RELATION BETWEEN DIOPHANTINE TRIPLE AND ELLIPTIC CURVE

Jinseo Park

ABSTRACT. A set $\{a_1, a_2, \ldots, a_m\}$ of positive integers is called Diophantine m-tuple if $a_i a_j + 1$ is a perfect square for all $1 \leq i < j \leq m$. In this paper, we find the structure of torsion group of elliptic curve E_k constructed by Diophantine triple, and find all integer points on E_k under assumption that $\text{rank}(E_k(\mathbb{Q})) = 1$.

1. Introduction

A Diophantine m-tuple is a set of m distinct positive integers with the property that the product of any two of its distinct elements is one less than a square. For example, the first Diophantine quadruple $\{1, 3, 8, 120\}$ was found by Fermat[2]. We can easily find that the set satisfies the property, indeed

$$1 \cdot 3 + 1 = 2^2, \quad 1 \cdot 8 + 1 = 3^2, \quad 1 \cdot 120 + 1 = 11^2,$$
$$3 \cdot 8 + 1 = 5^2, \quad 3 \cdot 120 + 1 = 19^2, \quad 8 \cdot 120 + 1 = 31^2.$$

For the rational case, Diophantus first found that the set

$$\{1/16, 33/16, 17/4, 105/16\}$$

satisfies the same property. If a set of nonzero rationals has the same property then it is called rational Diophantine m-tuple. Euler found that the Fermat's set is extended to rational Diophantine quintuple

$$\{1, 3, 8, 120, 777480/8288641\}.$$

There are lots of papers related to Diophantine m-tuple, but we have many problems which still remain open. The most interesting subject is the extendibility of Diophantine m-tuple.

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

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

A folklore conjecture was that there does not exist a Diophantine quintuple. Recently, the conjecture has been proved by He, Togbé and Ziegler [10]. The strong version of this 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. Recently, He, Pu, Shen and Togbé proved the regularity of Diophantine quadruple

$$\{k, 4k + 4\epsilon, c, d\},$$

where $\epsilon = \{\pm 1\}$ in [9].

The reason why the extendibility should be considered is related to the elliptic curves. We must solve the equations

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

to extend the the Diophantine triple $\{a, b, c\}$ to Diophantine quadruple. According to these three equations, we have the elliptic curve

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

Then we have always the integer points

$$(0, \pm 1), \ (d_+, \pm(at+rs)(bs+rt)(cr+st)), \ (d_-, \pm((at-rs)(bs-rt)(cr-st))),$$

and also $(-1, 0)$ if $1 \in \{a, b, c\}$. The non-extendiblity of Diophantine m-tuple suggests that there are no other integer points on E. Let us consider the Diophantine pair $\{1, 3\}$. If the set $\{1, 3, c\}$ is a Diophantine triple then the third element c should have the form

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

Dujella and Pethö[5] proved that the elliptic curve

$$E_k : y^2 = (x + 1)(3x + 1)(c_k x + 1)$$

has integer points

$$x \in \{-1, 0, c_{k-1}, c_{k+1}\}$$

under assumption that $\mathrm{rank}(E_k(\mathbb{Q})) = 2$. There are various papers which contain the similar results [3, 4, 6, 8, 14, 15, 16]. Hence, it is important not only how to prove the extendibility of Diophantine m-tuple but also which case of Diophantine m-tuple is proved.

It is obvious that every solution of system

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

induces an integer point on the elliptic curve E. It is natural to ask which points on the curve satisfy the original system of equations and give extensions to Diophantine quadruples. The purpose of this paper is to prove that the converse of this statement is true under some conditions. Actually, we find the structure of torsion subgroup and all integer points on the elliptic curves

$$y^2 = (kx + 1)((4k + 4)x + 1)((9k + 6)x + 1)$$

under assumption that the rank of elliptic curve is 1.

