JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **34**, No. 4, November 2021
http://dx.doi.org/10.14403/jcms.2021.34.4.327

FIBONACCI SEQUENCES IN kTH POWER RESIDUES

Youchan Chung, Eunyool Jang, Jinseo Park†, and Sanghoon Park

Abstract. In this paper, we find all the prime numbers p that satisfy the following statement. If a positive integer k is a divisor of $p-1$, then there is a sequence consisting of all k-th power residues modulo p, satisfying the recurrence equation of the Fibonacci sequence modulo p.

1. Introduction

Let us consider of the sequence (1,4,5,9,3). This sequence, consists of all of the quadratic residues modulo 11, satisfies the definition of the Fibonacci sequence with modulo 11, that is

$$1+4 \equiv 5 \pmod{11},\ 4+5 \equiv 9 \pmod{11},$$
$$5+9 \equiv 3 \pmod{11},\ 9+3 \equiv 1 \pmod{11}.$$

In addition, the sequence (1,24,25,20,16,7,23) includes all of the 4th power residues modulo 29, and likewise this sequence satisfies the definition of Fibonacci sequence with respect to modulo 29. In [1], Alexandru Gica proved the following Theorem.

Theorem 1.1. *If $p > 2$ is a prime number, there exists a sequence $(a_n)_{n>0}$ such that $a_{n+2} \equiv a_{n+1} + a_n \pmod{p}$ for any positive integer n, a_n is periodic modulo p with period $\frac{p-1}{2}$ and*

$$\left\{\overline{a_n} \mid 1 \leq n \leq \frac{p-1}{2}\right\} = \left\{b^2 \mid b \in \mathbb{F}_p^*\right\}$$

if and only if

Received October 27, 2021; Accepted November 30, 2021.
2010 Mathematics Subject Classification: Primary 11B39, 11D09, 11D45; Secondary 11B37, 11J68, 11J86.
Key words and phrases: Diophantine m-tuple, Fibonacci numbers, Pell equation.
† Corresponding author.
This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2019R1G1A1006396).

1. $p \equiv 1, 4 \pmod 5$ *and*
2. *ord* $\alpha = \frac{p-1}{2}$ *or ord* $\beta = \frac{p-1}{2}$, *where* $\alpha = \frac{1+\sqrt{5}}{2}$ *and* $\beta = \frac{1-\sqrt{5}}{2}$.

In the above theorem, $\mathbb{F}_p^*$ is the multiplicative group of the field of the residues modulo p and $\overline{a_n}$ is the class of a_n modulo p. Then it is natural to ask the following problem.

Problem 1.1. Let $p > 2$ be a prime number and k be a positive integer with $k \mid p-1$. What are the conditions of the prime number p which satisfies the following statement?
There exists a sequence $(a_n)_{n\geq 1}$ such that $a_{n+2} \equiv a_{n+1} + a_n \pmod p$ for any positive integer n, a_n is periodic modulo p with period $\frac{p-1}{k}$ and

$$\{\overline{a_n} \mid n \in \mathbb{N}\} = \left\{b^k \mid b \in \mathbb{F}_p^*\right\},$$

where $\mathbb{F}_p^*$ is reduced residue system by p.

This problem is the conjecture of A. Gica in [1]. In this paper, we prove the following theorem which is the answer of the conjecture.

Theorem 1.2. *Let n be the positive integer and $p > 2$ be a prime number except 5. There exists a sequence $(a_n)_{n\geq 1}$ such that $a_{n+2} \equiv a_{n+1} + a_n \pmod p$, a_n is periodic modulo p with period $\frac{p-1}{k}$ and*

$$\left\{\overline{a_n} \mid 1 \leq n \leq \frac{p-1}{k}\right\} = \left\{b^k \mid b \in \mathbb{F}_p^*\right\}$$

if and only if the prime number p satisfies the following conditions.

1. $p \equiv \pm 1 \pmod 5$
2. *ord* $\alpha = \frac{p-1}{k}$ *or ord* $\beta = \frac{p-1}{k}$, *where* $\alpha = \frac{1+\sqrt{5}}{2}$ *and* $\beta = \frac{1-\sqrt{5}}{2}$.

