Journal of Integer Sequences, Vol. 19 (2016),
Article 16.2.6

On Equivalence Classes of Generalized Fibonacci Sequences

Miho Aoki and Yuho Sakai
Department of Mathematics
Shimane University
Matsue, Shimane 690-8504
Japan
aoki@riko.shimane-u.ac.jp
s149410@matsu.shimane-u.ac.jp

Abstract

We consider a *generalized Fibonacci sequence* (G_n) by $G_1, G_2 \in \mathbb{Z}$ and $G_n = G_{n-1} + G_{n-2}$ for any integer n. Let p be a prime number and let $d(p)$ be the smallest positive integer n which satisfies $p \mid F_n$. In this article, we introduce equivalence relations for the set of generalized Fibonacci sequences. One of the equivalence relations is defined as follows. We write $(G_n) \sim^* (G'_n)$ if there exist integers m and n satisfying $G_{m+1}G'_n \equiv G'_{n+1}G_m \pmod{p}$. We prove the following: if $p \equiv \pm 2 \pmod{5}$, then the number of equivalence classes $\overline{(G_n)}$ satisfying $p \nmid G_n$ for any integer n is $(p+1)/d(p) - 1$. If $p \equiv \pm 1 \pmod{5}$, then the number is $(p-1)/d(p) + 1$. Our results are refinements of a theorem given by Kôzaki and Nakahara in 1999. They proved that there exists a generalized Fibonacci sequence (G_n) such that $p \nmid G_n$ for any $n \in \mathbb{Z}$ if and only if one of the following three conditions holds: (1) $p = 5$; (2) $p \equiv \pm 1 \pmod{5}$; (3) $p \equiv \pm 2 \pmod{5}$ and $d(p) < p + 1$.

1 Introduction and main results

We consider a generalized Fibonacci sequence (G_n) defined by

$$G_1, G_2 \in \mathbb{Z},\ G_n = G_{n-1} + G_{n-2}\ (n \in \mathbb{Z}).$$

If $G_1 = 1$ and $G_2 = 1$, then it is the Fibonacci sequence (F_n), and if $G_1 = 1$ and $G_2 = 3$, then it is the Lucas sequence (L_n). It is well-known that such generalized Fibonacci sequences are periodic modulo m for any natural numbers m. For example, the sequence $(F_n \bmod 3)$ is $\ldots 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, \ldots$ (the period is 8). There are many interesting results concerning the generalized Fibonacci sequences. We recommend two books by Koshy [2, §7] and Nakamura [4] as references.

We fix a prime number p, and define two relations $\sim$ and $\sim^*$ for the set of generalized Fibonacci sequences. The first relation $\sim$ is defined in our previous paper [1].

Definition 1. Let (G_n) and (G'_n) be generalized Fibonacci sequences. We write $(G_n) \sim (G'_n)$ if the congruence $G_2 G'_1 \equiv G'_2 G_1 \pmod{p}$ holds.

Definition 2. Let (G_n) and (G'_n) be generalized Fibonacci sequences. We write $(G_n) \sim^* (G'_n)$ if there are some integers m and n satisfying $G_{m+1} G'_n \equiv G'_{n+1} G_m \pmod{p}$.

By the definitions, the next lemma follows.

Lemma 3. *If $(G_n) \sim (G'_n)$, then we have $(G_n) \sim^* (G'_n)$.*

Note that if (G_n) satisfies $p \mid G_1$ and $p \mid G_2$, then we have $(G_n) \sim (G'_n)$ and $(G_n) \sim^* (G'_n)$ for any generalized Fibonacci sequences (G'_n). We can show by the definition that the first relation $\sim$ is an equivalence relation for the set $\{(G_n) | \, p \nmid G_1 \text{ or } p \nmid G_2\}$.

