ON DIVISIBILITY OF GENERALIZED FIBONACCI NUMBERS

Miho Aoki[1]
Department of Mathematics, Shimane University, Matsue, Shimane, Japan
aoki@riko.shimane-u.ac.jp

Yuho Sakai
Department of Mathematics, Shimane University, Matsue, Shimane, Japan
s149410@matsu.shimane-u.ac.jp

Received: 4/6/14, Revised: 2/15/15, Accepted: 4/8/15, Published: 6/5/15

Abstract

It is well-known that p divides some Fibonacci numbers F_n for any prime number p. Moreover, it is also known that any Lucas number L_n cannot be divided by 5. Let p be a prime number and $d(p)$ be the smallest positive integer n for which $p \mid F_n$. In this article, we consider the generalized Fibonacci sequence $\{G_n\}$, which satisfies the Fibonacci recurrence relation, but with arbitrary initial conditions. We define an equivalence relation among the sequences $\{G_n\}$ and give all equivalence classes $\overline{\{G_n\}}$, whose representatives $\{G_n\}$ satisfy $p \nmid G_n$ for any $n \in \mathbb{N}$. From the result, we know that if $p \equiv \pm 1 \pmod 5$, then there are infinitely many generalized Fibonacci sequences $\{G_n\}$ that satisfy $p \nmid G_n$ for any $n \in \mathbb{N}$, and if $p \equiv \pm 2 \pmod 5$ and $d(p) = p+1$, then for any generalized Fibonacci sequences $\{G_n\}$, we have $p|G_n$ for some $n \in \mathbb{N}$.

1. Introduction and Main Result

We define *the generalized Fibonacci sequence* $\{G_n\}$ by

$$G_1, G_2 \in \mathbb{Z} \quad \text{and} \quad G_{n+2} = G_{n+1} + G_n \text{ for any } n \geq 1.$$

Many interesting properties of the sequences are known ([2, especially see §7 and §17]). We fix a prime number p and let $d(p)$ be the order of appearance of p for the Fibonacci sequence $\{F_n\}$, which is defined as the smallest positive integer n such that $F_n \equiv 0 \pmod p$. By the periodicity modulo p ([2, §35]), we have $F_n \equiv 0 \pmod p$ if and only if $n \equiv 0 \pmod{d(p)}$. Furthermore, we know $d(p) \leq p+1$ from the well-known properties of Fibonacci numbers.

[1] This work was supported by JSPS KAKENHI Grant Numbers 26400015.

Lemma 1. ([2, §34, *Theorem* 34.8])

(1) *If* $p \equiv \pm 1 \pmod 5$, *then we have* $F_{p-1} \equiv 0 \pmod p$.

(2) *If* $p \equiv \pm 2 \pmod 5$, *then we have* $F_{p+1} \equiv 0 \pmod p$.

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., $GG^{-1} \equiv 1 \pmod p$). Let $\{G_n\}$ and $\{G'_n\}$ be generalized Fibonacci sequences that satisfy $p \nmid G_1, G_2$ and $p \nmid G'_1, G'_2$. If $G_2G_1^{-1} \equiv G'_2{G'_1}^{-1} \pmod p$, then we write $\{G_n\} \sim \{G'_n\}$. This relation $\sim$ is an equivalence relation. We denote the quotient set of this relation by

$$X_p = \{\{G_n\} \mid \text{generalized Fibonacci sequences that satisfy } p \nmid G_1, G_2\}/\sim .$$

By the definition of the relation $\sim$, each class $\overline{\{G_n\}} \in X_p$ contains infinitely many generalized Fibonacci sequences. The number of equivalence classes $\overline{\{G_n\}}$ of X_p is $|X_p| = |\mathbb{F}_p^{\times}| = p - 1$. Furthermore, we define the subset Y_p of X_p by

$$Y_p = \{\overline{\{G_n\}} \in X_p \mid p \nmid G_n \quad \text{for any} \quad n \in \mathbb{N}\}.$$

We know that Y_p is well-defined; the condition "$p \nmid G_n$ for any $n \in \mathbb{N}$" does not depend on a representative $\{G_n\}$ by the following lemma.

