}$ is $\overline{r}(\mathcal{G})$, there exists an integer ℓ satisfying $g'_0 = g_\ell$ and $1 \le \ell \le \overline{r}(\mathcal{G})$. □

Proof of Theorem 2. Let α be an integer such that $1 \le \alpha \le p-1$ and $\alpha \ne \mathfrak{f}_1, \dots, \mathfrak{f}_{r(p)-2}$. We consider the linear recurrence sequence $\mathcal{G} = (G_n) = (G(\alpha, 1))$ and its second sequence $\mathcal{A} = (g_n)$. Assume that $\mathcal{G} \underset{p}{\sim}^* \mathcal{F}$. Then by Lemma 1, there exists an integer n such that $\mathcal{F}_n \equiv G_1 \mathcal{F}_n \equiv \mathcal{F}_{n+1} G_0 \equiv \mathcal{F}_{n+1}\alpha \pmod{p}$. Since $p \nmid \alpha$, we have $n \not\equiv -1, 0 \pmod{r(p)}$, hence the congruence implies $\alpha = g_0 = \mathfrak{f}_m$ for some $m \in \mathbb{Z}$ satisfying $1 \le m \le r(p) - 2$. This is a contradiction. We conclude that $\mathcal{G} \underset{p}{\not\sim}^* \mathcal{F}$ and hence $p \nmid G_n$ for any $n \in \mathbb{Z}$ from Lemma 3.

Now, we choose another integer α' satisfying $1 \le \alpha' \le p-1$, $\alpha' \ne \mathfrak{f}_1, \dots, \mathfrak{f}_{r(p)-2}$ and $\alpha' \notin \mathcal{A} = (g_n)$. For $\mathcal{G}' = (G'_n) = (G(\alpha', 1))$, and its second sequence $\mathcal{A}' = (g'_n)$, if $g_n = g'_m$ for some $n, m \in \mathbb{Z}$ then we have $\alpha' = g'_0 = g_{n-m}$ from Lemma 1. This contradicts the assumption $\alpha' \notin \mathcal{A} = (g_n)$. Hence we have $\mathcal{A} \cap \mathcal{A}' = \emptyset$. By continuing this procedure, we can choose integers α_i $(i = 1, \dots, s)$ satisfying

$$\{a \in \mathbb{Z} \mid 1 \le a \le p-1,\ a \ne \mathfrak{f}_1, \cdots, \mathfrak{f}_{r(p)-2}\} = \coprod_{i=1}^{s} \mathcal{A}_i \qquad \text{(disjoint union)}. \tag{3.1}$$

where $\mathcal{A}_i$ is the second sequence of $(G(\alpha_i, 1))$. Finally, we will prove that

$$s = s(p) + \left(\frac{d}{p}\right) = \frac{p - (\frac{d}{p})}{r(p)} + \left(\frac{d}{p}\right).$$

If β^{-1} $(1 \leq \beta \leq p-1)$ be a solution of $f(X) = X^2 - TX + N \equiv 0 \pmod{p}$, then the sequence $\mathcal{G} = (g_n) = (G(\beta, 1))$ satisfies $\Lambda(\mathcal{G}) \equiv 0 \pmod{p}$. On the other hand, for the sequence $\mathcal{G}' = (g'_n) = (G(f_i, 1))$ $(i = 1, \ldots, r(p)-2)$, we have $\Lambda(\mathcal{G}') = \pm F_{i+1}^{-2}\Lambda(\mathcal{F}) \not\equiv 0 \pmod{p}$ from Lemma 6. Hence we conclude that $\beta \neq \mathfrak{f}_1, \ldots, \mathfrak{f}_{r(p)-2}$. The cardinality of the second sequence of $(G(\beta, 1))$ is 1 from Proposition 1. On the other hand, for any integer α sucn that $1 \leq \alpha \leq p-1$, $\alpha \neq \mathfrak{f}_1, \ldots, \mathfrak{f}_{r(p)-2}$ and $f(\alpha^{-1}) \not\equiv 0 \pmod{p}$, the cardinality of the second sequence of $(G(\alpha, 1))$ is $r(p)$. Then the equality (3.1) and Lemma 10 yields

$$(p-1) - (r(p)-2) = \left(\frac{d}{p}\right) + 1 + \left\{s - \left(\left(\frac{d}{p}\right) + 1\right)\right\} r(p).$$

From this equality, we get

$$s = \frac{p - (\frac{d}{p})}{r(p)} + \left(\frac{d}{p}\right) \quad \left(= s(p) + \left(\frac{d}{p}\right)\right).$$

□

Finally, we will give the proof of Theorem 3.

