Publ. Math. Debrecen
83/3 (2013), 481–515
DOI: 10.5486/PMD.2013.5640

Elliptic divisibility sequences, squares and cubes

By BETÜL GEZER (Bursa)

Abstract. Elliptic divisibility sequences (EDSs) are generalizations of a class of integer divisibility sequences called Lucas sequences. There has been much interest in cases where the terms of Lucas sequences are squares or cubes. In this work, using the Tate normal form having one parameter of elliptic curves with torsion points, the general terms and periods of all elliptic divisibility sequences with a zero term are given in terms of this parameter by means of Mazur's theorem. It is shown that which term h_n of an EDS with zero terms can be a square or a cube by using the general terms of these sequences.

1. Introduction

A *divisibility sequence* is a sequence (h_n) $(n \in \mathbb{N})$ of integers with the property that $h_n | h_m$ if $n | m$. There are also divisibility sequences satisfying a nonlinear recurrence relation. These are the elliptic divisibility sequences and this recurrence relation comes from the recursion formula for division polynomials on an elliptic curve.

An *elliptic divisibility sequence* (EDS) is a sequence (h_n) of integers satisfying a nonlinear recurrence relation

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2 \tag{1.1}$$

and such that h_n divides h_m whenever n divides m for all $m \geq n \geq 1$. The recurrence relation (1.1) is less straightforward than a linear recurrence.

Mathematics Subject Classification: Primary: 11B37, 11B39; Secondary: 11B83, 11G05.
Key words and phrases: elliptic curves, torsion points, elliptic divisibility sequences, squares, cubes.

EDSs are generalizations of a class of integer divisibility sequences called *Lucas sequences.* EDSs are quite interesting because of the close relation with elliptic curves. EDSs have applications to cryptography and the elliptic curve discrete logarithm problem. They were the first nonlinear divisibility sequences to be studied. Morgan Ward wrote several papers detailing the arithmetic theory of EDSs [28], [29].

In order to calculate terms, there are two useful formulas (known as *duplication formulas*) which are obtained from (1.1) by setting first $m = k+1$, $n = k$ and then $m = k+1$, $n = k-1$:

$$h_{2k+1} = h_{k+2}h_k^3 - h_{k-1}h_{k+1}^3, \tag{1.2}$$

$$h_{2k}h_2 = h_k(h_{k+2}h_{k-1}^2 - h_{k-2}h_{k+1}^2) \tag{1.3}$$

for all $k \in \mathbb{N}$. A solution of (1.1) is proper if $h_0 = 0$, $h_1 = 1$, and $h_2h_3 \neq 0$. Such a proper solution will be an EDS if and only if h_2, h_3, h_4 are integers with $h_2|h_4$. The sequence (h_n) with initial values $h_0 = 0$, $h_1 = 1$, h_2, h_3 and h_4 is denoted by $[1; h_2; h_3; h_4]$.

Ward [29] gave formulas for a very special case of the EDSs whose second or third term is zero which are called *improper sequences.* In fact, there are also the EDSs for which the other term is zero. In this paper we give general terms all of these sequences. This will also help us to determine the square or cube terms in these sequences as described in the following sections.

In this paper we are interested in sequences with zero terms, i.e., the sequences in certain ranks. Thus we need to explain the concept of a rank of an EDS: An integer m is said to be a *divisor* of the sequence (h_n) if it divides some term h_k with $k > 0$. Let m be a divisor of (h_n). We define the *rank of apparition* of m in (h_n) to be the integer ρ such that $m|h_\rho$ and there is no integer j such that j is a divisor of ρ with $m|h_j$. Notice that this definition of the rank used for elliptic divisibility sequences in this paper in this sense.

One of the well known theorems in the theory of elliptic curves is Mazur's theorem [14]. It states that there are no points of order 11, nor are there any points of order 13 or more on an elliptic curve over $\mathbb{Q}$. Hence, the rank of apparition of the elliptic divisibility sequences associated to elliptic curves with points of finite order can not be 11, nor 13 or more. Therefore, any of second, …, tenth and twelfth terms of an elliptic divisibility sequence can be zero.

In this work we will answer the following questions:

- What are the initial values of the EDSs with second, …, tenth and twelfth term zero ?

- Is there any formula to calculate the terms of the EDSs with second, $\dots$, tenth and twelfth term zero which is more useful than relations above, i.e., what are the general terms of these sequences ?
- What are the periods of these sequences?
- Which terms of these sequences can be a square or a cube ?

The first two questions are discussed in Section 3. The initial values of the EDSs with zero terms and the general terms of these sequences are given in Theorem 3.1, and Theorem 3.2, respectively. The third question is considered in Section 4, and the periods of these sequences are given in Theorem 4.2. In Section 5, the question of when a term of an elliptic divisibility sequence with zero terms can be a square or a cube is discussed in detail.

2. Some preliminaries on elliptic curves and EDSs

An *elliptic curve* over $\mathbb{Q}$, is the set of solutions to an equation of the normal form, or generalized Weierstrass form,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

with coefficients $a_1, \dots, a_6$ in $\mathbb{Q}$. The set of all solutions $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ to the equation (2.1) together with the point $\mathbf{O}$, called the *point at infinity*, is denoted by $E(\mathbb{Q})$ and called the set of $\mathbb{Q}$-*rational points* on E. The set of $\mathbb{Q}$-points on E forms an abelian subgroup of E known as the Mordell–Weil group of E and the point $\mathbf{O}$ is the identity element of this group. For more details on elliptic curves in general, see [24], [25]. One of the most important theorems in the theory of elliptic curves is the Mordell–Weil theorem, which implies that, if $\mathbb{K}$ is a number field containing $\mathbb{Q}$, then $E(\mathbb{K})$ is a finitely generated abelian group. Also, the Mordell–Weil theorem shows that $E_{\text{tors}}(\mathbb{K})$, the *torsion subgroup* of $E(\mathbb{K})$, is finitely generated and abelian, hence it is finite, since its generators are of finite order. It is always interesting to characterize the torsion subgroup of a given elliptic curve. The question of a uniform bound on $E_{\text{tors}}(\mathbb{Q})$ was studied from the point of view of modular curves by Shimura, Ogg, and others. In 1976, B. Mazur proved the following strongest result which had been conjectured by Ogg:

Theorem 2.1 (Mazur [14]). *Let E be an elliptic curve defined over $\mathbb{Q}$. Then the torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ is either isomorphic to $\mathbb{Z}/N\mathbb{Z}$ for $N = 1, 2, \dots, 10, 12$ or to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ for $N = 1, 2, 3, 4$. Further, each of these groups does occur as an $E_{\text{tors}}(\mathbb{Q})$.*

It is a classical result that all elliptic curves with a torsion point of order N lie in a one parameter family where $N \in \{4, \ldots, 10, 12\}$. The *Tate normal form* of an elliptic curve E with point $P = (0, 0)$ is defined by

$$E : y^2 + (1 - c)xy - by = x^3 - bx^2.$$

If an elliptic curve in normal form has a point of order $N > 3$, then admissible change of variables transforms the curve to the Tate normal form, in this case the point $P = (0, 0)$ is a torsion point of maximal order. Especially, if we want a classification with respect to the order of the torsion points, the use of Tate normal form of elliptic curves is unavoidable.

In [12], Kubert listed one parameter family of elliptic curves E defined over $\mathbb{Q}$ with a torsion point of order N where $N = 4, \ldots, 10, 12$. Most cases are proved by Husemöller, [11]. Also some algorithms are given by using the existence of such a family, [6]. To decide when an elliptic curve defined over $\mathbb{Q}$ has a point of given order N, we need a result on parametrization of torsion structures:

Theorem 2.2 ([6]). *Every elliptic curve with a point P of order $N = 4, \ldots, 10, 12$ can be written in the following Tate normal form*

$$E : y^2 + (1 - c)xy - by = x^3 - bx^2,$$

with the following relations:

1. *If $N = 4$, $b = \alpha$, $c = 0$,*
2. *if $N = 5$, $b = \alpha$, $c = \alpha$,*
3. *if $N = 6$, $b = \alpha + \alpha^2$, $c = \alpha$,*
4. *if $N = 7$, $b = \alpha^3 - \alpha^2$, $c = \alpha^2 - \alpha$,*
5. *if $N = 8$, $b = (2\alpha - 1)(\alpha - 1)$, $c = b/\alpha$,*
6. *if $N = 9$, $c = \alpha^2(\alpha - 1)$, $b = c(\alpha(\alpha - 1) + 1)$,*
7. *if $N = 10$, $c = (2\alpha^3 - 3\alpha^2 + \alpha)/(\alpha - (\alpha - 1)^2)$, $b = c\alpha^2/(\alpha - (\alpha - 1)^2)$,*
8. *if $N = 12$, $c = (3\alpha^2 - 3\alpha + 1)(\alpha - 2\alpha^2)/(\alpha - 1)^3$, $b = c(-2\alpha^2 + 2\alpha - 1)/(\alpha - 1)$ where $\alpha \in \mathbb{Z}$.*

Theorem 2.2 states that, if any elliptic curve has a point of finite order then this curve is birationally equivalent to one of the Tate normal forms given in the theorem above. Therefore, in this work, we are only interested in the elliptic curves in Tate normal forms with one integer parameter α and general terms of the elliptic divisibility sequences given as functions of the integer parameter α.

Ward proved, in [29], that birationally equivalent elliptic curves are associated to equivalent elliptic divisibility sequences, so it is not a restriction to give the general terms by using Tate normal forms, that is, we will be giving general terms of all elliptic divisibility sequences with zero terms under this equivalence.

The relation between an elliptic curve and an elliptic divisibility sequence is given by Morgan Ward, see for details and formulas, [29]. Ward proved that elliptic divisibility sequences arise as values of the division polynomials of an elliptic curve, i.e., if $P = (x, y)$ is a rational point on an elliptic curve E over $\mathbb{Q}$ then the elliptic divisibility sequence (h_n) is defined by $h_n = \psi_n(x, y)$ for $n \in \mathbb{N}$ where ψ_n is the n-th division polynomial of E. Therefore, if E is an elliptic curve over $\mathbb{Q}$ then the initial values of the elliptic divisibility sequence are given by the coefficients of an elliptic curve. Conversely, if (h_n) is an elliptic divisibility sequence in which neither h_2 nor h_3 is zero then there exists an elliptic curve E and the coefficients of the elliptic curve are given by the initial values of the sequence. In this paper, under this fact, we first give initial values and the general terms of an elliptic divisibility sequence associated to an elliptic curve in Tate normal form with a torsion point P. We will now give a short account of material about elliptic divisibility sequences, for more detailed information about these sequences in general, see [4], [5], [23], [27], [28], [29].

Two elliptic divisibility sequences (h_n) and (h'_n) are said to be equivalent if there exists a rational ω such that

$$h'_n = \omega^{n^2-1} h_n \tag{2.2}$$

for all $n \in \mathbb{N}$.

Ward established that the multiples of the rank of apparition ρ are regularly spaced in (h_n) in the following theorem.

Theorem 2.3 ([29])**.** *Let p be a prime divisor of an elliptic divisibility sequence (h_n), and let ρ be its smallest rank of apparition. Let $h_{\rho+1} \not\equiv 0\ (p)$. Then*

$$h_n \equiv 0\ (p) \quad \textit{if and only if} \quad n \equiv 0\ (\rho).$$

The following theorem shows us that the initial values of the EDS given by the coefficients of the elliptic curve.

Theorem 2.4 ([23])**.** *Let (h_n) be an elliptic divisibility sequence. Then the elliptic curves $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x$ where $a_1, a_2, a_3, a_4 \in \mathbb{Q}$, associated to (h_n) are precisely those with:*

$$h_2 = a_3, \tag{2.3}$$

$$h_3 = a_2a_3^2 - a_4^2 - a_1a_3a_4 \tag{2.4}$$

$$h_4 = 2a_3a_4h_3 + a_1a_3^2h_3 - a_3^5. \tag{2.5}$$

3. The initial values and the general terms of the EDSs

The problem of finding the general terms of the elliptic divisibility sequences whose second (resp. third, fourth, fifth, sixth) term is zero are given in [9]. However, it was seen that the general terms of the other sequences with zero terms can not be easily obtained.

