ACTA ARITHMETICA
144.2 (2010)

Squares in elliptic divisibility sequences

by

BETÜL GEZER and OSMAN BİZİM (Bursa)

This paper is dedicated to Professor Turgut Başkan
on the occasion of his seventieth birthday

1. Introduction. A *divisibility sequence* is a sequence (h_n) $(n \in \mathbb{N})$ of integers with the property that $h_m \mid h_n$ if $m \mid n$. One of the oldest examples of a divisibility sequence is the Fibonacci sequence. There are also elliptic divisibility sequences satisfying a nonlinear recurrence relation that comes from the recursion formula for elliptic division polynomials associated to an elliptic curve.

An *elliptic divisibility sequence* (or EDS) is a sequence (h_n) of integers satisfying the 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 $m \geq n \geq 1$.

EDSs are generalizations of a class of integer divisibility sequences called *Lucas sequences*. EDSs are interesting because they were the first nonlinear divisibility sequences to be studied. Morgan Ward wrote several papers detailing the arithmetic theory of EDSs [10, 11]. For the arithmetic properties of EDSs, see also [4, 5, 6, 8, 9]. Shipsey [8] used EDSs to study some applications to cryptography and the elliptic curve discrete logarithm problem (ECDLP). The Chudnovsky brothers considered prime values of EDSs in [3]. EDSs are connected to heights of rational points on elliptic curves and to the elliptic Lehmer problem.

2. Some preliminaries on elliptic divisibility sequences. There are two useful formulas (known as duplication formulas) to calculate the terms of an EDS. These formulas are obtained from (1.1) by setting first

2010 *Mathematics Subject Classification*: 11B37, 11B39, 11D09.
Key words and phrases: elliptic divisibility sequences, squares in EDSs.

$m = n+1, n = m$ and then $m = n+1$, $n = m-1$:

$$h_{2n+1} = h_{n+2}h_n^3 - h_{n-1}h_{n+1}^3, \tag{2.1}$$

$$h_{2n}h_2 = h_n(h_{n+2}h_{n-1}^2 - h_{n-2}h_{n+1}^2). \tag{2.2}$$

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 $h_2 \mid h_4$. The sequence (h_n) with initial values $h_0 = 0, h_1 = 1, h_2, h_3$ and h_4 is denoted by $[1\ h_2\ h_3\ h_4]$.

In this work, first, we give the general terms of the EDSs. Then we determine which terms h_n are squares. To classify EDSs we need to know the 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). If ρ is an integer such that $m \mid h_\rho$ and there is no integer j such that j is a divisor of ρ with $m \mid h_j$, then ρ is said to be the *rank of apparition* of m in (h_n). Ward established that the multiples of ρ are regularly spaced in (h_n) in the following theorem.

Theorem 1 ([11]). *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*

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

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

$$s_{n+\pi} \equiv s_n\ (m) \tag{2.3}$$

for all sufficiently large n. If (2.3) holds for all n, then (s_n) is said to be *purely periodic modulo m*. The smallest π for which (2.3) 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 how the period and rank are connected.

Theorem 2 ([11]). *Let (h_n) be an EDS and p 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 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 $\tau = 2^\alpha[e,k]$. Here $[e,k]$ is the least common multiple of e and k, and the exponent α is determined as follows:*

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

3. Elliptic divisibility sequences with zero terms. In this section we give general terms of the elliptic divisibility sequences with zero terms and we discuss some properties of these sequences. We determine the general terms of the EDSs whose second (resp. third, fourth, fifth, sixth) term is zero. First we consider the EDSs for which the second term is zero. We know that if $h_2 = 0$ then $h_{2n} = 0$ for all $n \in \mathbb{N}$. Ward gave the general term of these sequences. We rearrange his formula as follows: if (h_n) is an elliptic divisibility sequence with initial values $[1\ 0\ h_3\ h_4]$ $(h_3 \neq 0)$ and n is odd, then (h_n) is given by

$$h_n = h_{2k+1} = \varepsilon h_3^{k(k+1)/2} \tag{3.1}$$

where

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

3.1. Sequences for which the third term is zero. Now consider the EDSs for which the third term is zero. We know that if $h_3 = 0$ then $h_{3n} = 0$ for all $n \in \mathbb{N}$.

