Commun. Korean Math. Soc. **36** (2021), No. 3, pp. 401–411
https://doi.org/10.4134/CKMS.c200247
pISSN: 1225-1763 / eISSN: 2234-3024

# DIOPHANTINE TRIPLE WITH FIBONACCI NUMBERS AND ELLIPTIC CURVE

Jinseo Park

Abstract. A Diophantine $m$-tuple is a set $\{a_1, a_2, \dots, a_m\}$ of positive integers such that $a_i a_j + 1$ is a perfect square for all $1 \le i < j \le m$. Let $E_k$ be the elliptic curve induced by Diophantine triple $\{F_{2k}, 5F_{2k+2}, 3F_{2k} + 7F_{2k+2}\}$. In this paper, we find the structure of a torsion group of $E_k$, and find all integer points on $E_k$ under assumption that $\mathrm{rank}(E_k(\mathbb{Q})) = 1$ and some further conditions.

## 1. Introduction

A Diophantine $m$-tuple is a set which consists of $m$ distinct positive integers satisfying the property that the product of any two of them is one less than a perfect square. If the set which consists of rational numbers satisfy the same property, then we call it a rational Diophantine $m$-tuple. Fermat first found the Diophantine triple $\{1, 3, 8, 120\}$. Many famous mathematicians made lots of results related to the problems of a Diophantine $m$-tuple, but still there are many open problems. An old conjecture was that there does not exist a Diophantine quintuple. Recently, the conjecture has been proved by B. He, A. Togbé and V. Ziegler [11]. For any Diophantine triple $\{a, b, c\}$ with $a < b < c$, the set $\{a, b, c, d_\pm\}$ is a Diophantine quadruple, where

$$d_\pm = a + b + c + 2abc \pm 2rst$$

and $r, s, t$ are the positive integers satisfying

$$ab + 1 = r^2, \quad ac + 1 = s^2, \quad bc + 1 = t^2.$$

The strong version of the conjecture states that if $\{a, b, c, d\}$ is a Diophantine quadruple and $d > \max\{a, b, c\}$, then $d = d_+$. These Diophantine quadruples are called regular.

Received July 16, 2020; Revised October 22, 2020; Accepted January 12, 2021.
2010 *Mathematics Subject Classification.* Primary 11B39, 11G05, 11D09; Secondary 11D45.
*Key words and phrases.* Diophantine $m$-tuple, Fibonacci numbers, elliptic curve.
This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2019R1G1A1006396).

©2021 Korean Mathematical Society

In 1969, A. Baker and H. Davenport [1] proved that the Diophantine triple $\{1,3,8\}$ is regular, which implies that it cannot be extended to a quintuple and not the other way round. In 1998, A. Dujella and A. Pethö [8] proved that if the set $\{1,3,c_k\}$ is the Diophantine triple, where

$$c_k = \frac{1}{6}[(2+\sqrt{3})(7+4\sqrt{3})^k + (2-\sqrt{3})(7-4\sqrt{3})^k - 4],$$

then there are only two numbers $c_{k-1}$ and $c_{k+1}$ which make the set $\{1,3,c_k\}$ to the Diophantine quadruple.

Let $F_n$ be the $n$-th Fibonacci number, defined by $F_0 = 0, F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$. In 1977, V. E. Hoggatt and G. E. Bergum [12] conjectured that if $\{F_{2k}, F_{2k+2}, F_{2k+4}, d\}$ is a Diophantine quadruple, then $d$ is a unique. The conjecture was proved by Dujella [4] in 1999. There are many papers which contain generalizations of the result of Hoggatt and Bergum [7,10,16]. The reason why the extendibility is important is related to the elliptic curves. We should solve the equations

$$ax+1=\square,\ bx+1=\square,\ cx+1=\square$$

to extend the Diophantine triple $\{a,b,c\}$ to a Diophantine quadruple. This leads naturally to the following elliptic curve

$$y^2 = (ax+1)(bx+1)(cx+1).$$

Then we have always integer points

$$(0,\pm1),\ (d_+, \pm(at+rs)(bs+rt)(cr+st)),\ (d_-, \pm((at-rs)(bs-rt)(cr-st))),$$

and also $(-1,0)$ if $1 \in \{a,b,c\}$. Dujella [5] proved that the elliptic curve

$$E: y^2 = ((k-1)x+1)((k+1)x+1)(4kx+1)$$

has four integer points

$$(0,\pm1),\ (16k^3-4k, \pm(128k^6-112k^4-20k^2-1))$$

under assumption that $\text{rank}(E(\mathbb{Q})) = 1$. In [18], the author found all integer points on the elliptic curve

$$y^2 = (F_{2k}x+1)(F_{2k+2}x+1)(4F_{2k+1}F_{2k+2}F_{2k+3}x+1)$$

under assumption that the rank of the elliptic curve is 2. There are various papers which contain similar results [6,9,10].