2. Preliminaries

2.1. The form of third element in the Diophantine triple

Let $\{a, b, c\}$ be a Diophantine triple, and r, s, t be the positive integers satisfying $ab + 1 = r^2$, $ac + 1 = s^2$, $bc + 1 = t^2$. Then we have the equation

$$at^2 - bs^2 = a - b.$$

Let ν be a positive integer. The solution of equation above is

$$(t\sqrt{a} + s\sqrt{b}) = (t_0\sqrt{a} + s_0\sqrt{b})(r + \sqrt{bc})^\nu.$$

If (t_0, s_0) belongs to the same class as either of the solutions $(\pm 1, 1)$ then s can be expressed as $s = s_\nu^\tau$, where $\tau \in \{\pm 1\}$ and

$$s_0 = s_0^\tau = 1, \ s_1^\tau = r + \tau a, \ s_{\nu+2}^\tau = 2r s_{\nu+1}^\tau - s_\nu^\tau.$$

Define $c_\nu^\tau = ((s_\nu^\tau)^2 - 1)/a$. Then, we obtain

$$c = c_\nu^\tau = \frac{1}{4ab}[(a + b + 2\tau\sqrt{ab})(2ab + 1 + 2r\sqrt{ab})^\nu$$
$$+ (a + b - 2\tau\sqrt{ab})(2ab + 1 - 2r\sqrt{ab})^\nu - 2(a + b)].$$

Let us consider the form of third element c in the Diophantine triple $\{a, b, c\}$.

LEMMA 2.1. [7, Lemma 4.1] *Let $\{a, b, c\}$ be a Diophantine triple. Assume that $a < b \leq 8a$. Then $c = c_\nu^\tau$ for some ν and τ.*

According to Lemma 2.1 and regularity of Diophantine quadruple $\{k, 4k + 4\epsilon, c, d\}$, if $\{k, 4k + 4, c, d\}$ is a Diophantine quadruple with $c < d$ then d has to be d_+. Recently, the upper bound of b is more generalized. The following lemma is the result.

LEMMA 2.2. [13, Lemma 3.1] *Let $\{a, b, c\}$ be a Diophantine triple and $a < b \leq 24a$. Suppose that $\{1, 3, a, b\}$ is not a Diophantine quadruple. Then $c = c_\nu^\tau$ for some n and τ.*

2.2. Points on the elliptic curve

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

$$(2.1) \qquad ax + 1 = \square, \quad bx + 1 = \square, \quad cx + 1 = \square$$

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

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

It is natural to ask which points on E can be a solution of system (2.1). The answer is given in the following proposition with $P = (0, 1) \in E(\mathbb{Q})$.

PROPOSITION 2.3. [4, 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 2.4. [11, 4.1, p.37], [12, 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 $2Q = P$ iff $x' - \alpha, x' - \beta, x' - \gamma$ are all $\mathbb{Q}$-rational squares.

2.3. 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 2.5. [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 $M = d^2 u^4$ and $N = d^2 v^4$, or $M = -d^2 v^4$ and $N = d^2(u^4 - v^4)$, or $M = d^2(u^4 - v^4)$ and $N = -d^2 v^4$ 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 exists integers a and b such that

$$\frac{a}{b} \notin \{-2, -1, -\frac{1}{2}, 0, 1\}$$

and $M = a^4 + 2a^3 b$ 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 used to be more specific.

THEOREM 2.6. [4, Theorem 2]

$$E'(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{or} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.$$

3. Torsion group of the elliptic curve

We get the following elliptic curve

$$E_k : (kx + 1)((4k + 4)x + 1)((9k + 6)x + 1)$$

by Diophantine triple $\{k, 4k+4, 9k+6\}$. The coordinate transformation

$$x \leftrightarrow \frac{x}{k(4k + 4)(9k + 6)}, \quad y \leftrightarrow \frac{y}{k(4k + 4)(9k + 6)}$$

applied on the curve E_k leads to the elliptic curve

$$E'_k : y^2 = (x + (4k + 4)(9k + 6))(x + k(9k + 6))(x + k(4k + 4)).$$

There are three integer points on E'_k

$$A'_k = (-(4k+4)(9k+6), 0), \quad B'_k = (-k(9k+6), 0), \quad C'_k = (-k(4k+4), 0).$$

These points have order 2. Also, there is another point

$$P'_k = (0, k(4k + 4)(9k + 6)),$$

which is not of finite order. First, let us find the structure of torsion group of E'_k. By using the Theorem 2.5 and Theorem 2.6, we can find the answer.