Theorem 3. *Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ 0\ h_4]$ $(h_2, h_4 \neq 0)$. Then (h_n) is given by*

$$h_n = h_{3k+a} = \varepsilon h_4^{k(k+1)/2} h_2^{(k+2a-2)(k+2a-3)/2} \tag{3.2}$$

where

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

Proof. It is clear that the result is true for $n = 4$. Hence we assume that $n > 4$. If (h_n) is an EDS then we know that

$$h_{n+2}h_{n-2} = h_{n+1}h_{n-1}h_2^2 - h_3h_1h_n^2. \tag{3.3}$$

We argue by induction on n. First suppose that $n+1 \equiv 4\ (12)$ and (3.2) is true for $n+1$. Then since $n+1 \equiv 4\ (12)$, we have $n+1 = 3(4r+1)+1$ $(r \in \mathbb{N})$ and so $n+2 = 3(4r+1)+2$. Thus we have to prove that $h_{n+2} = h_4^{8r^2+6r+1} h_2^{8r^2+10r+3}$. Indeed, we see that

$$\begin{aligned} h_{n+1} &= h_4^{8r^2+6r+1} h_2^{8r^2+2r}, \\ h_n &= 0, \\ h_{n-1} &= h_4^{8r^2+2r} h_2^{8r^2+6r+1}, \\ h_{n-2} &= h_4^{8r^2+2r} h_2^{8r^2-2r}. \end{aligned}$$

Substituting these expressions into (3.3) gives $h_{n+2} = h_4^{8r^2+6r+1} h_2^{8r^2+10r+3}$. Thus we have proved the conclusion for $n+1 \equiv 4\ (12)$. Other cases can be proved in the same way. ∎

3.2. Sequences for which the fourth term is zero. Now let (h_n) be an elliptic divisibility sequence for which the fourth term is zero. We know that if $h_4 = 0$ then $h_{4n} = 0$ for all $n \in \mathbb{N}$. The general term of (h_n) is determined in the following theorem.

THEOREM 4. *Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ 0]$ $(h_2, h_3 \neq 0)$. Then (h_n) is given by*

$$h_n = h_{4k+a} = \varepsilon h_2^{\beta} h_3^{2k^2+ak+\alpha} \tag{3.4}$$

where

$$\varepsilon = \begin{cases} +1 & \text{if } n \equiv 1,2,3\ (8), \\ -1 & \text{if } n \equiv 5,6,7\ (8), \end{cases} \qquad \alpha = \tfrac{1}{2}a^2 - \tfrac{3}{2}a + 1, \qquad \beta = \begin{cases} 1 & \text{if } 2 \mid n, \\ 0 & \text{if } 2 \nmid n. \end{cases}$$

Proof. We again argue by induction using (3.3). It is clear that the result is true for $n = 5$. Hence we assume that $n > 5$.

Now first suppose that $n+1 \equiv 2\ (8)$ and (3.4) is true for $n+1$. We wish to show that this equation is also true for $n+2$, i.e., $h_{n+2} = h_3^{8r^2+6r+1}$ for $n+2 = 4 \cdot 2r + 3$, $r \in \mathbb{N}$. On the other hand we know from assumption that $h_{n-2} = -h_3^{8r^2-2r}$ and similarly $h_n = h_3^{8r^2+2r}$. Substituting these relations into equation (3.3) gives

$$h_{n+2}(-h_3^{8r^2-2r}) = -h_3^{16r^2+4r+1}$$

and so we indeed obtain $h_{n+2} = h_3^{8r^2+6r+1}$. Thus we have proved the conclusion for $n+1 \equiv 2\ (8)$. Other cases can be proved in the same way. ∎

Now we give the period of (h_n) for which the fourth term is zero.