In this paper, we find the structure of the torsion subgroup of

$$E_k: y^2 = (F_{2k}x+1)(5F_{2k+2}x+1)((3F_{2k}+7F_{2k+2})x+1)$$

and find all integer points on the $E_k$ under assumption that $\text{rank}(E_k(\mathbb{Q})) = 1$ and $k$ is a positive even integer with $k \not\equiv 4 \pmod 6$. It is obvious that every solution of system

$$F_{2k}x+1=\square,\quad 5F_{2k+2}x+1=\square,\quad (3F_{2k}+7F_{2k+2})x+1=\square \tag{1.1}$$

induce an integer point on the elliptic curve $E_k$. The aim of this paper is to prove that the converse of this statement, that is the $x$-coordinates of all integer points on $E_k$ satisfy the system (1.1) under the same conditions.

## 2. Preliminaries

### 2.1. Points on the elliptic curve

Let $\{a, b, c\}$ be a Diophantine triple. We should solve the system

$$ax + 1 = \square, \quad bx + 1 = \square, \quad cx + 1 = \square \tag{2.1}$$

to extend the Diophantine triple to a Diophantine quadruple. According to this system, we have the following elliptic curve

$$E : y^2 = (ax + 1)(bx + 1)(cx + 1).$$

There are two obvious rational points

$$P = (0, 1), \quad R = \left(\frac{1}{abc}, \frac{rst}{abc}\right),$$

where $r = \sqrt{ab + 1}$, $s = \sqrt{ac + 1}$ and $t = \sqrt{bc + 1}$. Then we wonder which points on $E$ satisfy the system (2.1). We get the answer by the following Propositions.

**Proposition 2.1** ([6, Proposition 1]). *The $x$-coordinate of the point $T \in E(\mathbb{Q})$ satisfies* (2.1) *if and only if $T - P \in 2E(\mathbb{Q})$.*

The following Proposition is called 2-descent proposition which can confirm $T \in 2E(\mathbb{Q})$.

**Proposition 2.2** ([13, 4.1, p. 37], [15, 4.2, p. 85]). *Let $P = (x', y')$ be a $\mathbb{Q}$-rational point on $E$, an elliptic curve over $\mathbb{Q}$ given by*

$$y^2 = (x - \alpha)(x - \beta)(x - \gamma),$$

*where $\alpha, \beta, \gamma \in \mathbb{Q}$. Then there exists a $\mathbb{Q}$-rational point $Q = (x, y)$ on $E$ such that $2Q = P$ if and only if $x' - \alpha, x' - \beta, x' - \gamma$ are all $\mathbb{Q}$-rational squares.*

### 2.2. Structure of torsion group

Let $E_{\mathbb{Q}}(M, N)$ be the elliptic curve defined by

$$y^2 = x^3 + (M + N)x^2 + MNx.$$

Then we can find that the torsion group is classified according to the following Theorem.

**Theorem 2.3** ([17, Main Theorem 1]). *The torsion subgroups of $E_{\mathbb{Q}}(M, N)$ are uniquely determined by:*

- *The torsion subgroup of $E_{\mathbb{Q}}(M, N)$ contains $\mathbb{Z}_2 \times \mathbb{Z}_4$ if $M$ and $N$ are both squares, or $-M$ and $N - M$ are both squares, or if $-N$ and $M - N$ are both squares.*

