Hacettepe Journal of Mathematics and Statistics
Volume 38 (2) (2009), 161 – 171

ELLIPTIC DIVISIBILITY SEQUENCES IN CERTAIN RANKS OVER FINITE FIELDS

B. Gezer*† and O. Bizim*

Received 09 : 02 : 2009 : Accepted 04 : 05 : 2009

Abstract

We develop techniques first studied by Morgan Ward to characterize sequences which arise from elliptic curves and which contain a zero term. We first define elliptic divisibility sequences over finite fields by noting that they are not the sequences which arise by reduction from integer sequences. After that, we give general terms of these sequences over the finite fields $\mathbb{F}_p$ ($p > 3$ is a prime) and then we determine elliptic curves and singular curves associated with them.

Keywords: Elliptic divisibility sequences, Singular sequences, Elliptic curves, Singular curves.

2000 AMS Classification: 11 B 50, 11 A 07, 11 G 05.

1. Introduction

A *divisibility sequence* is a sequence (h_n) $(n \in \mathbb{N})$ of positive integers with the property that $h_m | h_n$ if $m|n$. The oldest example of a divisibility sequence is the Fibonacci sequence. 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 elliptic division polynomials associated with an elliptic curve.

An *elliptic divisibility sequence* (or EDS) is a sequence of integers (h_n) satisfying a non-linear 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 with the divisibility property that h_m divides h_n whenever m divides n for all $m \geq n \geq 1$.

*Uludag University, Faculty of Science, Department of Mathematics, Görükle, 16059, Bursa, Turkey.
E-mail: (B. Gezer) betulgezer@uludag.edu.tr (O. Bizim obizim@uludag.edu.tr
†Corresponding author

†This work was supported by The Scientific and Technological Research Council of Turkey, Project No: 107T311.

EDSs are a generalization of a class of integer divisibility sequences called *Lucas sequences* [10]. EDSs were of interest because they were the first non-linear divisibility sequences to be studied. Morgan Ward wrote several papers detailing the arithmetic theory of EDSs, [11, 12]. For the arithmetic properties of EDSs, see also [2, 3, 4, 5, 9]. Shipsey and Swart, [5, 9], were interested in the properties of EDSs reduced modulo primes. Shipsey [5] 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 [1]. EDSs are connected to the heights of rational points on elliptic curves and the elliptic Lehmer problem.

2. Some preliminaries on elliptic divisibility sequences and elliptic curves

There are two useful formulas (known as duplication formulas) used to calculate the terms of an EDS. The duplication formulas are obtained by setting first $m = r+1$, $n = r$ and then $m = r+1$, $n = r-1$ in (1.1):

$$h_{2r+1} = h_{r+2}h_r^3 - h_{r-1}h_{r+1}^3, \tag{2.1}$$

$$h_{2r}h_2 = h_r(h_{r+2}h_{r-1}^2 - h_{r-2}h_{r+1}^2) \tag{2.2}$$

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

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 and h_4 are integers with $h_2|h_4$. The sequence (h_n) with initial values $h_1 = 1, h_2, h_3$ and h_4, is denoted by $[1\ h_2\ h_3\ h_4]$. The *discriminant* of an elliptic divisibility sequence (h_n) is defined by the formula:

$$\Delta(h_2,h_3,h_4) = h_4h_2^{15} - h_3^3h_2^{12} + 3h_4^2h_2^{10} - 20h_4h_3^3h_2^7 + 3h_4^3h_2^5 + 16h_3^6h_2^4 + 8h_4^2h_3^3h_2^2 + h_4^4.$$

An elliptic divisibility sequence (h_n) is said to be *singular* if and only if its discriminant $\Delta(h_2, h_3, h_4)$ vanishes.

In this work we discuss the behavior of some special EDSs over a finite field $\mathbb{F}_p$, where $p > 3$ is a prime, and also the elliptic curves associated with (h_n). To classify EDSs modulo p 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 with positive suffix. Let m be a divisor of (h_n). If ρ is an integer such that $m \,|\, h_\rho$ and there is no integer j such that j is a divisor of ρ with $m \,|\, h_j$, then ρ is said to be the *rank of apparition* of m in (h_n). In the following theorem Ward said that the multiples of p are regularly spaced in (h_n).

2.1. Theorem. [12] *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*

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

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 such integer π for which (2.3) is true is called the *period* of (s_n) modulo m. All other periods are multiples of it.

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

2.2. Theorem. [12] *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 $a_1 \equiv \frac{h_2}{h_{\rho-2}}\ (p)$ and let e and k be the exponents of a_1 and $a_2 \equiv h_{\rho-1}\ (p)$. 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:*

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

We will now give a short account of material about elliptic curves. More details of the theory of elliptic curves can be found in [6, 8]. Consider an elliptic curve defined over the rational numbers determined by a short Weierstrass equation $y^2 = x^3 + ax + b$ with coefficients $a, b \in \mathbb{Q}$ and discriminant $\Delta = -16(4a^3 + 27b^2)$.

