International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:4, No:7, 2010

Elliptic Divisibility Sequences over Finite Fields

Betül Gezer, Ahmet Tekcan and Osman Bizim

***Abstract*—**In this work, we study elliptic divisibility sequences over finite fields. Morgan Ward in [14], [15] gave arithmetic theory of elliptic divisibility sequences and formulas for elliptic divisibility sequences with rank two over finite field $\mathbf{F}_p$. We study elliptic divisibility sequences with rank three, four and five over a finite field $\mathbf{F}_p$, where $p > 3$ is a prime and give general terms of these sequences and then we determine elliptic and singular curves associated with these sequences.

***Keywords*—**Elliptic divisibility sequences, singular elliptic divisibility sequences, elliptic curves, singular curves.

I. Introduction

A divisibility sequence is a sequence (h_n) $(n \in \mathbf{N})$ 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 (see [5], [12], [13]). There are also divisibility sequences satisfying a nonlinear recurrence relation. These are the elliptic divisibility sequences and this relation comes from the recursion formula for elliptic division polynomials associated to an elliptic curve.

An elliptic divisibility sequence (or EDS) is a sequence of integers (h_n) satisfying a non-linear recurrence relation

$$h_{n+m}h_{n-m} = h_{n+1}h_{n-1}h_m^2 - h_{m+1}h_{m-1}h_n^2 \qquad (1)$$

and with the divisibility property that h_m divides h_n whenever m divides n for all $m \geq n \geq 1$.

EDSs are generalizations of a class of integer divisibility sequences called Lucas sequences in [11]. EDSs were interesting because of being the first non-linear divisibility sequences to be studied. Morgan Ward wrote several papers detailing the arithmetic theory of EDSs [14], [15]. For the arithmetic properties of EDSs, see also [2], [3], [4], [6], [10]. The Chudnovsky brothers considered prime values of EDSs in [1]. Rachel Shipsey [6] used EDSs to study some applications to cryptography and elliptic curve discrete logarithm problem (ECDLP). EDSs are connected to heights of rational points on elliptic curves and the elliptic Lehmer problem.

II. Some Preliminaries On Elliptic Divisibility Sequences and Elliptic Curves.

There are two useful formulas (known as duplication formulas) to calculate the terms of an EDS. These formulas are obtained from (1) setting first $m = n+1, n = m$ and then $m = n+1, n = m-1$ and so

$$h_{2n+1} = h_{n+2}h_n^3 - h_{n-1}h_{n+1}^3 \qquad (2)$$
$$h_{2n}h_2 = h_n(h_{n+2}h_{n-1}^2 - h_{n-2}h_{n+1}^2). \qquad (3)$$

A solution of (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 $h_1 = 1, h_2, h_3$ and h_4 is denoted by $[1\ h_2\ h_3\ h_4]$. The discriminant of (h_n) is defined by

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

Definition 2.1: 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 behavior of EDSs over a finite field $\mathbf{F}_p$, where $p > 3$ is a prime and the elliptic and singular curves associated to (h_n). To classify singular EDSs modulo p we need to know the following definition.

Definition 2.2: An integer m is said to be a divisor of the sequence (h_n) if it divides some term with positive suffix. If m divides h_ρ but does not divide h_r if r divides ρ, then ρ is called a rank of apparition of m in (h_n).

Theorem 2.1: Let p be a prime divisor of an elliptic divisibility sequence (h_n), and let ρ be rank of apparition. Let $h_{\rho+1}$ is not congruent to $0(mod\ p)$. Then $h_n \equiv 0(mod\ p) \Leftrightarrow n \equiv 0\ (mod\ \rho)$. [15]

Ward says that the multiples of p are regularly spaced in (h_n). A sequence (s_n) of rational integers is said to be numerically periodic modulo p if there exists a positive integer π such that $s_{n+\pi} \equiv s_n(mod\ p)$ for all sufficiently large n. If last equation holds for all n, then (s_n) is said to be purely periodic modulo p. The smallest such integer π for which this equation is true is called the period of (s_n) modulo p. All other periods are multiples of it. The following theorem of Ward shows us how the period and rank are connected.

Theorem 2.2: Let (h_n) be an EDS and p an odd prime whose rank of apparition ρ is greater than three. Let a_1 be an integral solution of the congruence $a_1 \equiv \frac{h_2}{h_{\rho-2}}(mod\ p)$ and let e and k be the exponents to which a_1 and $a_2 \equiv h_{\rho-1}(mod\ p)$, respectively belong modulo p. Then (h_n) is purely periodic modulo p and its period π is given by the formula $\pi = \tau\rho$,

Betül Gezer, Ahmet Tekcan and Osman Bizim are with the Uludag University, Department of Mathematics, Faculty of Science, Bursa-TURKIYE. email: betulgezer@uludag.edu.tr, tekcan@uludag.edu.tr, obizim@uludag.edu.tr.
This work was supported by The Scientific and Technological Research Council of Turkey, project no: 107T311

where $\tau = 2^{\alpha}[e,k]$. Here $[e,k]$ is the least common multiple of e and k and the exponent α is 1 if e and k are both odd, -1 if e and k are both even, both divisible by exactly the same power of 2 or 0 otherwise. [15]

We will now give a short account of material that we need. All of the theory of elliptic curves can be found in [7], [9]. Consider an elliptic curve defined over rational numbers determined by a short Weierstrass equation $y^2 = x^3 + ax + b$ with the coefficients $a, b \in \mathbf{Q}$ and the discriminant is $\Delta = -16(4a^3 + 27b^2)$. Ward proved that EDSs arise as values of the division polynomials of an elliptic curve. The following theorem shows us the relations between EDSs and the elliptic curves (for further details see [6], [8], [10], [15]).