Proof of Theorem 3. Let $\overline{\mathcal{G}} = \overline{(G(a,1))}$, $\overline{\mathcal{G}'} = \overline{(G(a',1))} \in Y_p(f)$ $(1 \leq a, a' \leq p-1,\ a, a' \neq \mathfrak{f}_1, \cdots, \mathfrak{f}_{r(p)-2})$, and $\mathcal{A}$ be the second sequence of $\mathcal{G}$. By Lemma 11, we have $\mathcal{G} \underset{p}{\sim}^* \mathcal{G}'$ if and only if $a' \in \mathcal{A}$. By Theorem 2 and its proof, since the set $\{\alpha_i \mid i = 1, \ldots, s(p) + (d/p)\}$ is the representatives of $\mathcal{A}_i$ $(i = 1, \ldots, s(p) + (d/p))$, we get the first assertion of the theorem. The equality $|Y_p^*(f)| = s(p) + (d/p)$ follows from the first assertion. □

4. Relation to Laxton's Equivalence Classes. In this section, we will explain the relation between our modulo p equivalence classes and Laxton's one [**6**]. We also recommend the book [**3**] written by Ballot. We consider two relations $\sim$ and $\sim^*$ (without modulo p). Let $\mathcal{G} = (G_n)$ and $\mathcal{G}' = (G'_n)$ be linear recurrence sequences defined by (1.1).

Definition. (1) If there are some non-zero integers λ and μ satisfying $\lambda G_n = \mu G'_n$ for any $n \in \mathbb{Z}$, then we write $\mathcal{G} \sim \mathcal{G}'$.
(2) If there are some non-zero integers λ, μ and an integer ν satisfying $\lambda G_{n+\nu} = \mu G'_n$ for any $n \in \mathbb{Z}$, then we write $\mathcal{G} \sim^* \mathcal{G}'$.

These two relations are equivalence relations for the set

$$F(f) := \{\mathcal{G} \mid \text{linear recurrence sequences defined by (1.1) with } G_0 \neq 0 \text{ or } G_1 \neq 0\}.$$

Note that the assumption $G_0 \neq 0$ or $G_1 \neq 0$ is equivalent to $\Lambda(\mathcal{G}) \neq 0$ by our assumptions of $f(X)$. Consider the quotient sets using the relations.

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

Laxton introduced a commutative group structure on $G^*(f)$. For any $\mathcal{G} = (G_n), \mathcal{H} = (H_n) \in F(f)$, with

$$G_n := \frac{B\theta_2^n - A\theta_1^n}{\theta_2 - \theta_1}, \qquad H_n := \frac{D\theta_2^n - C\theta_1^n}{\theta_2 - \theta_1},$$

where $B = G_1 - G_0\theta_1$, $A = G_1 - G_0\theta_2$, $D = H_1 - H_0\theta_1$ and $C = H_1 - H_0\theta_2$, he defined the product $\mathcal{G} \times \mathcal{H} = \mathcal{W} = (W_n) \in F(f)$ by

$$W_n = \frac{BD\theta_2^n - AC\theta_1^n}{\theta_2 - \theta_1} \quad (n \in \mathbb{Z}). \tag{4.1}$$

He showed that this product yields commutative group structures on $G^*(f)$ with the identity $\overline{\mathcal{F}}$ (the class of Lucas sequence). Namely, for $\overline{\mathcal{G}}, \overline{\mathcal{H}} \in G^*(f)$ their product is given by $\overline{\mathcal{W}}$. We consider not only $G^*(f)$ but also $G(f)$ to correspond to our set $X_p(f)$. Put

$$\begin{aligned} I(f,p) &:= \{\mathfrak{G} \in G(f) \mid \Lambda(\mathcal{G}) \not\equiv 0 \pmod p \text{ for some } \mathcal{G} \in \mathfrak{G}\}, \\ I^*(f,p) &:= \{\mathfrak{G} \in G^*(f) \mid \Lambda(\mathcal{G}) \not\equiv 0 \pmod p \text{ for some } \mathcal{G} \in \mathfrak{G}\}, \\ G(f,p) &:= \{\mathfrak{G} \in G(f) \mid p|G_0 \text{ for all } \mathcal{G} = (G_n) \in \mathfrak{G}\}, \\ G^*(f,p) &:= \{\mathfrak{G} \in G^*(f) \mid p|G_n \text{ for all } \mathcal{G} = (G_n) \in \mathfrak{G} \text{ and some } n \in \mathbb{Z}\}. \end{aligned}$$