Ward proved that EDSs arise as values of the division polynomials of an elliptic curve. We will write $\psi_n(P)$ for ψ_n evaluated at the point $P = (x_1, y_1)$. The following theorem shows us the relations between EDSs and the elliptic curves (for further details see [5, 7, 9, 12]).

2.3. Theorem. [7] *Let (h_n) be an elliptic divisibility sequence $[1\ h_2\ h_3\ ch_2]$. Then there exists an elliptic curve $E : y^2 = x^3 + ax + b$ where $a, b \in \mathbb{Q}$, and a non singular rational point $P = (x_1, y_1)$ on E such that $\psi_n(x_1, y_1) = h_n$ for all $n \in \mathbb{Z}$ where ψ_n is the n-th polynomial of E. These quantities are given by*

$$a = 3^3\left(\begin{array}{r}(-h_2^{16} - 4ch_2^{12} + (16h_3^3 - 6c^2)h_2^8 + (8ch_3^3 - 4c^3)h_2^4 \\ -(16h_3^6 + 8c^2h_3^3 + c^4)\end{array}\right), \tag{2.4}$$

$$b = 2.3^3\left(\begin{array}{r}h_2^{24} + 6ch_2^{20} - (24h_3^3 - 15c^2)h_2^{16} - (60ch_3^3 - 20c^3)h_2^{12} \\ +(120h_3^6 - 36c^2h_3^3 + 15c^4)h_2^8 + (-48ch_3^6 + 12c^3h_3^3)h_2^4 \\ +(64h_3^9 + 48c^2h_3^6 + 12c^4h_3^3 + c^6)\end{array}\right), \tag{2.5}$$

$$P = (x_1, y_1) = \left(3(h_2^8 + 2ch_2^4 + 4h_3^3 + c^2), -108h_3^3h_2^4\right), \tag{2.6}$$

and

$$\Delta = 2^8 3^{12} h_3^9 h_2^8 (ch_2^{12} + (-h_3^3 + 3c^2)h_2^8 + (-20ch_3^3 + 3c^3)h_2^4 + (16h_3^6 + 8c^2h_3^3 + c^4)).$$

By Theorem 2.3, we can say that the EDS $[1\ h_2\ h_3\ ch_2]$ is associated with the elliptic curve $E : y^2 = x^3 + ax + b$ and the rational point $P \in E$. Note that if E is a singular curve, then possibly P is a singular point. In this case we move P to any non singular point P' on E.

In the following theorem, Ward showed that the discriminant of an elliptic divisibility sequence is equal to the discriminant of the elliptic curve associated with this sequence.

2.4. Theorem. [12] *Let (h_n) be an elliptic divisibility sequence in which $h_2h_3 \neq 0$, and let E be an elliptic curve associated with (h_n). Then the discriminant of (h_n) is equal to discriminant of the elliptic curve E.*

3. Elliptic divisibility sequences in certain ranks

In this section we work with elliptic divisibility sequences in certain ranks over $\mathbb{F}_p$, where $p > 3$ is a prime, and we discuss some properties of these sequences. Firstly, we define elliptic sequences and then elliptic divisibility sequences over $\mathbb{F}_p$.

3.1. Definition. An elliptic sequence over $\mathbb{F}_p$ is a sequence of elements of $\mathbb{F}_p$ satisfying the formula

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

If (h_n) is an elliptic sequence over $\mathbb{F}_p$ then (h_n) is an *elliptic divisibility sequence over* $\mathbb{F}_p$ since any non-zero element of $\mathbb{F}_p$ divides any other. Therefore, in this paper, the term elliptic sequence over $\mathbb{F}_p$ will mean an elliptic divisibility sequence over $\mathbb{F}_p$. Of course, the concept of the rank of an elliptic divisibility sequence over $\mathbb{F}_p$ is the same as that for an elliptic divisibility sequence defined above.