In this paper we first give the general terms of all elliptic divisibility sequences with zero terms by using Tate normal form of an elliptic curve E which has a torsion point $P=(0,0)$ of order N. By Mazur's theorem we know that there exists an elliptic curve containing a point of order N. Clearly, every N-th term h_N of the associated elliptic divisibility sequence (h_n) is zero, since these terms correspond to the point at infinity $\mathbf{O}$. In particular, if (h_n) is an elliptic divisibility sequence, in which $h_N=0$ for some minimal index N then $N\in\{2,\dots,10,12\}$. The aim of this section is to give general terms of these sequences. Naturally, it is sufficient to give the general terms only for the sequences with one of the terms $h_2,\dots,h_{10},h_{12}$ are zero. But we begin by the case $N>3$, since we use Tate normal form of an elliptic curve. The general terms of improper elliptic divisibility sequences where h_2 or h_3 is equal to zero will be discussed at the end of this section and general terms of them will be given in Theorem 3.5. In the following theorem, by using the Tate normal form of an elliptic curve, the initial values of the sequences with zero terms are given for $N>3$.

Theorem 3.1. *Let (h_n) be an elliptic divisibility sequence in which $h_N=0$ for some minimal index $N\in\{4,\dots,10,12\}$. Then the initial values of (h_n) with $\alpha\in\mathbb{Z}$ given by the following:*

1. *If $N=4, [1;-\alpha;-\alpha^3;0]$, $\alpha\neq 0$.*
2. *If $N=5, [1;-\alpha;-\alpha^3;\alpha^6]$, $\alpha\neq 0$.*
3. *If $N=6, [1;-\alpha(\alpha+1);-\alpha^3(\alpha+1)^3;\alpha^6(\alpha+1)^5]$, $\alpha\neq -1,0$.*
4. *If $N=7, [1;-\alpha^2(\alpha-1);-\alpha^6(\alpha-1)^3;\alpha^{11}(\alpha-1)^6]$, $\alpha\neq 0,1$.*
5. *If $N=8, [1;-\alpha^3\xi;-\alpha^8\xi^3;\alpha^{14}\xi^6]$, where $\xi=(\alpha-1)(2\alpha-1), \alpha\neq 0,1$.*
6. *If $N=9, [1;-\alpha^2(\alpha-1)\gamma;-\alpha^6(\alpha-1)^3\gamma^3;\alpha^{12}(\alpha-1)^6\gamma^5]$, where $\gamma=\alpha^2-\alpha+1$, $\alpha\neq 0,1$.*
7. *If $N=10, [1;-\alpha^3\delta\zeta^4;-\alpha^9\delta^3\zeta^{10};\alpha^{16}\delta^6\zeta^{19}]$, where $\zeta=\alpha-(\alpha-1)^2$ and $\delta=(\alpha-1)(2\alpha-1), \alpha\neq 0,1$.*
8. *If $N=12, [1;-(\alpha-1)^8\lambda\theta;-(\alpha-1)^{20}\lambda^3\theta^3;(\alpha-1)^{37}\lambda^6\theta^5]$, where $\lambda=(3\alpha^2-3\alpha+1)(\alpha-2\alpha^2)$ and $\theta=2\alpha-2\alpha^2-1$, $\alpha\neq 0, 1$.*

Proof. 1. We first consider an elliptic curve E with a point P of order $N = 4$. Then by Theorem 2.2, the Tate normal form of E is

$$E : y^2 + xy - \alpha y = x^3 - \alpha x^2. \tag{3.1}$$

By Theorem 2.4, E is associated to the elliptic sequence (h_n) and the initial values of the sequence are

$$h_1 = 1, \quad h_2 = -\alpha, \quad h_3 = -\alpha^3, \quad h_4 = 0.$$

It is known that, if P is an integer point, and the coefficients a_i of the elliptic curve are integers, then the values h_n are integers, and have the divisibility property, that is, (h_n) is an EDS. Therefore coefficients α in (3.1) must be an integer, since we want to work with elliptic divisibility sequences.

2. Similarly for $N = 5$, we have

$$E : y^2 + (1-\alpha)xy - \alpha y = x^3 - \alpha x^2,$$

and so, the initial values of the sequence are

$$h_1 = 1, \quad h_2 = -\alpha, \quad h_3 = -\alpha^3, \quad h_4 = \alpha^6.$$

3. For $N = 6$, we have

$$E : y^2 + (1-\alpha)xy - \alpha(\alpha+1)y = x^3 - \alpha(\alpha+1)x^2,$$

and so, the initial values of the sequence are

$$h_1 = 1, \quad h_2 = -\alpha(\alpha+1), \quad h_3 = -\alpha^3(\alpha+1)^3, \quad h_4 = \alpha^6(\alpha+1)^5.$$

4. For $N = 7$, we have

$$E : y^2 + (1-\alpha^2+\alpha)xy - (\alpha^3-\alpha^2)y = x^3 - (\alpha^3-\alpha^2)x^2,$$

and so, the initial values of the sequence are

$$h_1 = 1,\ h_2 = -\alpha^2(\alpha-1), \quad h_3 = -\alpha^6(\alpha-1)^3, \quad h_4 = \alpha^{11}(\alpha-1)^6.$$

5. Now let E be an elliptic curve in normal form with a point P of order $N = 8$. Then by Theorem 2.2, the Tate normal form of E is

$$E : y^2 + (1-(2\alpha-1)(\alpha-1)/\alpha)xy - (2\alpha-1)(\alpha-1)y = x^3 - (2\alpha-1)(\alpha-1)x^2.$$

Since we work with elliptic divisibility sequences, coefficients of the elliptic curve must be integer, so we transform the elliptic curve E to a birationally equivalent curve $\widetilde{E}$ under admissible change of variables

$$\widetilde{E} : y^2 + (\alpha-\xi)xy - \alpha^3\xi y = x^3 - \alpha^2\xi x^2$$

where $\xi = (2\alpha-1)(\alpha-1)$. By Theorem 2.4, $\widetilde{E}$ is associated to the elliptic divisibility sequence (h_n) and the initial values of the sequence are

$$h_1 = 1, \quad h_2 = -\alpha^3\xi, \quad h_3 = -\alpha^8\xi^3, \quad h_4 = \alpha^{14}\xi^6.$$

6. For $N = 9$ we have

$$E : y^2 + (1-c)xy - by = x^3 - bx^2$$

where $c = \alpha^2(\alpha-1)$, $b = c(\alpha(\alpha-1)+1)$, and so, the initial values of this sequence are

$$h_1 = 1, \quad h_2 = -\alpha^2(\alpha-1)\gamma, \quad h_3 = -\alpha^6(\alpha-1)^3\gamma^3, \quad h_4 = \alpha^{12}(\alpha-1)^6\gamma^5$$

where $\gamma = \alpha^2 - \alpha + 1$.

7. Now let E be an elliptic curve in normal form with a point P of order $N = 10$. By Theorem 2.2, the Tate normal form of E is

$$E : y^2 + (1-c)xy - by = x^3 - bx^2$$

where

$$c = \frac{\alpha(2\alpha^2 - 3\alpha + 1)}{\alpha - (\alpha-1)^2}, \quad b = \frac{c\alpha^2}{\alpha - (\alpha-1)^2}$$

and E birationally equivalent to the curve $\widetilde{E}$ under admissible change of variables given by

$$\widetilde{E} : y^2 + (\zeta^2 - \alpha\delta\zeta)xy - \alpha^3\delta\zeta^4 y = x^3 - \alpha^3\delta\zeta^2x^2,$$

where $\zeta = \alpha - (\alpha-1)^2$ and $\delta = (\alpha-1)(2\alpha-1)$. By Theorem 2.4, $\widetilde{E}$ is associated to the elliptic divisibility sequence (h_n) and the initial values of this sequence are

$$h_1 = 1, \quad h_2 = -\alpha^3\delta\zeta^4, \quad h_3 = -\alpha^9\delta^3\zeta^{10}, \quad h_4 = \alpha^{16}\delta^6\zeta^{19}.$$

8. Now let E be an elliptic curve in normal form with a point P of order $N = 12$. By Theorem 2.2, the Tate normal form of E is

$$E : y^2 + (1-c)xy - by = x^3 - bx^2,$$

where

$$c = \frac{(3\alpha^2 - 3\alpha + 1)\alpha(1-2\alpha)}{(\alpha-1)^3}, \quad b = \frac{c(2\alpha - 2\alpha^2 - 1)}{\alpha - 1}$$

and E birationally equivalent to the curve $\widetilde{E}$ under admissible change of variables given by

$$\widetilde{E} : y^2 + (\alpha-1)((\alpha-1)^3 - \lambda)xy - (\alpha-1)^8\lambda\theta y = x^3 - (\alpha-1)^4\lambda\theta x^2,$$

where $\lambda = (3\alpha^2 - 3\alpha + 1)(\alpha - 2\alpha^2)$, $\theta = 2\alpha - 2\alpha^2 - 1$. By Theorem 2.4, $\widetilde{E}$ is associated to the elliptic divisibility sequence (h_n) and the initial values of this sequence are

$$h_1 = 1, \quad h_2 = -(\alpha-1)^8\lambda\theta, \quad h_3 = -(\alpha-1)^{20}\lambda^3\theta^3, \quad h_4 = (\alpha-1)^{37}\lambda^6\theta^5. \quad \square$$

Thus we know the initial values of the sequences (h_n) with zero terms. We now give the general terms of the sequences (h_n) with zero terms depending on only one integer parameter α in the following theorem.

Theorem 3.2. *Let (h_n) be an elliptic divisibility sequence with N-th term zero, i.e., with rank $N \in \{4, \dots, 10, 12\}$. Let α, γ, δ, λ, θ be as in Theorem 3.1. Then the general term of (h_n) given by the following formulas:*

1. *If $N = 4$,*

$$h_n = \varepsilon\alpha^{\{(3n^2-p)/8\}} \tag{3.2}$$

where

$$\varepsilon = \begin{cases} +1 & \text{if } n \equiv 1,5,6 \ (8) \\ -1 & \text{if } n \equiv 2,3,7 \ (8), \end{cases} \qquad p = \begin{cases} 3 & \text{if } n \equiv 1,3 \ (4) \\ 4 & \text{if } n \equiv 2 \ (4). \end{cases}$$

2. If $N = 5$,

$$h_n = \varepsilon\alpha^{\{(2n^2-p)/5\}} \tag{3.3}$$

where

$$\varepsilon = \begin{cases} +1 & \text{if } n \equiv 1,4,7,8 \ (10) \\ -1 & \text{if } n \equiv 2,3,6,9 \ (10), \end{cases} \qquad p = \begin{cases} 2 & \text{if } n \equiv 1,4 \ (5) \\ 3 & \text{if } n \equiv 2,3 \ (5). \end{cases}$$

3. If $N = 6$,

$$h_n = \varepsilon\alpha^{\{(5n^2-p)/12\}}(\alpha+1)^{\{(n^2-k)/3\}} \tag{3.4}$$

where

$$\varepsilon = \begin{cases} +1 & \text{if } n \equiv 1,4,5,9,10 \ (12) \\ -1 & \text{if } n \equiv 2,3,7,8,11 \ (12), \end{cases}$$

and

$$p = \begin{cases} 5 & \text{if } n \equiv 1,5 \ (6) \\ 8 & \text{if } n \equiv 2,4 \ (6) \\ 9 & \text{if } n \equiv 3 \ (6), \end{cases} \qquad k = \begin{cases} 1 & \text{if } n \equiv 1,2,4,5 \ (6) \\ 0 & \text{if } n \equiv 3(6). \end{cases}$$

4. If $N = 7$,

$$h_n = \varepsilon\alpha^{\{(5n^2-p)/7\}}(\alpha-1)^{\{(3n^2-q)/7\}} \tag{3.5}$$

where

$$\varepsilon = \begin{cases} +1 & \text{if } n \equiv 1,4,5 \ (7) \\ -1 & \text{if } n \equiv 2,3,6 \ (7), \end{cases}$$

and

$$p = \begin{cases} 5 & \text{if } n \equiv 1,6 \ (7) \\ 6 & \text{if } n \equiv 2,5 \ (7) \\ 3 & \text{if } n \equiv 3,4 \ (7), \end{cases} \qquad q = \begin{cases} 3 & \text{if } n \equiv 1,6 \ (7) \\ 5 & \text{if } n \equiv 2,5 \ (7) \\ 6 & \text{if } n \equiv 3,4 \ (7). \end{cases}$$