This theorem can be considered as a generalization of the Theorem 1.1. In Theorem 1.2, if $\left(\frac{5}{p}\right) = 1$, then there exists a positive integer $m \leq \frac{p-1}{2}$ such that $m^2 \equiv 5$ (mod p). We denote $m = \sqrt{5}$. If $p \equiv \pm 1 \pmod 5$ and *ord* $\alpha = \frac{p-1}{k}$ or *ord* $\beta = \frac{p-1}{k}$, then two roots of the equation

$$x^2 - x - 1 = 0$$

are $x = \frac{1\pm\sqrt{5}}{2}$. Hence, $\alpha^2 \equiv \alpha + 1 \pmod p$ and $\beta^2 \equiv \beta + 1 \pmod p$. In the case of *ord* $\alpha = \frac{p-1}{k}$, if we define $a_n = \alpha^n$, then the sequence a_n safisfies the congrunece equation

$$a_{n+2} \equiv a_{n+1} + a_n \pmod p.$$

At this point, let us prove the following lemma.

Lemma 1.3. *If ord* $\gamma \mid \frac{p-1}{k}$, *then* γ *is* k*th power residue of modulo* p.

Proof. Let g be the primitive root of modulo p. Then, we can denote

$$\gamma \equiv g^c \pmod{p}.$$

Because $\gamma^{\frac{p-1}{k}} \equiv 1 \pmod{p}$, we have

$$g^{\frac{c(p-1)}{k}} \equiv 1 \pmod{p}.$$

It follows that $k \mid c$, so γ is kth power residue of modulo p. □

By Lemma 1.3, the sequence (a_n) exists as $a_n = \alpha^n$. In the case of *ord* $\beta = \frac{p-1}{k}$, the sequence (a_n) exists as $a_n = \beta^n$. Replacing the sequence $(a_n)_{n\geq 1}$ with the sequence $\left(b_n = \frac{a_n}{a_1}\right)_{n\geq 1}$ which has the same properties as the initial one, we can suppose that $a_1 = 1$ and $a_2 = x \not\equiv 1 \pmod{p}$. On the other hand, the proof of the first statement, $p \equiv \pm 1 \pmod{5}$, is similar to the proof in the previous papers(see [1, p.69] and [2, p.157]), because k is a divisor of $p-1$ and the period of the sequence (a_n) is a divisor of $p-1$.

2. The case $k \equiv 1\ (\mathbf{mod}\ 2)$.

Because the first statement of the theorem has been proved, we prove the second statement of the theorem when $k \equiv 1 (\mathrm{mod} 2)$. Because $a_1 = 1$ and $a_2 = x \not\equiv 1 \pmod{p}$, we have

$$a_{n+2} \equiv F_n + xF_{n+1} \pmod{p} \tag{2.1}$$

for all positive integers n, where (F_n) is the Fibonacci sequence.

Lemma 2.1. *If* $2 \mid \frac{p-1}{k}$ *and* $\alpha^{\frac{p-1}{k}} \equiv 1 \pmod{p}$, *then*

$$ord\ \alpha = \frac{p-1}{k} \text{ or } ord\ \beta = \frac{p-1}{k}.$$

Proof. Let us denote $d = ord\ \alpha$ in $\mathbb{F}_p^*$. Because $\alpha^{\frac{p-1}{k}} \equiv 1 \pmod{p}$, we have

$$\frac{p-1}{k} = ld$$

for some positive integer l. If $l = 1$, then we have proved the theorem. Let us suppose now that $l \geq 2$. From formula (2.1), it follows that

$$F_{n+2d} \equiv F_n \pmod{p}$$

for any positive integer n and that

$$a_{n+2d} \equiv a_n \pmod{p}$$

for any positive n. Because the period of the sequence a_n is $\frac{p-1}{k}$, it follows that $2d \geq \frac{p-1}{k} = ld$. Therefore,

$$l = 2 \quad \text{and} \quad d = \frac{p-1}{2k}.$$

If $d \equiv 0 \pmod 2$, then from formula (2.1) it follows that

$$F_{n+d} \equiv F_n \pmod p$$

for any positive integer n and that

$$a_{n+d} \equiv a_n \pmod p$$

for any positive n. Thus, the period of the sequence a_n would be smaller than $d = \frac{p-1}{2k}$, which is a contradiction, because the period of the sequence a_n is $\frac{p-1}{k}$. Therefore, d is odd. Now, we show that $ord\,\beta = \frac{p-1}{k}$. Let us denote $d_1 = ord\ \beta$ in $\mathbb{F}_p^*$. We have