Note that, as for integral sequences, elliptic divisibility sequences satisfy the further conditions that $h_0 = 0,\ h_1 = 1$, that two consecutive terms of (h_n) cannot vanish over $\mathbb{F}_p$ and if some term is zero, then multiples of this term are zero too, that is; if $h_2 = 0$ then $h_4 = 0$ and so $h_{2n} = 0$ for all $n \in \mathbb{N}$. This relation is shown below:

3.2. Lemma. *Let (h_n) be an elliptic divisibility sequence with rank ρ over $\mathbb{F}_p$. Then $h_{\rho n} \equiv 0\ (p)$.*

Proof. Let (h_n) be an elliptic divisibility sequence over $\mathbb{F}_p$. If (h_n) has rank ρ then $h_{\rho n} \equiv 0\ (p)$ since h_ρ divides $h_{\rho n}$ as ρ divides ρn. □

Now we consider the EDSs with rank two. We know that if $h_2 = 0$ then we must have $h_{2n} = 0$ for all integers $n \neq 0$. Thus every term of the sequence with even subscript is zero. Ward proved that such a sequence is given by the following formula for all odd n:

$$(h_n) = (-1)^{\lfloor \frac{n}{4} \rfloor} h_3^{\frac{n^2-1}{8}},$$

where $\lfloor x \rfloor$ denotes the greatest integer in x.

3.1. Sequences with rank three. Now consider the EDSs with rank three. We know that if $h_3 = 0$ then we must have $h_{3n} = 0$ for all integers $n \neq 0$.

3.3. Theorem. *Let (h_n) be an elliptic divisibility sequence $[1\ h_2\ 0\ h_4]$, $(h_2, h_4 \in \mathbb{F}_p^*)$. Then (h_n) is given by the following formula:*

$$h_n = h_{3k+a} = \varepsilon\ h_4^{\frac{k(k+1)}{2}}\ h_2^{\frac{(k+2a-2)(k+2a-3)}{2}}, \tag{3.1}$$

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

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

It suffices to prove our main result by induction based on equation (3.1). Now first suppose that $n + 1 \equiv 4\ (12)$ and let the equation (3.1) be 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 find that $h_{n+2} = h_4^{8r^2+6r+1}h_2^{8r^2+10r+3}$. On the other hand 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 (3.1) gives $h_{n+2} = h_4^{8r^2+6r+1} h_2^{8r^2+10r+3}$. Thus we proved this theorem for $n+1 \equiv 4$ (12). Other cases can be proved by induction in the same way. □

We know that if (h_n) is a proper EDS, then $h_2 \mid h_4$, so we may write $h_4 = ch_2$ where $c \in \mathbb{F}_p^*$. Thus we can give a new formula for the general terms of EDSs with rank three and parameter c.

3.4. Theorem. *Let (h_n) be an elliptic divisibility sequence* $[1\ h_2\ 0\ h_4]$, *($h_4 = ch_2$ and $c \in \mathbb{F}_p^*$). Then (h_n) is given by the following formula:*

$$h_n = h_{3k+a} = \varepsilon\, c^{\frac{k(k+1)}{2}} h_2^{(k+a-1)^2}$$

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

Proof. The theorem can be proved by induction in the same way as Theorem 3.1. □

3.2. Sequences with rank four. Now let (h_n) be an elliptic divisibility sequence with rank four, namely consider the sequences whose fourth term is zero. We know that if $h_4 = 0$, then $h_{4n} = 0$ for all integers $n \neq 0$. Firstly we give the general term of (h_n) with rank four in the following theorem:

3.5. Theorem. *Let (h_n) be an elliptic divisibility sequence* $[1\ h_2\ h_3\ 0]$ *and $(h_2, h_3 \in \mathbb{F}_p^*)$. Then (h_n) is given by the following formula:*

$$h_n = h_{4k+a} = \varepsilon\ h_2^{\beta} h_3^{2k^2+ak+\alpha}, \tag{3.2}$$

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

Proof. If (h_n) is an EDS, we know that

$$h_{n+2}h_{n-2} = h_{n+1}h_{n-1}h_2^2 - h_3 h_1 h_n^2 .$$

Then it suffices to prove our main result by induction based on equation (3.2). 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 let the equation (3.2) be true for $n+1$. We wish to show that this equation is also true for $n+2$. We want to see that $h_{n+2} = h_3^{8r^2+6r+1}$ is true, where $n+2 = 4 \cdot 2r+3$, $r \in \mathbb{N}$. On the other hand we know from the assumption that $h_{n-2} = -h_3^{8r^2-2r}$ and similarly $h_n = h_3^{8r^2+2r}$. Substituting these relations into equation (3.2) gives

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

and so we obtain that $h_{n+2} = h_3^{8r^2+6r+1}$. Thus we proved this theorem for $n+1 \equiv 2$ (8). Other cases of the theorem can be proved by induction in the same way. □

Now we give the period of (h_n) with rank four in the following theorem:

3.6. Theorem. *Let (h_n) be an elliptic divisibility sequence* $[1\ h_2\ h_3\ 0]$, *$(h_2, h_3 \in \mathbb{F}_p^*)$ and q 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 $r = \begin{cases} q & \text{if } q \text{ is odd} \\ \frac{q}{2} & \text{if } q \text{ is even.} \end{cases}$