Theorem 2.3: Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ ch_2]$. Then there exists an elliptic curve $E : y^2 = x^3 + ax + b$ with discriminant Δ, where

$$a = 3^3 \left(\begin{array}{c} (-h_2^{16} - 4ch_2^{12} + (16h_3^3 - 6c^2)h_2^8 \\ +(8ch_3^3 - 4c^3)h_2^4 \\ -(16h_3^6 + 8c^2h_3^3 + c^4) \end{array} \right) \quad (5)$$

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

$$\Delta = 2^8 3^{12} h_3^9 h_2^8 \left(\begin{array}{c} ch_2^{12} + (-h_3^3 + 3c^2)h_2^8 \\ +(-20ch_3^3 + 3c^3)h_2^4 \\ +(16h_3^6 + 8c^2h_3^3 + c^4) \end{array} \right) \quad (7)$$

and a non singular rational point

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

on E such that $\psi_n(x_1, y_1) = h_n$ for all $n \in \mathbf{Z}$ where ψ_n is the $n-$th polynomial of E. [8]

By Theorem 2.3, we can say that the EDS with the initial values $[1\ h_2\ h_3\ ch_2]$ is associated to $E : y^2 = x^3 + ax + b$ and rational point $P \in E$. Ward showed that the discriminant of the elliptic divisibility sequence is equal to discriminant of elliptic curve associated to this sequence.

III. Elliptic Divisibility Sequences in Certain Ranks and Associated Curves.

In this section we work with elliptic divisibility sequences having special initial values in certain ranks over $\mathbf{F}_p$, and we will see that all EDSs with rank two and three are singular and so these are associated to singular curves. Also we will see that EDSs with rank four and five are associated to elliptic curves or singular curves and so we then determine which of these sequences are associated to elliptic and singular curves. Firstly, we define the elliptic sequences and then elliptic divisibility sequences over $\mathbf{F}_p$, where $p > 3$ is a prime.

Definition 3.1: An elliptic sequence over $\mathbf{F}_p$ is a sequence of elements of $\mathbf{F}_p$ which is a particular solution of (1).

If (h_n) is an elliptic sequence over $\mathbf{F}_p$, then (h_n) is an elliptic divisibility sequence over $\mathbf{F}_p$ since any non-zero elements of $\mathbf{F}_p$ divides any other. Therefore the term elliptic sequence over $\mathbf{F}_p$ will mean, in this paper, elliptic divisibility sequence over $\mathbf{F}_p$. Note that as in the integral sequences, elliptic divisibility sequences satisfy the further conditions $h_0 = 0,\ h_1 = 1$ and two consecutive terms of (h_n) can not vanish over $\mathbf{F}_p$. So we can give an alternative theorem of Theorem 2.1 for finite fields.

Lemma 3.1: Let (h_n) be an elliptic divisibility sequence with rank ρ over $\mathbf{F}_p$. Then $h_{\rho n} \equiv 0 (mod\ p)$.

Proof: If (h_n) has rank ρ, then $h_{\rho n} \equiv 0 (mod\ p)$ since h_ρ divides $h_{\rho n}$ for ρ divides ρn. ■

A. Sequences with Rank Two and Associated Curves.

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 sequence with even subscript is zero (except for the term h_0). Ward proved that such a sequence is given by the following theorem.

Theorem 3.1: Let (h_n) be an elliptic divisibility sequence with initial values $[1\ 0\ h_3\ 0]$ for $h_3 \in \mathbf{F}_p^* = \mathbf{F}_p \backslash \{0\}$ and n is odd. Then (h_n) is given by

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

where $\lfloor x \rfloor$ denotes the lower function. [15]

We will find associated singular curves to (h_n) with rank two. Note that all elliptic divisibility sequences with rank two are singular since their discriminant is zero.

Theorem 3.2: Let (h_n) be a singular elliptic divisibility sequence with initial values $[1\ 0\ h_3\ ch_2]$ for $c \in \mathbf{F}_p$ and $h_3 \in \mathbf{F}_p^*$. Then (h_n) is associated to a singular curve given by the equation

$$E : y^2 = x^3 - 27(4h_3^3 + c^2)^2 x + 54(4h_3^3 + c^2)^3.$$

Also if $P = (x_1, y_1)$ is a point on E, then $P = (3(h_3^3 + c^2), 0)$.

Proof: Since (h_n) is a singular elliptic divisibility sequence, the associated curve is singular. Putting $h_2 = 0$ in the equations (5), (6) and (8), we have

$$\begin{aligned} a &= -27(16h_3^6 + 8c^2h_3^3 + c^4) = -27(4h_3^3 + c^2)^2 \\ b &= 54(64h_3^9 + 48c^2h_3^6 + 12c^4h_3^3 + c^6) = 54(4h_3^3 + c^2)^3 \end{aligned}$$

and $P = (3(4h_3^3 + c^2), 0)$. ■

Theorem 3.2 says that the singular elliptic divisibility sequence $[1\ 0\ h_3\ ch_2]$ for $c \in \mathbf{F}_p$ and $h_3 \in \mathbf{F}_p^*$ is associated to the singular curve $E : y^2 = x^3 - 27(4h_3^3 + c^2)^2 x + 54(4h_3^3 + c^2)^3$. So if we write $\alpha = 4h_3^3 + c^2$ and $\beta = 3\alpha^2$, then we obtain $a = -3\beta^2$ and $b = 2\beta^3$. Hence $E : y^2 = x^3 - 3\beta^2 x + 2\beta^3$ and $P = (\beta, 0)$.

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

$$\begin{array}{lll} y^2 = x^3 + 3x + 1 & y^2 = x^3 + 2x + 2 & y^2 = x^3 + 2x + 3 \\ y^2 = x^3 + 3x + 4 & y^2 = x^3 & y^2 = x^3 + 2x + 3 \\ y^2 = x^3 + 3x + 1 & y^2 = x^3 + 2x + 2 & y^2 = x^3 + 2x + 3 \\ y^2 = x^3 + 2x + 4 & y^2 = x^3 + 2x + 2 & y^2 = x^3 \end{array}$$

respectively.

B. Sequences with Rank Three and Associated Curves.

We know that $h_{3n} = 0$ for all integers $n \neq 0$. Note that all elliptic divisibility sequences with rank three are singular since their discriminant is zero. We give general terms of (h_n) when $h_4 = 1$ and $h_4 = -1$ in the following theorems.

Theorem 3.3: Let (h_n) be a singular elliptic divisibility sequence with initial values $[1\ h_2\ 0\ 1]$ for $h_2 \in \mathbf{F}_p^*$. Then (h_n) is given by the following formula

$$h_n = \begin{cases} h_2^k & if\ n \equiv 1, 2, 4, 5 (mod\ 12) \\ -h_2^k & if\ n \equiv 7, 8, 10, 11 (mod\ 12), \end{cases}$$

where $k = \frac{(t-1)t}{2}$ for $n = 3t + 1$ and $k = \frac{(t+1)(t+2)}{2}$ for $n = 3t + 2$.