THEOREM 5. *Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ 0]$ $(h_2, h_3 \neq 0)$ and let q be the order of h_3 . Then the period of (h_n) is*

$$\pi(h_n) = \begin{cases} 4(p-1) & \text{if } h_3 \text{ is a primitive root in } \mathbb{F}_p, \\ 8r & \text{otherwise,} \end{cases}$$

where

$$r = \begin{cases} q & \text{if } q \text{ is odd,} \\ q/2 & \text{if } q \text{ is even.} \end{cases}$$

Proof. It is clear that $\rho = 4$ since $h_4 = 0$. Then since $a_1 = h_2/h_{\rho-2} = h_2/h_2 = 1$ and $a_2 = h_{\rho-1} = h_3$ we see that the orders of a_1 and a_2 are $e = 1$ and $k = p-1$ if h_3 is a primitive root in $\mathbb{F}_p$, and $k = q$ otherwise. Thus $[e,k] = k$. If h_3 is a primitive root in $\mathbb{F}_p$ then $\alpha = 0$ and in this case $\tau = 2^{\alpha}[e,k] = p-1$. Then $\pi(h_n) = 4(p-1)$, since $\rho = 4$. If h_3 is not a primitive root in $\mathbb{F}_p$ then the order of h_3 is q. So in this case $\alpha = 0$ or 1, hence $\tau = q$ or $2q$. Then $\pi(h_n) = 4q$ or $8q$ since $\rho = 4$. ∎

3.3. Sequences for which the fifth term is zero. Now let (h_n) be an elliptic divisibility sequence for which the fifth term is zero. We know that if $h_5 = 0$ then $h_{5n} = 0$ for all $n \in \mathbb{N}$. The general term of (h_n) is determined in the following theorem.

THEOREM 6. *Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ h_4]$ $(h_2, h_3, h_4 \neq 0)$ and for which the fifth term is zero. Then (h_n) is given by*

$$h_n = h_{5k+a} = \varepsilon h_3^{5k^2+2ak+\alpha} h_2^{-(5k^2+2ak+\beta)} \tag{3.5}$$

where

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

Proof. This can be proved in the same way as Theorems 3 and 4. ∎

Now we give the period of (h_n) for which the fifth term is zero.

THEOREM 7. *Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ h_4]$ $(h_2, h_3, h_4 \neq 0)$ and for which the fifth term is zero. Let q be the order of h_2/h_3. Then the period of (h_n) is*

$$\pi(h_n) = \begin{cases} \frac{5}{2}(p-1) & \text{if } h_2/h_3 \text{ is a primitive root in } \mathbb{F}_p, \\ 10r & \text{otherwise,} \end{cases}$$

where

$$r = \begin{cases} q & \text{if } q \text{ is odd,} \\ q/2 & \text{if } q \text{ is even.} \end{cases}$$

Proof. We know that the rank of (h_n) is $\rho = 5$. Then since

$$a_1 = \frac{h_2}{h_{\rho-2}} = \frac{h_2}{h_3} \quad \text{and} \quad a_2 = h_{\rho-1} = h_4 = \left(\frac{h_3}{h_2}\right)^3,$$

we see that the orders of a_1 and a_2 are respectively $e = p-1$ and $k = (p-1)/3$ if h_2/h_3 is a primitive root in $\mathbb{F}_p$, and $e = q$ and $k = q/3$ otherwise. If h_2/h_3 is a primitive root in $\mathbb{F}_p$ then $\alpha = -1$, since $p-1$ and $(p-1)/3$ are divisible by the same power of two, and in this case $\tau = 2^\alpha[e,k] = (p-1)/2$. Then $\pi(h_n) = \frac{5}{2}(p-1)$. If h_2/h_3 is not a primitive root in $\mathbb{F}_p$ then $\alpha = 1$ if q is odd, and $\alpha = -1$ if q is even, so $\tau = 2q$ and $q/2$, respectively. Then $\pi(h_n) = 10q$ if q is odd and $\frac{5}{2}q$ if q is even. ∎

3.4. Sequences for which the sixth term is zero. Now let (h_n) be an elliptic divisibility sequence for which the sixth term is zero. We know that if $h_6 = 0$ then $h_{6n} = 0$ for all $n \in \mathbb{N}$. We determine the general term of (h_n) in the following theorem.