Lemma 2. *Assume* $p \nmid G_1, G_2$, $p \nmid G'_1, G'_2$, *and* $\{G_n\} \sim \{G'_n\}$. *Then we have* $p \nmid G_n$ *if and only if* $p \nmid G'_n$ *for any* $n \in \mathbb{N}$.

For any positive integers i which satisfy $i \not\equiv 0 \pmod{d(p)}$, let g_i $(0 \le g_i \le p-1)$ be the integer such that $g_i \equiv F_{i+1}F_i^{-1} \pmod p$. The next lemma is the key to proving our main theorem. The key lemma shows that the ratios of successive Fibonacci numbers modulo p have the period $d(p)$.

Lemma 3. *Let* i *and* j *be positive integers which satisfy* $i, j \not\equiv 0 \pmod{d(p)}$. *We have* $g_i = g_j$ *if and only if* $i \equiv j \pmod{d(p)}$.

We denote the generalized Fibonacci sequence $\{G_n\}$ such that $G_1 = a$, and $G_2 = b$ $(a, b \in \mathbb{Z})$ by $\{G(a, b)\}$. For example, $\{F_n\} = \{G(1, 1)\}$ and $\{L_n\} = \{G(1, 3)\}$. We can write $X_p = \{\overline{\{G(1, k)\}} \mid 1 \le k \le p - 1\}$. Our main theorem is as follows.

Theorem 1. (1) $Y_p = X_p - \{\overline{\{G(1, g_i)\}} \mid 1 \le i \le d(p) - 2\}$.

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

The next corollary immediately follows from Theorem 1, Lemma 1, and $d(5) = 5$.

Corollary 1. (1) $|Y_5| = 1$.

(2) *If* $p \equiv \pm 1 \pmod 5$, *then there are infinitely many generalized Fibonacci sequences* $\{G_n\}$ *that satisfy* $p \nmid G_n$ *for any* $n \in \mathbb{N}$.

(3) *If $p \equiv \pm 2 \pmod 5$ and $d(p) = p + 1$, then for any generalized Fibonacci sequence $\{G_n\}$, we have $p | G_n$ for some $n \in \mathbb{N}$.*

If $p \equiv \pm 2 \pmod 5$, then we have $d(p) \le p + 1$ by Lemma 1 (2). Furthermore, we get $d(p) | p+1$ by a brief discussion (cf. [3, Lemma 2.2 (c)]). We give a necessary condition for $d(p) = p + 1$ below. We obtained the following lemma from a private discussion with Yasuhiro Kishi.

Lemma 4. *Let p be an odd prime number. If $d(p) = p + 1$, then we have $p \equiv 3 \pmod 4$.*

Proof. Applying the property $F_{n+m} = F_m F_{n+1} + F_{m-1} F_n$ for $(n, m) = \left(\frac{p-1}{2}, \frac{p+1}{2}\right)$ and $(n, m) = \left(\frac{p+1}{2}, \frac{p+3}{2}\right)$, we get $F^2_{\frac{p+1}{2}} + F^2_{\frac{p-1}{2}} = F_p$ and $F^2_{\frac{p+3}{2}} + F^2_{\frac{p+1}{2}} = F_{p+2}$. By our assumption $d(p) = p + 1$, Lemma 1, and $d(5) = 5$, we have $p \equiv \pm 2 \pmod 5$. On the other hand, we get $F_p \equiv -1 \pmod p$ ([1, Theorem 6]), and also $F_{p+2} \equiv -1 \pmod p$ since $F_{p+1} \equiv 0 \pmod p$. Hence we get $F^2_{\frac{p+1}{2}} + F^2_{\frac{p-1}{2}} \equiv -1 \pmod p$ and $F^2_{\frac{p+3}{2}} + F^2_{\frac{p+1}{2}} \equiv -1 \pmod p$. Furthermore, since

$$
\begin{aligned}
-1 \equiv F^2_{\frac{p+3}{2}} + F^2_{\frac{p+1}{2}} \pmod p \quad &= \left(F_{\frac{p+1}{2}} + F_{\frac{p-1}{2}}\right)^2 + F^2_{\frac{p+1}{2}} \\
&\equiv 2F_{\frac{p+1}{2}} F_{\frac{p-1}{2}} - 1 + F^2_{\frac{p+1}{2}} \pmod p,
\end{aligned}
$$