- *The torsion subgroup of* $E_{\mathbb{Q}}(M,N)$ *is* $\mathbb{Z}_2\times\mathbb{Z}_8$ *if there exists a non-zero integer* $d$ *such that* $M=d^2u^4$ *and* $N=d^2v^4$*, or* $M=-d^2v^4$ *and* $N=d^2(u^4-v^4)$*, or* $M=d^2(u^4-v^4)$ *and* $N=-d^2v^4$ *where* $(u,v,w)$ *forms a Pythagorean triple (i.e.,* $u^2+v^2=w^2$*).*
- *The torsion subgroup of* $E_{\mathbb{Q}}(M,N)$ *is* $\mathbb{Z}_2\times\mathbb{Z}_6$ *if there exist integers* $a$ *and* $b$ *such that*
$$\frac{a}{b}\notin\{-2,-1,-\frac{1}{2},0,1\}$$
*and* $M=a^4+2a^3b$ *and* $N=2ab^3+b^4$.
- *In all other cases, the torsion subgroup of* $E_{\mathbb{Q}}(M,N)$ *is* $\mathbb{Z}_2\times\mathbb{Z}_2$.

The coordinate transformation
$$x\to\frac{x}{abc},\quad y\to\frac{y}{abc}$$
applied on the curve $E$ leads to the elliptic curve
$$E':y^2=(x+bc)(x+ac)(x+ab).$$
The following Theorem is more specific to find the structure of a torsion group.

**Theorem 2.4** ([6, Theorem 2])**.** $E'(\mathbb{Q})_{tors}\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ *or* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$.

## 3. Torsion group on elliptic curve

Let $E_k$ be the elliptic curve induced by Diophantine triple
$$\{F_{2k},5F_{2k+2},3F_{2k}+7F_{2k+2}\},$$
that is
$$E_k:y^2=(F_{2k}x+1)(5F_{2k+2}x+1)(3F_{2k}+7F_{2k+2}x+1).$$
Then we have the elliptic curve
$$E_k':y^2=(x+5F_{2k+2}(3F_{2k}+7F_{2k+2}))(x+F_{2k}(3F_{2k}+7F_{2k+2}))(x+5F_{2k}F_{2k+2})$$
by coordinate transformation
$$x\to\frac{x}{5F_{2k}F_{2k+2}(3F_{2k}+7F_{2k+2})},\quad y\to\frac{y}{5F_{2k}F_{2k+2}(3F_{2k}+7F_{2k+2})}.$$
Using Theorem 2.3 and Theorem 2.4, we can find the structure of torsion group of $E_k'$.

**Lemma 3.1.** *The torsion group of* $E_k'$ *is isomorphic to* $\mathbb{Z}_2\times\mathbb{Z}_2$*, that is*
$$E_k'(\mathbb{Q})_{tors}\cong\mathbb{Z}_2\times\mathbb{Z}_2.$$

*Proof.* It is sufficient to show that there do not exist $\alpha$ and $\beta$ such that
$$\frac{\alpha}{\beta}\notin\{-2,-1,-\frac{1}{2},0,1\},$$
$$M=F_{2k}(3F_{2k}+2F_{2k+2})=\alpha^4+2\alpha^3\beta$$

and

$$N = 5F_{2k+2}(2F_{2k} + 7F_{2k+2}) = 2\alpha\beta^3 + \beta^4.$$

Then we have

$$M + N = (\alpha^2 + \alpha\beta + \beta^2)^2 - 3\alpha^2\beta^2. \tag{3.1}$$

Since

$$F_{2k} \equiv \begin{cases} 0 \pmod 8 & \text{if } k \equiv 0 \pmod 6, \\ 1 \pmod 8 & \text{if } k \equiv 1 \pmod 6, \\ 3 \pmod 8 & \text{if } k \equiv 2 \pmod 6, \\ 0 \pmod 8 & \text{if } k \equiv 3 \pmod 6, \\ 5 \pmod 8 & \text{if } k \equiv 4 \pmod 6, \\ 7 \pmod 8 & \text{if } k \equiv 5 \pmod 6, \end{cases}$$

the left side of (3.1) is congruent to 2 or 3 modulo 8. However, the right side is congruent to $0, 1, 5$ or 6 modulo 8. Therefore,

$$E'_k(\mathbb{Q})_{tors} \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

□

There are integer points on $E'_k$ such that

$$A'_k = (-5F_{2k+2}(3F_{2k} + 7F_{2k+2}), 0), \ B'_k = (-F_{2k}(3F_{2k} + 7F_{2k+2}), 0),$$

and

$$C'_k = (-5F_{2k}F_{2k+2}, 0)$$

of order 2, and the obvious integer point

$$P'_k = (0, 5F_{2k}F_{2k+2}(3F_{2k} + 7F_{2k+2})).$$

Hence, we have the following results.