THEOREM 8. *Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ h_4]$ $(h_2, h_3, h_4 = ch_2 \neq 0)$ and for which the sixth term is zero. Then (h_n) is given by*

$$h_n = h_{6k+a} = \varepsilon h_2^{\alpha} h_3^{\beta} c^{3k^2+ak+\gamma} \tag{3.6}$$

where

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

$$\alpha = \begin{cases} 1 & \text{if } 2 \mid n, \\ 0 & \text{if } 2 \nmid n, \end{cases} \qquad \beta = \begin{cases} 1 & \text{if } 3 \mid n, \\ 0 & \text{if } 3 \nmid n, \end{cases} \qquad \gamma = \begin{cases} 0 & \text{if } a \leq 3, \\ a-3 & \text{if } a > 3. \end{cases}$$

Proof. This can be proved in the same way as Theorems 3 and 4. ∎

Now we give the period of (h_n):

THEOREM 9. *Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ h_4]$ $(h_2, h_3, h_4 \neq 0)$ for which the sixth term is zero and let q be the order of h_2/h_4. Then period of (h_n) is*

$$\pi(h_n) = \begin{cases} 6(p-1) & \text{if } h_2/h_4 \text{ is a primitive root in } \mathbb{F}_p, \\ 12r & \text{otherwise}, \end{cases}$$

where

$$r = \begin{cases} q & \text{if } q \text{ is odd}, \\ q/2 & \text{if } q \text{ is even}. \end{cases}$$

Proof. This can be proved in the same way as Theorems 5 and 7. ∎

4. Squares in elliptic divisibility sequences. As we mentioned above, EDSs are generalizations of a class of integer divisibility sequences called Lucas sequences. The question of when a term of the Lucas sequence can be a square has generated some interest in the literature [1, 2, 7]. However, the question of which terms of EDS are perfect squares has not been studied.

In this section, we determine which term h_n of an EDS with zero terms can be a square. We consider the EDSs with second (resp. third, fourth, fifth, sixth) term zero. The symbol $\square$ means the square of a nonzero rational integer.

We first discuss the EDSs for which the second term is zero.

THEOREM 10. *Let (h_n) be an elliptic divisibility sequence with initial values $[1\ 0\ h_3\ 0]$ and $h_3 \neq 0$.*

(i) *If $n \equiv 1, 7\ (8)$, then $h_n = \square$.*
(ii) *If $n \equiv 3, 5\ (8)$, then $h_n = \square$ iff $h_3 = \square$.*

Proof. Let $n = 2k + 1$ ($k \in \mathbb{N}$). For (i), if $n \equiv 1$ or 7 (8), then $k = 4r$ or $4r + 3$ ($r, k \in \mathbb{N}$). Substituting these values into (3.1), we have

$$h_n = h_3^{8r^2+2r} \quad \text{and} \quad h_n = -h_3^{8r^2+14r+6},$$

respectively. Hence, $h_n = \square$.

For (ii), if $n \equiv 3$ or 5 (8), then $k = 4r + 1$ or $4r + 2$ ($r, k \in \mathbb{N}$). So

$$h_n = h_3^{8r^2+6r+1} \quad \text{and} \quad h_n = -h_3^{8r^2+10r+3},$$

respectively, by (3.1). Hence, $h_n = \square$ iff $h_3 = \square$. ∎

As particular cases of the preceding results and Theorem 10 we deduce the following corollary.

Corollary 11. *Let (h_n) be an elliptic divisibility sequence with initial values $[1\ 0\ h_3\ h_4]$ and $h_3 \neq 0$.*

(i) *If $h_3 = \square$, then $h_n = \square$ for all n.*
(ii) *If $h_3 \neq \square$, then $h_n = \square$ for $n \equiv 1, 7$ (8).*

Now consider the EDSs for which the third term is zero.