Proof. It is clear that the rank of (h_n) is 4 since $h_4 = 0$, that is $\rho = 4$. Since $a_1 = \frac{h_2}{h_{\rho-2}} = \frac{h_2}{h_2} = 1$ and $a_2 = h_{\rho\ -1} = h_3$, by Theorem 2.2 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, then $\tau = q$ or $2q$. Hence $\pi(h_n) = 4q$ or $8q$ since $\rho = 4$. □

3.3. Sequences with rank five. Now let (h_n) be an elliptic divisibility sequence with rank five. We know that if $h_5 = 0$, then we must have $h_{5n} = 0$ for all integers $n \neq 0$. The general term of (h_n) is determined in the following theorem:

3.7. Theorem. *Let (h_n) be an elliptic divisibility sequence $[1\ h_2\ h_3\ h_4]$, $(h_2, h_3, h_4 \in \mathbb{F}_p^*)$, and having rank five. Then (h_n) is given by the following formula:*

$$h_n = h_{5k+a} = \varepsilon\ h_3^{5k^2+2ak+\alpha} h_2^{-(5k^2+2ak+\beta)}, \tag{3.3}$$

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

Proof. Since (h_n) is an EDS with rank five and $h_5 = h_4h_2^3 - h_3^3$, we have $h_4 = \left(\frac{h_3}{h_2}\right)^3$. It is clear that the result is true for $n = 6$. Hence we assume that $n > 6$. If (h_n) is an EDS, we know that

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

It suffices to prove our main result by induction based on equation (3.3). Now first suppose that $n+1 \equiv 2\ (10)$, and let the equation (3.3) be true for $n+1$. We want to see that $h_{n+2} = h_3^{20r^2+12r+1}\, h_2^{-(20r^2+12r)}$ is true, where $n+2 = 5\cdot 2r+3,\ r \in \mathbb{N}$. On the other hand we know from the assumption that $h_n = h_3^{20r^2+4r}\, h_2^{-(20r^2+4r)}$ and $h_{n-2} = -h_3^{20r^2-4r}\ h_2^{-(20r^2-4r)}$. Substituting these expressions into the equation (3.3), we have

$$h_{n+2}\left(-h_3^{20r^2-4r}\, h_2^{-(20r^2-4r)}\right) = -h_3\left(h_3^{20r^2+4r}\, h_2^{-(20r^2+4r)}\right)^2$$

and so $h_{n+2} = h_3^{20r^2+12r+1}\, h_2^{-(20r^2+12r)}$. Thus we have proved this theorem for $n+1 \equiv 2(10)$. Other cases can be proved by induction in the same way. □

Now we give the period of (h_n) with rank five in the following theorem:

3.8. Theorem. *Let (h_n) be an elliptic divisibility sequence $[1\ h_2\ h_3\ h_4]$, $(h_2, h_3 \in \mathbb{F}_p^*)$ with rank five and q the order of $\frac{h_2}{h_3}$. Then the period of (h_n) is*

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

where $r = \begin{cases} q & \text{if } q \text{ is odd} \\ \frac{q}{4} & \text{if } q \text{ is even.} \end{cases}$

Proof. We know that the rank of (h_n) is $\rho = 5$. Since $a_1 = \dfrac{h_2}{h_{\rho-2}} = \dfrac{h_2}{h_3}$ and $a_2 = h_{\rho-1} = h_4 = \left(\dfrac{h_3}{h_2}\right)^3$, by Theorem 2.2, let e and k be the orders of a_1 and a_2 respectively. If $\frac{h_2}{h_3}$

is a primitive root in $\mathbb{F}_p$, then $e = p-1$, $k = \frac{p-1}{3}$ when 3 divides $p-1$, and $e = p-1$, $k = p-1$ when 3 does not divide $p-1$. If $\dfrac{h_2}{h_3}$ is not a primitive root in $\mathbb{F}_p$, then $e = q$, $k = \frac{q}{3}$ when 3 divides q, and $e = q$, $k = q$ when 3 does not divide q. If $\dfrac{h_2}{h_3}$ is a primitive root in $\mathbb{F}_p$, then $\alpha = -1$, since $p-1$ and $\frac{p-1}{3}$ are divisible by the same power of two, and in this case $\tau = 2^{\alpha}[e,\ k] = \dfrac{p-1}{2}$. Then $\pi(h_n) = \frac{5}{2}(p-1)$.