**Corollary 3.2.** $E'_k(\mathbb{Q})_{tors} = \{O, A'_k, B'_k, C'_k\}$ *and* $rank(E'_k(\mathbb{Q})) \geq 1$.

*Proof.* The point $P'_k$ is not finite order. Hence, $\text{rank}(E'_k(\mathbb{Q})) \geq 1$ by Lemma 3.1. □

## 4. Integer points on $E_k$

Using Proposition 2.2, we find all integer points on $E'_k$ under the assumption that $\text{rank}(E'_k(\mathbb{Q})) = 1$ and some further conditions.

**Lemma 4.1.** $P'_k, P'_k + A'_k, P'_k + B'_k, P'_k + C'_k \notin 2E'_k(\mathbb{Q})$.

*Proof.* We have

$$\begin{aligned} x(P'_k) &= 0, \\ x(P'_k + A'_k) &= -F_{2k}(2F_{2k} + 12F_{2k+2}), \\ x(P'_k + B'_k) &= -5F_{2k+2}(4F_{2k} + 2F_{2k+2}), \\ x(P'_k + C'_k) &= 2(F_{2k} + F_{2k+2})(3F_{2k} + 7F_{2k+2}). \end{aligned}$$

(1) The case $P_k'$.
If $P_k' \in 2E(\mathbb{Q})$, then the numbers

$$\begin{cases} 5F_{2k}F_{2k+2}, \\ F_{2k}(3F_{2k}+7F_{2k+2}), \\ 5F_{2k+2}(3F_{2k}+7F_{2k+2}) \end{cases}$$

are all squares.

(a) For $k \equiv 0 \pmod 3$, $5F_{2k+2}(3F_{2k}+7F_{2k+2})$ is congruent to 3 modulo 4. So, this number cannot be a square.
(b) For $k \equiv 1 \pmod 3$, $5F_{2k}F_{2k+2}$ is congruent to 3 modulo 4, which means this number cannot be a square.
(c) For $k \equiv 2 \pmod 3$, $F_{2k}(3F_{2k}+7F_{2k+2})$ is congruent to 3 modulo 4. Therefore, this number cannot be a square.

Hence, we have $P_k' \notin 2E(\mathbb{Q})$.
(2) The case $P_k' + A_k'$.
Suppose that $P_k' + A_k' \in 2E(\mathbb{Q})$. Then the numbers

$$\begin{cases} -2F_{2k}^2 + 3F_{2k}F_{2k+2} + 35F_{2k+2}^2, \\ F_{2k}^2 - 5F_{2k}F_{2k+2}, \\ -2F_{2k}^2 - 7F_{2k}F_{2k+2} \end{cases}$$

are all squares, but there is a contradiction by following results.

(a) For $k \equiv 0 \pmod 3$, $-2F_{2k}^2 + 3F_{2k}F_{2k+2} + 35F_{2k+2}^2$ is congruent to 3 modulo 4. This means this number cannot be a square.
(b) For $k \equiv 1 \pmod 3$, $F_{2k}^2 - 5F_{2k}F_{2k+2}$ is congruent to 2 modulo 4. This means this number cannot be a square.
(c) For $k \equiv 2 \pmod 3$, $-2F_{2k}^2 - 7F_{2k}F_{2k+2}$ is congruent to 2 modulo 4. This means this number cannot be a square.

Hence, we have $P_k' + A_k' \notin 2E(\mathbb{Q})$.
(3) The case $P_k' + B_k'$.
Assume that $P_K' + B_k' \in 2E(\mathbb{Q})$. Then we have

$$\begin{cases} 5F_{2k+2}(-F_{2k}+5F_{2k+2}), \\ 3F_{2k}^2 - 13F_{2k}F_{2k+2} - 10F_{2k+2}^2, \\ -15F_{2k}F_{2k+2} - 10F_{2k+2} \end{cases}$$

are all squares.