LEMMA 3.1. *The torsion group $E'_k(\mathbb{Q})_{tors}$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

Proof. It is sufficient to show that the torsion group $E'_k(\mathbb{Q})_{tors}$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_6$. Let α and β be the integers satisfying the properties

$$\frac{\alpha}{\beta} \notin \{-2, -1, -\frac{1}{2}, 0, 1\},$$

$M = k(5k + 2) = \alpha^4 + 2\alpha^3\beta$ and $N = 8(k + 1)(4k + 3) = 2\alpha\beta^3 + \beta^4$. Then we get the equation

(3.1) $M + N = 37k^2 + 58k + 24 = (\alpha^2 + \alpha\beta + \beta^2)^2 - 3\alpha^2\beta^2.$

Then the right side of equation (3.1) is congruent to $0, 1, 5$ or 6 modulo 8. Especially, the right side is congruent to 0 modulo 8 when α, β are both even. Therefore,

$$\alpha^4 + 2\alpha^3\beta \equiv 0 \pmod{16}, \quad 2\alpha\beta^3 + \beta^4 \equiv 0 \pmod{16}.$$

Let us consider the left side of equation (3.1). The left side is congruent to $0, 3$ or 7 modulo 8. Especially, the left side is congrunet to 0 modulo 8 when k is an even. First, if $k \equiv 0, 6, 8, 14 \pmod{16}$ then $N \equiv 8 \pmod{16}$. Next, if $k \equiv 2, 4, 10, 12 \pmod{16}$ then $M \equiv 8 \pmod{16}$, which is a contradiction. Hence, we have the desired result.

□

Since we already get the points of order 2, we have the following result.

COROLLARY 3.2. $E'_k(\mathbb{Q})_{tors} = \{O, A'_k, B'_k, C'_k\}.$

COROLLARY 3.3. $rank(E'_k(\mathbb{Q})) \geq 1.$

Proof. The point $P'_k = (0, k(4k + 4)(9k + 6))$ is not of finite order. Hence, $rank(E'_k(\mathbb{Q})) \geq 1$ by Lemma 3.1.   □

4. Integer points on elliptic curve

In this section, we find the integer points on E'_k under assumption that $rank(E'_k(\mathbb{Q})) = 1$.

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

$$
\begin{aligned}
x(P'_k) &= 0, \\
x(P'_k + A'_k) &= -2k(6k+5), \\
x(P'_k + B'_k) &= -8(k+1)(3k+1), \\
x(P'_k + C'_k) &= 6(2k+1)(3k+2).
\end{aligned}
$$

- The case P'_k

  If $P'_k \in 2E'_k(\mathbb{Q})$ then $k(4k+4) = (2k+1)^2 - 1$ is a perfect square, which is a contradiction. Therefore, $P'_k \notin 2E'_k(\mathbb{Q})$.

- The cases $P'_k + A'_k$ and $P'_k + B'_k$

  If $P'_k + A'_k$ and $P'_k + B'_k \in 2E'_k(\mathbb{Q})$ then

  $$
  -2(4k+3) \quad \text{and} \quad -(5k+2)(3k+4)
  $$

  are perfect squares, respectively. These are also contradictions since they are negative numbers. Therefore, $P'_k + A'_k, P'_k + B'_k \notin 2E'_k(\mathbb{Q})$.