5. If $N = 8$,

$$h_n = \varepsilon\alpha^{\{(15n^2-p)/16\}}(\alpha-1)^{\{(7n^2-q)/16\}}(2\alpha-1)^{\{(3n^2-k)/8\}} \tag{3.6}$$

where

$$\varepsilon = \begin{cases} +1 & \textit{if } n \equiv 1,4,5,9,10,13,14 \ (16) \\ -1 & \textit{if } n \equiv 2,3,6,7,11,12,15 \ (16), \end{cases}$$

and

$$p = \begin{cases} 15 & \textit{if } n \equiv 1,7\,(8) \\ 12 & \textit{if } n \equiv 2,6\,(8) \\ 7 & \textit{if } n \equiv 3,5\,(8) \\ 16 & \textit{if } n \equiv 4\,(8), \end{cases} \quad q = \begin{cases} 7 & \textit{if } n \equiv 1,7\,(8) \\ 12 & \textit{if } n \equiv 2,6\,(8) \\ 15 & \textit{if } n \equiv 3,5\,(8) \\ 16 & \textit{if } n \equiv 4\,(8), \end{cases} \quad k = \begin{cases} 3 & \textit{if } n \equiv 1,3,5,7\,(8) \\ 4 & \textit{if } n \equiv 2,6\,(8) \\ 0 & \textit{if } n \equiv 4\,(8). \end{cases}$$

6. If $N = 9$,

$$h_n = \varepsilon\alpha^{\{(7n^2-p)/9\}}(\alpha-1)^{\{(4n^2-q)/9\}}\gamma^{\{(n^2-k)/3\}} \tag{3.7}$$

where

$$\varepsilon = \begin{cases} +1 & \textit{if } n \equiv 1,4,5,8,11,12,15,16 \ (18) \\ -1 & \textit{if } n \equiv 2,3,6,7,10,13,14,17 \ (18), \end{cases}$$

and

$$p = \begin{cases} 7 & \textit{if } n \equiv 1,8 \ (9) \\ 10 & \textit{if } n \equiv 2,7 \ (9) \\ 9 & \textit{if } n \equiv 3,6 \ (9) \\ 4 & \textit{if } n \equiv 4,5 \ (9), \end{cases} \quad q = \begin{cases} 4 & \textit{if } n \equiv 1,8 \ (9) \\ 7 & \textit{if } n \equiv 2,7 \ (9) \\ 9 & \textit{if } n \equiv 3,6 \ (9) \\ 10 & \textit{if } n \equiv 4,5 \ (9), \end{cases} \quad k = \begin{cases} 0 & \textit{if } n \equiv 3,6 \ (9) \\ 1 & \textit{otherwise.} \end{cases}$$

7. If $N = 10$,

$$h_n = \varepsilon\alpha^{\{(21n^2-p)/20\}}(\alpha-1)^{\{(9n^2-q)/20\}}(2\alpha-1)^{\{(2n^2-k)/5\}}\delta^{\{(5n^2-s)/4\}} \tag{3.8}$$

where

$$\varepsilon = \begin{cases} +1 & \textit{if } n \equiv 1,4,5,8,9,13,14,17,18 \ (20) \\ -1 & \textit{if } n \equiv 2,3,6,7,11,12,15,16,19 \ (20), \end{cases}$$

and

$$p=\begin{cases}21 & \textit{if } n\equiv 1,9\ (10)\\ 24 & \textit{if } n\equiv 2,8\ (10)\\ 9 & \textit{if } n\equiv 3,7\ (10)\\ 16 & \textit{if } n\equiv 4,6\ (10)\\ 25 & \textit{if } n\equiv 5\ (10),\end{cases}\qquad q=\begin{cases}9 & \textit{if } n\equiv 1,9\ (10)\\ 16 & \textit{if } n\equiv 2,8\ (10)\\ 21 & \textit{if } n\equiv 3,7\ (10)\\ 24 & \textit{if } n\equiv 4,6\ (10)\\ 25 & \textit{if } n\equiv 5\ (10),\end{cases}$$

$$k=\begin{cases}2 & \textit{if } n\equiv 1,4,6,9\ (10)\\ 3 & \textit{if } n\equiv 2,3,7,8\ (10)\\ 0 & \textit{if } n\equiv 5\ (10),\end{cases}\qquad s=\begin{cases}5 & \textit{if } n\equiv 1,3,5,7,9\ (10)\\ 4 & \textit{if } n\equiv 2,4,6,8\ (10).\end{cases}$$

8. If $N=12$,

$$h_n=\varepsilon\alpha^{\{(n^2-p)/12\}}(\alpha-1)^{\{(59n^2-q)/24\}}\\ \times(2\alpha-1)^{\{(n^2-k)/24\}}\lambda^{\{(3n^2-s)/8\}}\theta^{\{(n^2-t)/3\}} \qquad (3.9)$$

where

$$\varepsilon=\begin{cases}+1 & \textit{if } n\equiv 1,5,9,13,14,16,17,18,20,21,22\ (24)\\ -1 & \textit{if } n\equiv 2,3,4,6,7,8,10,11,15,19,23\ (24),\end{cases}$$

and

$$p=\begin{cases}1 & \textit{if } n\equiv 1,11\,(12)\\ 4 & \textit{if } n\equiv 2{,}10\,(12)\\ 9 & \textit{if } n\equiv 3,9\,(12)\\ 16 & \textit{if } n\equiv 4,8\,(12)\\ 13 & \textit{if } n\equiv 5,7\,(12)\\ 12 & \textit{if } n\equiv 6\,(12),\end{cases}\quad q=\begin{cases}59 & \textit{if } n\equiv 1{,}11\,(12)\\ 44 & \textit{if } n\equiv 2{,}10\,(12)\\ 51 & \textit{if } n\equiv 3,9\,(12)\\ 56 & \textit{if } n\equiv 4,8\,(12)\\ 35 & \textit{if } n\equiv 5,7\,(12)\\ 60 & \textit{if } n\equiv 6\,(12),\end{cases}\quad k=\begin{cases}1 & \textit{if } n\equiv 1{,}5{,}7{,}11(12)\\ 4 & \textit{if } n\equiv 2,10\,(12)\\ 9 & \textit{if } n\equiv 3,9\,(12)\\ 16 & \textit{if } n\equiv 4,8\,(12)\\ 12 & \textit{if } n\equiv 6\,(12),\end{cases}$$

$$s=\begin{cases}3 & \textit{if } n\equiv 1,3,5,7,9,11\,(12)\\ 4 & \textit{if } n\equiv 2,6,10\,(12)\\ 0 & \textit{if } n\equiv 4,8\,(12),\end{cases}\qquad t=\begin{cases}1 & \textit{if } n\equiv 1,2,4,5,7,8,10,11\,(12)\\ 0 & \textit{if } n\equiv 3,6,9\,(12).\end{cases}$$

Proof. 1. It is clear that the result is true for $n\le 5$. Hence we assume that $n>5$. If (h_n) is an EDS, then we know that

$$h_{n+2}h_{n-2}=h_{n+1}h_{n-1}h_2^2\ -h_3h_1h_n^2\ . \qquad (3.10)$$

We argue by induction on n. First suppose that $n \equiv 1\ (4)$ and (3.2) is true for $n+1$. Then we have

$$h_{n+2} = -\alpha^{6m^2+9m+3}$$

by (3.2). On the other hand we see that

$$h_{n-2} = -\alpha^{6m^2-3m}, \qquad h_n = \alpha^{6m^2+3m}, \qquad h_{n-1} = 0.$$

Substituting these expressions into (3.10) gives $h_{n+2} = -\alpha_2^{6m^2+9m+3}$. Thus we proved the equation (3.2) is true for $n+2$ which completes the proof for $n \equiv 1\ (4)$. The other cases are proved similarly.

2. It is clear that the result is true for $n \leq 6$. Hence we assume that $n > 6$. If (h_n) is an EDS, then it satisfies the relation (3.10). We again argue by induction using (3.3). First suppose that $n \equiv 1\ (5)$ and (3.3) is true for $n+1$. Then we have

$$h_{n+2} = \begin{cases} -\alpha^{10m^2+12m+3} & \text{if } \ m \equiv 2,4\ (5) \\ \alpha^{10m^2+12m+3} & \text{if } \ m \equiv 1,3\ (5) \end{cases}$$

by (3.3). On the other hand we see that

$$h_{n-2} = \begin{cases} -\alpha^{10m^2-4m} & \text{if } m \equiv 2,4\ (5) \\ \alpha^{10m^2-4m} & \text{if } m \equiv 1,3\ (5) \end{cases} \qquad h_n = \begin{cases} \alpha^{10m^2+4m} & \text{if } m \equiv 2,4\ (5) \\ -\alpha^{10m^2+4m} & \text{if } m \equiv 1,3\ (5) \end{cases}$$

$$h_{n-1} = 0.$$

Substituting these expressions into (3.10) gives $h_{n+2}h_{n-2} = \alpha^3 h_n^2$, hence we have

$$h_{n+2} = \begin{cases} -\alpha^{10m^2+12m+3} & \text{if } m \equiv 2,4\ (5) \\ \alpha^{10m^2+12m+3} & \text{if } m \equiv 1,3\ (5). \end{cases}$$

Thus we proved that the equation (3.3) is true for $n+2$. The other cases are proved similarly.

The same proof works for the remaining parts of the theorem. □

	p	q	k	s	t
$n \equiv 1(12)$	1	59	1	3	1
$n \equiv 2(12)$	4	44	4	4	1
$n \equiv 3(12)$	9	51	9	3	0
$n \equiv 4(12)$	16	56	16	0	1
$n \equiv 5(12)$	13	35	1	3	1
$n \equiv 6(12)$	**12**	**60**	**−12**	**4**	**0**
$n \equiv 7(12)$	13	35	1	3	1
$n \equiv 8(12)$	16	56	16	0	1
$n \equiv 9(12)$	9	51	9	3	0
$n \equiv 10(12)$	4	44	4	4	1
$n \equiv 11(12)$	1	59	1	3	1

Table 1: The values p, q, k, s and t of the general term of the EDS with $N = 12$.

It is seen that the values p, q, k, s and t of the general term of the elliptic divisibility sequences with twelfth term zero in the table above. According to this table, we have the following terms for $n \equiv 6\ (12)$:

$$h_6 = \alpha^2(\alpha-1)^{86}(2\alpha-1)^2\lambda^{13}\delta^{12}, \qquad h_{18} = -\alpha^{26}(\alpha-1)^{794}(2\alpha-1)^{14}\lambda^{121}\delta^{108}$$

$$h_{30} = \alpha^{74}(\alpha-1)^{2210}(2\alpha-1)^{38}\lambda^{337}\delta^{300}$$

$$h_{42} = -\alpha^{146}(\alpha-1)^{4334}(2\alpha-1)^{74}\lambda^{661}\delta^{588}$$

In addition, if we take $\alpha = 3$, the first eight terms of the EDS with $N = 12$ are

$$\begin{gathered}1; -948480; -53329136320512000; -27346122891266847865307136000000;\\ 17500141386070121786711926566237801283584; -3319445579395304657\\ 078796371004775655798907736824977188454400000000000000000; -45938\\ 24222798666425039100328482290559063213427355998727370793872053\\ 34329698182758400000000000000000; -1884349228191035614337748\\ 21043991142309132528994842811514985817859497226098776607161543\\ 93938175478135259136000000000000000000000000000; \ldots\end{gathered}$$

Remark 3.3. There are also elliptic curves with a torsion point which are not in the Tate normal form as in Theorem 2.2. For example the point $P = (0, 0)$ on the elliptic curve

$$E : y^2 + 17xy - 120y = x^3 - 60x^2$$

is a torsion point of order eight. The initial values of elliptic divisibility sequence

(h_n) associated to the curve E are

$$h_1 = 1, \quad h_2 = -120, \quad h_3 = -864000, \quad h_4 = -186624000000$$

and $h_8 = 0$, that is, the sequence has rank eight. E is birationally equivalent to the curve $\widetilde{E}$ under the transformation $\binom{x}{y} \to \binom{4x}{8y}$ given by

$$\widetilde{E} : y^2 + \frac{17}{2}xy - 15y = x^3 - 15x^2$$

which is in Tate normal form. This curve gives us an elliptic sequence, so we need to make another transformation to have an elliptic divisibility sequence. Hence we have

$$E' : y^2 + 34xy - 960y = x^3 - 240x^2$$

and the initial values of elliptic divisibility sequence (h'_n) associated to the elliptic curve E' are

$$h'_1 = 1, \ h'_2 = -960, \ h'_3 = -221184000, \ h'_4 = -6115295232000000.$$

It can easily be seen that (h_n) and (h'_n) are equivalent by taking $\omega = -2$ in the equation (2.2). So, the general terms of the elliptic divisibility sequences associated to the elliptic curves in Tate normal form are the general terms of all elliptic divisibility sequences with zero terms under the equivalence.