If $\frac{h_2}{h_3}$ is not a primitive root in $\mathbb{F}_p$, then $\alpha = 1$ when q is odd, and $\alpha = -1$ when q is even; and $\tau = 2q$ and $\frac{q}{4}$, respectively. Then $\pi(h_n) = 10q$ if q is odd and $\frac{5}{2}q$ if q is even. □

3.4. Sequences with rank six. Now let (h_n) be an elliptic divisibility sequence with rank six. We know that if $h_6 = 0$ then we must have $h_{6n} = 0$ for all integers $n \neq 0$. We determine the general term of (h_n) in the following theorem:

3.9. Theorem. *Let (h_n) be an elliptic divisibility sequence $[1\ h_2\ h_3\ h_4]$, $(h_2,\ h_3,\ h_4 = ch_2 \in \mathbb{F}_p^*)$, and with rank six. Then (h_n) is given by the following formula:*

$$h_n = h_{6k+a} = \varepsilon\, h_2^{\alpha}\, h_3^{\beta}\, c^{3k^2+ak+\gamma}, \tag{3.4}$$

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

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

Proof. Since (h_n) is an EDS with rank six and $h_6 = \dfrac{h_3}{h_2}(h_5h_2^2 - h_4^2)$ we have $h_5 = \left(\dfrac{h_4}{h_2}\right)^2$. It is clear that the result is true for $n = 7$. Hence we assume that $n > 7$. If (h_n) is an EDS we know that

$$h_{n+2}h_{n-2} = h_{n+1}h_{n-1}h_2^2 - h_3h_1h_n^2$$

Then we prove our main result by induction based on equation (3.4). Now first suppose that $n+1 \equiv 2\ (12)$ and let the equation (3.4) be true for $n+1$. We want to see that $h_{n+2} = h_3\, c^{12r^2+6r}$ is true, where $n+2 = 6 \cdot 2r + 3$, $r \in \mathbb{N}$. On the other hand we know from the assumption that $h_n = c^{12r^2+2r}$ and $h_{n-2} = -c^{12r^2-2r}$. Substituting these expressions into (3.4) we have

$$h_{n+2}\left(-c^{12r^2-2r}\right) = -h_3\left(c^{12r^2+2r}\right)^2,$$

and so $h_{n+2} = h_3\, c^{12r^2+6r}$. Thus we have proved this theorem for $n+1 \equiv 2(10)$. Other cases can be proved by induction in the same way. □

Now we give the period of (h_n) in the following theorem:

3.10. Theorem. *Let (h_n) be an elliptic divisibility sequence $[1\ h_2\ h_3\ h_4]$, $(h_2,\ h_3 \in \mathbb{F}_p^*)$ with rank six and q the order of $\frac{h_2}{h_4}$. Then the period of (h_n) is*

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

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

Proof. We know that the rank of (h_n) is $\rho = 6$. Let e and k be the orders of $a_1 = \dfrac{h_2}{h_{\rho-2}} = \dfrac{h_2}{h_4}$ and $a_2 = h_{\rho-1} = h_5 = \left(\dfrac{h_4}{h_2}\right)^2$, respectively, where a_1 and a_2 are as in Theorem 2.2. If $\frac{h_2}{h_4}$ is a primitive root in $\mathbb{F}_p$, then $e = p-1$ and $k = \frac{p-1}{2}$. In this case $\alpha = 0$ and $\tau = p-1$, so that $\pi(h_n) = 6(p-1)$.

If $\dfrac{h_2}{h_4}$ is not a primitive root in $\mathbb{F}_p$, then there are two cases. In the first case, let q be even. Then $e = q$ and $k = q$, so that $\alpha = 1$ and $\tau = q$. Hence $\pi(h_n) = 6q$. In the second case, let q be odd. Then $e = q$ and $k = \frac{q}{2}$, so that $\alpha = 0$ and $\tau = 2q$. Hence $\pi(h_n) = 12q$. □

4. Elliptic divisibility sequences in certain ranks and the associated curves

In this section we determine the curves associated with (h_n) for ranks two, three, four, five and six.

First we find the associated curves for a (h_n) with rank two. Note that all elliptic divisibility sequences with rank two are singular since their discriminant is zero and so they are associated with a singular curve.

4.1. Theorem. *Let (h_n) be a singular elliptic divisibility sequence $[1\ 0\ h_3\ ch_2 = 0]$, $(c \in \mathbb{F}_p$ and $h_3 \in \mathbb{F}_p^*)$. Then (h_n) is associated with a singular curve given by the equation*

$$E : y^2 = x^3 - 27(4h_3^3 + c^2)^2 x + 54(4h_3^3 + c^2)^3, \tag{4.1}$$

and if $P = (x_1, y_1)$ is a non-singular point on E then $P = (3(h_3^3 + c^2),\ 0)$.