The sets $I(f,p)$ and $G(f,p)$ (resp. $I^*(f,p)$ and $G^*(f,p)$) are subgroups of $G(f)$ (resp. $G^*(f)$) [**6,** Lemma 2.3 and Proposition 3.1].

For the exact sequence of groups

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

if $p \neq 2$, then Laxton [**6,** Theorem 3.7] showed the following.

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

and

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

where $s(p) = \dfrac{p-(d/p)}{r(p)}$. On the other hand, let $\mathscr{X}_p(f)$ be the set in §1. For any $\mathcal{G} = (G_n), \mathcal{H} = (H_n) \in \mathscr{X}_p(f)$, the product $\mathcal{W} = \mathcal{G} \times \mathcal{H}$ (4.1) is not always in $\mathscr{X}_p(f)$ (for example, in the case $1 + N - T \equiv 0 \pmod p$, if $G_0 \equiv G_1 \not\equiv 0 \pmod p$ and $H_1 \equiv NH_0 \not\equiv 0 \pmod p$, then we have $\mathcal{G} = (G_n), \mathcal{H} = (H_n) \in \mathscr{X}_p(f)$ but the product sequence $\mathcal{W} = (W_n) \notin \mathscr{X}_p(f)$ since $W_0 \equiv W_1 \equiv 0 \pmod p$ (see [**3,** p15 (2.6)]). However, we will prove that certain subsets $Z_p(f)$ and $Z_p^*(f)$ of $X_p(f)$ and $X_p^*(f)$ respectively have group structures defined by (4.1).

Lemma 12. *Let $\mathcal{G} = (G_n), \mathcal{G}' = (G'_n) \in \mathscr{X}_p(f)$ and assume that $\Lambda(\mathcal{G}) \not\equiv 0 \pmod p$.*

1. *If $\mathcal{G} \underset{p}{\sim} \mathcal{G}'$, then we have $\Lambda(\mathcal{G}') \not\equiv 0 \pmod p$.*
2. *If $\mathcal{G} \underset{p}{\sim}^* \mathcal{G}'$, then we have $\Lambda(\mathcal{G}') \not\equiv 0 \pmod p$.*

Proof. We only give the proof for (2). Since $\mathcal{G} \underset{p}{\sim}^* \mathcal{G}'$, there exist integers m and n satisfying $G_{m+1}G'_n \equiv G'_{n+1}G_m \pmod p$. If $p|G'_n$ or $p|G'_{n+1}$, then we have $\Lambda(\mathcal{G}') \not\equiv 0 \pmod p$ from Lemma 8. If $p \nmid G'_n, G'_{n+1}$, then we have $p \nmid G_m, G_{m+1}$. By Lemma 6 and the congruence $G_{m+1}G'_n \equiv G'_{n+1}G_m \pmod p$, we have $\Lambda(\mathcal{G}') \equiv \pm G'^2_{n+1} G^{-2}_{m+1} \Lambda(\mathcal{G}) \not\equiv 0 \pmod p$. □

From Lemma 12, the following sets

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

are well-defined. The next lemmas show that the product (4.1) on $Z_p(f), Z_p^*(f)$ are well-defined.