(a) For $k \equiv 0 \pmod 3$, $3F_{2k}^2 - 13F_{2k}F_{2k+2} - 10F_{2k+2}^2$ is congruent 2 modulo 4. Hence, this number cannot be a square.
(b) For $k \equiv 1, 2 \pmod 3$, $5F_{2k+2}(-F_{2k}+5F_{2k+2})$ is congruent to 2 modulo 4. Hence, this number also cannot be a square.

Hence, we have $P_K' + B_k' \notin 2E(\mathbb{Q})$.

(4) The case $P'_k + C'_k$.
Suppose that $P'_k + C'_k \in 2E(\mathbb{Q})$. Then we have

$$\begin{cases} (3F_{2k}+7F_{2k+2})(2F_{2k}+7F_{2k+2}), \\ (3F_{2k}+7F_{2k+2})(3F_{2k}+2F_{2k+2}), \\ 6F_{2k}^2+25F_{2k}F_{2k+2}+14F_{2k+2}^2 \end{cases}$$

are all squares. Let us find a contradiction for each cases of $k$. For $k \equiv 0, 2 \pmod 3$ and $k \equiv 1 \pmod 3$, the number

$$6F_{2k}^2+25F_{2k}F_{2k+2}+14F_{2k+2}^2$$

is congruent to 2 and 3 modulo 4, respectively. Hence, this number cannot be a square. This means $P'_k + C'_k \notin 2E(\mathbb{Q})$. Therefore, we proved the lemma. $\square$

Let $E'_k(\mathbb{Q})/E'_k(\mathbb{Q})_{tors} = \langle U \rangle$ and $X \in E'_k(\mathbb{Q})$. Then we can represent $X$ in the form $X = mU + T$, where $m$ is an integer and $T$ is a torsion point, that is $T \in \{O, A'_k, B'_k, C'_k\}$. Similarly, $P'_k = m_P U + T_P$ for an integer $m_P$ and a torsion point $T_P \in \{O, A'_k, B'_k, C'_k\}$. By Lemma 4.1, $m_P$ is an odd. Therefore, we have $X \equiv X_1 \pmod{2E'_k(\mathbb{Q})}$, where

$$X_1 \in \mathcal{S} = \{O, A'_k, B'_k, C'_k, P'_k, P'_k + A'_k, P'_k + B'_k, P'_k + C'_k\}.$$

Let $\{a, b, c\} = \{F_{2k}, 5F_{2k+2}, 3F_{2k}+7F_{2k+2}\}$. By [15, 4.6, p. 89], the function $\varphi : E'_k(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ defined by

$$\varphi(X) = \begin{cases} (x+bc)\mathbb{Q}^{*2} & \text{if} \quad X = (x,y) \neq O, (-bc, 0), \\ (ac-bc)(ab-bc)\mathbb{Q}^{*2} & \text{if} \quad X = (-bc, 0), \\ \mathbb{Q}^{*2} & \text{if} \quad X = O \end{cases}$$

is a group homomorphism. All integer points have the form $X = X_1 + 2X_2$, where $X_1 \in \mathcal{S}$. Since $\varphi$ is a homomorphism, we have

$$\varphi(X) = \varphi(X_1).$$

It means that

$$(abcu + ab)(abcu_1 + ab) = \square,$$
$$(abcu + ac)(abcu_1 + ac) = \square,$$
$$(abcu + bc)(abu_1 + bc) = \square,$$

where $X = (abcu, abcv), X_1 = (abcu_1, abcv_1)$. Hence, if

$$au_1 + 1 = \alpha\square, \ bu_1 + 1 = \beta\square, \ cu_1 + 1 = \gamma\square,$$

then

$$au + 1 = \alpha\square, \ bu + 1 = \beta\square, \ cu + 1 = \gamma\square.$$

Thus, it suffice to solve the systems induced by points $X_1$, since all other points $X$ induce the same systems. More precisely, we should solve in integers all systems of the form

$$(4.1) \quad F_{2k}x + 1 = \alpha\square, \quad 5F_{2k+2}x + 1 = \beta\square, \quad (3F_{2k}+7F_{2k+2})x + 1 = \gamma\square,$$

where for $X_1 = (5F_{2k}F_{2k+2}(3F_{2k}+7F_{2k+2})u, 5F_{2k}F_{2k+2}(3F_{2k}+7F_{2k+2})v) \in \mathcal{S}$, the numbers $\alpha, \beta, \gamma$ are defined by

$$\alpha = F_{2k}u + 1, \quad \beta = 5F_{2k+2}u + 1, \quad \gamma = (3F_{2k} + 7F_{2k+2})u + 1$$

if all of these three expressions are nonzero, and satisfy the following condition.