Remark 3.4. There is no Tate normal form of an elliptic curve with the torsion point of order two or three, but Kubert in [12], listed the elliptic curves with torsion point of order two or three are

$$E : y^2 = x^3 + ax^2 + bx \quad \text{and} \quad E : y^2 + a_1xy + a_3y = x^3,$$

respectively. In this case, the elliptic divisibility sequences associated to an elliptic curve with the torsion point of order two or three give improper sequences and the initial values of these sequences are

$$h_1 = 1, \ h_2 = 0, \ h_3 = -b^2, \ h_4 = 0 \quad \text{and} \quad h_1 = 1, \ h_2 = a_3, \ h_3 = 0, \ h_4 = -a_3^5,$$

respectively.

Under these considerations, an easy computation gives the general terms of the improper divisibility sequences.

Theorem 3.5. i. *Let* (h_n) *be an elliptic divisibility sequence* $[1; 0; -b^2; 0]$.

Then the general term of (h_n) *is given by the following formula:*

$$h_n = \varepsilon b^{\{(n^2-1)/4\}}$$

where

$$\varepsilon = \begin{cases} +1 & \textit{if } n \equiv 1, 5 \ (8) \\ -1 & \textit{if } n \equiv 3, 7 \ (8). \end{cases}$$

ii. *Let* (h_n) *be an elliptic divisibility sequence* $[1; a_3; 0; -a_3^5]$. *Then the general term of* (h_n) *is given by the following formula:*

$$h_n = \varepsilon a_3^{\{(n^2-1)/3\}}$$

where

$$\varepsilon = \begin{cases} +1 & \textit{if } n \equiv 1, 2 \ (6) \\ -1 & \textit{if } n \equiv 4, 5 \ (6). \end{cases}$$

4. The periods of the EDSs

In this section we will give the periods of all elliptic divisibility sequences with zero terms by using general terms of these sequences which are given in previous section.

A sequence (s_n) of rational integers is said to be *numerically periodic modulo* m if there exists a positive integer π such that

$$s_{n+\pi} \equiv s_n \ (m) \tag{4.1}$$

for all sufficiently large n. If (4.1) holds for all n, then (s_n) is said to be *purely periodic modulo* m. The smallest π for which (4.1) is true is called the *period* of (s_n) modulo m. All other π's are multiples of it.

The following theorem of Ward shows us how the period and rank are connected.

Theorem 4.1 ([29]). *Let* (h_n) *be an EDS and* p *be an odd prime whose rank of apparition* ρ *is greater than* 3. *Let* a_1 *be an integral solution of the congruence* $a_1 \equiv h_2/h_{\rho-2}$ (p) *and let* e *and* k *be the exponents* [1] *to which* a_1 *and* $a_2 \equiv h_{\rho-1}$ (p) *respectively belong modulo* p. *Then* (h_n) *is purely periodic modulo* p, *and its period* π *is given by the formula* $\pi(h_n) = \tau\rho$ *where* $\tau = 2^{\nu}[e, k]$. *Here* $[e, k]$ *is the*

[1] That is, let e and k be the smallest positive integers such that $a_1^e \equiv 1$ and $a_2^k \equiv 1(p)$ respectively.

least common multiple of e and k, and the exponent ν is determined as follows:

$$\nu = \begin{cases} +1 & \text{if } e \text{ and } k \text{ are both odd} \\ -1 & \text{if } e \text{ and } k \text{ are both even and both divisible by} \\ & \qquad \text{exactly the same power of } 2 \\ 0 & \text{otherwise.} \end{cases}$$

We give the periods of all elliptic divisibility sequences with zero terms in the following theorem.

Theorem 4.2. *Let (h_n) be an elliptic divisibility sequence with N-th term zero, where $N \in \{4, 5, \dots, 10, 12\}$ and let p be an odd prime. Then the period of (h_n) is*

$$\pi(h_n) = \begin{cases} t(p-1) & \text{if } \ q = [e,k] \text{ is a primitive root modulo } p \\ 2Nl & \text{otherwise} \end{cases}$$

$$\text{where} \qquad l = \begin{cases} q & \text{if } \ q \text{ is odd} \\ q/2 & \text{if } q \text{ is even,} \end{cases} \qquad t = \begin{cases} N & \text{if } N \text{ is even} \\ N/2 & \text{if } N \text{ is odd.} \end{cases}$$

Proof. The cases $N = 4$ and 5, can easily be seen, so we give $N = 6$, the other cases can be proved in similar way. In this case the period of (h_n) is $\pi(h_n) = 6(p-1)$ or $12l$. By Theorem 3.1 and Theorem 4.1, we have $a_1 = h_2/h_4 = -1/\alpha^5(\alpha+1)^4$ and $a_2 = h_5 = \alpha^{10}(\alpha+1)^8$. Let e and k be the orders of a_1 and a_2, respectively. Then $k = e/2$ when e is even, and $k = e$ when e is odd, since $a_2 = 1/a_1^2$. Let a_1 be a primitive root modulo p. Then $e = p-1$, $k = (p-1)/2$ and so $q = p-1$. Hence $\nu = 0$ and so $\tau = p-1$. Therefore in this case $\pi(h_n) = 6(p-1)$. If a_1 is not a primitive root modulo p, then there are two cases. In the first case, let q be odd. Then $e = k = q$, so that $\nu = 1$. Thus $\tau = q$, therefore $\pi(h_n) = 6q$. In the second case, let q be even. Then $e = q$ and $k = q/2$, so that $\nu = 0$. Thus $\tau = 2q$ therefore $\pi(h_n) = 12q$. □

α	$p=5$	$p=7$	$p=11$	$p=13$	$p=17$	$p=19$	$p=23$	$p=29$	$p=31$
-5	–	36	60	72	96	108	132	84	180
-4	12	12	60	36	12	108	132	84	180
-3	24	36	60	12	96	36	12	168	180
-2	24	36	12	72	48	108	132	168	12
1	12	36	60	36	12	108	132	84	60
2	24	36	60	24	48	36	132	168	180
3	24	12	60	36	96	108	132	168	180
4	–	36	60	36	12	108	132	12	36
5	–	36	60	72	96	108	132	84	36

Table 2: The periods of the EDSs with $N = 6$ modulo $p > 3$ for some α.

5. Squares and cubes in EDSs

The question of when a term of a Lucas sequence can be square has generated interest in the literature [2], [3], [21], [22]. Similar results concerning cubes were also obtained for specific sequences such as Fibonacci, Lucas and Pell numbers [17], [20]. In [9], [10], we describe when a term of an elliptic divisibility sequence can be a square or a cube, if one of the first six terms is zero. Recently, Reynolds [19] consider perfect powers in elliptic divisibility sequences whose first term is divisible by 2 or 3.

The ultimate purpose of this section is to determine square or cube terms in some special family of the elliptic divisibility sequences whose contain a zero term. In this section we determine square or cube terms of these sequences by using the general terms of them. Throughout this paper the symbols $\square$ and C mean a square and a cube of a non-zero rational number, i.e. $\square = \pm\beta^2$ where β is an integer. In particular, we will investigate the answers of the following questions:

- *Which terms of* (h_n) *can be a square or a cube independent of* α ? This question is answered for each case. For example, consider an elliptic divisibility sequence for which sixth term is zero,
  i. if $n \equiv 1,\ 5,\ 7,\ 11\ (12)$, then $h_n = \square$ for all $\alpha \neq -1, 0$,
  ii. if $n \equiv 1,\ 3,\ 9,\ 15,\ 17\ (18)$, then $h_n = C$ for all $\alpha \neq -1, 0$.
- *Which terms of* (h_n) *can not be a square or a cube*? Starting with the fact that square or cube terms can be arise dependent on the parameter α it is seen that some terms of (h_n) can not be a square or a cube for any choice of α for each case. For example, consider an elliptic divisibility sequence for which sixth term is zero,
  i. if $n \equiv 2,\ 3,\ 9,\ 10\ (12)$, then h_n is not a square for all $\alpha \neq -1, 0$,
  ii. if $n \equiv 2,\ 5,\ 7,\ 11,\ 13,\ 16\ (18)$, then h_n is not a cube for all $\alpha \neq -1, 0$.
- *Which terms of* (h_n) *can be a square or a cube with admissible choice of* α ? In addition to square or cube terms which determined in question one it is seen that a term of an EDS can be a square or a cube depending on the admissible choice of α. For example, consider an elliptic divisibility sequence for which sixth term is zero,
  i. if $n \equiv 4,\ 8\ (12)$ then h_n is a square iff $\alpha + 1 = \square$,
  ii. if $n \equiv 4,\ 14\ (18)$ then h_n is a cube iff $\alpha + 1 = C$,
  iii. if $n \equiv 8,\ 10\ (18)$ then h_n is a cube iff $\alpha = C$.

Especially when we look for the answers of our problems, we are led to some Diophantine equations whose solutions give the desired answers. These equations fall into five main classes: Pell equations, classical well-known cubic equations, trivial equations, elliptic equations of rank zero or one. Many of these equations are very similar, so that we can present the solutions of all equations in one table (see Table 3). For example, consider an elliptic divisibility sequence for which the eighth term is zero. If $n \equiv 3,\ 13\ (16)$, then we see that $h_n = \square$ iff

$$(\alpha - 1)(2\alpha - 1) = \square,$$

this leads to a Pell's equation $(4\alpha-3)^2 - 8\beta^2 = 1$ or a trivial equation $(4\alpha-3)^2 + 8\beta^2 = 1$ where α, β are integers. Equations encountered in some cases turned into elliptic curves. In particular, if we have an elliptic curve with rank zero then the only integral points on this curve are the torsion points. These, in turn, can be computed by the Lutz–Nagell Theorem. In [8], the authors find all integer solutions of Mordell's equation $y^2 = x^3 + k$ for $0 < |k| \leq 10^4$ and also for all but about 1000 values with $|k| \leq 10^5$. They also give tables listing, curves with large integer points and large numbers of integer points. A complete list of all integer solutions of Mordell's equation can be found in [18]. Therefore if our elliptic equation is a Mordell's equation we use the tables in [18]. If the elliptic curve has a rank different from zero then the *Elliptic Logarithm Method* is applied to find the all integral solutions.

For the convenience of the reader, we present the solutions of all these equations in the table below before the proofs of the following results. A basic observation is the following: For every equation, the distinct irreducible factors (over $\mathbb{Q}[\alpha]$) appearing in the left-hand side (if they are at least two) are pairwise relatively prime[2]. This implies that, if the right hand-side is $\square$ (respectively, C), then every irreducible factor is $\square$ (respectively, C). We use of this fact for a quite number of equations; in most cases it was necessary to consider all factors in the left-hand side[3].

[2] As a characteristic example, take equation 38. Firstly, α can not have a common prime factor p with any of $\alpha - 1$, $2\alpha - 1$, $2\alpha^2 - 2\alpha + 1$, $3\alpha^2 - 3\alpha + 1$. Indeed, $\alpha \equiv 0\ (p)$ implies that both $\alpha - 1$ and $2\alpha - 1$ are $\equiv -1(p)$ and both $2\alpha^2 - 2\alpha + 1$ and $3\alpha^2 - 3\alpha + 1$ are $\equiv 1(p)$. Next, $\alpha - 1$ can not have prime factor p with any of $2\alpha - 1$, $2\alpha^2 - 2\alpha + 1$, $3\alpha^2 - 3\alpha + 1$, because $\alpha - 1 \equiv 0\ (p)$ implies $\alpha \equiv 1(p)$ and, hence $2\alpha^2 - 2\alpha + 1$ and $3\alpha^2 - 3\alpha + 1$ are both $\equiv 1\ (p)$. Analogously, $2\alpha - 1$ can not have a common prime factor p with neither $2\alpha^2 - 2\alpha + 1$ nor $3\alpha^2 - 3\alpha + 1$, because, p should be odd, hence $\alpha \equiv 1/2\ (p)$ and, consequently $2\alpha^2 - 2\alpha + 1 \equiv 1/2(p)$ and $3\alpha^2 - 3\alpha + 1 \equiv 1/4(p)$. Finally, $2\alpha^2 - 2\alpha + 1$ and $3\alpha^2 - 3\alpha + 1$ are relatively prime because $3(2\alpha^2 - 2\alpha + 1) - 2(3\alpha^2 - 3\alpha + 1) = 1$.