Lemma 13. *Let $\mathcal{G} = (G_n), \mathcal{H} = (H_n) \in \mathscr{X}_p(f)$. For fixed integer ν, let $\mathcal{Z} = (Z_n) \in \mathscr{X}_p(f)$ be the sequence defined by $Z_n = H_{n+\nu}$ $(n \in \mathbb{Z})$. Then we have $\mathcal{G} \times \mathcal{H} \underset{p}{\sim}^* \mathcal{G} \times \mathcal{Z}$.*

Proof. Put

$$G_n = \frac{B\theta_2^n - A\theta_1^n}{\theta_2 - \theta_1}, \qquad H_n = \frac{D\theta_2^n - C\theta_1^n}{\theta_2 - \theta_1}, \qquad Z_n = \frac{E\theta_2^n - F\theta_1^n}{\theta_2 - \theta_1},$$

then we have $E = D\theta_2^\nu, F = C\theta_1^\nu$. Hence the nth term of $\mathcal{G} \times \mathcal{Z}$ is the $(n+\nu)$th term of $\mathcal{G} \times \mathcal{H}$, and we get $\mathcal{G} \times \mathcal{H} \underset{p}{\sim}^* \mathcal{G} \times \mathcal{Z}$. □

Lemma 14. *Let $\mathcal{G} = (G_n), \mathcal{G}' = (G'_n), \mathcal{H} = (H_n), \mathcal{H}' = (H'_n) \in \mathscr{X}_p(f)$.*

1. *If $\mathcal{G} \underset{p}{\sim} \mathcal{G}'$ and $\mathcal{H} \underset{p}{\sim} \mathcal{H}'$, then we have $\mathcal{G} \times \mathcal{H} \underset{p}{\sim} \mathcal{G}' \times \mathcal{H}'$.*
2. *If $\mathcal{G} \underset{p}{\sim}^* \mathcal{G}'$ and $\mathcal{H} \underset{p}{\sim}^* \mathcal{H}'$, then we have $\mathcal{G} \times \mathcal{H} \underset{p}{\sim}^* \mathcal{G}' \times \mathcal{H}'$.*

Proof. We only give the proof for (2). It is enough to show $\mathcal{G} \times \mathcal{H} \underset{p}{\sim}^* \mathcal{G}' \times \mathcal{H}$ since the product (4.1) is commutative and $\underset{p}{\sim}^*$ is an equivalence relation. By the assumption $\mathcal{G} \underset{p}{\sim}^* \mathcal{G}'$, using Lemma 1, there exists an integer ν satisfying $G_1 G'_\nu \equiv G_0 G'_{\nu+1} \pmod{p}$. Let $\mathcal{Z} = (Z_n) \in \mathscr{X}_p(f)$ be the sequence defined by $Z_n = G'_{n+\nu}$ $(n \in \mathbb{Z})$, then we have $G_1 Z_0 \equiv G_0 Z_1 \pmod{p}$. By Lemma 13, it is enough to show that $\mathcal{G} \times \mathcal{H} \underset{p}{\sim}^* \mathcal{Z} \times \mathcal{H}$. Put $\mathcal{G} \times \mathcal{H} = (W_n)$ and $\mathcal{Z} \times \mathcal{H} = (Y_n)$, then we have

$$\begin{cases} W_0 &= G_1H_0 + G_0H_1 - TG_0H_0, \\ W_1 &= G_1H_1 - NG_0H_0, \end{cases} \qquad \begin{cases} Y_0 &= Z_1H_0 + Z_0H_1 - TZ_0H_0, \\ Y_1 &= Z_1H_1 - NZ_0H_0, \end{cases} \tag{4.2}$$

(see [**3,** p15 (2.6)]). Assume that $p | G_0$, then we have $p | Z_0$ since $G_1 Z_0 \equiv G_0 Z_1 \pmod{p}$. From (4.2), we have $Y_1 W_0 \equiv G_1 H_0 Z_1 H_1 \equiv W_1 Y_0 \pmod{p}$, and hence we have $\mathcal{G} \times \mathcal{H} \underset{p}{\sim}^* \mathcal{Z} \times \mathcal{H}$. Next, assume that $p \nmid G_0$, then we have $p \nmid Z_0$. From (4.2) and the congruence $G_1 Z_0 \equiv G_0 Z_1 \pmod{p}$, we have $W_0 \equiv G_0 Z_0^{-1} Y_0 \pmod{p}$ and $W_1 \equiv G_0 Z_0^{-1} Y_1 \pmod{p}$, and we conclude that $W_0 Y_1 \equiv Y_0 W_1 \pmod{p}$, and hence $\mathcal{G} \times \mathcal{H} \underset{p}{\sim}^* \mathcal{Z} \times \mathcal{H}$. □