We will show in §2 that the second relation $\sim^*$ is also an equivalence relation. Since the relations $\sim$ and $\sim^*$ are equivalence relations, we can consider the quotient sets using these relations. We put

$$X_p := \{(G_n) \mid p \nmid G_1 \text{ or } p \nmid G_2\}/\sim, \qquad Y_p := \{\overline{(G_n)} \in X_p \mid p \nmid G_n \text{ for any } n \in \mathbb{Z}\}.$$
$$X_p^* := \{(G_n) \mid p \nmid G_1 \text{ or } p \nmid G_2\}/\sim^*, \qquad Y_p^* := \{\overline{(G_n)} \in X_p^* \mid p \nmid G_n \text{ for any } n \in \mathbb{Z}\}.$$

The sets Y_p and Y_p^* are well-defined by [1, Lemma 2] and Lemma 10 in §2. We considered the set $X'_p = \{(G_n) \mid p \nmid G_1 \text{ and } p \nmid G_2\}/\sim$ and $Y'_p = \{\overline{(G_n)} \in X'_p \mid p \nmid G_n \text{ for any } n \in \mathbb{Z}\}$ instead of X_p and Y_p [1]. Note that the cardinality of Y_p and Y'_p are equal. Let p be a prime number and let $d(p)$ be the smallest positive integer n for which $p \mid F_n$. We proved the following theorem in a previous paper [1].

Theorem 4 ([1, Theorem 1 (2)])**.**

$$|Y_p| = p + 1 - d(p)$$

In this article, we will reduce the number of equivalence classes by using the new relation $\sim^*$ instead of $\sim$, and will prove the following theorem in §3.

Theorem 5. (1) *If $p \equiv \pm 2 \pmod{5}$, then we have*

$$|Y_p^*| = \frac{|Y_p|}{d(p)} = \frac{p+1}{d(p)} - 1.$$

(2) *If* $p \equiv \pm 1 \pmod 5$*, then we have*

$$|Y_p^*| = 2 + \frac{|Y_p| - 2}{d(p)} = \frac{p-1}{d(p)} + 1.$$

(3) *If* $p = 5$*, then we have* $|Y_p^*| = |Y_p| = 1$*.*

In §4, we will show that our results imply the following result given by Kôzaki and Nakahara in 1999. An integer m is called the type of a non-divisor when there exists a generalized Fibonacci sequence (G_n) such that $m \nmid G_n$ for any $n \in \mathbb{Z}$. For a prime number p, we denote the period of $(F_n \bmod p)$ by $k(p)$.

Theorem 6 ([3, Kôzaki and Nakahara])**.** *A prime number p is the type of non-divisor if and only if one of the following three conditions holds.*

(1) $p = 5$.

(2) $p \equiv 1, 9, 11, 13, 17, 19 \pmod{20}$.

(3) $p \equiv 3, 7 \pmod{20}$ *and* $k(p) < 2(p+1)$*.*

In §5, we will give some examples of the cardinalities of the set Y_p and Y_p^*.

2 Equivalence relations

In this section, we will give some lemmas on the relation $\sim^*$. The following lemma follows from the recurrence relation $G_n = G_{n-1} + G_{n-2}$.

Lemma 7. *Let (G_n) be a generalized Fibonacci sequence that satisfies $p \nmid G_1$ or $p \nmid G_2$. If $p \mid G_n$, then we have $p \nmid G_{n-1}$ and $p \nmid G_{n+1}$.*

Lemma 8. *Let (G_n) and (G'_n) be generalized Fibonacci sequences. If $G_{m+1}G'_n \equiv G'_{n+1}G_m \pmod p$, then we have $G_{m+2}G'_{n+1} \equiv G'_{n+2}G_{m+1} \pmod p$.*

Proof.

$$\begin{aligned}
G_{m+2}G'_{n+1} &= (G_{m+1} + G_m)G'_{n+1} \\
&= G_{m+1}G'_{n+1} + G_m G'_{n+1} \\
&\equiv G_{m+1}G'_{n+1} + G_{m+1}G'_n \qquad \text{(by the assumption)} \\
&= G_{m+1}(G'_{n+1} + G'_n) \\
&= G_{m+1}G'_{n+2}.
\end{aligned}$$

□

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., $GG^{-1} \equiv 1 \pmod{p}$).