we conclude $F_{\frac{p+1}{2}} \left(2F_{\frac{p-1}{2}} + F_{\frac{p+1}{2}}\right) \equiv 0 \pmod p$ and hence $F_{\frac{p+1}{2}} \equiv -2F_{\frac{p-1}{2}} \pmod p$ by our assumption that $d(p) = p+1$. We get $-1 \equiv F^2_{\frac{p+1}{2}} + F^2_{\frac{p-1}{2}} \equiv 5F^2_{\frac{p-1}{2}} \pmod p$. If we assume $p \equiv 1 \pmod 4$, then we have

$$
\left(\frac{5F^2_{\frac{p-1}{2}}}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{\pm 2}{5}\right) = -1 \quad \text{and} \quad \left(\frac{-1}{p}\right) = 1.
$$

These contradict $5F^2_{\frac{p-1}{2}} \equiv -1 \pmod p$. Hence we get $p \equiv 3 \pmod 4$. □

The primes p which satisfy $p < 100$ and the condition $d(p) = p + 1$ are $p = 3, 7, 23, 43, 67, 83$.

2. Proofs

First, we prove Lemma 2 and Lemma 3.

Proof of Lemma 2. Let a be the integer which satisfies $a \equiv G_2 G_1^{-1} \equiv G'_2 {G'_1}^{-1} \pmod p$ and $1 \le a \le p - 1$, and $\{A_n\}$ be the generalized Fibonacci sequence defined by $A_1 = 1$ and $A_2 = a$. Then, we have $G_n \equiv A_n G_1$ and $G'_n \equiv A_n G'_1 \pmod p$

for all $n \in \mathbb{N}$. As p does not divide G_1 and G'_1, we have $p|G_n$ if and only if $p|G'_n$. □

Proof of Lemma 3. We consider two subsequences of F_n mod p:

$$F_i,\ F_{i+1} \equiv g_i F_i,\ F_{i+2} \equiv (1+g_i)F_i,\ F_{i+3} \equiv (1+2g_i)F_i, \cdots,$$

$$F_j, F_{j+1} \equiv g_j F_j,\ F_{j+2} \equiv (1+g_j)F_j,\ F_{j+3} \equiv (1+2g_j)F_j, \cdots.$$

Assume $g_i = g_j$ and let k be a positive integer. Because p does not divide F_i and F_j, we have $F_{i+k} \equiv 0 \pmod p$ if and only if $F_{j+k} \equiv 0 \pmod p$. We conclude that $i + k \equiv j + k \pmod{d(p)}$ for some $k \in \mathbb{N}$, and obtain $i \equiv j \pmod{d(p)}$.

Conversely, we assume $i \equiv j \pmod{d(p)}$. Let $\{I_n\}$ and $\{J_n\}$ be the generalized Fibonacci sequences which are defined as $I_1 = J_1 = 1$ and $I_2 = g_i,\ J_2 = g_j$. We denote the above two subsequences mod p by

$$F_i,\ F_{i+1} \equiv I_2 F_i,\ F_{i+2} \equiv I_3 F_i,\ F_{i+3} \equiv I_4 F_i, \cdots,$$

$$F_j, F_{j+1} \equiv J_2 F_j,\ F_{j+2} \equiv J_3 F_j,\ F_{j+3} \equiv J_4 F_j, \cdots.$$

By the assumption that $i \equiv j \pmod{d(p)}$, for any positive integer k, we have $i + k \equiv 0 \pmod{d(p)}$ if and only if $j + k \equiv 0 \pmod{d(p)}$. Therefore, we have $F_{i+k} \equiv 0 \pmod p$ if and only if $F_{j+k} \equiv 0 \pmod p$. Since p does not divide F_i and F_j, we get $I_{k+1} \equiv 0 \pmod p$ if and only if $J_{k+1} \equiv 0 \pmod p$. By the formulas

$$I_{k+1} = F_{k-1}I_1 + F_k I_2 = F_{k-1} + F_k g_i \quad \text{and} \quad J_{k+1} = F_{k-1}J_1 + F_k J_2 = F_{k-1} + F_k g_j,$$

we have $F_k g_i \equiv F_k g_j \pmod p$. Since $k \not\equiv 0 \pmod{d(p)}$ by $i, j \not\equiv 0 \pmod{d(p)}$, we have $g_i \equiv g_j \pmod p$. Furthermore, since $0 \le g_i, g_j \le p-1$, we get $g_i = g_j$. □