Proof: By setting $m = 2$ in (1), we have

$$h_{n+2}h_{n-2} = h_{n+1}h_{n-1}h_2^2 \tag{9}$$

since $h_3 = 0$. It suffices to prove our main result by induction based on equation (9). If we take $n = 3$ in this equation, then we obtain $h_5 = h_2^3$ and we observe that this is true since $k = 3$ and so $h_5 = h_2^3$. Hence we assume that $n > 3$.

Now first suppose that $n + 1 \equiv 1(mod\ 12)$. Then we can write $n = 12r$ for $r \in \mathbf{N}$. Let the equation (9) be true for $n+1$. We wish to show that this equation is also true for $n+2$. Then $t = 4r$ for $r \in \mathbf{N}$ and so $k = 8r^2 + 6r + 1$. Therefore $h_{n+2} = -h_2^{8r^2+6r+1}$. Since $n + 1 = 12r + 1$, we have $t = 4r$ and so $k = 2r(4r - 1)$. Thus we find that $h_{n+1} = h_2^{2r(4r-1)}$.

Similarly we see that

$$h_{n-1} = -h_2^{2r(4r+1)}\ and\ h_{n-2} = h_2^{(2r-1)(4r-1)}.$$

So if we substitute this relations in the equation (9), then we have

$$h_{n+2}h_2^{(2r-1)(4r-1)} = h_2^{2r(4r-1)}(-h_2^{2r(4r+1)})h_2^2$$

and so we obtained that $h_{n+2} = -h_2^{8r^2+6r+1}$. Thus we proved this theorem for $n + 1 \equiv 1(mod\ 12)$. Other cases of the theorem can be proved in the same way. ∎

There are $p-1$ singular EDSs with initial values $[1\ h_2\ 0\ 1]$ since $h_2 \in \mathbf{F}_p^*$. Moreover if $p \equiv 5(mod\ 6)$, then there are $p - 1$ alternatives and if $p \equiv 1(mod\ 6)$, then there are $\frac{p-1}{3}$ alternatives for the fifth term. It is easily seen that by taking $n = 2$ in duplication formula, we have $h_5 = h_4h_2^3 - h_3^3$ and since $h_3 = 0, h_4 = 1$ we see that $h_5 = h_2^3 \in \mathbf{K}_p^*$, where $\mathbf{K}_p$ denotes the set of cubic residues modulo p and $\mathbf{K}_p^* = \mathbf{K}_p \backslash \{0\}$.

Theorem 3.4: Let (h_n) be a singular elliptic divisibility sequence with initial values $[1\ h_2\ 0\ -1]$ for $h_2 \in \mathbf{F}_p^*$. Then (h_n) is given by the following formula

$$h_n = \begin{cases} h_2^k & if\ n \equiv 1, 2, 7, 8 (mod\ 12) \\ -h_2^k & if\ n \equiv 4, 5, 10, 11 (mod\ 12), \end{cases}$$

where $k = \frac{(t-1)t}{2}$ for $n = 3t + 1$ and $k = \frac{(t+1)(t+2)}{2}$ for $n = 3t + 2$.

Proof: Theorem can be proved by induction in the same way as Theorem 3.3 was proved. ∎

Similarly there are also $p - 1$ singular elliptic divisibility sequences with initial values $[1\ h_2\ 0\ -1]$ and if $p \equiv 5(mod\ 6)$, then there are $p - 1$ alternatives and if $p \equiv 1(mod\ 6)$, then there are $\frac{p-1}{3}$ alternatives for the fifth term.

Theorem 3.5: Let (h_n) be a singular elliptic divisibility sequence with initial values $[1\ 1\ 0\ h_4]$ for $h_4 \in \mathbf{F}_p^*$. Then (h_n) is given by the following formula

$$h_n = \begin{cases} h_4^k & if\ n \equiv 1, 2, 4, 5 (mod\ 12) \\ -h_4^k & if\ n \equiv 7, 8, 10, 11 (mod\ 12), \end{cases}$$

where $k = \frac{(t+1)t}{2}$ so that $t = \left\lfloor \frac{n}{3} \right\rfloor$. Moreover two consecutive terms with suffices not divisible by three of (h_n) are equal.

Proof: By setting $m = 2$ in (1), we have

$$h_{n+2}h_{n-2} = h_{n+1}h_{n-1} \tag{10}$$

since $h_3 = 0$ and $h_2 = 1$. It suffices to prove our main result by induction based on equation (11). If we take $n = 3$, then we obtain $h_5 = h_4$. We observe that this is true, since $k = 1$ and so $h_5 = h_4$. Hence we assume that $n > 3$.

Now first suppose that $n + 1 \equiv 1(mod\ 12)$. Then we have $n = 12r$ for $r \in \mathbf{N}$. Let the equation (11) be true for $n + 1$. We wish to show that this equation is also true for $n+2$. Then $t = \left\lfloor \frac{n+2}{3} \right\rfloor = 4r$ for $r \in \mathbf{N}$ and so $k = 8r^2 + 2r$ and therefore $h_{n+2} = h_4^{8r^2+2r}$. Since $n + 1 = 12r + 1$, we have $t = 4r$ and so $k = 2r(4r + 1)$. Thus we find that $h_{n+1} = h_4^{2r(4r+1)}$.

Similarly we see that

$$h_{n-1} = h_4^{2r(4r-1)}\ and\ h_{n-2} = h_4^{2r(4r-1)}.$$

So if we substitute this relations in the equation (11), then we have

$$h_{n+2}h_4^{8r^2-2r} = h_4^{8r^2+2r}h_4^{8r^2-2r} \Leftrightarrow h_{n+2} = h_4^{8r^2+2r}.$$

Thus we proved for $n + 1 \equiv 1(mod\ 12)$. Other cases of the theorem can be proved in the similar way. Moreover if $n, n + 1 \neq 3k$ for $k \in \mathbf{N}$, then we have $h_n = h_{n+1}$ since $t = \left\lfloor \frac{n}{3} \right\rfloor = \left\lfloor \frac{n+1}{3} \right\rfloor$. ∎

Note that there are $p - 1$ singular elliptic divisibility sequences with initial values $[1\ 1\ 0\ h_4]$ since $h_4 \in \mathbf{F}_p^*$.