Lemma 9. *The relation $\sim^*$ is an equivalence relation for the set $\{(G_n) \mid p \nmid G_1 \text{ or } p \nmid G_2\}$.*

Proof. Since this relation is reflexive and symmetric, we will prove the transitivity: if $(G_n) \sim^* (G'_n)$ and $(G'_n) \sim^* (G''_n)$, then $(G_n) \sim^* (G''_n)$. By the assumption, there exist integers m, n, k and ℓ satisfying

$$G_{m+1}G'_n \equiv G'_{n+1}G_m \pmod{p} \quad \text{and} \quad G'_{k+1}G''_\ell \equiv G''_{\ell+1}G'_k \pmod{p}.$$

Put $t = \max(n, k)$. Using Lemma 8, we get integers m and ℓ satisfying

$$G_{m+1}G'_t \equiv G'_{t+1}G_m \pmod{p} \quad \text{and} \quad G'_{t+1}G''_\ell \equiv G''_{\ell+1}G'_t \pmod{p}. \tag{1}$$

If we assume $p \mid G'_t$, then we get $p \nmid G'_{t+1}$ using Lemma 7. From (1), we get $p \mid G_m$ and $p \mid G''_\ell$. Therefore we have $(G_n) \sim^* (G''_n)$ since $G_{m+1}G''_\ell \equiv 0 \equiv G''_{\ell+1}G_m \pmod{p}$. If we assume $p \mid G'_{t+1}$, then we get $(G_n) \sim^* (G''_n)$ by the same argument. Next, we assume $p \nmid G'_t$ and $p \nmid G'_{t+1}$. Then we get $p \nmid G_m$ and $p \nmid G''_\ell$ from (1). Hence we get $G_{m+1}G_m^{-1} \equiv G'_{t+1}{G'_t}^{-1} \equiv G''_{\ell+1}{G''_\ell}^{-1} \pmod{p}$, and hence $G_{m+1}G''_\ell \equiv G''_{\ell+1}G_m \pmod{p}$. This congruence implies $(G_n) \sim^* (G''_n)$. □

Lemma 10. *Assume $(G_n), (G'_n) \in \{(G_n) \mid p \nmid G_1 \text{ or } p \nmid G_2\}$. If $(G_n) \sim^* (G'_n)$ and $p \nmid G_n$ for any $n \in \mathbb{Z}$. Then we have $p \nmid G'_n$ for any $n \in \mathbb{Z}$.*

Proof. We can assume that there exist integers m, n satisfying $G_{m+1}G'_n \equiv G'_{n+1}G_m \pmod{p}$. We assume that there exists an integer ℓ such that $p \mid G'_\ell$. Due to the periodicity of $(G'_n \bmod p)$, we can assume $\ell \geq n$. Using Lemma 8, there exists an integer k such that $G_{k+1}G'_\ell \equiv G'_{\ell+1}G_k \pmod{p}$. Since p divides G'_ℓ and does not divide $G'_{\ell+1}$, we get $p \mid G_k$. This contradicts the assumption. □

Lemma 11. *Let (G_n) be a generalized Fibonacci sequence. Then there exists an integer n which satisfies $p|G_n$ if and only if $(G_n) \sim^* (F_n)$.*

Proof. We first assume that there is an integer n that satisfies $p \mid G_n$. We have $(G_n) \sim^* (F_n)$ since $F_1G_n \equiv 0 \equiv G_{n+1}F_0 \pmod{p}$ (note that $F_0 = 0$).

Next, we assume $(G_n) \sim^* (F_n)$. Then there must exist some integers m and n satisfying $G_{m+1}F_n \equiv F_{n+1}G_m \pmod{p}$. On the other hand, since $F_0 = 0$ and the periodicity of $(F_n \bmod p)$, there exists an integer ℓ satisfying $p|F_\ell$ and $\ell \geq n$. By using Lemma 8, we get an integer k such that $G_{k+1}F_\ell \equiv F_{\ell+1}G_k \pmod{p}$. Since $p \nmid F_{\ell+1}$ by Lemma 7, we have $p \mid G_k$. □

Lemma 12.