Proposition 1. *Assume $p \nmid G_1, G_2$. For all positive integers n which satisfy $n \not\equiv 2 \pmod{d(p)}$, we have $p \mid G_n$ if and only if $-G_1G_2^{-1} \equiv g_{n-2} \pmod p$.*

Proof. This follows from the well-known formula $G_n = F_{n-2}G_1 + F_{n-1}G_2$. □

Proposition 2. *Assume $p \nmid G_1, G_2$. We have $p|G_n$ for some $n \in \mathbb{N}$ if and only if $-G_1G_2^{-1} \equiv g_i \pmod p$ for some i which satisfies $1 \le i \le d(p) - 2$.*

Proof. If $n \equiv 2 \pmod{d(p)}$, then we have $G_n = F_{n-2}G_1 + F_{n-1}G_2 \equiv F_{n-1}G_2 \not\equiv 0 \pmod p$. Furthermore, if $i = d(p) - 1$, then we have $-G_1G_2^{-1} \not\equiv g_i \pmod p$ as we have assumed $p \nmid G_1$ and $g_{d(p)-1} \equiv F_{d(p)}F_{d(p)-1}^{-1} \equiv 0 \pmod p$. Hence it suffices to show that we have $p|G_n$ for some $n \in \mathbb{N}$ which satisfies $n \not\equiv 2 \pmod{d(p)}$ if and only if $-G_1G_2^{-1} \equiv g_i \pmod p$ for some i which satisfies $1 \le i \le d(p) - 1$. This follows from Proposition 1 and Lemma 3. □

Next, we prove the main theorem.

Proof of Theorem 1. (1) Since the Fibonacci numbers satisfy $F_{n+m} = F_m F_{n+1} + F_{m-1}F_n$, we have $0 \equiv F_{d(p)} = F_{i+(d(p)-i)} = F_{d(p)-i}F_{i+1} + F_{d(p)-i-1}F_i \pmod{p}$ for any i $(1 \le i \le d(p)-2)$. Therefore, $g_i \equiv -g_{d(p)-i-1}^{-1} \pmod{p}$. By Lemma 3 and Proposition 2, we have

$$\begin{aligned} Y_p &= X_p - \{\overline{\{G_n\}} \in X_p \mid p | G_n \text{ for some } n \in \mathbb{N}\} \\ &= X_p - \{\overline{\{G(1,k)\}} \mid 1 \le k \le p-1,\ -k^{-1} \equiv g_i \pmod{p} \\ &\qquad\qquad \text{for some } i\ (1 \le i \le d(p)-2)\} \\ &= X_p - \{\overline{\{G(1,k)\}} \mid 1 \le k \le p-1,\ -k^{-1} \equiv g_{d(p)-i-1} \pmod{p} \\ &\qquad\qquad \text{for some } i\ (1 \le i \le d(p)-2)\} \\ &= X_p - \{\overline{\{G(1,k)\}} \mid 1 \le k \le p-1,\ k \equiv -g_{d(p)-i-1}^{-1} \pmod{p} \\ &\qquad\qquad \text{for some } i\ (1 \le i \le d(p)-2)\} \\ &= X_p - \{\overline{\{G(1,g_i)\}} \mid 1 \le i \le d(p)-2\}. \end{aligned}$$

(2) By Lemma 3, we know $g_i \ne g_j$ if $1 \le i, j \le d(p)-2$ and $i \ne j$. Hence we conclude $|Y_p| = |X_p| - (d(p)-2) = (p-1) - (d(p)-2) = p+1-d(p)$. □

3. Examples

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

Table 1. Y_p for small prime numbers p

Acknowledgments The authors would like to express their gratitude to the referee and the editor for their valuable comments and suggestions. We added Lemma 4 by referee's suggestion. We also want to thank Y. Kishi for telling us the proof of Lemma 4.

References

[1] V. E., Jr. Hoggatt and M. Bicknell, Some congruences of the Fibonacci numbers modulo a prime p, Math. Mag. 47, 210–214 (1974).

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

[3] D. Marques, The order of appearance of integers at most one away from Fibonacci numbers, Fibonacci Quart. 50, no.1, 36–43(2012).