[3] For example, although equation 44 implies that all three α, $2\alpha^2 - 2\alpha + 1$, $3\alpha^2 - 3\alpha + 1$ are C, we only use the fact that the second one is C.

Eq. No	**implies or is equivalent to**	**is reduced to or is equivalent to**	**Comments**
1	$\alpha(\alpha+1)=\Box$	$(2\alpha+1)^2 \pm \beta^2 = 1$	trivial eq.
$5, 9$	$\alpha(\alpha-1)=\Box$ $\alpha(\alpha-1)(2\alpha-1)=\Box$	$(2\alpha-1)^2 \pm \beta^2 = 1$	trivial eq.
$2, 3, 4$	$\alpha=\beta_1^3$ & $\alpha+1=\beta_2^3$	$\beta_2^3-\beta_1^3=1$	trivial eq.
$6, 10, 15,$ $16, 17, 18,$ $19, 29, 30,$ $38, 39, 40$ $41, 42$	$\alpha=\beta_1^3$ & $\alpha-1=\beta_2^3$	$\beta_1^3-\beta_2^3=1$	trivial eq.
7	$(\alpha-1)(2\alpha-1)=\Box$	$(4\alpha-3)^2-8\beta^2=1$ $(4\alpha-3)^2+8\beta^2=1$	Pell eq. trivial eq.
$8, 33$	$\alpha(2\alpha-1)=\Box$ $\alpha(2\alpha-1)(2\alpha^2-2\alpha+1)$ $\times(3\alpha^2-3\alpha+1)=\Box$	$(2\alpha-1)^2-2\beta^2=1$ $(2\alpha-1)^2+2\beta^2=1$	Pell eq. trivial eq.
$11, 25, 47$ $48, 49$	$\alpha-1=\beta_1^3$ & $2\alpha-1=\beta_2^3$	$\beta_2^3+2(-\beta_1^3)=1$	'classical' equation[4]
$12, 13$	$\alpha^2-\alpha+1=\Box$ $(\alpha-1)(\alpha^2-\alpha+1)=\Box$	$(2\alpha-1)^2 \pm \beta^2 = -3$	trivial eq.
$14, 20, 21$	$\alpha^2-\alpha+1=C$	$\beta^3-48=(8\alpha-4)^2$	Mordell eq.
$22, 23$	$-\alpha^2+3\alpha-1=\Box$ $(2\alpha-1)(-\alpha^2+3\alpha-1)=\Box$	$(2\alpha-3)^2 \pm \beta^2 = 5$	trivial eq.
24, 26, 27, 28	$-\alpha^2+3\alpha-1=C$	$\beta^3+80=(8\alpha-12)^2$	Mordell eq.
$31, 45, 46$	$\alpha=\beta_1^3$ & $2\alpha-1=\beta_2^3$	$(-\beta_2)^3+2\beta_1^3=1$	'classical' equation[4]
34	$(\alpha-1)(-2\alpha^2+2\alpha-1)=\Box$	$(-2\alpha)^3+4(-2\alpha)^2$ $+6(-2\alpha)+4=\beta^2,$ $(2\alpha)^3-4(2\alpha)^2$ $+6(2\alpha)-4=\beta^2$	Ellog used[6] zero rank[5]
32	$3\alpha^2-3\alpha+1=\Box$	$\beta^2-3(2\alpha-1)^2=1$ $\beta^2+3\alpha^2=-1$	Pell eq. impossible
$35, 36$	$\alpha(3\alpha^2-3\alpha+1=\Box$	$(3\alpha)^3-3(3\alpha)^2$ $+3(3\alpha)=\beta^2,$ $(-3\alpha)^3+3(-3\alpha)^2$ $+3(-3\alpha)=\beta^2$	zero rank[5] zero rank[5]
37	$(2\alpha-1)(-2\alpha^2+2\alpha-1)=\Box$	$(4\alpha)^3-6(4\alpha)^2$ $+16(4\alpha)-16=\beta^2,$ $(-4\alpha)^3+6(-4\alpha)^2$ $+16(-4\alpha)+16=\beta^2$	zero rank[5] zero rank[5]
$43, 44$	$2\alpha^2-2\alpha+1=C$	$\beta^3-4=(4\alpha-2)^2$	Mordell eq.

Table 3: Solutions of the equations, (footnotes on the next page).

5.1. The case $N=$ 4. In this part we will answer the question of when a term of an EDS for which the fourth term is zero can be a perfect square or a cube. Although the terms of the EDSs can be a square or a cube dependent only on the integer parameter α, there are cases when square or cube terms independent of the any choice of α.

Theorem 5.1. *Let (h_n) be an elliptic divisibility sequence for which the fourth term is zero (so that $h_n=0$, for every $n\equiv 0\ (4)$).*

1. i. *If $n\equiv 1,\ 7\ (8)$, then $h_n=\square$ for every non-zero α.*
   ii. *$\alpha=\square$ iff $h_n=\square$ for all $n\geq 0$*
2. i. *If $n\equiv 1,\ 3,\ 5,\ 7\ (8)$, then $h_n=C$ for every non-zero α.*
   ii. *$\alpha=C$ iff $h_n=C$ for all $n\geq 0$.*

Proof. 1. For (i), if $n\equiv 1$ or $7\ (8)$, then $n=8k+1$ or $8k+7$ for $k\in\mathbb{N}$. Substituting these values into (3.2), we have

$$h_{8k+1}=\alpha^{24k^2+6k},h_{8k+7}=-\alpha^{24k^2+42k+18},$$

respectively. Hence, $h_n=\square$ for every non-zero α.

For (ii), we know that $h_n=\square$ for every non-zero α when $n\equiv 1,\ 7\ (8)$ by part (i). Now suppose $n\equiv 5\ (8)$. Then $n=8k+5$ for $k\in\mathbb{N}$. Putting this into (3.2), we have

$$h_{8k+5}=\alpha^{24k^2+30k+9}.$$

Hence we have $\alpha=\square$ iff $h_{8k+5}=\square$. The cases $n\equiv 2,3,6\ (8)$ are proved similarly. Therefore, $\alpha=\square$ iff $h_n=\square$ for all $n\geq 0$.

2. For (i), if $n\equiv 1,\ 3,\ 5$ or $7\ (8)$, then $n=8k+1,\ 8k+3,\ 8k+5$ or $8k+7$ ($k\in\mathbb{N}$). Putting these into (3.2), we have

$$h_{8k+1}=\alpha^{24k^2+6k},h_{8k+3}=-\alpha^{24k^2+18k+3},h_{8k+5}=\alpha^{24k^2+30k+9}$$

and

$$h_{8k+7}=-\alpha^{24k^2+42k+18},$$

respectively. Therefore $h_n=C$ for every non-zero α.

For (ii), We have seen that if $n\equiv 1,3,5$ or $7\ (8)$, then $h_n=C$ for every non zero α by part (i). Now consider the cases $n\equiv 2$ or $6\ (8)$. Then we have

$$h_{8k+2}=-\alpha^{24k^2+12k+1}\text{ and }h_{8k+6}=\alpha^{24k^2+36k+13}$$

for $k\in\mathbb{N}$, respectively, by (3.2). Hence we get $\alpha=C$ iff $h_{8k+2}=C$ or $\alpha=C$ iff $h_{8k+6}=C$. Therefore $\alpha=C$ iff $h_n=C$ for all $n\geq 0$. □

[4] The equation $x^3+2y^3=1$ has the integer solution $(x,y)=(-1,1)$, hence, by Theorem 5, Chapter 24 of [15] can not have further solutions with $xy\neq 0$.

[5] The only solutions are those given by coordinates of the torsion points. These, in turn, can be computed by the Lutz–Nagell Theorem (see, for example, Corollary 7.2, Chapter VIII.7 of [24]); automatically, they can be calculated using e.g. the PARI-GP calculator [16] or the online MAGMA calculator [13].

[6] The *Elliptic Logarithm Method* is applied. This has been developed in [26] and, independently, in [7] and now is implemented in MAGMA [13]; see also [1].

$N=4$	h_{8k}	h_{8k+1}	h_{8k+2}	h_{8k+3}	h_{8k+4}	h_{8k+5}	h_{8k+6}	h_{8k+7}
$\alpha \in \mathbb{Z}\backslash\{0\}$	0	$\square$			0			$\square$
$\alpha = \square$	0	$\square$	$\square$	$\square$	0	$\square$	$\square$	$\square$
$\alpha \in \mathbb{Z}\backslash\{0\}$	0	C		C	0	C		C
$\alpha = C$	0	C	C	C	0	C	C	C

Table 4: Square and cube terms in EDSs with $N=4$.

5.2. The Case $N=5$**.** An easy calculation as in Theorem 5.1 gives the following theorem.

Theorem 5.2. *Let* (h_n) *be an elliptic divisibility sequence for which the fifth term is zero (so that* $h_n = 0$*, for every* $n \equiv 0$ (5)*).*

1. i. *If* $n \equiv 1, 4, 6, 9$ (10)*, then* $h_n = \square$ *for every non-zero* α*.*
   ii. $\alpha = \square$ *iff* $h_n = \square$ *for all* $n \geq 0$*.*
2. i. *If* $n \equiv 1, 3, 4, 11, 12, 14$ (15)*, then* $h_n = C$ *for every non-zero* α*.*
   ii. $\alpha = C$ *iff* $h_n = C$ *for all* $n \geq 0$*.*

5.3. The Case $N=6$**.** This case is little more complicated than the first two cases. We determine the square or cube terms dependent on the any choice of α and we also determine the square or cube terms dependent on the admissible choice of α. Moreover, it is shown that the terms of these sequences can not be a square or a cube for any choice of α in the following theorem.

Theorem 5.3. *Let* (h_n) *be an elliptic divisibility sequence for which the sixth term is zero (so that* $h_n = 0$*, for every* $n \equiv 0$ (6)*).*

1. i. *If* $n \equiv 1, 5, 7, 11$ (12)*, then* $h_n = \square$ *for every* $\alpha \neq -1, 0$*.*
   ii. *If* $n \equiv 4, 8$ (12)*,* $h_n = \square$ *iff* $\alpha + 1 = \square$*.*
   iii. *Otherwise,* $h_n \neq \square$ *for every* $\alpha \neq -1, 0$*.*
2. i. *If* $n \equiv 1, 3, 9, 15, 17$ (18)*, then* $h_n = C$ *for every* $\alpha \neq -1, 0$*.*
   ii. *If* $n \equiv 4, 14$ (18)*,* $\alpha + 1 = C$ *iff* $h_n = C$*.*
   iii. *If* $n \equiv 8, 10$ (18)*,* $\alpha = C$ *iff* $h_n = C$*.*
   iv. *Otherwise,* $h_n \neq C$ *for every* $\alpha \neq -1, 0$*.*

Proof. 1. The cases (i) and (ii) can be proved in the same way as in Theorem 5.1. For (iii), if $n \equiv 2$ (12) then $n = 12k + 2$ $(k \in \mathbb{N})$. Substituting this into (3.4), we have

$$h_{12k+2} = -\alpha^{60k^2+20k+1}(\alpha+1)^{48k^2+16k+1}.$$

Therefore $h_n = \square$ iff

$$\alpha(\alpha+1) = \square. \tag{1}$$

This last equation leads to trivial equation

$$(2\alpha+1)^2 \pm \beta^2 = 1$$

where β is an integer. It is clear that these equations do not provide any acceptable α. The cases where $n \equiv 3, 9, 10\ (12)$ can be proved in the same way.