$$\beta^{\frac{p-1}{k}} = \left(-\frac{1}{\alpha}\right)^{\frac{p-1}{k}} = \frac{1}{\alpha^{\frac{p-1}{k}}} \equiv 1 \pmod p \tag{2.2}$$

and so d_1 divides $\frac{p-1}{k}$. We have

$$1 \equiv \beta^{2d_1} = \left(-\frac{1}{\alpha}\right)^{2d_1} = \frac{1}{\alpha^{2d_1}} \pmod p$$

and so $\alpha^{2d_1} \equiv 1 \pmod p$ and d divides $2d_1$. Because d is odd, it follows that d divides d_1 and from (2.2), it follows that d_1 divides $\frac{p-1}{k}$. We deduce that $d_1 = \frac{p-1}{2k}$ or $d_1 = \frac{p-1}{k}$. If $d_1 = \frac{p-1}{2k}$, then

$$1 \equiv \beta^{d_1} = \left(-\frac{1}{\alpha}\right)^{d_1} = -\frac{1}{\alpha^{d_1}} \equiv -1 \pmod p,$$

which is a contradiction. Therefore, we obtain

$$d_1 = \frac{p-1}{k} = ord\ \beta$$

and we have the desired result. □

Now, we show the second statement of the theorem when $k \equiv 1 \pmod 2$.

Proof. By Lemma 2.1, it is sufficient to show that $\alpha^{\frac{p-1}{k}} \equiv 1 \pmod p$. Let us denote $c = \frac{p-1}{k}$. From formula (2.1), it follows that

$$F_{tc} \equiv \frac{1}{\sqrt{5}}\left(\alpha^{tc} - \frac{1}{\alpha^{tc}}\right) \equiv \frac{1}{\sqrt{5}}\left(\alpha^{tc} - \alpha^{(k-t)c}\right) \pmod p \tag{2.3}$$

and
(2.4)

$$F_{tc+1} \equiv \frac{1}{\sqrt{5}}\left(\alpha^{tc+1} + \frac{1}{\alpha^{tc+1}}\right) \equiv \frac{1}{\sqrt{5}}\left(\alpha^{tc+1} + \alpha^{(k-t)c-1}\right) \pmod{p}$$

for any integer t such that $1 \le t \le k-1$.

Because the sequence $(a_n)_{n\ge1}$ modulo p has period c, we have

$$x = a_2 \equiv a_{t'c+2} = F_{t'c} + xF_{t'c+1} \pmod{p}. \tag{2.5}$$

for any positive integer t'.

From formulas (2.3), (2.4) and (2.5), it follows that

$$\begin{aligned}
(k-1)\,x &\equiv \sum_{t=1}^{k-1} (F_{tc} + xF_{tc+1}) \\
&= \sum_{t=1}^{\frac{k-1}{2}} \left(F_{tc} + F_{(k-t)c} + xF_{tc+1} + xF_{(k-t)c+1}\right) \\
&\equiv \sum_{t=1}^{\frac{k-1}{2}} \frac{x}{\sqrt{5}} \left(\alpha^{tc-1} + \alpha^{tc+1} + \alpha^{(k-t)c-1} + \alpha^{(k-t)c+1}\right) \\
&= \sum_{t=1}^{\frac{k-1}{2}} x\left(\alpha^{tc} + \alpha^{(k-t)c}\right) \\
&= \sum_{t=1}^{k-1} \alpha^{tc} x \pmod{p}. \qquad (2.6)
\end{aligned}$$

Let us suppose that $\alpha^c \not\equiv 1 \pmod{p}$. Because $\alpha^{p-1} - 1 \equiv 0 \pmod{p}$, we have

$$(\alpha^c - 1)\left(\alpha^{(k-1)c} + \alpha^{(k-2)c} + \cdots + \alpha + 1\right) \equiv 0 \pmod{p}$$

and it follows that $\sum_{t=0}^{k-1} \alpha^{tc} \equiv 0 \pmod{p}$. Substituting in equation (2.6), we obtain

$$(k-1)x \equiv -x \pmod{p}.$$

Because $0 < k < p$ and $x \not\equiv 0 \pmod{p}$, this leads to a contradiction. Therefore, we proved that $\alpha^c \equiv 1 \pmod{p}$ and we finished the proof of the theorem when $k \equiv 1 \pmod{2}$. □

3. The case $k \equiv 0 \pmod 2$.

Let us suppose $k = 2^t q$, where t is a positive integer and q is an odd number. Before proving the theorem, we prove the following lemma.