(1) $X_p^* = Y_p^* \cup \{\overline{(F_n)}\}$.

(2) *For any equivalence classes* $\overline{(G_n)}$ *of* X_p^**, we can choose the representative* (G_n) *satisfying* $p \nmid G_1, G_2$.

(3) *Let* $\overline{(G_n)}$ *be an equivalence class of* Y_p^**. For any sequences* $(G'_n) \in \overline{(G_n)}$*, we have* $p \nmid G'_1, G'_2$.

Proof. The assertion (1) follows from Lemma 11. We will prove (2). If $p \mid G_1$ or $p \mid G_2$, then we have $(G_n) \sim^* (F_n)$ by Lemma 11. Therefore, we have $\overline{(G_n)} = \overline{(F_n)}$ and $F_1 = F_2 = 1$. The assertion (3) follows from Lemma 10. □

3 Equivalence classes

In our previous paper [1], we gave the cardinality of the set Y_p. In this section, using this result, we will prove the main theorem (Theorem 5 in §1) that gives the cardinality of the set Y_p^*.

Lemma 13. *Let* p $(\neq 2, 5)$ *be a prime number.*

(1) *If* $p \equiv \pm 1 \pmod 5$*, then* $X^2 - X - 1 = 0$ *has different two solutions in* $\mathbb{F}_p$.

(2) *If* $p \equiv \pm 2 \pmod 5$*, then* $X^2 - X - 1 = 0$ *does not have a solution in* $\mathbb{F}_p$.

Proof. The solutions of $X^2 - X - 1 = 0$ in $\overline{\mathbb{F}}_p$ (the algebraic closure of $\mathbb{F}_p$) are $X = 2^{-1}(1 \pm \sqrt{5})$. By the assumption $p \neq 2, 5$, these solutions are different. We get $2^{-1}(1 \pm \sqrt{5}) \in \mathbb{F}_p$ if and only if $\sqrt{5} \in \mathbb{F}_p$. Furthermore, this is equivalent to $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1$, that is, $p \equiv \pm 1 \pmod 5$. □

We next define the number $d(p)$ for a prime number p, and the sequences (f_n) and (g_n). These are important in this article.

Definition 14. Let p be a prime number. Let $d(p)$ denote the smallest positive integer n which satisfies $F_n \equiv 0 \pmod p$.

(1) For any integer n which satisfies $n \not\equiv 0 \pmod{d(p)}$, we define the integer f_n $(0 \leq f_n \leq p - 1)$ such that $f_n \equiv F_{n+1} F_n^{-1} \pmod p$.

(2) Let (G_n) be a generalized Fibonacci sequence that satisfies $p \nmid G_n$ for any $n \in \mathbb{Z}$. We can then define the integer g_n $(1 \leq g_n \leq p - 1)$ such that $g_n \equiv G_{n+1} G_n^{-1} \pmod p$.

We will prove some relations between (f_n), (g_n) and $d(p)$. The following lemma was given in [1, Lemma 3].

Lemma 15 ([1, Lemma 3])**.** *Let* m *and* n *be integers that satisfy* $m, n \not\equiv 0 \pmod{d(p)}$*. We then have* $f_m = f_n$ *if and only if* $m \equiv n \pmod{d(p)}$.

We can show the following two lemmas by induction on n and the recurrence relation.

Lemma 16. *For any $n, m \in \mathbb{Z}$, we have $G_n = F_{n-m}G_{m+1} + F_{n-m-1}G_m$.*

Lemma 17. *For any $n \in \mathbb{Z}$, we have*

$$G_{n+1}^2 - G_nG_{n+1} - G_n^2 = -(G_n^2 - G_{n-1}G_n - G_{n-1}^2).$$

For simplicity, we introduce a new notation. If a generalized Fibonacci sequence (G_n) satisfies $G_1 = a$ and $G_2 = b$, then we denote it as $(G_n) = (G(a,b))$.