Theorem 12. *Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ 0\ h_4]$ with $h_2, h_4 = ch_2 \neq 0$.*

(i) *If $n \equiv 1, 11$ (12), then $h_n = \square$.*
(ii) *If $n \equiv 2, 10$ (12), then $h_n = \square$ iff $h_2 = \square$.*
(iii) *If $n \equiv 4, 8$ (12), then $h_n = \square$ iff $h_4 = \square$.*
(iv) *If $n \equiv 5, 7$ (12), then $h_n = \square$ iff $h_4 = h_2\square$.*

Proof. Let $n = 3k + a$ ($k \in \mathbb{N}$ and $a = 0, 1$ or 2). For (i), if $n \equiv 1$ or 11 (12) then $k = 4r$ or $4r + 3$ ($r, k \in \mathbb{N}$). Substituting these into (3.2), we have

$$h_n = h_4^{8r^2+2r} h_2^{8r^2-2r} \quad \text{and} \quad h_n = -h_4^{8r^2+14r+6} h_2^{8r^2+18r+10},$$

respectively, hence, $h_n = \square$.

For (ii), if $n \equiv 2$ or 10 (12) then $k = 4r$ or $4r + 3$ ($r, k \in \mathbb{N}$). Putting these into (3.2), we have

$$h_n = h_4^{8r^2+2r} h_2^{8r^2+6r+1} \quad \text{and} \quad h_n = -h_4^{8r^2+14r+6} h_2^{8r^2+10r+3},$$

respectively, so $h_n = \square$ iff $h_2 = \square$.

For (iii), if $n \equiv 4$ or 8 (12) then $k = 4r + 1$ or $4r + 2$ ($r, k \in \mathbb{N}$), and so

$$h_n = h_4^{8r^2+6r+1} h_2^{8r^2+2r} \quad \text{and} \quad h_n = -h_4^{8r^2+10r+3} h_2^{8r^2+14r+6},$$

respectively, by (3.2). Therefore, $h_n = \square$ iff $h_4 = \square$.

For (iv), if $n \equiv 5$ or 7 (12) then $k = 4r + 1$ or $4r + 2$ ($r, k \in \mathbb{N}$) and by (3.2) we have

$$h_n = h_4^{8r^2+6r+1} h_2^{8r^2+10r+3} = h_4^{2t+1} h_2^{2m+1} = h_2^{2(t+m+1)} c^{2t+1}$$

and

$$h_n = -h_4^{8r^2+10r+3} h_2^{8r^2+6r+1} = h_4^{2m+1} h_2^{2t+1} = h_2^{2(t+m+1)} c^{2m+1},$$

respectively, where $t, m \in \mathbb{N}$. Hence, $h_n = \square$ iff $c = \square$. ∎

As particular cases of the preceding results and Theorem 12 we deduce the following corollary.

Corollary 13. *Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ 0\ h_4]$ and $h_2, h_4 \neq 0$.*

(i) *If $h_2, h_4 = \square$, then $h_n = \square$ for all n.*
(ii) *If $h_2, h_4 \neq \square$, then $h_n = \square$ for* $\begin{cases} n \equiv 1, 11\ (12), \\ n \equiv 5, 7\ (12) \text{ if } c = \square. \end{cases}$
(iii) *If $h_2 = \square$ and $h_4 \neq \square$, then $h_n = \square$ for $n \equiv 1, 2, 10, 11\ (12)$.*
(iv) *If $h_2 \neq \square$ and $h_4 = \square$, then $h_n = \square$ for $n \equiv 1, 4, 8, 11\ (12)$.*

Now consider the sequences for which the fourth term is zero.

Theorem 14. *Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ 0]$ and $h_2, h_3 \neq 0$.*

(i) *If $n \equiv 1, 7\ (8)$, then $h_n = \square$.*
(ii) *If $n \equiv 2, 6\ (8)$, then $h_n = \square$ iff $h_2 = \square$.*
(iii) *If $n \equiv 3, 5\ (8)$, then $h_n = \square$ iff $h_3 = \square$.*

Proof. Let $n = 4k + a$ ($k \in \mathbb{N}$ and $a = 0, 1, 2$ or 3). For (i), if $n \equiv 1$ or $7\ (8)$ then $k = 2r$ or $2r + 1$ ($r, k \in \mathbb{N}$). Substituting these into (3.4), we have

$$h_n = h_3^{8r^2+2r} \quad \text{and} \quad h_n = -h_3^{8r^2+14r+6},$$

respectively. Hence, $h_n = \square$.