Theorem 3.6: Let (h_n) be a singular elliptic divisibility sequence with initial values $[1\ -1\ 0\ h_4]$ for $h_4 \in \mathbf{F}_p^*$. Then (h_n) is given by the following formula

$$h_n = \begin{cases} h_4^k & if\ n \equiv 1(mod\ 3) \\ -h_4^k & if\ n \equiv 2(mod\ 3), \end{cases}$$

where $k = \frac{(t+1)t}{2}$ so that $t = \left\lfloor \frac{n}{3} \right\rfloor$. Moreover two consecutive terms with suffices not divisible by three of (h_n) have opposite parity.

Proof: Theorem can be proved by induction in the same way as Theorem 3.5 was proved. ∎

There are also $p-1$ singular elliptic divisibility sequence with initial values $[1\ -1\ 0\ h_4]$ since $h_4 \in \mathbf{F}_p^*$. We consider (h_n) and (u_n) with initial values $[1\ 1\ 0\ 1]$ and $[1\ -1\ 0\ 1]$. Then by using the equations (2) and (3) we find that

$$\begin{aligned} h_5 &= h_4h_2^3 - h_1h_3^3 = 1 \\ h_7 &= h_5h_3^3 - h_2h_4^3 = -1 \\ h_8 &= h_4(h_6h_3^2 - h_2h_5^2) = -1. \end{aligned}$$

Similarly we can find other terms of the sequence. Then (h_n) and (u_n) are

$$0\ 1\ 1\ 0\ 1\ 1\ 0\ -1\ -1\ 0\ -1\ -1\ \cdots$$

and

$$0\ 1\ -1\ 0\ 1\ -1\ \cdots,$$

respectively. Notice that these are singular EDSs with rank 3 and period 12, rank 3 and period 6, respectively. So we proved the following theorem.

Theorem 3.7: Let (h_n) and (u_n) be two singular elliptic divisibility sequences with initial values $[1\ 1\ 0\ 1]$ and $[1\ -1\ 0\ 1]$. Then (h_n) and (u_n) are the sequences

$$0\ 1\ 1\ 0\ 1\ 1\ 0\ -1\ -1\ 0\ -1\ -1\ \cdots$$

and

$$0\ 1\ -1\ 0\ 1\ -1\ \cdots$$

periods of (h_n) and (u_n) are 12 and 6, respectively.

Now we determine singular curves associated to (h_n) with rank three.

Theorem 3.8: Let (h_n) be a singular elliptic divisibility sequence with initial values $[1\ h_2\ 0\ ch_2]$ for $c, h_2 \in \mathbf{F}_p^*$. Then (h_n) is associated to a singular curve E given by the equation

$$E : y^2 = x^3 - 27(h_2^4 + c)^4x + 54(h_2^4 + c)^6.$$

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

Proof: Since (h_n) is a singular elliptic divisibility sequence then the associated curve is singular. Putting $h_3 = 0$ in the equations (5), (6) and (8), then we have

$$\begin{aligned} a &= -27(h_2^{16} + 4ch_2^{12} + 6c^2h_2^8 + 4c^3h_2^4 + c^4) \\ &= -27(h_2^4 + c)^4 \\ \\ b &= 54(h_2^{24} + 6ch_2^{20} + 15c^2h_2^{16} + 20c^3h_2^{12} + \\ &\quad 15c^4h_2^8 + 6c^5h_2^4 + c^6) \\ &= 54(h_2^4 + c)^6 \end{aligned}$$

and $P = (3(h_2^8 + 2ch_2^4 + c^2),\ 0) = (3(h_2^4 + c)^2, 0)$. ∎

By Theorem 3.8, we see that singular elliptic divisibility sequence $[1\ h_2\ 0\ ch_2]$ for $c, h_2 \in \mathbf{F}_p^*$ is associated to the singular curve $E : y^2 = x^3 - 27(h_2^4 + c)^4x + 54(h_2^4 + c)^6$. So if we write $\alpha = h_2^4 + c$ and $\beta = 3\alpha^2$, then we obtain $a = -3\beta^2$ and $b = 2\beta^3$. Hence $E : y^2 = x^3 - 3\beta^2x + 2\beta^3$ and $P = (\beta, 0)$.

Theorem 3.9: If $P = (x_1, y_1) = (3(h_2^4 + c)^2, 0)$ is a point on $E : y^2 = x^3 - 27(h_2^4 + c)^4x + 54(h_2^4 + c)^6$, then

$$x_1 \in \mathbf{Q}_p \Leftrightarrow p \equiv \pm 1(mod\ 12)$$

and

$$x_1 \notin \mathbf{Q}_p \Leftrightarrow p\ is\ not\ congruent\ to\ \pm 1(mod\ 12),$$

where $\mathbf{Q}_p$ denotes the set of quadratic residues modulo p. Therefore there are $\frac{p-1}{2}$ alternatives for the point P in both cases.

Proof: Note that $(h_2^4 + c)^2, 3 \in \mathbf{Q}_p \Leftrightarrow p \equiv \pm 1(mod\ 12)$. So we have $3(h_2^4 + c)^2 = x_1 \in \mathbf{Q}_p \Leftrightarrow p \equiv \pm 1(mod\ 12)$. Further since $|\mathbf{Q}_p| = \frac{p-1}{2}$, there are $\frac{p-1}{2}$ alternatives for the point P in both cases. ∎

Theorem 3.10: Let (h_n) be a singular elliptic divisibility sequence with initial values $[1\ 1\ 0\ c]$ or $[1\ -1\ 0\ c]$ for $c \in \mathbf{F}_p^*$. Then

$$a = -27(c+1)^4, \quad b = (c+1)^6 \quad and\ P = (3(c+1)^2, 0).$$

In particular if $c = -1$, then singular elliptic divisibility sequences $[1\ 1\ 0\ -1]$ or $[1\ -1\ 0\ -1]$ are associated to the singular curve $E : y^2 = x^3$.

Proof: If we take $h_2 = 1$, then by (5), (6) and (8), we have $a = -27(c+1)^4$, $b = (c+1)^6$ and $P = (3(c+1)^2, 0)$. In particular if we write $c = -1$ in these equations, then we have the singular curve $E : y^2 = x^3$. ∎

Theorem 3.11: If $P = (x_1, y_1) = (3(c+1)^2, 0)$ is a point on $E : y^2 = x^3 - 27(c+1)^4x + 54(c+1)^6$, then

$$x_1 \in \mathbf{Q}_p \Leftrightarrow p \equiv \pm 1(mod\ 12)$$

and

$$x_1 \notin \mathbf{Q}_p \Leftrightarrow p\ \ is\ not\ congruent\ to\ \pm 1(mod\ 12).$$

Therefore there are $\frac{p-1}{2}$ alternatives for the point P in both cases.