Theorem 18. *Assume that $(G_n) = (G(a,b))$ satisfies $p \nmid G_n$ for any $n \in \mathbb{Z}$. Furthermore, let a and b satisfy $b^2 - ab - a^2 \not\equiv 0 \pmod{p}$. For any integers n and m, we have $g_n = g_m$ if and only if $n \equiv m \pmod{d(p)}$.*

Proof. First, by the definition of g_n and g_m, we have $g_n = g_m$ if and only if $G_mG_{n+1} \equiv G_{m+1}G_n \pmod{p}$. Since $G_{n+1} = F_{n-m+1}G_{m+1} + F_{n-m}G_m$ and $G_n = F_{n-m}G_{m+1} + F_{n-m-1}G_m$ from Lemma 16, we have $g_n \equiv g_m$ if and only if

$$G_{m+1}^2F_{n-m} - G_mG_{m+1}(F_{n-m+1} - F_{n-m-1}) - G_m^2F_{n-m} \equiv 0 \pmod{p}. \tag{2}$$

By Lemma 17, for the left side of (2), we have

$$\begin{aligned}
G_{m+1}^2F_{n-m} - G_mG_{m+1}&(F_{n-m+1} - F_{n-m-1}) - G_m^2F_{n-m} \\
&\equiv G_{m+1}^2F_{n-m} - G_mG_{m+1}F_{n-m} - G_m^2F_{n-m} \\
&\equiv (G_{m+1}^2 - G_mG_{m+1} - G_m^2)F_{n-m} \\
&\equiv (-1)^{m-1}(G_2^2 - G_1G_2 - G_1^2)F_{n-m} \\
&\equiv (-1)^{m-1}(b^2 - ab - a^2)F_{n-m} \pmod{p}.
\end{aligned}$$

By the assumption $b^2 - ab - a^2 \not\equiv 0 \pmod{p}$, we conclude that $g_n \equiv g_m$ if and only if $n \equiv m \pmod{d(p)}$. ☐

For a generalized Fibonacci sequence (G_n), let (g_n) be the sequence defined in Definition 14.

Definition 19. Assume $(G_n) = (G(a,b))$ satisfies $p \nmid G_n$ for any $n \in \mathbb{Z}$. We define the *second period* of (G_n) by the period of (g_n).

Then we get the following corollary concerning the second period.

Corollary 20. *Assume that $(G_n) = (G(a,b))$ satisfies $p \nmid G_n$ for any $n \in \mathbb{Z}$.*

(1) *If $b^2 - ab - a^2 \equiv 0 \pmod{p}$, then the second period of (G_n) is equal to 1.*

(2) *If $b^2 - ab - a^2 \not\equiv 0 \pmod{p}$, then the second period of (G_n) is equal to $d(p)$.*

Proof. The assertion (2) follows from Theorem 18. We will prove (1) by showing $g_n = g_1 \equiv ba^{-1} \pmod p$ for any $n \in \mathbb{Z}$. Due to the periodicity of (G_n) mod p, it is sufficient to consider $n \in \mathbb{N}$. We use the induction. When $n = 1$, the result is shown. We assume that it holds for any natural numbers less than $n+1$. We then have the following congruences.

$$
\begin{aligned}
g_{n+1} &\equiv G_{n+2}G_{n+1}^{-1} \\
&\equiv (G_{n+1} + G_n)(G_n + G_{n-1})^{-1} \\
&\equiv (G_{n+1}G_n^{-1} + 1)(1 + G_{n-1}G_n^{-1})^{-1} \\
&\equiv (g_n + 1)(1 + g_{n-1}^{-1})^{-1} \\
&\equiv (ba^{-1} + 1)(1 + b^{-1}a)^{-1} \\
&\qquad \text{(by the assumption of the second period 1)} \\
&\equiv (ba^{-1} + 1) \times \{b^{-1}a(ba^{-1} + 1)\}^{-1} \\
&\equiv ba^{-1} \equiv g_1 \pmod p.
\end{aligned}
$$