Proof. Putting $h_2 = 0$ in the equations (2.4), (2.5), (2.6), we have

$$a = -27(16h_3^6 + 8c^2h_3^3 + c^4) = -27(4h_3^3 + c^2)^2,$$
$$b = 54(64h_3^9 + 48c^2h_3^6 + 12c^4h_3^3 + c^6) = 54(4h_3^3 + c^2)^3$$

and $P = (3(4h_3^3 + c^2),\ 0)$. □

These singular curves have singular point as a cusp or a node. Now we determine when these curves have cusps, namely when they have the form $y^2 = x^3$.

4.2. Theorem. *Let (h_n) be an elliptic divisibility sequence $[1\ 0\ h_3\ 0]$, $(h_3 \in \mathbb{F}_p^*)$. Then*

$$(h_n) \text{ is associated with a singular curve with a cusp} \iff \begin{cases} h_3 \in Q_p & \text{if } p \equiv 1\ (4) \\ h_3 \notin Q_p & \text{if } p \equiv 3\ (4), \end{cases}$$

$$(h_n) \text{ is associated with a singular curve with a node} \iff \begin{cases} h_3 \notin Q_p & \text{if } p \equiv 1\ (4) \\ h_3 \in Q_p & \text{if } p \equiv 3\ (4), \end{cases}$$

where Q_p denotes the set of quadratic residues in $\mathbb{F}_p$.

Proof. The theorem can be proved by putting $h_3^3 = -\frac{c^2}{4}$ in (4.1). In this case the point P is a singular point on E. □

The elliptic divisibility sequence $[1\ 0\ h_3\ h_4 = ch_2 = 0]$, $(c \in \mathbb{F}_p$ and $h_3 \in \mathbb{F}_p^*)$, is an improper EDS. So, when we determine the fourth term $h_4 = ch_2$, we choose all elements of $\mathbb{F}_p$ for the number c. Therefore, such sequences can be associated with more than one curve. For example, in $\mathbb{F}_5$, the sequence $[1\ 0\ 1\ 0]$ is associated with the singular curves $y^2 = x^3 + 3x + 1$ for $c = 0$; $y^2 = x^3$ for $c = 1, 4$; and $y^2 = x^3 + 2x + 3$ for $c = 2, 3$.

Now we find the curves associated with (h_n) having rank three. Note that all elliptic divisibility sequences with rank three are singular since their discriminant is zero and so they are associated with a singular curve.

4.3. Theorem. *Let (h_n) be a singular elliptic divisibility sequence $[1\ h_2\ 0\ ch_2]$ and $(c,\ h_2 \in \mathbb{F}_p^*)$. Then (h_n) is associated with the singular curve E given by the equation*

$$E : y^2 = x^3 - 27(h_2^4 + c)^4 x + 54(h_2^4 + c)^6, \tag{4.2}$$

and if $P = (x_1, y_1)$ is a non-singular point on E then $P = (3(h_2^4 + c)^2, 0)$.

Proof. The theorem can be proved in the same way as Theorem 4.1. □

Now we see that when these singular EDSs are associated with the curve $y^2 = x^3$.

4.4. Theorem. *Let (h_n) be a singular elliptic divisibility sequence $[1\ h_2\ 0\ ch_2]$, $(c, h_2 \in \mathbb{F}_p^*)$. Then (h_n) is associated with the singular curve $E : y^2 = x^3$ if and only if $h_4 = -h_2^5$.*

Proof. The theorem can be proved by putting $h_2^4 = -c$ in (4.2). In this case the point P is a singular point on E. □

Now we will find elliptic curves associated with (h_n) having rank four.

4.5. Theorem. *Let (h_n) be an elliptic divisibility sequence $[1\ h_2\ h_3\ 0]$, $(h_2,\ h_3 \in \mathbb{F}_p^*)$. Then (h_n) is associated with an elliptic curve E given by the equation:*

$$E : y^2 = x^3 + 27(-h_2^{16} + 16ch_3^3h_2^8 - 16h_3^6)x + 54(h_2^{24} - 24h_3^3h_2^{16} + 120h_3^6h_2^8 + 64h_3^9),$$

and if $P = (x_1, y_1)$ is a point on E then $P = (3(h_2^8 + 4h_3^3), -108h_3^3h_2^4)$.

Proof. Since $h_4 = 0$ and since $h_2h_3 \neq 0$ we obtain $c = 0$. Putting $c = 0$ in (2.4), (2.5), (2.6), we find that

$$a = 27(-h_2^{16} + 16ch_3^3h_2^8 - 16h_3^6), \tag{4.3}$$

$$b = 54(h_2^{24} - 24h_3^3h_2^{16} + 120h_3^6h_2^8 + 64h_3^9), \tag{4.4}$$

$$P = (3(h_2^8 + 4h_3^3), -108h_3^3h_2^4). \tag{4.5}$$

□

Now we determine which of these curves are singular curves.