Proof: Theorem can be proved in the same way as Theorem 3.10 was proved. ■

Theorem 3.10 tells us that singular elliptic divisibility sequences $[1\ 1\ 0\ -1]$ or $[1\ -1\ 0\ -1]$ are associated to the singular curve $E: y^2 = x^3$. Conversely if P is a not a singular point on E, then we can not have these sequences, that is, even though we have curves from sequences we can not have sequences from a nonsingular point on E. For example, if $y^2 = x^3$ is a singular curve over $\mathbf{F}_5$, then we have the points $O, (0,0), (1,1), (1,4), (4,2), (4,3)$ on E. Notice that only the point $(0,0)$ is a singular point and we find that other points on this curve give the singular elliptic divisibility sequences $[1\ 2\ 3\ 4], [1\ 3\ 3\ 1], [1\ 4\ 3\ 3]$ and $[1\ 1\ 3\ 2]$, respectively. Note that we do not have the singular EDSs $[1\ 1\ 0\ 4]$ and $[1\ 4\ 0\ 4]$. This is because the EDSs $[1\ 1\ 0\ -1]$ and $[1\ -1\ 0\ -1]$ are improper sequences.

Theorem 3.12: Let (h_n) be a singular elliptic divisibility sequence with initial values $[1\ h_2\ 0\ 1]$ for $h_2 \in \mathbf{F}_p^*$. Then (h_n) is associated to E given by the equation

$$E: y^2 = x^3 - 27\left(\frac{h_2^5+1}{h_2}\right)^4 x + 54\left(\frac{h_2^5+1}{h_2}\right)^6.$$

Also if $P = (x_1, y_1)$ is a point on E, then

$$P = \left(3\left(\frac{h_2^5+1}{h_2}\right)^2, 0\right).$$

In particular, the elliptic divisibility sequence $[1\ -1\ 0\ 1]$ is associated to the singular curve $E: y^2 = x^3$.

Proof: Recall that singular EDSs with $h_3 = 0$ are associated to curve

$$E: y^2 = x^3 - 27(h_2^4 + c)^4 + 54(h_2^4 + c)^6. \tag{11}$$

Since $h_4 = ch_2 = 1$ we have $c = \frac{1}{h_2}$. If we substitute this in (11), then we have

$$E: y^2 = x^3 - 27\left(\frac{h_2^5+1}{h_2}\right)^4 x + 54\left(\frac{h_2^5+1}{h_2}\right)^6.$$

With the same argument, by using the point $P = (3(h_2^4 + c)^2, 0)$ on E, we find that

$$P = \left(3\left(\frac{h_2^5+1}{h_2}\right)^2, 0\right).$$

In particular, if we substitute $h_2 = -1$ in the last equation, then we find that the singular EDS $[1\ -1\ 0\ 1]$ is associated to the singular curve $E: y^2 = x^3$. ■

Theorem 3.12 tells us that singular elliptic divisibility sequence $[1\ h_2\ 0\ 1]$ for $h_2 \in \mathbf{F}_p^*$ is associated to elliptic curve E given by the equation $E: y^2 = x^3 - 27\left(\frac{h_2^5+1}{h_2}\right)^4 x + 54\left(\frac{h_2^5+1}{h_2}\right)^6$. So if we write $\alpha = \frac{h_2^5+1}{h_2}$ and $\beta = 3\alpha^2$, then we obtain $a = -3\beta^2$ and $b = 2\beta^3$. Hence $E: y^2 = x^3 - 3\beta^2 x + 2\beta^3$ and $P = (\beta, 0)$.

Theorem 3.13: Let (h_n) be a singular elliptic divisibility sequence with initial values $[1\ h_2\ 0\ -1]$ for $h_2 \in \mathbf{F}_p^*$. Then (h_n) is associated to E given by the equation

$$E: y^2 = x^3 - 27\left(\frac{h_2^5-1}{h_2}\right)^4 x + 54\left(\frac{h_2^5-1}{h_2}\right)^6.$$

Also if $P = (x_1, y_1)$ is a point on E, then

$$P = \left(3\left(\frac{h_2^5-1}{h_2}\right)^2, 0\right).$$

In particular, the elliptic divisibility sequence $[1\ 1\ 0\ -1]$ is associated to the singular curve $E: y^2 = x^3$.

Proof: Theorem can be proved in the same way as Theorem 3.12 was proved. ■

Theorem 3.13 shows us that singular elliptic divisibility sequence (h_n) with initial values $[1\ h_2\ 0\ -1]$ for $h_2 \in \mathbf{F}_p^*$ associated to an elliptic curve E given by $E: y^2 = x^3 - 27\left(\frac{h_2^5-1}{h_2}\right)^4 x + 54\left(\frac{h_2^5-1}{h_2}\right)^6$. So if we write $\alpha = \frac{h_2^5-1}{h_2}$ and $\beta = 3\alpha^2$, then we obtain $a = -3\beta^2$ and $b = 2\beta^3$. Hence $E: y^2 = x^3 - 3\beta^2 x + 2\beta^3$ and $P = (\beta, 0)$.

C. Sequences with Rank Four and Associated Curves.

Now let (h_n) be an elliptic divisibility sequence with rank four. We know that $h_{4n} = 0$ for all integers $n \neq 0$. These sequences are not singular at all. So we first give the general terms of the EDSs and then we will determine when these sequences are singular, then we find associated elliptic and singular curves.

Theorem 3.14: Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ 0]$ for $h_2, h_3 \in \mathbf{F}_p^*$. Then (h_n) is given by the following formula:

$$h_n = \begin{cases} \varepsilon h_3^k & if\ n\ is\ odd \\ \varepsilon h_3^k h_2 & if\ n \equiv 2(mod\ 4), \end{cases}$$

where

$$k = \begin{cases} \frac{r(r+1)}{2} & if\ n = 2r+1 \\ 2r(r+1) & if\ n = 4r+2 \end{cases}$$

and

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

Proof: By setting $m = 2$ in (1), we have

$$h_{n+2}h_{n-2} = h_{n+1}h_{n-1}h_2^2 - h_3 h_1 h_n^2. \tag{12}$$

It suffices to prove our main result by induction based on equation (12). If we take $n = 3$ in this equation and since $h_1 = 1$, $h_4 = 0$ we obtained that $h_5 = -h_3^3$ and we observe that this is true, since $k = 3, \varepsilon = -1$ and so $h_5 = -h_3^3$.