LEMMA 3.1. *If* $2^t \mid p-1$, *then*

$$\alpha^{\frac{p-1}{2^{t-1}}} \equiv 1 \pmod p.$$

Proof. We first show that if $2^{t'} \mid p-1$ and $\alpha^{\frac{p-1}{2^{t'-2}}} \equiv 1 \pmod p$, then $\alpha^{\frac{p-1}{2^{t'-1}}} \equiv 1 \pmod p$. Suppose $\alpha^{\frac{p-1}{2^{t'-1}}} \equiv -1 \pmod p$. Then we have

$$F_{\frac{p-1}{2^{t'-1}}} \equiv \frac{1}{\sqrt{5}}\left(\alpha^{\frac{p-1}{2^{t'-1}}} - \frac{1}{\alpha^{\frac{p-1}{2^{t'-1}}}}\right) \equiv 0 \pmod p.$$

This means

$$F_{\frac{p-1}{2^{t'-1}}+1} \equiv \frac{1}{\sqrt{5}}\left(\alpha^{\frac{p-1}{2^{t'-1}}+1} + \frac{1}{\alpha^{\frac{p-1}{2^{t'-1}}+1}}\right) \equiv -\frac{1}{\sqrt{5}}\left(\alpha + \frac{1}{\alpha}\right) \equiv -1 \pmod p.$$

Hence,

$$x = a_2 \equiv a_{\frac{p-1}{2^{t'-1}}+2} \equiv F_{\frac{p-1}{2^{t'-1}}} + xF_{\frac{p-1}{2^{t'-1}}+1} \equiv -x \pmod p.$$

It follows that $x \equiv 0 \pmod p$, which is a contradiction. Therefore, we have $\alpha^{\frac{p-1}{2^{t'-1}}} \equiv 1 \pmod p$ when $2^{t'} \mid p-1$ and $\alpha^{\frac{p-1}{2^{t'-2}}} \equiv 1 \pmod p$. Because $\alpha^{p-1} \equiv 1 \pmod p$, we get $\alpha^{\frac{p-1}{2^{t-1}}} \equiv 1 \pmod p$ when $2^t \mid p-1$. □

We can show that $\alpha^{\frac{p-1}{q}} \equiv 1 \pmod p$ in a simliar way as when $k \equiv 1 \pmod 2$. Now, we show the second statement of the theorem when k is an even.

Proof. (1) The case $p \equiv 1 \pmod{2^{t+1}}$.

By Lemma 3.1, we have $\alpha^{\frac{p-1}{2^t}} \equiv 1 \pmod p$, and we obtain $\alpha^{\frac{p-1}{k}} \equiv 1 \pmod p$. The proof of the second statement is finished by Lemma 2.1 because $\frac{p-1}{k}$ is an even number.

(2) The case $p \equiv 2^t + 1 \pmod{2^{t+1}}$.

By Lemma 3.1, we have $\alpha^{\frac{p-1}{2^{t-1}}} \equiv 1 \pmod p$, and we obtain $\alpha^{\frac{p-1}{2^t}} \equiv \pm 1 \pmod p$. If $\alpha^{\frac{p-1}{2^t}} \equiv 1 \pmod p$, then

$$F_{\frac{p-1}{2^t}} \equiv \frac{1}{\sqrt{5}}\left(\alpha^{\frac{p-1}{2^t}} + \frac{1}{\alpha^{\frac{p-1}{2^t}}}\right) \equiv \frac{1}{\sqrt{5}}\left(\frac{1+1}{\alpha^{\frac{p-1}{2^t}}}\right) \equiv \frac{2}{\sqrt{5}} \pmod p$$

and

$$F_{\frac{p-1}{2^t}+1} \equiv \frac{1}{\sqrt{5}}\left(\alpha^{\frac{p-1}{2^t}+1} - \frac{1}{\alpha^{\frac{p-1}{2^t}+1}}\right) \equiv \frac{1}{\sqrt{5}}\left(\frac{\alpha^2-1}{\alpha^{\frac{p-1}{2^t}+1}}\right) \equiv \frac{1}{\sqrt{5}} \pmod{p}.$$