4.6. Theorem. *Let (h_n) be an elliptic divisibility sequence $[1\ h_2\ h_3\ 0]$, $(h_2 \in \mathbb{F}_p^*)$ and $h_3^3 = \dfrac{h_2^8}{16}$. Then (h_n) is associated with the singular curve E given by the equation $E : y^2 = x^3 - \frac{27}{16}h_2^{16}x - \frac{54}{64}h_2^{24}$ and if $P = (x_1, y_1)$ is a non singular point on E then $P = \left(\frac{15h_2^8}{4}, -\frac{27h_2^{12}}{4}\right)$.*

Proof. Since E is a singular curve if and only if (h_n) is a singular sequence, and $h_3^3 = \frac{h_2^8}{16}$, putting this equation in (4.3), (4.4) and (4.5) we have desired result. □

Note that in this case we have no singular curve of the form $y^2 = x^3$ since $h_2 \neq 0$.

Now we find elliptic curves associated with (h_n) having rank five.

4.7. Theorem. *Let (h_n) be an elliptic divisibility sequence $[1\ h_2\ h_3\ h_4]$, $(h_2,\ h_3, h_4 \in \mathbb{F}_p^*)$ and let $h_5 = 0$. Then (h_n) is associated with the elliptic curve E given by the equation:*

$$\begin{aligned} E : y^2 = x^3 &+ 27(-h_2^{16} + 12h_2^{12}c - 14h_2^8c^2 - 12h_2^4c^3 - c^4)x \\ &+ 54(h_2^{24} - 18h_2^{20}c + 75h_2^{16}c^2 + 75h_2^8c^4 + 18h_2^4c^5 + c^6), \end{aligned} \tag{4.6}$$

and if $P = (x_1, y_1)$ is a point on E then $P = (3(h_2^8 + 4h_3^3), -108h_3^3h_2^4)$.

Proof. Since $h_5 = 0$ we obtain $h_3^3 = h_2^4 c$. Putting $h_3^3 = h_2^4 c$ in (2.4), (2.5) and (2.6) we find the desired results. □

We will see when singular curves arise:

4.8. Theorem. *Let (h_n) be an elliptic divisibility sequence $[1\ h_2\ h_3\ ch_2]$, $(c,\ h_2,\ h_3 \in \mathbb{F}_p^*$ where $p > 5)$, and having rank five. Then there exists a singular curve E associated to (h_n) if and only if $p \equiv 1, 9\ (10)$.*

Proof. Since (h_n) is an EDS of rank five and $h_5 = h_4 h_2^3 - h_3^3 = 0$ we have $h_4 = ch_2 = \left(\frac{h_3}{h_2}\right)^3$. If the elliptic divisibility sequence $[1\ h_2\ h_3\ ch_2]$ is associated with a singular curve E then we know that this sequence is singular. That is,

$$\Delta = -h_2^4 h_3^6 + 11\frac{h_3^9}{h_2^4} + \frac{h_3^{12}}{h_2^{12}} = -h_2^{16} + 11h_2^{12}c + h_2^8 c^2 = 0.$$

So, we have $-h_2^8 + 11h_2^4 c + c^2 = 0$. If we substitute $h_2^4 = t$ in (4.6), then we have

$$t_{1,2} = h_2^4 = \frac{11 \pm 5\sqrt{5}}{2}c.$$

Thus (h_n) is associated with a singular curve if and only if 5 is a quadratic residue in $\mathbb{F}_p$. But, 5 is a quadratic residue in $\mathbb{F}_p$ if and only if $p \equiv 1, 9\ (10)$. □

Now we will find singular curves associated with (h_n).

4.9. Theorem. *Let (h_n) be an elliptic divisibility sequence $[1\ h_2\ h_3\ ch_2]$, $(c,\ h_2,\ h_3 \in \mathbb{F}_p^*$ where $p > 5)$, having rank five and satisfying $h_2^4 = \frac{11\pm5\sqrt{5}}{2}c$, where 5 is a quadratic residue in $\mathbb{F}_p$. Then (h_n) is associated with the singular curve E given by the equation*

$$E : y^2 = x^3 - \left(\frac{16605 \pm 7425\sqrt{5}}{2}\right)c^4 x - \left(411750 \pm 184140\sqrt{5}\right)c^6, \tag{4.7}$$

and if $P = (x_1, y_1)$ is a non-singular point on E then

$$P = (x_1, y_1) = \left(\left(\frac{573 \pm 255\sqrt{5}}{2}\right)c^2,\ \left(-6642 \pm 2970\sqrt{5}\right)c^3\right).$$

Proof. The theorem can be proved by substituting $h_2^4 = \dfrac{11 \pm 5\sqrt{5}}{2}c$ in (4.6). □

Now we will see that all EDSs are associated with the singular curve $y^2 = x^3$ when $p = 5$.