2. The proof of (i), (ii) and (iii) are similar to proof of Theorem 5.1. For (iv), if $n \equiv 2$ or $16\ (18)$ then $n = 18k + 2$ or $n = 18k + 16$ ($k \in \mathbb{N}$). Putting these into (3.4), we have

$$h_{18k+2} = -\alpha^{135k^2+30k+1}(\alpha+1)^{108k^2+24k+1}$$

and

$$h_{18k+16} = \alpha^{135k^2+240k+106}(\alpha+1)^{108k^2+192k+85}$$

respectively. Thus $h_n = C$ iff

$$\alpha(\alpha+1) = C. \tag{2}$$

If $n \equiv 5$ or $13\ (18)$ then we have

$$h_{18k+5} = \alpha^{135k^2+75k+10}(\alpha+1)^{108k^2+60k+8}$$

and

$$h_{18k+13} = \alpha^{135k^2+195k+70}(\alpha+1)^{108k^2+156k+56}$$

respectively, by (3.4). From these equations we see that $h_n = C$ iff

$$\alpha(\alpha+1)^2 = C. \tag{3}$$

Now suppose that $n \equiv 7$ or $11\ (18)$ then we have

$$h_{18k+7} = \alpha^{135k^2+105k+20}(\alpha+1)^{108k^2+84k+16}$$

and

$$h_{18k+11} = -\alpha^{135k^2+165k+50}(\alpha+1)^{108k^2+132k+40}$$

respectively, by (3.4). In this case we have $h_n = C$ iff

$$\alpha^2(\alpha+1) = C. \tag{4}$$

It follows that equations (2), (3) and (4) lead to trivial equation

$$\beta_2^3 - \beta_1^3 = 1$$

where $\alpha = \beta_1^3$, $\alpha + 1 = \beta_2^3$ and β_1, β_2 are integers. This equation does not provide any acceptable α. □

5.4. The Case $N = 7$. We determine the square or cube terms of the elliptic divisibility sequences for which the seventh term is zero in the following theorem.

Theorem 5.4. *Let (h_n) be an elliptic divisibility sequence for which the seventh term is zero (so that $h_n = 0$, for every $n \equiv 0\ (7)$).*

1. i. *If $n \equiv 1, 13\ (14)$, then $h_n = \square$ for every $\alpha \neq 0, 1$.*
   ii. *If $n \equiv 2, 3, 11, 12\ (14)$, then $h_n = \square$ iff $\alpha - 1 = \square$.*
   iii. *If $n \equiv 4, 5, 9, 10\ (14)$, then $h_n = \square$ iff $\alpha = \square$.*
   iv. *Otherwise, $h_n \neq \square$ for all $\alpha \neq 0, 1$.*

2. i. *If* $n \equiv 1, 3, 8, 13, 18, 20$ (21), *then* $h_n = C$ *for every* $\alpha \neq 0, 1$.
   ii. *If* $n \equiv 4, 6, 10, 11, 15, 17$ (21), *then* $h_n = C$ *iff* $\alpha = C$.
   iii. *If* $n \equiv 9, 12$ (21), *then* $h_n = C$ *iff* $\alpha - 1 = C$.
   iv. *Otherwise,* $h_n \neq C$ *for every* $\alpha \neq 0, 1$.

Proof. 1. The proof of (i), (ii) and (iii) are similar to proof of Theorem 5.1. For (iv), if $n \equiv 6$ or 8 (14) then we have

$$h_{14k+6} = -\alpha^{140k^2+120k+1}(\alpha - 1)^{84k^2+72k+15}$$

and

$$h_{14k+8} = \alpha^{140k^2+160k+45}(\alpha - 1)^{84k^2+96k+27}$$

respectively, by (3.5). From these equations we see that $h_n = \square$ iff

$$\alpha(\alpha - 1) = \square. \tag{5}$$

This last equation leads to trivial equations

$$(2\alpha - 1)^2 \pm \beta^2 = 1$$

where β is an integer. It is clear that these equations do not provide any acceptable α.

2. The proof of (i), (ii) and (iii) are similar to proof of Theorem 5.1. For (iv), if $n \equiv 2, 5, 16$ or 19 (21) then we have

$$h_{21k+2} = -\alpha^{315k^2+60k+2}(\alpha - 1)^{189k^2+36k+1}$$
$$h_{21k+5} = \alpha^{315k^2+150k+17}(\alpha - 1)^{189k^2+90k+10}$$
$$h_{21k+16} = -\alpha^{315k^2+480k+182}(\alpha - 1)^{189k^2+288k+109}$$
$$h_{21k+19} = \alpha^{315k^2+570k+257}(\alpha - 1)^{189k^2+342k+154}$$

respectively, by (3.5). Therefore, $h_n = C$ iff

$$\alpha^2(\alpha - 1) = C. \tag{6}$$

This last equation leads to trivial equation

$$\beta_1^3 - \beta_2^3 = 1$$

where $\alpha = \beta_1^3$, $\alpha - 1 = \beta_2^3$ and β_1, β_2 are integers and this equation does not provide any acceptable α. □

5.5. The Case $N=8$. We determine the square or cube terms of the elliptic divisibility sequences for which the eighth term is zero in the following theorem.

Theorem 5.5. *Let (h_n) be an elliptic divisibility sequence for which the eighth term is zero (so that $h_n=0$, for every $n\equiv 0\ (8)$).*

1. i. *If $n\equiv 1,4,12,15\ (16)$, then $h_n=\square$ for every $\alpha\neq 0,1$.*
   ii. *If $n\equiv 3,13\ (16)$, then $h_n=\square$ iff $(\alpha-1)(2\alpha-1)=\square$.*
   iii. *If $n\equiv 5,11\ (16)$, then $h_n=\square$ iff $\alpha(2\alpha-1)=\square$.*
   iv. *Otherwise $h_n\neq\square$ for every $\alpha\neq 0,1$.*
2. i. *If $n\equiv 1,7,17,23\ (24)$, then $h_n=C$ for every $\alpha\neq 0,1$.*
   ii. *If $n\equiv 3,4,20,21\ (24)$, then $h_n=C$ iff $\alpha=C$.*
   iii. *If $n\equiv 6,18\ (24)$, then $h_n=C$ iff $2\alpha-1=C$.*
   iv. *If $n\equiv 9,15\ (24)$, then $h_n=C$ iff $\alpha-1=C$.*
   v. *Otherwise $h_n\neq C$ for every $\alpha\neq 0,1$.*

Proof. 1. The proof of (i) is similar to proof of Theorem 5.1. For (ii), if $n\equiv 3,13\ (16)$ then we have

$$h_{16k+3}=-\alpha^{240k^2+90k+8}(\alpha-1)^{112k^2+42k+3}(2\alpha-1)^{96k^2+36k+3}$$

and

$$h_{16k+13}=\alpha^{240k^2+390k+158}(\alpha-1)^{112k^2+182k+73}(2\alpha-1)^{96k^2+156k+63},$$

respectively by (3.6). Hence, $h_n=\square$ iff

$$(\alpha-1)(2\alpha-1)=\square. \tag{7}$$

It follows that

$$(4\alpha-3)^2-8\beta^2=1 \tag{5.1}$$

or

$$(4\alpha-3)^2+8\beta^2=1$$

where β is an integer. From the last equation we have no solutions of α. The first equation leads to Pell equation. If we rewrite this equation as

$$(\tau+2\beta\sqrt{2}\,)(\tau-2\beta\sqrt{2}\,)=1$$

where $\tau=4\alpha-3$ we see that the only solutions of the form $\tau_k+3\equiv 0\ (4)$ give the desired solution of α and their number is infinite.

For (iii), if $n\equiv 5$ or $11\ (16)$ then we have

$$h_{16k+5}=\alpha^{240k^2+150k+23}(\alpha-1)^{112k^2+70k+10}(2\alpha-1)^{96k^2+60k+9}$$

and

$$h_{16k+11}=-\alpha^{240k^2+330k+113}(\alpha-1)^{112k^2+154k+52}(2\alpha-1)^{96k^2+132k+45},$$

respectively, by (3.6). Hence, $h_n=\square$ iff

$$\alpha(2\alpha-1)=\square. \tag{8}$$

It follows that $(\alpha, 2\alpha-1) = (\beta_1^2, \beta_2^2), (-\beta_1^2, -\beta_2^2), (-\beta_1^2, \beta_2^2)$ or $(\beta_1^2, -\beta_2^2)$, where β_1, β_2 are positive integers. The latter two possibilities give the trivial equations $2\beta_1^2+\beta_2^2 = -1$ and $2\beta_1^2+\beta_2^2 = 1$, respectively. The first equation is impossible and the second one does not give desired α. The former two possibilities lead to Pell equations

$$\beta_2^2 - 2\beta_1^2 = -1, \qquad \beta_2^2 - 2\beta_1^2 = 1$$

respectively. The solutions to the first equation are $(1,1)$, $(7,5)$, $(41,29)$, ... and parameters α corresponding to these solutions are $1, 25, 841, \ldots$. Note that α can not be 1 by the assumption. Thus the solutions to the last equation are $(3,2), (17,12), (99,70), \ldots$ and parameters α corresponding to these solutions are $-4, -144, -4900, \ldots$.

For (iv), if $n \equiv 2$, 6, 10 or 14 (16) then we have

$$h_{16k+2} = -\alpha^{240k^2+60k+3}(\alpha-1)^{112k^2+28k+1}(2\alpha-1)^{96k^2+24k+1},$$

$$h_{16k+6} = -\alpha^{240k^2+180k+33}(\alpha-1)^{112k^2+84k+15}(2\alpha-1)^{96k^2+72k+13},$$

$$h_{16k+10} = \alpha^{240k^2+420k+93}(\alpha-1)^{112k^2+140k+43}(2\alpha-1)^{96k^2+120k+37},$$

and

$$h_{16k+14} = \alpha^{240k^2+420k+183}(\alpha-1)^{112k^2+196k+85}(2\alpha-1)^{96k^2+168k+73},$$

respectively, by (3.6). From these equations we see that $h_n = \square$ iff

$$\alpha(\alpha-1)(2\alpha-1) = \square. \tag{9}$$

Notice that the factors α, $\alpha-1$ and $2\alpha-1$ are pairwaise coprime. Now the product of three pairwaise coprime number is a square only when each is a square. This implies that $\alpha = \square$, $\alpha - 1 = \square$ which is impossible by the proof of Theorem 5.4.

Let $n \equiv 7$, 9 (16). Then we have

$$h_{16k+7} = -\alpha^{240k^2+210k+45}(\alpha-1)^{112k^2+98k+21}(2\alpha-1)^{96k^2+84k+18},$$

and

$$h_{16k+9} = \alpha^{240k^2+270k+75}(\alpha-1)^{112k^2+126k+35}(2\alpha-1)^{96k^2+108k+30},$$

respectively, by (3.6). From these equations we see that $h_n = \square$ iff

$$\alpha(\alpha-1) = \square. \tag{5}$$

This equation give trivial equations $(2\alpha-1)^2 \pm \beta^2 = 1$. It is clear that these equations do not provide any acceptable α.

2. The proof of (i) is similar to proof of Theorem 5.1. For (ii), if $n \equiv 3, 4, 20$ or 21 (24), then $n = 24k+3$, $n = 24k+4$, $n = 24k+20$, or $24k+21$ ($k \in \mathbb{N}$). Substituting these values into (3.6), we have

$$h_{24k+3} = -\alpha^{540k^2+135k+8}(\alpha-1)^{252k^2+63k+3}(2\alpha-1)^{216k^2+54k+3},$$

$$h_{24k+4} = -\alpha^{540k^2+180k+14}(\alpha-1)^{252k^2+84k+6}(2\alpha-1)^{216k^2+72k+6},$$

$$h_{24k+20} = -\alpha^{540k^2+900k+374}(\alpha-1)^{252k^2+420k+174}(2\alpha-1)^{216k^2+360k+150},$$

and

$$h_{24k+21} = \alpha^{540k^2+945k+413}(\alpha-1)^{252k^2+441k+192}(2\alpha-1)^{216k^2+378k+165},$$

respectively. Thus $h_n = C$ iff $\alpha^2 = C$. The cases (iii) and (iv) can be proved in the same way.

For (v), if $n \equiv 5$ (24) then

$$h_{24k+5} = \alpha^{540k^2+225k+23}(\alpha-1)^{252k^2+105k+10}(2\alpha-1)^{216k^2+90k+9}$$

by (3.6). So, $h_n = C$ iff

$$\alpha^2(\alpha-1) = C. \tag{6}$$

Let $n \equiv 12$ (24). Then we have

$$h_{24k+12} = \alpha^{540k^2+540k+134}(\alpha-1)^{252k^2+252k+62}(2\alpha-1)^{216k^2+216k+54},$$

by (3.6). Therefore $h_n = C$ iff

$$\alpha^2(\alpha-1)^2 = C. \tag{10}$$

The equations (6) and (10) lead to trivial equation

$$\beta_1^3 - \beta_2^3 = 1$$

where $\alpha = \beta_1^3$, $\alpha - 1 = \beta_2^3$ and β_1, β_2 are integers and this equation does not provide any acceptable α. The cases where $n \equiv 11, 13, 19$ (24) can be proved in the same way.