Now first suppose that $n+1 \equiv 2(mod\ 8)$. Then $n = 8r+1$ for $r \in \mathbf{N}$. Let the equation (12) be true for $n+1$. We wish to show that this equation is also true for $n+2$, that is, we want to show that if $n+2 \equiv 3(mod\ 8)$, then $n+2 = 8r+3$

for $r \in \mathbf{N}$ and hence $k = \frac{(4r+1)(4r+2)}{2}$. Since $\varepsilon = 1$, we have $h_{n+2} = h_3^{8r^2+6r+1}$. Further since $n+1 = 8r+2$, we have $k = 4r(2r+1)$ and since $\varepsilon = 1$ we find that $h_{n+1} = h_3^{4r(2r+1)}$.

Similarly we see that $h_n = h_3^{2r(4r+1)}$ for $h_{n-1} = 0$ and $h_{n-2} = -h_3^{2r(4r-1)}$. So if we substitute this relations in the equation (12), then we have $h_{n+2}(-h_3^{2r(4r-1)}) = -h_3(h_3^{2r(4r+1)})^2$ and hence $h_{n+2} = h_3^{8r^2+6r+1}$. Thus we proved this theorem for $n+1 \equiv 2(mod\ 8)$. Other cases of the theorem can be proved in the same way. ■

There are $(p-1)^2$ EDSs with initial values $[1\ h_2\ h_3\ 0]$ since $h_2, h_3 \in \mathbf{F}_p^*$. Moreover if $p \equiv 5(mod\ 6)$, then there are $p-1$ alternatives and if $p \equiv 1(mod\ 6)$, then there are $\frac{p-1}{3}$ alternatives for the fifth term since $h_5 = -h_3^3 \in \mathbf{K}_p^*$.

Theorem 3.15: Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ 0]$ for $h_2, h_3 \in \mathbf{F}_p^*$. Then the period of (h_n) is

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

where q is a prime divisor of $p-1$.

Proof: It is clear that rank of the (h_n) is $\rho = 4$. Then since $a_1 = \frac{h_2}{h_{\rho-2}} = \frac{h_2}{h_2} = 1$ and $a_2 = h_{\rho-1} = h_3$, we see that orders of a_1 and a_2 are $e = 1$ and $k = p-1$ if h_3 is a primitive root in $\mathbf{F}_p$ or $k = q$ otherwise. Thus $[e,k] = k$. If h_3 is a primitive root in $\mathbf{F}_p$, 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 $\mathbf{F}_p$, then the order of h_3 is q a prime divisor of $p-1$. So in this case $\alpha = 0$ or 1. Then $\tau = q$ or $2q$. So $\pi(h_n) = 4q$ or $8q$ since $\rho = 4$. ■

Now we will see when the EDSs with rank four are singular.

Theorem 3.16: Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ 0]$ for $h_2, h_3 \in \mathbf{F}_p^*$. Then (h_n) is a singular elliptic divisibility sequence if and only if $h_3^3 = \frac{h_2^8}{16}$.

Proof: Putting $h_4 = 0$ in (4), we find that $\Delta = h_3^3 h_2^4 (-h_2^8 + 16h_3^3)$. So

$$\Delta = 0 \Leftrightarrow 16h_3^3 - h_2^8 = 0$$

since $h_2 h_3 \neq 0$. ■

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

Theorem 3.17: Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ 0]$ for $h_2, h_3 \in \mathbf{F}_p^*$. Then (h_n) is associated to an elliptic curve E given by the equation

$$\begin{aligned} E: y^2 &= x^3 + 27(-h_2^{16} + 16ch_3^3h_2^8 - 16h_3^6)x \\ &\quad +54(h_2^{24} - 24h_3^3h_2^{16} + 120h_3^6h_2^8 + 64h_3^9). \end{aligned}$$

Also 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 $h_2h_3 \neq 0$ we obtain $c = 0$. Putting $c = 0$ in (5), (6) and (8), we find that

$$a = 27(-h_2^{16} + 16ch_3^3h_2^8 - 16h_3^6) \quad (13)$$
$$b = 54(h_2^{24} - 24h_3^3h_2^{16} + 120h_3^6h_2^8 + 64h_3^9) \quad (14)$$

and

$$P = (3(h_2^8 + 4h_3^3), -108h_3^3h_2^4) \quad (15)$$

as we claimed. ■

Now we determine which of these curves are singular.

Theorem 3.18: Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ 0]$ for $h_2 \in \mathbf{F}_p^*$ and $h_3^3 = \frac{h_2^8}{16}$. Then (h_n) is associated to the singular curve E given by the equation

$$E: y^2 = x^3 - \frac{27}{16}h_2^{16}x - \frac{54}{64}h_2^{24}.$$

If $P = (x_1, y_1)$ is a point on E, then $P = \left(\frac{15h_2^8}{4}, -\frac{27h_2^{12}}{4}\right)$.

Proof: Note that E is a singular curve if and only if (h_n) is a singular sequence and also $h_3^3 = \frac{h_2^8}{16}$ by assumption. Putting these quantities in (13), (14) and (15), then we have the desired results. ■

By Theorem 3.18, we see that elliptic divisibility sequence $[1\ h_2\ h_3\ 0]$ is associated to the singular curve $E: y^2 = x^3 - \frac{27}{16}h_2^{16}x - \frac{54}{64}h_2^{24}$. So if we write $\alpha = \frac{3}{4}h_2^8$ and $\beta = 3\alpha^2$, then we obtain $a = -\beta$ and $b = -2\beta^3$. Hence $E: y^2 = x^3 + \beta x + 2\beta^3$.

Remark 3.19: Note that if $Q \in E$ is a singular point on E, then Q is a node. Indeed (h_n) is associated to $E: y^2 = x^3$ when $h_2 = 0$. In this case we have $h_2 \neq 0$.

D. Sequences with Rank Five and Associated Curves.

Now let (h_n) be an elliptic divisibility sequence with rank five. We know that $h_{5n} = 0$ for all integers $n \neq 0$. First consider the case where $h_4 = 1$.