By the above congruences and $1 \le g_1, g_{n+1} \le p-1$, we have $g_{n+1} = g_1$. □

Lemma 21. *Assume that (G_n) and (G'_n) satisfy $p \nmid G_n, G'_n$ for any $n \in \mathbb{Z}$. Let ν be the second period of (G'_n). Then we have $(G_n) \sim^* (G'_n)$ if and only if there exists an integer n $(1 \le n \le \nu)$ such that $g'_n = g_1 (\equiv G_2G_1^{-1} \pmod p))$.*

Proof. First, we assume $g'_n = g_1$ for an integer n $(1 \le n \le \nu)$. Then we obtain $G'_{n+1}{G'_n}^{-1} \equiv G_2G_1^{-1} \pmod p$ and hence we get $(G_n) \sim^* (G'_n)$.

Next, we assume $(G_n) \sim^* (G'_n)$. Then there must exist integers m and n such that $G_{m+1}G'_n \equiv G'_{n+1}G_m \pmod p$. By Lemma 8 on the forward shift index and the periodicity of (G_n) mod p, there exists an integer n such that $G_2G'_n \equiv G'_{n+1}G_1 \pmod p$. Therefore we obtain $g'_n \equiv g_1 \pmod p$. We have $g_1 = g'_n$ since $1 \le g_1 \le p-1$ and $1 \le g_n \le p-1$. Furthermore, we can choose such an integer n satisfying $1 \le n \le \nu$ because the period of (g'_n) is equal to ν. □

Next, we will prove the main theorem in §1.

Proof of Theorem 5. We can prove (3) directly using [1, Corollary 1 (1)]. We will prove (1) and (2). Using [1, Theorem 1 (1)], we obtain

$$
\begin{aligned}
Y_p &= X'_p - \{\overline{(G(1, f_i))} \mid 1 \le i \le d(p) - 2\} \\
X'_p &:= \{(G_n) \mid p \nmid G_1 \text{ and } p \nmid G_2\}/\sim \\
&= \{\overline{(G(1, b))} \mid 1 \le b \le p-1\}.
\end{aligned}
$$

(1) We consider an equivalence class $\overline{(G_n)}$ $((G_n) = (G(1, b)))$ of Y_p. Since $p \equiv \pm 2 \pmod 5$, we have $b^2 - b - 1 \not\equiv 0 \pmod p$ because $X^2 - X - 1 = 0$ does not have a solution in $\mathbb{F}_p$ from Lemma 13 (2). Therefore, the second period of (G_n) is $d(p)$ from Corollary 20

(2), and all of the values $g_1, g_2, \ldots, g_{d(p)}$ are different from each other from Theorem 18 , where g_n is the integer such that $g_n = G_{n+1}G_n^{-1} \pmod p$ and $1 \le g_n \le p-1$. From the definition of the relation $\sim^*$, we have $(G_n) = (G(1,b)) \sim^* (G(1,g_i))$ for any i $(1 \le i \le d(p))$. On the other hand, for any equivalence classes $\overline{(G'_n)}$ $((G'_n) = (G(1,b')))$ of Y_p satisfying $b' \not\equiv g_1, \ldots, g_{d(p)} \pmod p$, we have $(G_n) \not\sim^* (G'_n)$ from Lemma 21. Then for any class $\overline{(G(1,b))}$ in Y_p^*, it produces distinct $d(p)$ classes $\overline{(G(1,g_i))}$ $(1 \le i \le d(p))$ under the equivalence relation $\sim$. Therefore we obtain $|Y_p^*| = \dfrac{|Y_p|}{d(p)}$. The last equality: $\dfrac{|Y_p|}{d(p)} = \dfrac{p+1}{d(p)} - 1$ follows from [1, Theorem 1 (2)].