If $n \equiv 2, 10, 14, 22$ (24) then

$$h_{24k+2} = \alpha^{540k^2+90k+3}(\alpha-1)^{252k^2+42k+1}(2\alpha-1)^{216k^2+36k+1},$$

$$h_{24k+10} = -\alpha^{540k^2+450k+93}(\alpha-1)^{252k^2+210k+43}(2\alpha-1)^{216k^2+180k+37},$$

$$h_{24k+14} = -\alpha^{540k^2+630k+183}(\alpha-1)^{252k^2+294k+85}(2\alpha-1)^{216k^2+252k+73},$$

$$h_{24k+22} = \alpha^{540k^2+990k+453}(\alpha-1)^{252k^2+462k+211}(2\alpha-1)^{216k^2+396k+181},$$

respectively, by (3.6). From these equations we see that $h_n = C$ iff

$$(\alpha-1)(2\alpha-1) = C. \tag{11}$$

It follows that $(\alpha-1, 2\alpha-1) = (\beta_1^3, \beta_2^3)$ where β_1, β_2 are integers. This gives the classical equation

$$\beta_2^3 + 2(-\beta_1)^3 = 1$$

and the only solution of this equation is $(\beta_1, \beta_2) = (-1, -1)$ and this solution does not provide any acceptable α. □

5.6. The Case $N = 9$. We determine the square or cube terms of the elliptic divisibility sequences for which the ninth term is zero in the following theorem.

Theorem 5.6. *Let (h_n) be an elliptic divisibility sequence for which the ninth term is zero (so that $h_n = 0$, for every $n \equiv 0\ (9)$).*

1. i. *If $n \equiv 1, 17\ (18)$, then $h_n = \square$ for every $\alpha \neq 0, 1$.*
   ii. *If $n \equiv 5, 13\ (18)$, then $h_n = \square$ iff $\alpha = \square$.*
   iii. *Otherwise, $h_n \neq \square$ for every $\alpha \neq 0, 1$.*
2. i. *If $n \equiv 1, 3, 6, 12, 15, 21, 24, 26\ (27)$, then $h_n = C$ for every $\alpha \neq 0, 1$.*
   ii. *If $n \equiv 4, 23\ (27)$, then $h_n = C$ iff $(\alpha^2 - \alpha + 1)^2 = C$.*
   iii. *Otherwise $h_n \neq C$ for every $\alpha \neq 0, 1$.*

Proof. 1. The proof of (i), (ii) are similar to proof of Theorem 5.1. For (iii), if $n \equiv 6, 7, 8, 10, 11$ or $12\ (18)$ then $h_n = \square$ iff

$$\alpha(\alpha - 1) = \square \tag{5}$$

by (3.7). But this is impossible by proof of Theorem 5.4.

Let $n \equiv 4, 14\ (18)$. Then $h_n = \square$ iff

$$\alpha^2 - \alpha + 1 = \square \tag{12}$$

by (3.7). This last equation leads to trivial equations

$$(2\alpha - 1)^2 - \beta^2 = -3 \qquad \text{or} \qquad (2\alpha - 1)^2 + \beta^2 = -3$$

where β is an integer. The last equation is impossible and from the first one we only have $\alpha = 0$ and 1.

If $n \equiv 2, 3, 15, 16\ (18)$ then $h_n = \square$ iff

$$(\alpha - 1)(\alpha^2 - \alpha + 1) = \square \tag{13}$$

by (3.7). As the products $\alpha - 1$ and $\alpha^2 - \alpha + 1$ are coprime we see that $\alpha^2 - \alpha + 1 = \square$ and this equation do not provide any acceptable α by above.

2. The proof of (i), is similar to proof of Theorem 5.1. For (ii), if $n \equiv 4$, 23 (27), then $h_n = C$ iff

$$(\alpha^2 - \alpha + 1)^2 = C \tag{14}$$

or equivalently $\alpha^2 - \alpha + 1 = C$ by (3.7). This last equation leads to a Mordell's equation

$$\beta^3 - 48 = (8\alpha - 4)^2$$

where β is an integer. From the tables in [18], we see that the only integer solutions to the equation are $(4, \pm 4)$, $(28, \pm 148)$. An easy computation shows that the only acceptable solutions of α are -18 and 19.

For (iii), if $n \equiv 8, 19$ (27), then $h_n = C$ iff

$$\alpha(\alpha - 1) = C, \tag{15}$$

if $n \equiv 10, 17$ (27), then $h_n = C$ iff

$$\alpha^2(\alpha - 1)^2 = C, \tag{16}$$

if $n \equiv 2, 25$ (27), then $h_n = C$ iff

$$\alpha^2(\alpha - 1)(\alpha^2 - \alpha + 1) = C, \tag{17}$$

if $n \equiv 5, 22$ (27), then $h_n = C$ iff

$$\alpha(\alpha - 1)(\alpha^2 - \alpha + 1)^2 = C, \tag{18}$$

and if $n \equiv 13, 14$ (27), then $h_n = C$ iff

$$\alpha^2(\alpha - 1)^2(\alpha^2 - \alpha + 1)^2 = C. \tag{19}$$

respectively by (3.7). These equations lead to trivial equation

$$\beta_1^3 - \beta_2^3 = 1$$

where $\alpha = \beta_1^3$, $\alpha - 1 = \beta_2^3$ and β_1, β_2 are integers. It is clear that this equation does not provide any acceptable α.

If $n \equiv 7, 20$ (27) then $h_n = C$ iff

$$\alpha(\alpha^2 - \alpha + 1) = C, \tag{20}$$

and if $n \equiv 11, 16$ (27) then $h_n = C$ iff

$$(\alpha - 1)^2(\alpha^2 - \alpha + 1) = C \tag{21}$$

respectively by (3.7). These equations lead to

$$\beta^3 - 48 = (8\alpha - 4)^2$$

where β is an integer. This equation was treated above. □

5.7. The Case $N = 10$. We determine the square or cube terms of the elliptic divisibility sequences for which the tenth term is zero in the following theorem.

Theorem 5.7. *Let (h_n) be an elliptic divisibility sequence for which the tenth term is zero (so that $h_n = 0$, for every $n \equiv 0$ (10)).*

1. i. *If $n \equiv 1, 9, 11, 19$ (20), then $h_n = \square$ for every $\alpha \neq 0, 1$.*
   ii. *If $n \equiv 4, 16$ (20), then $h_n = \square$ iff $-\alpha^2 + 3\alpha - 1 = \square$.*
   iii. *If $n \equiv 5, 15$ (20), then $h_n = \square$ iff $\alpha = \square$.*
   iv. *Otherwise $h_n \neq \square$ for every $\alpha \neq 0, 1$.*
2. i. *If $n \equiv 1, 11, 19, 29$ (30), then $h_n = C$.*
   ii. *If $n \equiv 3, 27$ (30), then $h_n = C$ iff $-\alpha^2 + 3\alpha - 1 = C$.*
   iii. *If $n \equiv 7, 13, 17, 23$ (30), then $h_n = C$ iff $2\alpha - 1 = C$.*
   iv. *Otherwise $h_n \neq C$ for every $\alpha \neq 0, 1$.*

Proof. 1. The cases (i) and (iii) can be proved in the same way as in Theorem 5.1. For (ii), if $n \equiv 4, 16$ (20), then $h_n = \square$ iff

$$-\alpha^2 + 3\alpha - 1 = \square \tag{22}$$

by (3.8). This equation leads to trivial equations

$$(2\alpha - 3)^2 \pm \beta^2 = 5$$

where β is an integer. The only solutions of these equations are $\alpha = 2$ and 3.

For (iv), if $n \equiv 2, 3, 7, 13, 17, 18$ (20), then $h_n = \square$ iff

$$\alpha(\alpha - 1)(2\alpha - 1) = \square \tag{9}$$

by (3.8). But this is impossible by proof of Theorem 5.5.

If $n \equiv 6, 14$ (20), then $h_n = \square$ iff

$$\alpha(\alpha - 1) = \square \tag{5}$$

by (3.8), but this is impossible by proof of Theorem 5.4.

If $n \equiv 8, 12$ (20), then $h_n = \square$ iff

$$(2\alpha - 1)(-\alpha^2 + 3\alpha - 1) = \square \tag{23}$$

by (3.8). Since the factors $2\alpha - 1$ and $-\alpha^2 + 3\alpha - 1$ are coprime we have $2\alpha - 1 = \square$ and $-\alpha^2 + 3\alpha - 1 = \square$. But this is impossible by case (ii).

2. The cases (i) and (iii) can be proved in the same way as in Theorem 5.1. For (ii), if $n \equiv 3, 27$ (30), then $h_n = C$ iff

$$-\alpha^2 + 3\alpha - 1 = C \tag{24}$$

by (3.8). This equation leads to Mordell's equation

$$\beta^3 + 80 = (8\alpha - 12)^2 \tag{5.2}$$

where β is an integer. From the tables in [18] we see the only integer solutions to the equation are $(-4, \pm 4)$, $(4, \pm 12)$, $(1, \pm 9)$, $(44, \pm 292)$. Now we can easily verify that the only acceptable solutions of α are 2, 3, 38 and -35.

For (iv), if $n \equiv 2, 8, 22, 28$ (30), then $h_n = C$ iff

$$(\alpha - 1)(2\alpha - 1)(-\alpha^2 + 3\alpha - 1) = C \tag{25}$$

by (3.8). This equation leads to classical equation

$$\beta_2^3 + 2(-\beta_1^3) = 1$$

where $\alpha - 1 = \beta_1^3$, $2\alpha - 1 = \beta_2^3$ and β_1, β_2 are integers and the only solution of this equation is $(\beta_1, \beta_2) = (-1, -1)$ and this equation does not provide any acceptable α.

If $n \equiv 4, 14, 16, 26$ (30), then $h_n = C$ iff

$$\alpha(-\alpha^2 + 3\alpha - 1) = C, \tag{26}$$

if $n \equiv 9, 21$ (30), then $h_n = C$ iff

$$(2\alpha - 1)^2(-\alpha^2 + 3\alpha - 1) = C, \tag{27}$$

if $n \equiv 12, 18$ (30), then $h_n = C$ iff

$$(\alpha - 1)(-\alpha^2 + 3\alpha - 1)^2 = C, \tag{28}$$

by (3.8) or equivalently $\alpha^2 - 3\alpha + 1 = C$. This last equation leads to equation (5.2). This equation does not provide any acceptable α.

If $n \equiv 5, 25$ (30), then $h_n = C$ iff

$$\alpha(\alpha - 1)(2\alpha - 1) = C, \tag{29}$$

if $n \equiv 15$ (30), then $h_n = C$ iff

$$\alpha(\alpha - 1)(-\alpha^2 + 3\alpha - 1) = C. \tag{30}$$

by (3.8). These equations leads to trivial equation

$$\beta_1^3 - \beta_2^3 = 1$$

where $\alpha = \beta_1^3$, $\alpha - 1 = \beta_2^3$ and β_1, β_2 are integers. The solutions of this equation do not provide any acceptable α.

If $n \equiv 6, 24$ (30), then $h_n = C$ iff

$$\alpha(2\alpha - 1)^2(-\alpha^2 + 3\alpha - 1)^2 = C. \tag{31}$$

This equation leads to classical equation

$$(-\beta_2)^3 + 2\beta_1^3 = 1$$

where $\alpha = \beta_1^3$, $2\alpha - 1 = \beta_2^3$ and β_1, β_2 are integers. The only solution of this equation is $(\beta_1, \beta_2) = (1, 1)$ and this solution does not provide any acceptable α. □

5.8. The Case $N = 12$. We determine the square or cube terms of the elliptic divisibility sequences for which the twelfth term is zero in the following theorem.