By Lemma 14, we know that the products (4.1) on $Z_p(f)$ and $Z_p^*(f)$ are well-defined. The sets $Z_p(f)$ and Z_p^* are commutative groups with identity $\overline{\mathcal{F}}$. For $\overline{\mathcal{G}} \in Z_p(f)$ (or $Z_p^*(f)$), $\mathcal{G} = (G_n)$ with $G_n = \dfrac{B\theta_2^n - A\theta_1^n}{\theta_2 - \theta_1}$, the inverse element of $\overline{\mathcal{G}}$ is given by $\overline{\mathcal{G}'} \in Z_p(f), \mathcal{G}' = (G'_n)$ with $G'_n = \dfrac{A\theta_2^n - B\theta_1^n}{\theta_2 - \theta_1}$.

Theorem 4. *There exist natural group homomorphisms*

$$I(f,p)/G(f,p) \simeq Z_p(f) \quad \text{and} \quad I^*(f,p)/G^*(f,p) \simeq Z_p^*(f).$$

Proof. Consider the following maps.

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

where $\mathfrak{G}_p := \{\mathcal{G} = (G_n) \in \mathfrak{G} \mid p \nmid G_0 \text{ or } p \nmid G_1\}$. By the definitions of relations $\sim, \sim^*, \underset{p}{\sim}$ and $\underset{p}{\sim}^*$, these maps ψ and ψ^* are well-defined group homomorphisms. Furthermore, both ψ_p and ψ_p^* are surjective with kernels $\mathrm{Ker}(\psi_p) = G(f,p)$ and $\mathrm{Ker}(\psi_p^*) = G^*(f,p)$ by Lemma 3. □

Put $F = \mathbb{Q}(\theta_1)$ and let $\mathcal{O}_F$ be the ring of integers of F. For any prime ideal $\mathfrak{p}$ of F which is above p, let $K_1 := \mathcal{O}_F/\mathfrak{p}$ and $K_2 := \mathbb{Z}/p\mathbb{Z}$ be the residue fields. Assume $p \neq 2$. From the isomorphisms ψ_p and ψ_p^* and the group strctures given by Laxton [**6,** Theorem 3.7 and its proof], we get the following commutative diagrams. Note that $(G(\mathfrak{f}_0, 1)) = (G(0,1)) = \mathcal{F}$.

(I) In the case $\left(\dfrac{d}{p}\right) = 1$.

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ker}(\iota) \arrow[r] \arrow[d, "\wr"] & I(f,p)/G(f,p) \arrow[r, "\iota"] \arrow[d, "\psi_p"', "\wr"] & I^*(f,p)/G^*(f,p) \arrow[r] \arrow[d, "\psi_p^*"', "\wr"] & 0 \\
0 \arrow[r] & \{\overline{(G(\mathfrak{f}_i,1))} \mid i = 0,\ldots, r(p)-2\} \cup \{\overline{(G(1,0))}\} \arrow[r] \arrow[d, "\wr"] & Z_p(f) \arrow[r] \arrow[d, "\varphi_p^+"', "\wr"] & Z_p^*(f) \arrow[r] \arrow[d, "\wr"] & 0 \\
0 \arrow[r] & \langle \theta_2/\theta_1 \rangle \arrow[r] & K_1^* \arrow[r] & K_1^*/\langle \theta_2/\theta_1 \rangle \arrow[r] & 0
\end{tikzcd}$$

where ι is the natural surjection, the map φ_p^+ is given by $\varphi_p^+(\overline{\mathcal{G}}) = (G_1 - G_0\theta_1)/(G_1 - G_0\theta_2)$, $(\mathcal{G} = (G_n))$, and each row is an exact sequence.

(II) In the case $\left(\dfrac{d}{p}\right) = -1$.