(2) If $p \equiv \pm 1 \pmod 5$, then $X^2 - X - 1 = 0$ has two different solutions α and β in $\mathbb{F}_p$ from Lemma 13 (1). We consider the generalized Fibonacci sequence $(G(1,\alpha)) = (G_n)$. Since $p \nmid G_n$ for any $n \in \mathbb{Z}$ from $\alpha^2 - \alpha - 1 \equiv 0 \pmod p$, Lemma 7 and Corollary 20 (1), we have $\overline{(G(1,\alpha))} \in Y_p$. Similarly, we have $\overline{(G(1,\beta))} \in Y_p$. Let b be an integer satisfying $1 \le b \le p-1$. Since the second periods of $(G(1,\alpha))$ and $(G(1,\beta))$ are 1 from Corollary 20 (1), we obtain $(G(1,b)) \sim^* (G(1,\alpha))$ if and only if $b = \alpha$ from Lemma 21. By these same arguments, we obtain the same result for $(G(1,\beta))$. On the other hand, $d(p)$ classes $\overline{(G(1,b))}$ of Y_p satisfying $b \neq \alpha, \beta$ become the same class of Y_p^*. We obtain $|Y_p^*| = 2 + \dfrac{|Y_p| - 2}{d(p)}$, and the last equality follows from [1, Theorem 1 (2)].

□

4 Comparison with a results of Kôzaki and Nakahara

In the section, we will show that our result implies a result given by Kôzaki and Nakahara in 1999.

Definition 22. An integer m is called the type of a non-divisor when there exists a generalized Fibonacci sequence (G_n) such that $m \nmid G_n$ for any $n \in \mathbb{Z}$.

Definition 23. For a prime number p, we let $k(p)$ denote the period of $(F_n \bmod p)$.

We can get the following corollary from [1, Theorem 1 and Corollary 1].

Corollary 24 ([1, §1])**.** *A prime number p is the type of non-divisor if and only if one of the following three conditions holds.*

(1) $p = 5$.

(2) $p \equiv \pm 1 \pmod 5$.

(3) $p \equiv \pm 2 \pmod 5$ *and* $d(p) < p + 1$.

We will prove that Theorem 6 in §1 is equivalent to Corollary 24. More specifically, we will prove (1) or (2) or (3) of Theorem 6 holds if and only if (1) or (2) or (3) of Corollary 24 holds.

Proof. First, we prove that if (1) or (2) or (3) of Theorem 6 holds, then one of (1), (2), or (3) of Corollary 24 holds.

The case in which (1) of Theorem 6 holds already.

We assume that (2) of Theorem 6 holds. If $p \equiv 1, 9, 11, 19 \pmod{20}$, then we have $p \equiv \pm 1 \pmod 5$. If $p \equiv 13, 17 \pmod{20}$, then we have $p \equiv \pm 2 \pmod 5$ and $p \equiv 1 \pmod 4$. Using [1, Lemma 1 (2) and Lemma 4], we have $d(p) < p + 1$.

We assume (3) of Theorem 6 holds. In this case, we have $p \equiv 3 \pmod 4$ and $p \equiv \pm 2 \pmod 5$. By $p \equiv \pm 2 \pmod 5$, we have $F_p \equiv -1 \pmod p$ and $F_{p+1} \equiv 0 \pmod p$ (cf. [4, §6]), and hence we obtain $k(p) \neq p + 1$. If $d(p) = p + 1$, then we obtain $p + 1 \mid k(p)$ since $d(p) \mid k(p)$. However this is a contradiction, since $k(p) \neq p + 1,\ \kappa(p) < 2(p + 1)$ and $k(p) \mid 2(p + 1)$ hold (cf. [4, §9]). We conclude that $d(p) < p + 1$.

Next, we prove that if (1) or (2) or (3) of Corollary 24 holds, then one of (1), (2), or (3) of Theorem 6 holds. When (1) of Corollary 24 holds, it is the same as in (1) of Theorem 6. We assume (2) of Corollary 24 holds. If $p \equiv 1 \pmod 5$, then we have $p \equiv 1, 11 \pmod{20}$. If $p \equiv -1 \pmod 5$, then we have $p \equiv 9, 19 \pmod{20}$.