Theorem 3.20: Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ 1]$ for $h_2, h_3 \in \mathbf{F}_p^*$ and $h_5 = 0$. Then (h_n) is given by

$$h_n = \begin{cases} (-1)^k h_r & for\ n \geq 15 \\ h_r & for\ n < 15, \end{cases}$$

where $n = 15k + r$ or $n = 15 - r$ for $r > 0$.

Proof: First we will see that this equation holds for $n < 15$, we have $h_5 = h_4h_2^3 - h_3^3 = h_2^3 - h_3^3 = 0$. So we have to consider two cases to determine terms of this sequence.

i) Let $p \equiv 1(mod\ 6)$. Then the solutions of the congruence $h_2^3 \equiv h_3^3(mod\ p)$ are $h_3 \equiv h_2, h_2\omega, h_2\omega^2(mod\ p)$, where ω is the cubic root of unity. So there is three alternatives for the term h_3 for the given term h_2.

ii) Let $p \equiv 5(mod\ 6)$. Then the solutions of the congruence $h_2^3 \equiv h_3^3(mod\ p)$ is only $h_3 \equiv h_2(mod\ p)$.

Now we will prove the theorem only for $p \equiv 1(mod\ 6)$ and $h_3 \equiv h_2\omega^2(mod\ p)$. Other cases can be seen in the same way. Therefore using the duplications formulas we get,

$$\begin{aligned} h_6 &= \frac{h_3(h_5h_2^2 - h_4^2)}{h_2} = -\omega^2 \\ h_7 &= h_5h_3^3 - h_2h_4^3 = -h_2 \\ h_8 &= \frac{h_4(h_6h_3^2 - h_5^2h_2)}{h_2} = -h_2 \end{aligned}$$

and similarly $h_9 = -\omega, h_{10} = 0, h_{11} = 1, h_{12} = \omega h_2, h_{13} = h_2, h_{14} = 1, h_{15} = 0$. Thus $h_{15-r} = h_r$ for $n < 15$.

Now we consider the equation

$$h_{n+2}h_{n-2} = h_{n+1}h_{n-1}h_2^2 - h_3h_1h_n^2. \tag{16}$$

Since $h_{15} = 0$ it suffices to prove our result by induction based on equation (16) for $n > 15$. We want to show that the equation (16) is true for $n = 16$. If we take $n = 14$ in this equation and since $h_{12} = h_3, h_{14} = 1$, then we obtain $h_{16} = -1$ and we observe that this is true, since $k = 1$ we have $r = 1$ and so $h_{16} = -1, h_1 = -1$ namely our result is true for $n = 16$.

Let the equation (16) be true for $n + 1 > 15$. We wish to show that this equation is also true for $n+2$. Now first suppose that $n + 1 = 15k + 1$ for $k > 1 \in \mathbf{Z}$. This is not a restriction; the theorem also holds if we take $n + 1 = 15k + 2, 15k + 3$ or $15k + 4$. So for $n = 15k, 15k + 1, 15k + 2$, then we have $h_n = 0, h_{n+1} = (-1)^k h_1, h_{n+2} = (-1)^k h_2$, respectively and for $n - 1 = 15(k - 1) + 14$ and $n - 2 = 15(k - 1) + 13$, we have $h_{n-1} = (-1)^{k-1}$ and $h_{n-2} = (-1)^{k-1}h_2$. Therefore we have $h_{n+2}(-1)^k h_2 = (-1)^k h_1(-1)^{k-1}h_2^2$ and so $h_{n+2} = (-1)^k h_2$. Then we see that the equation (16) is also true for $n + 2$ and this completes the induction. ■

If we want to have a sequence as in Theorem 3.20 with fifth term is zero, then we have to think two cases for choosing second and third term: if $p \equiv 1(mod\ 6)$, then we must choose $h_3 = h_2, h_2\omega$ and $h_2\omega^2$ and if $p \equiv 5(mod\ 6)$, then we must choose $h_3 = h_2$.

We have seen in Theorem 3.20 that if $p \equiv 5(mod\ 6)$, then $h_2 = h_3$ and since $h_2, h_3 \in \mathbf{F}_p^*$ there are $p - 1$ EDSs with initial values $[1\ h_2\ h_3\ 1]$ and $h_5 = 0$ in $\mathbf{F}_p$. Similarly if $p \equiv 1(mod\ 6)$, then $h_3 = h_2, h_2\omega, h_2\omega^2$ and so there are $3(p - 1)$ sequences in $\mathbf{F}_p$.

Theorem 3.21: Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ 1]$ for $h_2, h_3 \in \mathbf{F}_p^*$ and $h_5 = 0$. Then the period of (h_n) is

$$\pi(h_n) = \begin{cases} 10 & if\ h_3 = h_2 \\ 30 & if\ h_3 = h_2\omega, h_2\omega^2. \end{cases}$$

Proof: It is clear that rank of the (h_n) is $\rho = 5$. Now we want to see that the period of (h_n) is 10 or 30. First suppose that $h_3 = h_2$. Then since $a_1 = \frac{h_2}{h_{\rho-2}} = 1$, we see that the order of a_1 is $e = 1$ and since $a_2 = h_{\rho-1} = h_4 = 1$, we see that the order of a_2 is $k = 1$. Thus $\alpha = 1$ and since $\tau = 2^\alpha[e, k]$ we have $\tau = 2$. So $\pi(h_n) = \tau\rho = 10$. Now suppose that $h_3 = h_2\omega$. Then since $a_1 = \frac{h_2}{h_{\rho-2}} = \frac{1}{\omega}$, we derive that the order of a_1 is $e = 3$ and since $a_2 = h_{\rho-1} = h_4 = 1$, we see that the order of a_2 is $k = 1$. Thus $\alpha = 1$ and since $\tau = 2^\alpha[e, k]$, we have $\tau = 6$. So $\pi(h_n) = \tau\rho = 30$.