- The case $P'_k + C'_k$

  If $P'_k + C'_k \in 2E'_k(\mathbb{Q})$ then

  $$
  (5k+2)(3k+2) = 3\square, \quad (5k+2)(4k+3) = 2\square.
  $$

  Let $d = \gcd(5k+2, 4k+3)$. Then we obtain $d \in \{1, 7\}$. Hence, we conclude that

  $$
  3k+2 = 6\square \quad \text{and} \quad 3k+2 = 42\square.
  $$

  This is a contradiction, since both left sides are congruent to 2 modulo 3, but both right sides are congruent to 0.

  $\square$

Let $E'_k(\mathbb{Q})/E'_k(\mathbb{Q})_{tors} =<U>$ 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. 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 $\{a, b, c\} = \{k-1, k+1, 4k(2k+1)(2k-1)\}$. From [12, 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. Therefore, we have to solve in integers all systems of the form

$$(4.1) \qquad kx + 1 = \alpha\square, \quad (4k+4)x + 1 = \beta\square, \quad (9k+6)x + 1 = \gamma\square,$$

where for $X_1 = (k(4k+4)(9k+6)u, k(4k+4)(9k+6)v) \in \mathcal{S}$, the numbers α, β, γ are defined by

$$\alpha = ku + 1, \quad \beta = (4k+4)u + 1, \quad \gamma = (9k+6)u + 1$$

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

$$\begin{cases} \alpha = \beta\gamma & \text{if} \quad ku + 1 = 0, \\ \beta = \alpha\gamma & \text{if} \quad (4k+4)u + 1 = 0, \\ \gamma = \alpha\beta & \text{if} \quad (9k+6)u + 1 = 0. \end{cases}$$

Using these facts and Theorem 2.1, we get the following theorem.

THEOREM 4.2. *Let k be a positive integer. If $\mathrm{rank}(E_k(\mathbb{Q})) = 1$ then the x-coordinates of all integer points on the elliptic curve*

$$E_k : (kx + 1)((4k+4)x + 1)((9k+6)x + 1)$$

are given by

$$x \in \{-1, \ 0, \ 144k^3 + 240k^2 + 124k + 20\}.$$

Proof. Let us consider that for $X_1 = P'_k$. Then we obtain the system

$$kx + 1 = \square, \quad (4k+4)x + 1 = \square, \quad (9k+6)x + 1 = \square,$$

which is solved in [9]. Hence, we have to prove that the system (4.1) has no integer solution for $X_1 \in \mathcal{S}\backslash\{P'_k\}$.
For $X_1 \in \{A'_k, B'_k, P'_k + A'_k, P'_k + B'_k\}$ exactly two of the numbers α, β, γ are negative and accordingly the system (4.1) has no integer solution. Therefore, we have to check three cases.

- The cases $X_1 = O$
  For $X_1 = O$ the system (4.1) becomes

$$\begin{cases} kx + 1 = (k+1)(9k+6)\square, \\ (4k+4)x + 1 = k(9k+6)\square, \\ (9k+6)x + 1 = k(k+1)\square. \end{cases}$$

Then we have a contradiction, since the left side of second equation is congruent to 1 modulo 4, but the right side is congruent to 0, 2 or 3 modulo 4. Therefore, the system has no integer solution.

- The case $X_1 = C_k'$
  For $X_1 = C_k'$ the system (4.1) becomes

$$\begin{cases} kx + 1 = (8k+6)(9k+6)\square, \\ (4k+4)x + 1 = (5k+2)(9k+6)\square, \\ (9k+6)x + 1 = (5k+2)(8k+6)\square. \end{cases}$$

The left side of third equation is congruent to 1 modulo 3, but the right side is congruent to 0 or 2 modulo 3, which is a contradiction. Therefore, we have the desired result.