We assume (3) of Corollary 24 holds. When $p \equiv 2 \pmod 5$, we have $p \equiv 7, 17 \pmod{20}$. When $p \equiv -2 \pmod 5$, we have $p \equiv 3, 13 \pmod{20}$. If $p \equiv 13, 17 \pmod{20}$, the condition (2) of Theorem 6 holds. We consider the case $p \equiv 3, 7 \pmod{20}$. In this case, we have $p \equiv 3 \pmod 4$ and $p \equiv \pm 2 \pmod 5$, and hence $k(p) \mid 2(p + 1)$. From the well-known formula $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$, we get $F_{d(p)-1}F_{d(p)+1} - F_{d(p)}^2 \equiv (-1)^{d(p)} \pmod p$. Therefore we have $F_{d(p)-1}^2 \equiv (-1)^{d(p)} \pmod p$ since $F_{d(p)} \equiv 0 \pmod p$ and $F_{d(p)-1} \equiv F_{d(p)+1} \pmod p$. If $F_{d(p)-1}^2 \equiv -1 \pmod p$, then this contradicts $\left(\frac{-1}{p}\right) = -1$ since $p \equiv 3 \pmod 4$. If $F_{d(p)-1}^2 \equiv 1 \pmod p$, then $F_{d(p)-1} \equiv \pm 1 \pmod p$ holds. In the case of $F_{d(p)-1} \equiv 1 \pmod p$, we have $k(p) = d(p)$, and hence $k(p) < p + 1$. In the case of $F_{d(p)-1} \equiv -1 \pmod p$, we have $k(p) \leq 2d(p) < 2(p + 1)$ since $F_{2d(p)-1} \equiv 1 \pmod p$. □

5 Examples

p	$d(p)$	Y_p	Y_p^*
3	4	$\emptyset$	$\emptyset$
5	5	$\overline{(G(1,3))}$	$\overline{(G(1,3))}$
7	8	$\emptyset$	$\emptyset$
11	10	$\overline{(G(1,4))}$, $\overline{(G(1,8))}$	$\overline{(G(1,4))}$, $\overline{(G(1,8))}$
13	7	$\overline{(G(1,3))}$, $\overline{(G(1,4))}$, $\overline{(G(1,5))}$, $\overline{(G(1,7))}$, $\overline{(G(1,9))}$, $\overline{(G(1,10))}$, $\overline{(G(1,11))}$	$\overline{(G(1,3))}$
17	9	$\overline{(G(1,3))}$, $\overline{(G(1,4))}$, $\overline{(G(1,6))}$, $\overline{(G(1,7))}$, $\overline{(G(1,9))}$, $\overline{(G(1,11))}$, $\overline{(G(1,12))}$, $\overline{(G(1,14))}$, $\overline{(G(1,15))}$	$\overline{(G(1,3))}$
19	18	$\overline{(G(1,5))}$, $\overline{(G(1,15))}$	$\overline{(G(1,5))}$, $\overline{(G(1,15))}$

Table 1: Examples

6 Acknowledgments

We thank the editor and the referee for reading carefully. We also express our gratitude to Toru Nakahara for valuable suggestions.

References

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

[2] T. Koshy, *Fibonacci and Lucas Numbers with Applications*, Pure and Applied Mathematics, 2001.

[3] M. Kôzaki and T. Nakahara, On arithmetic properties of generalized Fibonacci sequences, *Reports of the Faculty of Science and Engineering, Saga University, Mathematics* **28** (1999), 1–18.

[4] S. Nakamura, *Fibonacci Sū no Micro Cosmos* (Japanese), Nippon Hyoronsha, 2002.

2010 *Mathematics Subject Classification*: Primary 11B39.
Keywords: Fibonacci number, Lucas number, generalized Fibonacci sequence.

Received November 7 2015; revised versions received January 18 2016; January 20 2016; January 25 2016. Published in *Journal of Integer Sequences*, February 5 2016.

Return to Journal of Integer Sequences home page.