Now suppose that $h_3 = h_2\omega^2$. Then since $a_1 = \frac{h_2}{h_{\rho-2}} = \frac{1}{\omega^2}$, we see that order of a_1 is $e = 3$ and since $a_2 = h_{\rho-1} = h_4 = 1$, we find that order of a_2 is $k = 1$. Thus $\alpha = 1$ and since $\tau = 2^\alpha[e, k]$, we have $\tau = 6$. So $\pi(h_n) = \tau\rho = 30$. ■

Theorem 3.22: Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ 1]$ for $h_2, h_3 \in \mathbf{F}_p^*$ and $h_5 = 0$. If $h_2 = h_3$, then the period of (h_n) is 10 and terms of (h_n) are given by

$$\begin{aligned} &0\ 1\ h_2\ h_2\ 1\ 0\ -1\ -h_2\ -h_2\ -1 \\ &0\ -1\ -h_2\ -h_2\ -1\ \cdots. \end{aligned}$$

Proof: If $h_2 = h_3$, then we have seen that the period of (h_n) is 10. Therefore by using duplication formulas we have the desired result. ■

Theorem 3.23: Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ -1]$ for $h_2, h_3 \in \mathbf{F}_p^*$ and $h_5 = 0$. Then (h_n) is given by

$$h_n = \begin{cases} \varepsilon(-1)^{k+1}h_r & for\ n \geq 15 \\ h_r & for\ n < 15, \end{cases}$$

where $n = 15k + r$ or $n = 15 - r$ for $r > 0$ and $\varepsilon = -1$ if k is even or $+1$ if k is odd.

Proof: Theorem can be proved by induction in the same way as Theorem 3.22 was proved. ■

In this case, if $p \equiv 1(mod\ 6)$, then we must choose $h_3 = -h_2, -h_2\omega$ and $-h_2\omega^2$ and if $p \equiv 5(mod\ 6)$, then we must choose $h_3 = -h_2$. Similarly, we see that if $p \equiv 5(mod\ 6)$, then there are $p-1$ EDS with initial values $[1\ h_2\ h_3\ -1]$ and if $p \equiv 1(mod\ 6)$, then there are $3(p - 1)$ sequences in $\mathbf{F}_p$.

Theorem 3.24: Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ -1]$ for $h_2, h_3 \in \mathbf{F}_p^*$ and $h_5 = 0$. Then period of (h_n) is

$$\pi(h_n) = \begin{cases} 5 & if\ h_3 = -h_2 \\ 15 & if\ h_3 = -h_2\omega, -h_2\omega^2. \end{cases}$$

Proof: Theorem can be proved in the same way as Theorem 3.21 was proved. ■

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

Theorem 3.25: Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ h_4]$ for $h_2, h_3, h_4 \in \mathbf{F}_p^*$ and $h_5 = 0$.

Then (h_n) is associated to an elliptic curve E given by the equation

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

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 $h_3^3 = h_2^4c$. Putting $h_3^3 = h_2^4c$ in (5), (6) and (8) we find the desired results. ■

In this section, we determine curves associated to (h_n) with rank five and $h_4 = 1$ and then determine that when the EDSs associated to singular curves.

Theorem 3.26: Let (h_n) be an elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ 1]$ for $h_2h_3 \neq 0$ and $h_5 = 0$. Then there exists a singular curve E associated with (h_n) if and only if $p = 5$ or $p \equiv 1, 9(mod\ 10)$.

Proof: The sequence (h_n) is a singular EDS if and only if $\Delta = 0$. Since (h_n) be an EDS with rank five and $h_4 = 1$, then we have $h_2^3 = h_3^3$. Putting $h_2^3 = h_3^3$ and $h_4 = 1$ in (4), we have

$$\Delta = -h_2^{10} + 11h_2^5 + 1.$$

Substituting $h_2^5 = t$ in the last equation and taking $\Delta = 0$ we have

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

Thus (h_n) is associated to a singular curve if and only if $p = 5$ or 5 is a quadratic residue in $\mathbf{F}_p$. 5 is a quadratic residue in $\mathbf{F}_p$ if and only if $p \equiv 1, 9(mod\ 10)$. ■

Corollary 3.27: Let (h_n) be a singular elliptic divisibility sequence with initial values $[1\ h_2\ h_3\ 1]$ for $h_2h_3 \neq 0$ and $h_5 = 0$. Then the number of the singular curves associated to (h_n) is 2 or 5.

Proof: The number of the solutions of the congruence $h_2^5 \equiv t_1, t_2(mod\ p)$ is 10 (there are 5 solutions for t_1 and 5 for t_2) if $p \equiv 1(mod\ 10)$ and 2 if $p \equiv 9(mod\ 10)$. ■

REFERENCES

[1] D.V. Chudnovsky and G.V. Chudnovsky. *Sequences of numbers generated by addition in formal groups and new primality factorization tests.* Adv. in Appl. Math. **7**(1986), 385–434.
[2] M. Einsiedler, G. Everest, T. Ward. *Primes in elliptic divisibility sequences.* LMS J. Comput. Math. **4**(2001), 1–13, electronic.
[3] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward. *Recurrence Sequences.* Mathematical Surveys and Monographs **104**(2003), AMS, Providence, RI.
[4] G. Everest and T. Ward. *Primes in divisibility sequences.* Cubo Mat. Educ. **3**(2001), 245–259.
[5] T. Koshy. *Fibonacci and Lucas Numbers with Applications.* John Wiley and Sons, 2001.
[6] R. Shipsey. *Elliptic Divisibility Sequences.* PhD Thesis, Goldsmith's University of London, 2000.
[7] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Sringer-Verlag, 1986.
[8] J.H. Silverman and N. Stephens. *The Sign of an Elliptic Divisibility Sequences.* Journal of Ramanujan Math. Soc. **21**(2006), 1–17.
[9] J.H. Silverman and J. Tate. *Rational Points on Elliptic Curves.* Undergraduate Texts in Mathematics, Springer, 1992.
[10] C.S. Swart. *Elliptic Curves and Related Sequences.* PhD Thesis, Royal Holloway University of London, 2003.
[11] A. Tekcan, B. Gezer and O. Bizim. *Some relations on Lucas numbers and their sums.* Advanced Studies in Comtem. Maths. **15**(2)(2007), 195–211.
[12] A. Tekcan, A. Özkoç, B. Gezer and O. Bizim. *Some Relations Involving the Sums of Fibonacci Numbers.* Proc. of the Jangjeon Math. Soc. **11**(1) (2008), 1–12.
[13] N.N. Vorobiev. *Fibonacci Numbers.* Birkhauser, Basel, Boston, 2002.
[14] M. Ward. *The law of repetition of primes in an elliptic divisibility sequences.* Duke Math. J. **15**(1948), 941–946.
[15] M. Ward. *Memoir on elliptic divisibility sequences.* Amer. J. Math. **70** (1948), 31–74.