- The case $X_1 = P_k' + C_k'$
  For $X_1 = P_k' + C_k'$ the system (4.1) becomes

$$\begin{cases} kx + 1 = (4k+4)(8k+6)\square, \\ (4k+4)x + 1 = k(5k+2)\square, \\ (9k+6)x + 1 = k(4k+4)(5k+2)(8k+6)\square. \end{cases}$$

Similar as before, we obtain a contradiction. The left side of second equation is congruent to 1 modulo 4, but the right side is congruent to 0, 2 or 3 modulo 4. Therefore, all cases have no integer solution, and we proved the theorem.

$$\square$$

REMARK 4.3. As coefficients of E_k grow exponentially, computation of the rank of E_k for large k is difficult. The above values of $\mathrm{rank}(E_k(\mathbb{Q}))$ are computed using the programs **SIMATH**([18]) and *mwrank*([1]).

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

Case of k	$E_k(\mathbb{Q})$	rank$(E_k(\mathbb{Q}))$
$k = 1$	$y^2 = 120x^3 + 143x^2 + 24x + 1$	1
$k = 2$	$y^2 = 576x^3 + 360x^2 + 38x + 1$	1
$k = 3$	$y^2 = 1584x^3 + 675x^2 + 52x + 1$	1
$k = 4$	$y^2 = 3360x^3 + 1088x^2 + 66x + 1$	2
$k = 5$	$y^2 = 6120x^3 + 1599x^2 + 80x + 1$	2
$k = 6$	$y^2 = 10080x^3 + 2208x^2 + 94x + 1$	2
$k = 7$	$y^2 = 15456x^3 + 2915x^2 + 108x + 1$	1

References

[1] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge Univ. Press, 1997.

[2] L. E. Dickson, *History of the Theory of Numbers Vol.2*, Chelsea, New York, 1966.

[3] A. Dujella, *A parametric family of elliptic curves*, Acta Arith., **94** (2000), no. 1, 87–101.

[4] A. Dujella, *Diophantine m-tuples and elliptic curves*, 21st Journées Arithmétiques (Rome, 2001), J. Théor. Nombres Bordeaux, **13** (2001), no. 1, 111–124.

[5] A. Dujella and A. Pethö, *Integer points on a family of elliptic curves*, Publ. Math. Debrecen, **56** (2000), 321-335.

[6] A. Dujella and M. Milić, *On the torsion group of elliptic curves induced by $D(4)$-triples*, An. Stiint. Univ. ”Ovidius” Constanta Ser. Mat., **22** (2014), 79–90.

[7] A. Filipin, Y. Fujita, and A. Togbé, *The extendibility of Diophantine pairs I: The general case*, Glas. Mat. Ser. III, **49** (69) (2014), no. 1, 25–36.

[8] 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.

[9] B. He, K. Pu, R. Shen, and A. Togbé, *A note on the regularity of the Diophantine pair $\{k, 4k \pm 4\}$*, J. Théor. Nombres Bordeaux, **30** (2018), 879-892.

[10] B. He, A. Togbé, and V. Ziegler, *There is no Diophantine quintuple*, Trans. Amer. Math. Soc., **371** (2019), 6665–6709.

[11] D. Husemöller, *Elliptic curves*, Springer-Verlag, New York, 1987.

[12] A. Knapp, *Elliptic curves*, Princeton Univ. Press, 1992.

[13] J. B. Lee and J. Park, *Some conditions on the form of third element from Diophantine pairs and its application*, J. Korean Math. Soc., **55** (2018), no. 2, 425-445

[14] M. Mikić, *On the Mordell-Weil group of elliptic curves induced by the families of Diophantine triples*, Rocky Mountain J. Math., **45** (2015), 1565–1589.

[15] F. Najman, *Integer points on two families of elliptic curves*, Publ. Math. Debrecen, **75** (2009), 401–418.

[16] F. Najman, *Compact representation of quadratic integers and integer points on some elliptic curves*, Rochy Mountain J. Math., **40** (2010), 1979–2002.

[17] K. Ono, *Euler's concordant forms*, Acta Arith., **78** (1996), 101-123.

[18] SIMATH manual, Saarbrücken, 1997

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