4.10. Theorem. *Let (h_n) be an elliptic divisibility sequence $[1\ h_2\ h_3\ ch_2]$, $(c, h_2, h_3 \in \mathbb{F}_5^*)$, and having rank five in $\mathbb{F}_5$. Then (h_n) is associated to the singular curve $E : y^2 = x^3$.*

Proof. Considering the equation (4.7) in $\mathbb{F}_5$ gives the desired result. □

Now we find elliptic curves associated with (h_n) having rank six:

4.11. Theorem. *Let (h_n) be an elliptic divisibility sequence $[1\ h_2\ h_3\ h_4]$, $(h_2,\ h_3,\ h_4 \in \mathbb{F}_p^*)$, and let $h_6 = 0$. Then (h_n) is associated with an elliptic curve E given by the equation:*

$$\begin{aligned} E : y^2 = x^3 &+ 27(-h_2^{16} + 12h_2^{12}c - 30h_2^8 c^2 + 12h_2^4 c^3 - 9c^4)x \\ &+ 54(h_2^{24} - 18h_2^{20}c + 99h_2^{16}c^2 - 180h_2^{12}c^3 + 135h_2^8 c^4 + 54h_2^4 c^5 - 27c^6) \end{aligned} \tag{4.8}$$

and if $P = (x_1, y_1)$ is a point on E then $P = (3(h_2^8 + 6ch_2^4 - 3c^2),\ -108(ch_2^8 - c^2 h_2^4))$.

Proof. Since $h_6 = 0$ we obtain $h_3^3 = ch_2^4 - c^2$. Putting $h_3^3 = ch_2^4 - c^2$ in (2.4), (2.5) and (2.6) we find the desired results. □

Now we see when associated singular curves arise:

4.12. Theorem. *Let (h_n) be an elliptic divisibility sequence $[1\ h_2\ h_3\ h_4]$, $(h_2,\ h_3 \in \mathbb{F}_p^*)$ having rank six. Then there exists a singular curve E associated to (h_n) if and only if $h_4 = ch_2 = \frac{h_2^5}{9}$.*

Proof. Since (h_n) is an EDS with rank six and $h_6 = \frac{h_3}{h_2}(h_5h_2^2 - h_4^2) = 0$ we have $h_5 = \left(\frac{h_4}{h_2}\right)^2$ and $h_3^3 = ch_2^4 - c^2$. If the elliptic divisibility sequence $[1\ h_2\ h_3\ ch_2]$ is associated with the singular curve E then we know that this sequence is singular. That is,

$$\Delta = h_2^{16}c - h_2^{12}h_3^3 + 3h_2^{12}c^2 - 20h_2^8c^3 + 16h_2^4h_3^6 + 8h_2^4c^2h_3^3 + h_2^4c^4 = 0.$$

If we substitute $h_3^3 = ch_2^4 - c^2$ in this equation we have $9c = h_2^4$. □

Now we find the singular curves associated with (h_n).

4.13. Theorem. *Let (h_n) be an elliptic divisibility sequence $[1\ h_2\ h_3\ ch_2]$, $(c,\ h_2,\ h_3 \in \mathbb{F}_p^*)$, having rank six and let $h_4 = ch_2 = \frac{h_2^5}{9}$. Then (h_n) is associated with the singular curve E given by the equation $E : y^2 = x^3 - 3888c^4x - 93312c^6$, and if $P = (x_1, y_1)$ is a non-singular point on E then $P = (396c^2, -7776c^3)$.*

Proof. The theorem can be proved by substituting $h_2^4 = 9c$ in (4.8). □

References

[1] Chudnovsky, D. V. and Chudnovsky, G. V. *Sequences of numbers generated by addition in formal groups and new primality factorization tests*, Adv. in Appl. Math. **7**, 385–434, 1986.

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

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

[4] Everest, G. and Ward, T. *Primes in divisibility sequences*, Cubo Mat. Educ. **3**, 245–259, 2001.

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

[6] Silverman, J. H. *The Arithmetic of Elliptic Curves* (Springer-Verlag, 1986).

[7] Silverman, J. H. and Stephens, N. *The sign of an elliptic divisibility sequence*, Journal of Ramanujan Math. Soc. **21**, 1–17, 2006.

[8] Silverman, J. H. and Tate, J. *Rational Points on Elliptic Curves* (Undergraduate Texts in Mathematics, Springer, 1992).

[9] Swart, C. S. *Elliptic curves and related sequences* (PhD. Thesis, Royal Holloway (University of London), 2003).

[10] Tekcan, A., Gezer, B. and Bizim, O. *Some relations on Lucas numbers and their sums*, Advanced Studies in Comtemporary Mathematics **15** (2), 195–211, 2007.

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

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