$$\begin{cases} \alpha = \beta\gamma & \text{if} \quad F_{2k}u + 1 = 0, \\ \beta = \alpha\gamma & \text{if} \quad 5F_{2k+2}u + 1 = 0, \\ \gamma = \alpha\beta & \text{if} \quad (3F_{2k} + 7F_{2k+2})u + 1 = 0. \end{cases}$$

Using these facts, we get the following theorem.

**Theorem 4.2.** *Let $k$ be a positive even integer and $k \not\equiv 4 \pmod 6$. If Diophantine pair $\{F_{2k}, 5F_{2k+2}\}$ is regular and the rank of elliptic curve*

$$E_k : y^2 = (F_{2k}x + 1)(5F_{2k+2}x + 1)((3F_{2k} + 7F_{2k+2})x + 1)$$

*is 1, then the $x$-coordinates of all integer points on $E_k$ are given by*

$$x \in \{-1,\ 0,\ d_+\},$$

*where $d_+ = 4(F_{2k}(F_{2k}^2 + 1) + 3F_{2k+2}(F_{2k+2}^2 + 1) + F_{2k}F_{2k+2}(15F_{2k} + 27F_{2k+2}))$.*

*Proof.* First, let us consider that for $X_1 = P'_k$. Then we obtain the system

$$F_{2k}x + 1 = \Box, \quad 5F_{2k+2}x + 1 = \Box, \quad (3F_{2k} + 7F_{2k+2})x + 1 = \Box.$$

This system is solved by regularity of Diophantine pair $\{F_{2k}, 5F_{2k+2}\}$. Hence, we have to prove that the system (4.1) has no integer solution for $X_1 \in \mathcal{S}\backslash\{P'_k\}$. For $X_1 = \{A'_k, B'_k, P'_k + A'_k, P'_k + B'_k\}$ exactly two of the numbers $\alpha, \beta, \gamma$ are negative and accordingly the system (4.1) has no integer solution. Therefore, we have to check three cases, that is $X_1 = \{O, C'_k, P'_k + C'_k\}$. Here, $N''$ denotes the square-free part of $N$ and $N''' = \min\{|N''|, |2N|''\}$.

• The case $X_1 = O$.

For $X_1 = O$, the system (4.1) becomes

$$\begin{cases} F_{2k}x + 1 = 5F_{2k+2}(3F_{2k} + 7F_{2k+2})\Box, \\ 5F_{2k+2}x + 1 = F_{2k}(3F_{2k} + 7F_{2k+2})\Box, \\ (3F_{2k} + 7F_{2k+2})x + 1 = 5F_{2k}F_{2k+2}\Box. \end{cases}$$

From the second and third equations, we see that $F''_{2k}$ divides $7(5F_{2k+2}x + 1) - 5((3F_{2k} + 7F_{2k+2})x + 1)$. It means that $F''_{2k}$ divides 2, so, $F_{2k}$ is a square or twice a square. In [2], J. H. E. Cohn proved that the Fibonacci number $F_n$ can be a square or twice of a square when only $n = 0, 1, 2, 12$ or $n = 0, 3, 6$, respectively. In our situation, the only possible cases are $F_{2k} = 1, 8$ and 144.

(1) The case $F_{2k} = 1$.
We obtain the system

$$\begin{cases} x + 1 = 5 \cdot 3 \cdot 24\Box, \\ 15x + 1 = 24\Box, \\ 24x + 1 = 15\Box. \end{cases}$$

The left side of third equation is congruent to 1 modulo 8, but the right side is congruent to 0, 4 and 7 modulo 8. Therefore, we get a contradiction.

(2) The case $F_{2k} = 8$.
We obtain the system

$$\begin{cases} 8x + 1 = 105 \cdot 171\Box, \\ 105x + 1 = 8 \cdot 171\Box, \\ 171x + 1 = 8 \cdot 105\Box. \end{cases}$$

The left side of first equation is congruent to 1 modulo 8, but the right side is congruent to 0, 3 and 4 modulo 8. Therefore, we get a contradiction.