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ker}(\iota) \arrow[r] \arrow[d, "\wr"] & I(f,p)/G(f,p) \arrow[r, "\iota"] \arrow[d, "\psi_p"', "\wr"] & I^*(f,p)/G^*(f,p) \arrow[r] \arrow[d, "\psi_p^*"', "\wr"] & 0 \\
0 \arrow[r] & \{\overline{(G(\mathfrak{f}_i,1))} \mid i = 0,\ldots, r(p)-2\} \cup \{\overline{(G(1,0))}\} \arrow[r] \arrow[d, "\wr"] & Z_p(f) \arrow[r] \arrow[d, "\varphi_p^-"', "\wr"] & Z_p^*(f) \arrow[r] \arrow[d, "\wr"] & 0 \\
0 \arrow[r] & K_2^*\langle \theta_1 \rangle / K_2^* \arrow[r] & K_1^*/K_2^* \arrow[r] & K_1^*/K_2^*\langle \theta_1 \rangle \arrow[r] & 0
\end{tikzcd}$$

where ι is the natural surjection, the map φ_p^- is given by $\varphi_p^-(\overline{\mathcal{G}}) = G_1 - G_0\theta_2$, $(\mathcal{G} = (G_n))$, and each row is an exact sequence.

(III) In the case $\left(\dfrac{d}{p}\right) = 0$.

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

and

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

where the map φ_p^0 is given by $\varphi_p^0(\overline{(G(\mathcal{F}_i,\mathcal{F}_{i+1}))}) = i$. We can know that the map φ_p^0 is a group homomorphism since for $\mathcal{G}_i = (G(\mathcal{F}_i,\mathcal{F}_{i+1}))$, $\mathcal{G}_j = (G(\mathcal{F}_j,\mathcal{F}_{j+1}))$, the product $\mathcal{G}_i \times \mathcal{G}_j = \mathcal{W} = (W_n)$ is given by

$$\begin{aligned} &W_0 = \mathcal{F}_{i+1}\mathcal{F}_j + \mathcal{F}_i(\mathcal{F}_{j+1} - T\mathcal{F}_j) = \mathcal{F}_{i+1}\mathcal{F}_j - N\mathcal{F}_i\mathcal{F}_{j-1} = \mathcal{F}_{i+j}, \\ &W_1 = \mathcal{F}_{i+1}\mathcal{F}_{j+1} - N\mathcal{F}_i\mathcal{F}_j = \mathcal{F}_{i+j+1}, \end{aligned}$$

by using Lemma 5 and explicit formulas for W_0 and W_1 ([**3,** p15 (2.6)]).

From the diagrams, Lemma 3, Theorem 1 and Theorem 3, we get the following corollary.

Corollary 2. (1) *All the classes of $Z_p(f)$ and $I(f,p)/G(f,p)$ are given by*

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

(2) *Let α_i $(i = 1, \ldots, s(p) + (d/p))$ be the integers in Theorem 2, then all the classes of $Z_p^*(f)$ and $I^*(f,p)/G^*(f,p)$ are given by*

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

5. Examples. We give examples for the case $T = 1, N = -1$ and $T = 6, N = 1$. If $T = 1$ and $N = -1$, then $(G(0,1))$ is the original Fibonacci numbers and $(G(2,1))$ is the original Lucas numbers. If $T = 6$ and $N = 1$, then $(G(0,1))$ is the balancing numbers and $(G(1,3))$ is the Lucas balancing numbers ([**4**]). The numbers a^* with an asterisk in the tables means that a satisfies $f(a^{-1}) \equiv 0 \pmod{p}$.

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

TABLE 1. $T = 1,\ N = -1$

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

TABLE 2. $T = 6,\ N = 1$

6. Acknowledgments. We would like to express our gratitude to Christian Ballot for valuable suggestions.

REFERENCES

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

2. M. Aoki and Y. Sakai, On Equivalence Classes of Generalized Fibonacci sequences, J. Integer Seq. **19**, Article 16.2.6 (2016).

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

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

5. R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, Ann. of Math. (2) **15**, 30–70 (1913,1914).

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

7. E. Lucas, Théorie des fonctions numériques simplement périodiques, Amer. J. Math. **1**, 184–240 and 289–321 (1878).

8. T. Koshy, Fibonacci and Lucas Numbers with Applications, Pure and Applied Mathematics, 2001.

Department of Mathematics, Interdisciplinary Faculty of Science and Engineering, Shimane University, Matsue, Shimane, 690-8504, Japan
Email address: **aoki@riko.shimane-u.ac.jp**

Department of Mathematics, Interdisciplinary Faculty of Science and Engineering, Shimane University, Matsue, Shimane, 690-8504, Japan
Email address: **s169823@matsu.shimane-u.ac.jp**