For (ii), if $n \equiv 2$ or $6\ (8)$ then $k = 2r$ or $2r + 1$ ($r, k \in \mathbb{N}$). Putting these into (3.4), we have

$$h_n = h_2 h_3^{8r^2+4r} \quad \text{and} \quad h_n = -h_2 h_3^{8r^2+12r+4},$$

respectively. Hence $h_n = \square$ iff $h_2 = \square$.

For (iii), if $n \equiv 3$ or $5\ (8)$ then $k = 2r$ or $2r + 1$ ($r, k \in \mathbb{N}$), and so

$$h_n = h_3^{8r^2+6r+1} \quad \text{and} \quad h_n = -h_3^{8r^2+10r+3},$$

respectively, by (3.4). Hence, $h_n = \square$ iff $h_3 = \square$. ∎

As particular cases of the preceding results and Theorem 14 we deduce the following corollary.

Corollary 15. *Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ 0]$ and $h_2, h_3 \neq 0$.*

(i) *If $h_2, h_3 = \square$, then $h_n = \square$ for all n.*
(ii) *If $h_2, h_3 \neq \square$, then $h_n = \square$ for $n \equiv 1, 7\ (8)$.*

(iii) *If* $h_2 = \square$ *and* $h_3 \neq \square$, *then* $h_n = \square$ *for* $n \equiv 1, 2, 6, 7\ (8)$.
(iv) *If* $h_2 \neq \square$ *and* $h_3 = \square$, *then* $h_n = \square$ *for* $n \equiv 1, 3, 5, 7\ (8)$.

Consider the sequences for which the fifth term is zero.

THEOREM 16. *Let* (h_n) *be an elliptic divisibility sequence with initial values* $[1\ h_2\ h_3\ h_4]$ *where* $h_2, h_3, h_4 \neq 0$ *and for which the fifth term is zero.*

(i) *If* $n \equiv 1, 9\ (10)$, *then* $h_n = \square$.
(ii) *If* $n \equiv 2, 8\ (10)$, *then* $h_n = \square$ *iff* $h_2 = \square$.
(iii) *If* $n \equiv 3, 7\ (10)$, *then* $h_n = \square$ *iff* $h_3 = \square$.
(iv) *If* $n \equiv 4, 6\ (10)$, *then* $h_n = \square$ *iff* $h_3 = h_2\square$.

Proof. This can be proved in the same way as Theorems 10, 12 and 14. ∎

As particular cases of the preceding results and Theorem 16 we deduce the following corollary.

COROLLARY 17. *Let* (h_n) *be an elliptic divisibility sequence with initial values* $[1\ h_2\ h_3\ h_4]$ *where* $h_2, h_3, h_4 \neq 0$ *and for which the fifth term is zero.*

(i) *If* $h_2, h_3 = \square$, *then* $h_n = \square$ *for all* n.
(ii) *If* $h_2, h_3 \neq \square$, *then* $h_n = \square$ *for* $\begin{cases} n \equiv 1, 9\ (10), \\ n \equiv 4, 6\ (10) \text{ if } h_3 = h_2\square. \end{cases}$
(iii) *If* $h_2 = \square$ *and* $h_3 \neq \square$, *then* $h_n = \square$ *for* $n \equiv 1, 2, 8, 9\ (10)$.
(iv) *If* $h_2 \neq \square$ *and* $h_3 = \square$, *then* $h_n = \square$ *for* $n \equiv 1, 3, 7, 9\ (10)$.

Consider the sequences for which the sixth term is zero.

THEOREM 18. *Let* (h_n) *be an elliptic divisibility sequence with initial values* $[1\ h_2\ h_3\ h_4]$ *where* $h_2, h_3, h_4 = ch_2 \neq 0$ *and for which the sixth term is zero.*

(i) *If* $n \equiv 1, 5, 7, 11\ (12)$, *then* $h_n = \square$.
(ii) *If* $n \equiv 2, 10\ (12)$, *then* $h_n = \square$ *iff* $h_2 = \square$.
(iii) *If* $n \equiv 3, 9\ (12)$, *then* $h_n = \square$ *iff* $h_3 = \square$.
(iv) *If* $n \equiv 4, 8\ (12)$, *then* $h_n = \square$ *iff* $h_4 = \square$.