(3) The case $F_{2k} = 144$.
We obtain the system

$$\begin{cases} 144x + 1 = 1885 \cdot 3071\Box, \\ 1885x + 1 = 144 \cdot 3071\Box, \\ 3071x + 1 = 144 \cdot 1885\Box. \end{cases}$$

The left side of first equation is congruent to 1 modulo 8, but the right side is congruent to 0, 3 and 4 modulo 8. Therefore, we get a contradiction.

• The case $X_1 = C'_k$.

Let $a = F_{2k}, b = 5F_{2k+2}, c = 3F_{2k} + 7F_{2k+2}$. Then the system (4.1) for $X_1 = C'_k$ becomes

$$\begin{cases} ax + 1 = c(c-a)\Box, \\ bx + 1 = c(c-b)\Box, \\ cx + 1 = (c-a)(c-b)\Box. \end{cases}$$

Assume that a prime $p$ divides $c''$ and $(c-a)''$. Then we have $p \mid (c-b)''$ from the third equation. Therefore, we have $p$ divides $a, b$ and $c$. From the equation $c = a + b + 2r$ with $r = \sqrt{ab+1}$, we obtain $p \mid 2r$. Now from $2ab + 2 = 2r^2$ it follows that $p = 2$. Hence, we proved that

$$\gcd(c'', (c-a)'') = 1 \text{ or } 2$$

and in the similar manner, we can prove that

$$\gcd(c'', (c-b)'') = 1 \text{ or } 2 \quad \text{and} \quad \gcd((c-a)'', (c-b)'') = 1 \text{ or } 2.$$

Since $c'''$ divides $b - a = c - 2s$, where $s = \sqrt{ac+1}$ and $2ac + 2 = 2s^2$, we have $c''' \mid 2$. This implies $c = 3F_{2k} + 7F_{2k+2}$ is a square or twice a square. First, let us consider the case $k \equiv 0 \pmod 3$. Then

$$c = 3F_{2k} + 7F_{2k+2} \equiv 3 \pmod 4.$$

This means $c = 3F_{2k} + 7F_{2k+2}$ cannot be a square or twice a square. Therefore, we may assume that $k$ is not divisible by 3. Let $L_n$ be the $n$-th Lucas number, defined by $L_0 = 2, L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$. We may use the following congruence equation

$$F_{n+2k} \equiv -F_n \pmod{L_k} \quad \text{if} \quad 2 \mid k, 3 \nmid k.$$

From the above congruence equation, we have

$$F_{2k} \equiv -F_0 = 0 \pmod{L_k},$$
$$F_{2k+2} \equiv -F_2 = -1 \pmod{L_k}.$$

Therefore, $c = 3F_{2k} + 7F_{2k+2} \equiv -7 \pmod{L_k}$, but $-7$ is non-residue of $L_k$ by [14]. Hence, $c = 3F_{2k} + 7F_{2k+2}$ cannot be a square.

Lastly, $c$ can be an even number only if $k \equiv 1 \pmod 3$, which contradicts $k \not\equiv 4 \pmod 6$. Therefore, $c$ also cannot be twice a square.

• The case $X_1 = P'_k + C'_k$.

For $X_1 = P'_k + C'_k$ the system (4.1) becomes

$$\begin{cases} F_{2k}x + 1 = 5F_{2k+2}(2F_{2k} + 7F_{2k+2})\Box, \\ 5F_{2k+2}x + 1 = F_{2k}(3F_{2k} + 2F_{2k+2})\Box, \\ (3F_{2k} + 7F_{2k+2})x + 1 = 5F_{2k}F_{2k+2}(2F_{2k} + 7F_{2k+2})(3F_{2k} + 2F_{2k+2})\Box. \end{cases}$$

By the second and third equations, $F''_{2k}$ divides $7(5F_{2k+2}x + 1) - 5((3F_{2k} + 7F_{2k+2})x + 1)$. Therefore, $F''_{2k}$ is 1 or 2. Similarly as the case $X_1 = O$, we obtain a contradiction. □

*Remark* 4.3. As coefficients of $E_k$ grow exponentially, computation of the rank of $E_k$ for large $k$ is difficult. The following values of rank$(E_k(\mathbb{Q}))$ are computed using the programs **SIMATH**([19]) and *mwrank*([3]).