Theorem 5.8. *Let (h_n) be an elliptic divisibility sequence for which the twelfth term is zero (so that $h_n = 0$, for every $n \equiv 0\ (12)$).*

1. i. *If $n \equiv 1, 23\ (24)$, then $h_n = \square$ for every $\alpha \neq 0, 1$.*
   ii. *If $n \equiv 5, 19\ (24)$, then $h_n = \square$ iff $3\alpha^2 - 3\alpha + 1 = \square$.*
   iii. *Otherwise $h_n \neq \square$ for all $\alpha \neq 0, 1$.*
2. i. *If $n \equiv 1, 35\ (36)$, then $h_n = C$ for every $\alpha \neq 0, 1$.*
   ii. *If $n \equiv 3, 9, 15, 21, 27, 33\ (36)$, then $h_n = C$ iff $\alpha - 1 = C$.*
   iii. *Otherwise $h_n \neq C$ for all $\alpha \neq 0, 1$.*

Proof. 1. The case (i) can be proved in the same way as in Theorem 5.1. For (ii), if $n \equiv 5, 19\ (24)$, then $h_n = \square$ iff

$$3\alpha^2 - 3\alpha + 1 = \square \tag{32}$$

by (3.9). It follows that

$$\beta^2 - 3(2\alpha - 1)^2 = 1 \tag{5.3}$$

or

$$\beta^2 + 3(2\alpha - 1)^2 = -1,$$

where β is an integer. The last equation is impossible modulo 3, and the first leads to Pell equation. If we rewrite equation (5.3) as

$$(\beta + (2\alpha - 1)\sqrt{3}\,)(\beta - (2\alpha - 1)\sqrt{3}\,) = 1$$

we see that the solutions of this equation are $(2, 1), (7, 4), (26, 15), \dots$ and parameters α corresponding to these solutions are $1, \frac{5}{2}, 8, \dots$. It can easily be seen that the only odd solutions of this Pell equation gives the desired solution of α, i.e., for such an α, $3\alpha^2 - 3\alpha + 1$ is a square and their number is infinite.

For (iii), if $n \equiv 2, 3, 10, 14, 21, 22\ (24)$, then $h_n = \square$ iff

$$\alpha(2\alpha - 1)(2\alpha - 2\alpha^2 - 1)(3\alpha^2 - 3\alpha + 1) = \square \tag{33}$$

by (3.9). Notice that the factors α, $2\alpha - 1$, $2\alpha - 2\alpha^2 - 1$, $3\alpha^2 - 3\alpha + 1$ are pairwaise coprime. Now the product of four pairwaise coprime number is a square only when each is a square. This implies that $\alpha = \square$, $2\alpha - 1 = \square$ which is impossible by the above argument.

If $n \equiv 4, 8, 16, 20\ (24)$, then $h_n = \square$ iff

$$(\alpha - 1)(2\alpha - 2\alpha^2 - 1) = \square \tag{34}$$

by (3.9). This equation leads to

$$(-2\alpha)^3 + 4(-2\alpha)^2 + 6(-2\alpha) + 4 = \beta^2$$

or

$$(2\alpha)^3 - 4(2\alpha)^2 + 6(2\alpha) - 4 = \beta^2.$$

where β is an integer. From the last equation we have an elliptic curve with rank 0 and torsion points on this curve do not provide any acceptable α. From the first equation we have an elliptic curve with rank 1 and applying the *Elliptic Logarithm Method* we see that the only solutions to this equation are $\alpha = 0$, 1 and -3. So we have $\alpha = -3$.

If $n \equiv 6, 18$ (24), then $h_n = \square$ iff

$$\alpha(3\alpha^2 - 3\alpha + 1) = \square, \tag{35}$$

if $n \equiv 11, 13$ (24), then $h_n = \square$ iff

$$\alpha(\alpha - 1)(3\alpha^2 - 3\alpha + 1) = \square. \tag{36}$$

by (3.9), or equivalently $\alpha(3\alpha^2 - 3\alpha + 1) = \square$. This equation leads to

$$(3\alpha)^3 - 3(3\alpha)^2 + 3(3\alpha) = \beta^2$$

or

$$(-3\alpha)^3 + 3(-3\alpha)^2 + 3(-3\alpha) = \beta^2.$$

where β is an integer. From these equations we have elliptic curves with rank 0 and torsion points on these curves do not provide any acceptable α.

If $n \equiv 7, 17$ (24), then $h_n = \square$ iff

$$\alpha(\alpha - 1) = \square. \tag{5}$$

But this is impossible by proof of Theorem 5.4.

If $n \equiv 9, 15$ (24), then $h_n = \square$ iff

$$(\alpha - 1)(2\alpha - 1)(2\alpha - 2\alpha^2 - 1) = \square. \tag{37}$$

by (3.9). This equation leads to

$$(4\alpha)^3 - 6(4\alpha)^2 + 16(4\alpha) - 16 = \beta^2$$

or

$$(-4\alpha)^3 + 6(-4\alpha)^2 + 16(-4\alpha) + 16 = \beta^2$$

where β is an integer. From these equations we have elliptic curves with rank 0 and torsion points on these curves do not provide any acceptable α.

2. The cases (i) and (ii) can be proved in the same way as in Theorem 5.1. For (iii), if $n \equiv 2, 34$ (36), then $h_n = C$ iff

$$\alpha(2\alpha - 1)(\alpha - 1)^2(2\alpha - 2\alpha^2 - 1)(3\alpha^2 - 3\alpha + 1) = C, \tag{38}$$

if $n \equiv 8, 28$ (36), then $h_n = C$ iff

$$\alpha(\alpha-1)^2(2\alpha-1)^2 = C, \tag{39}$$

if $n \equiv 11, 25$ (36), then $h_n = C$ iff

$$\alpha(\alpha-1)(2\alpha-1)^2(2\alpha-2\alpha^2-1)^2 = C, \tag{40}$$

if $n \equiv 13, 23$ (36), then $h_n = C$ iff

$$\alpha^2(\alpha-1)^2(2\alpha-1)(2\alpha-2\alpha^2-1)^2 = C, \tag{41}$$

if $n \equiv 17, 19$ (36), then $h_n = C$ iff

$$\alpha^2(\alpha-1) = C \tag{42}$$

by (3.9). These equations lead to trivial equation

$$\beta_1^3 - \beta_2^3 = 1$$

where $\alpha = \beta_1^3$, $\alpha - 1 = \beta_2^3$ and β_1, β_2 are integers. This equation does not provide any acceptable α.

If $n \equiv 4, 32$ (36), then $h_n = C$ iff

$$(\alpha-1)(2\alpha-2\alpha^2-1)^2 = C, \tag{43}$$

if $n \equiv 14, 22$ (36), then $h_n = C$ iff

$$\alpha^2(2\alpha-2\alpha^2-1)^2(3\alpha^2-3\alpha+1) = C. \tag{44}$$

by (3.9). These equations lead to Mordell's equation

$$\beta^3 - 4 = (4\alpha-2)^2$$

where β is an integer. From the tables in [18], we see that the integral solutions to this equation do not provide any acceptable α.

If $n \equiv 5, 31$ (36), then $h_n = C$ iff

$$\alpha(2\alpha-1)(2\alpha-2\alpha^2-1)^2 = C, \tag{45}$$

if $n \equiv 16, 20$ (36), then $h_n = C$ iff

$$\alpha^2(2\alpha-1)(2\alpha-2\alpha^2-1) = C, \tag{46}$$

by (3.9). These equations lead to classical equation

$$(-\beta_2)^3 + 2\beta_1^3 = 1$$

where $\alpha = \beta_1^3$, $2\alpha - 1 = \beta_2^3$ and β_1, β_2 are integers. The only solution of this equation is $(\beta_1, \beta_2) = (1, 1)$ and this solution does not provide any acceptable α.

If $n \equiv 6, 18, 30$ (36), then $h_n = C$ iff

$$(\alpha - 1)^2(2\alpha - 1)^2(3\alpha^2 - 3\alpha + 1) = C, \tag{47}$$

if $n \equiv 7, 29$ (36), then $h_n = C$ iff

$$(\alpha - 1)^2(2\alpha - 1)^2(2\alpha - 2\alpha^2 - 1) = C, \tag{48}$$

if $n \equiv 10, 26$ (36), then $h_n = C$ iff

$$(\alpha - 1)(2\alpha - 1)^2(3\alpha^2 - 3\alpha + 1) = C, \tag{49}$$

by (3.9). These equations lead to classical equation

$${\beta_2}^3 + 2(-\beta_1)^3 = 1$$

where $\alpha - 1 = \beta_1^3$, $2\alpha - 1 = \beta_2^3$ and β_1, β_2 are integers. The solution of this equation is $(\beta_1, \beta_2) = (-1, -1)$ and this solution does not provide any acceptable α. □

Acknowledgements. I would like to thank Joseph H. Silverman for looking at the initial draft and making suggestions for the first parts of the paper. I am also grateful to Nikos Tzanakis for his helpful suggestions for improving the paper. Finally, I would like to thank the referee for his/her warnings to make the paper more readable.

References

[1] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I, The user language, *J. Symbolic Comput.* **24**, no. 3–4 (1997), 235–265.

[2] A. Bremner and N. Tzanakis, Lucas sequences whose 12th or 9th term is a square, *J. Number Theory* **107** (2004), 215–227.

[3] A. Bremner and N. Tzanakis, On squares in Lucas sequences, *J. Number Theory* **124** (2007), 511–520.

[4] M. Einsiedler, G. Everest and T. Ward, Primes in elliptic divisibility sequences, *LMS J. Comput. Math.* **4** (2001), electronic 1–13.

[5] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, Recurrence Sequences, Mathematical Surveys and Monographs 104, *AMS, Providence, RI*, 2003.

[6] I. Garcia-Selfa, M. A. Olalla and J. M. Tornero, Computing the rational torsion of an elliptic curve using Tate normal form, *J. Number Theory* **96** (2002), 76–88.

[7] J. Gebel, A. Pethő and H. G. Zimmer, Computing integral points on elliptic curves, *Acta Arith.* **68** (1994), 171–192.

[8] J. Gebel, A. Pethő and H. G. Zimmer, On Mordell's equation, *Compositio Math.* **110** (1998), 335–367.

[9] B. Gezer and O. Bizim, Squares in elliptic divisibility sequences, *Acta Arith.* **144**(2) (2010), 125–134.

[10] B. Gezer and O. Bizim, Cubes in elliptic divisibility sequences, *Math. Rep. (Bucur.)* **14**(64), no. 1 (2012), 21–29.

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

[12] D. S. Kubert, Universal bounds on the torsion of elliptic curves, *Proc. London Math. Soc.* **33**(3) (1976), 193–237.

[13] http://magma.maths.usyd.edu.au/calc/.

[14] B. Mazur, Modular curves and the Eisenstein ideal, *IHES Publ. Math.* **47** (1977), 33–186.

[15] L. J. Mordell, Diophantine Equations, Pure and Applied Mathematics 30, *Academic Press, London and New York*, 1970.

[16] http://pari.maths.u-bordeaux.fr/.

[17] A. Pethő, Full cubes in the Fibonacci sequence, *Publ. Math. Debrecen* **30** (1983), 117–127.

[18] A. Pethő, On Mordell's equation,
http://www.inf.unideb.hu/ ~pethoe/cikkek/Mordell_adat/MORDELL-.htm,
http://www.inf.unideb.hu/ ~pethoe/cikkek/Mordell_adat/MORDELL+.htm.

[19] J. Reynolds, Perfect powers in elliptic divisibility sequences, *J. Number Theory* **132** (2012), 998–1015.

[20] P. Ribenboim, Pell numbers, squares and cubes, *Publ. Math. Debrecen* **54** (1999), 131–152.

[21] P. Ribenboim and W. McDaniel, The square terms in Lucas sequences, *J. Number Theory* **58** (1996), 104–123.

[22] P. Ribenboim and W. McDaniel, Squares in Lucas sequences having an even first parameter, *Colloq. Math.* **78** (1998), 29–34.

[23] R. Shipsey, Elliptic divisibility sequences, Ph.D. thesis, *Goldsmith's (University of London)*, 2000.

[24] J. H. Silverman, The Arithmetic of Elliptic Curves 2nd Edition, Graduate Texts in Mathematics 106, *Springer, Dordrecht, Heidelberg, London New York*, 2009.

[25] J. H. Silverman and J. Tate, Rational Points on Elliptic Curves, Undergraduate Texts in Mathematics, *Springer-Verlag, New York*, 1992.

[26] R. J. Stroeker and N. Tzanakis, Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms, *Acta Arith.* **67** (1994), 177–196.

[27] C. S. Swart, Elliptic curves and related sequences, Ph.D. thesis, *Royal Holloway (University of London)*, 2003.

[28] M. Ward, The law of repetition of primes in an elliptic divisibility sequences, *Duke Math. J.* **15** (1948), 941–946.

[29] M. Ward, Memoir on elliptic divisibility sequences, *Amer. J. Math.* **70** (1948), 31–74.

BETÜL GEZER
DEPARTMENT OF MATHEMATICS
ULUDAG UNIVERSITY
GÖRÜKLE
16059, BURSA
TURKEY

E-mail: betulgezer@uludag.edu.tr.

(Received August 27, 2012; revised April 18, 2013)