Proof. This can be proved in the same way as Theorem 10, 12 and 14. ∎

As particular cases of the preceding results and Theorem 18 we deduce the following corollary.

COROLLARY 19. *Let* (h_n) *be an elliptic divisibility sequence with initial values* $[1\ h_2\ h_3\ h_4]$ *where* $h_2, h_3, ch_2 = h_4 \neq 0$ *and for which the sixth term is zero.*

(i) *If* $h_2, h_3, c = \square$, *then* $h_n = \square$ *for all* n.
(ii) *If* $h_2, h_3, c \neq \square$, *then* $h_n = \square$ *for* $\begin{cases} n \equiv 1, 5, 7, 11\ (12), \\ n \equiv 4, 8\ (12) \text{ if } h_4 = \square. \end{cases}$

(iii) *If* $h_2 = \square$ *and* $h_3, c \neq \square$, *then* $h_n = \square$ *for* $n \equiv 1, 2, 5, 7, 10, 11$ (12).
(iv) *If* $h_2, h_3 = \square$ *and* $c \neq \square$, *then* $h_n = \square$ *for* $n \equiv 1, 2, 3, 5, 7, 9, 10, 11$ (12).
(v) *If* $h_2, c = \square$ *and* $h_3 \neq \square$, *then* $h_n = \square$ *for* $n \equiv 1, 2, 4, 5, 7, 8, 10, 11$ (12).
(vi) *If* $h_3 = \square$ *and* $h_2, c \neq \square$, *then* $h_n = \square$ *for* $n \equiv 1, 3, 5, 7, 9, 11$ (12).
(vii) *If* $h_3, c = \square$ *and* $h_2 \neq \square$, *then* $h_n = \square$ *for* $n \equiv 1, 3, 5, 7, 9, 11$ (12).
(viii) *If* $c = \square$ *and* $h_2, h_3 \neq \square$, *then* $h_n = \square$ *for* $n \equiv 1, 5, 7, 11$ (12).

Acknowledgments. This work was supported by The Scientific and Technological Research Council of Turkey (project no. 107T311).

References

[1] A. Bremner and N. Tzanakis, *Lucas sequences whose 12th or 9th term is a square*, J. Number Theory 107 (2004), 215–227.
[2] —, —, *On squares in Lucas sequences*, ibid. 124 (2007), 511–520.
[3] D. V. Chudnovsky and G. V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality factorization tests*, Adv. Appl. Math. 7 (1986), 385–434.
[4] M. Einsiedler, G. Everest and T. Ward, *Primes in elliptic divisibility sequences*, LMS J. Comput. Math. 4 (2001), 1–13.
[5] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence Sequences*, Math. Surveys Monogr. 104, Amer. Math. Soc., Providence, RI, 2003.
[6] G. Everest and T. Ward, *Primes in divisibility sequences*, Cubo Mat. Educ. 3 (2001), 245–259.
[7] P. Ribenboim and W. McDaniel, *The square terms in Lucas sequences*, J. Number Theory 58 (1996), 104–123.
[8] R. Shipsey, *Elliptic divisibility sequences*, Ph.D. thesis, Goldsmith's (Univ. of London), 2000.
[9] C. S. Swart, *Elliptic curves and related sequences*, Ph.D. thesis, Royal Holloway (Univ. of London), 2003.
[10] M. Ward, *The law of repetition of primes in an elliptic divisibility sequence*, Duke Math. J. 15 (1948), 941–946.
[11] —, *Memoir on elliptic divisibility sequences*, Amer. J. Math. 70 (1948), 31–74.

Betül Gezer, Osman Bizim
Department of Mathematics
Faculty of Arts and Science
Uludag University
Görükle, 16059 Bursa, Turkey
E-mail: betulgezer@uludag.edu.tr
obizim@uludag.edu.tr

Received on 13.3.2009
and in revised form on 27.4.2010 (5970)