This means

$$x = a_2 \equiv a_{\frac{p-1}{2^t}+2} \equiv F_{\frac{p-1}{2^t}} + xF_{\frac{p-1+2^t}{2^t}} \equiv \frac{2}{\sqrt{5}} + \frac{1}{\sqrt{5}}x \pmod{p}.$$

Hence,

$$x \equiv \frac{2}{\sqrt{5}-1} \equiv \frac{1+\sqrt{5}}{2} \equiv \alpha \pmod{p}.$$

Therefore, $a_2 = x, a_3 = 1+x \equiv 1+\alpha \equiv \alpha^2 \pmod{p}$ and we deduce that $a_n \equiv \alpha^n \pmod{p}$ for any positive integer n by using mathematical induction. From the condition of the hypothesis, it follows that $ord\ \alpha = \frac{p-1}{k}$.

If $\alpha^{\frac{p-1}{2^t}} \equiv -1 \pmod{p}$, then

$$F_{\frac{p-1}{2^t}} \equiv \frac{1}{\sqrt{5}}\left(\alpha^{\frac{p-1}{2^t}} + \frac{1}{\alpha^{\frac{p-1}{2^t}}}\right) \equiv \frac{1}{\sqrt{5}}\left(\frac{1+1}{\alpha^{\frac{p-1}{2^t}}}\right) \equiv -\frac{2}{\sqrt{5}} \pmod{p}$$

and

$$F_{\frac{p-1}{2^t}+1} \equiv \frac{1}{\sqrt{5}}\left(\alpha^{\frac{p-1}{2^t}+1} - \frac{1}{\alpha^{\frac{p-1}{2^t}+1}}\right) \equiv \frac{1}{\sqrt{5}}\left(\frac{\alpha^2-1}{\alpha^{\frac{p-1}{2^t}+1}}\right) \equiv -\frac{1}{\sqrt{5}} \pmod{p}.$$

This means

$$x = a_2 \equiv a_{\frac{p-1}{2^t}+2} \equiv F_{\frac{p-1}{2^t}} + xF_{\frac{p-1+2^t}{2^t}} \equiv -\frac{2}{\sqrt{5}} - \frac{1}{\sqrt{5}}x \pmod{p}.$$

Hence,

$$x \equiv -\frac{2}{\sqrt{5}+1} \equiv \frac{1-\sqrt{5}}{2} \equiv \beta \pmod{p}.$$

Therefore, $a_2 = x, a_3 = 1+x \equiv 1+\beta \equiv \beta^2 \pmod{p}$ and we deduce that $a_n \equiv \beta^n \pmod{p}$ for any positive integer n by using mathematical induction. From the condition of the hypothesis, it follows that $ord\ \beta = \frac{p-1}{k}$. Hence, we have the desired result. □

REMARK 3.2. For $k=3$ and $p=139$, there exists a sequence $(a_n)_{n\geq 1}$ with initial terms $a_1 = 1, a_2 = 76$ which satisfies the definition of Fibonacci sequence with modulo 139 and (a_n) is periodic modulo 139 with period $\frac{139-1}{3} = 46$ and

$$\{\overline{a_n} \mid 1 \leq n \leq 46\} = \left\{b^3 \mid b \in \mathbb{F}_p^*\right\},$$

where $\mathbb{F}_p^*$ is reduced residue system by p.

References

[1] A. Gica, *Quaderatic Residues In Fibonacci Sequences*, Fibonacci Quart., **46/47** (2008/2009), 68–72.

[2] A. Gica and L. Panaitopol, *O Introducere n Aritmetic i Teoria Numerelor*, Bucharest University Press, Bucharest, 2001.

MSC2020: 11A15, 11B39

Youchan Chung
Institute of Science Education for the Gifted and Talented
Yonsei University
Sinchon-Dong, Seodaemun-Gu, Seoul, 03722, Korea
E-mail: ddoksooni0817@gmail.com

Eunyool Jang
Institute of Science Education for the Gifted and Talented
Yonsei University
Sinchon-Dong, Seodaemun-Gu, Seoul, 03722, Korea
E-mail: sanyp77@naver.com

Jinseo Park
Department of Mathematics Education
Catholic Kwandong University
Gangneung 25601, Republic of Korea
E-mail: jspark@cku.ac.kr

Sanghoon Park
Institute of Science Education for the Gifted and Talented
Yonsei University
Sinchon-Dong, Seodaemun-Gu, Seoul, 03722, Korea
E-mail: parksh4108@naver.com