TABLE 1. Results from rank $(E_k(\mathbb{Q}))$ for small $k$

| Case of $k$ | $E_k(\mathbb{Q})$ | rank$(E_k(\mathbb{Q}))$ |
|---|---|---|
| $k = 1$ | $y^2 = 360x^3 + 399x^2 + 40x + 1$ | 1 |
| $k = 2$ | $y^2 = 7800x^3 + 2915x^2 + 108x + 1$ | 2 |
| $k = 3$ | $y^2 = 143640x^3 + 20163x^2 + 284x + 1$ | 1 |
| $k = 4$ | $y^2 = 2587200x^3 + 138383x^2 + 744x + 1$ | 1 |
| $k = 5$ | $y^2 = 46450800x^3 + 948675x^2 + 1948x + 1$ | 3 |

## References


[1] A. Baker and H. Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, Quart. J. Math. Oxford Ser. (2) **20** (1969), 129–137. https://doi.org/10.1093/qmath/20.1.129

[2] J. H. E. Cohn, *Square Fibonacci Numbers, etc*, Fibonacci Quart. **2** (1964), 109–113.

[3] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, second edition, Cambridge University Press, Cambridge, 1997.

[4] A. Dujella, *A proof of the Hoggatt-Bergum conjecture*, Proc. Amer. Math. Soc. **127** (1999), no. 7, 1999–2005. https://doi.org/10.1090/S0002-9939-99-04875-3

[5] ______, *A parametric family of elliptic curves*, Acta Arith. **94** (2000), no. 1, 87–101. https://doi.org/10.4064/aa-94-1-87-101

[6] ______, *Diophantine m-tuples and elliptic curves*, J. Théor. Nombres Bordeaux **13** (2001), no. 1, 111–124.

[7] ______, *Diophantine quadruples and Fibonacci numbers*, Bull. Kerala Math. Assoc. **1** (2004), no. 2, 133–147.

[8] A. Dujella and A. Pethő, *A generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford Ser. (2) **49** (1998), no. 195, 291–306. https://doi.org/10.1093/qjmath/49.195.291

[9] ______, *Integer points on a family of elliptic curves*, Publ. Math. Debrecen **56** (2000), no. 3-4, 321–335.

[10] Y. Fujita, *The Hoggatt-Bergum conjecture on $D(-1)$-triples $\{F_{2k+1}, F_{2k+3}, F_{2k+5}\}$ and integer points on the attached elliptic curves*, Rocky Mountain J. Math. **39** (2009), no. 6, 1907–1932. https://doi.org/10.1216/RMJ-2009-39-6-1907

[11] B. He, A. Togbé, and V. Ziegler, *There is no Diophantine quintuple*, Trans. Amer. Math. Soc. **371** (2019), no. 9, 6665–6709. https://doi.org/10.1090/tran/7573

[12] V. E. Hoggatt, Jr., and G. E. Bergum, *A problem of Fermat and the Fibonacci sequence*, Fibonacci Quart. **15** (1977), no. 4, 323–330.

[13] D. Husemoller, *Elliptic Curves*, Graduate Texts in Mathematics, 111, Springer-Verlag, New York, 1987. https://doi.org/10.1007/978-1-4757-5119-2

[14] A. Kim, *Square Fibonacci numbers and square Lucas numbers*, Asian Res. J. Math. **3** (2017), no. 3, 1–8.

[15] A. W. Knapp, *Elliptic curves*, Mathematical Notes, 40, Princeton University Press, Princeton, NJ, 1992.

[16] J. Morgado, *Generalization of a result of Hoggatt and Bergum on Fibonacci numbers*, Portugal. Math. **42** (1983/84), no. 4, 441–445.

[17] K. Ono, *Euler's concordant forms*, Acta Arith. **78** (1996), no. 2, 101–123. https://doi.org/10.4064/aa-78-2-101-123

[18] J. Park, *Integer points on the elliptic curves induced by Diophantine triples*, Commun. Korean Math. Soc. **35** (2020), no. 3, 745–757. https://doi.org/10.4134/CKMS.c190364

[19] SIMATH manual, Saarbrücken, 1997

Jinseo Park
Department of Mathematics Education
Catholic Kwandong University
Gangneung 25601, Korea
*Email address*: jspark@cku.ac.kr