

On The Elliptic Divisibility Sequences over Finite Fields

Osman Bizim

Abstract—In this work we study elliptic divisibility sequences over finite fields. Morgan Ward in [11, 12] gave arithmetic theory of elliptic divisibility sequences. We study elliptic divisibility sequences, equivalence of these sequences and singular elliptic divisibility sequences over finite fields \mathbf{F}_p , $p > 3$ is a prime.

Keywords—Elliptic divisibility sequences, equivalent sequences, singular sequences.

I. PRELIMINARIES.

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. 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

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

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

There are some trivial examples such as the sequence of integers \mathbf{Z}

$$0, 1, 2, 3, 4, 5, 6, \dots$$

is an EDS but non-trivial examples abound. The simplest EDS is the sequence

$$0, 1, 1, -1, 1, 2, -1, -3, -5, 7, -4, -28, 29, 59, 129, \\ -314, -65, 1529, -3689, -8209, -16264, 83331, \\ 113689, -620297, 2382785, 7869898, 7001471, \\ -126742987, -398035821, 168705471, \dots$$

This is the sequence A006769 in the On-Line Encyclopedia of Integer Sequences maintained by Neil Sloane.

EDSs are generalizations of a class of integer divisibility sequences called Lucas sequences, [10]. 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 [11, 12]. For the arithmetic properties of EDSs, see also [2, 3, 4, 5, 9]. Shipsey and Swart [6, 9] interested in the properties of EDSs reduced modulo primes. The Chudnovsky brothers considered prime values of EDSs in [1]. Rachel Shipsey [5] used EDSs to study

Osman Bizim is with the Uludag University, Department of Mathematics, Faculty of Science, Bursa-TURKEY, email: obizim@uludag.edu.tr. This work was supported by The Scientific and Technological Research Council of Turkey, project no: 107T311.

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.

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 $h_2 | h_4$. An EDS which do not satisfy one (or more) of these conditions is called *improper elliptic divisibility sequence*. The sequence (h_n) with initial values $h_1 = 1, h_2, h_3$ and h_4 is denoted by $[1 \ h_2 \ h_3 \ h_4]$.

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 *rank of apparition* of m in (h_n) .

Elliptic divisibility sequences are a generalization of a class of divisibility sequences studied earlier by Edouard Lucas. In fact many of Ward's results about EDSs were prompted by similar results discovered by Lucas for his sequences.

Let α be a rational number, and let a and b the roots of the polynomial $x^2 - \alpha x + 1$. If $a \neq b$ let (l_n) be the sequence

$$l_n = \frac{a^n - b^n}{a - b}$$

for $n \in \mathbf{Z}$. If $a = b$ define

$$l_n = na^{n-1}.$$

Then (l_n) is called a *Lucas sequence* with parameter α . Ward said that the Lucas sequence (l_n) is an EDS if and only if α is an integer. Lucas sequences are special case of a type of EDS called a singular EDS. The following definition will show us that which EDSs are singular.

Discriminant of an elliptic divisibility sequence (h_n) is defined by the formula

$$\Delta(h_2, h_3, h_4) = \frac{1}{h_2^8 h_3^3} \begin{bmatrix} (h_4^4 + 3h_2^5 h_4^3 + (3h_2^8 + 8h_3^3)h_4^2) \\ + h_2^7 (h_2^8 - 20h_3^3)h_4 \\ + h_2^4 h_3^3 (16h_3^3 - h_2^8) \end{bmatrix}.$$

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. Now we see that when two EDSs are equivalent so we need to know following definition:

Definition 1.1: Two elliptic divisibility sequences (h_n) and (h'_n) are said to be equivalent if there exists a constant θ such that

$$h'_n = \theta^{n^2-1} h_n$$

for all $n \in \mathbf{Z}$.

Ward used diophantine equations to characterize singular EDSs in terms of their initial values in the following theorem:

Theorem 1.1: [12] An elliptic divisibility sequence (h_n) with $h_2h_3 \neq 0$ is singular if and only if there exist integers r and s such that

$$h_2 = r, \quad h_3 = s(r^2 - s^3), \quad h_4 = rs^3(r^2 - 2s^3).$$

Ward proved further that Lucas sequences with $h_2h_3 \neq 0$ are singular in the following theorem.

Theorem 1.2: [12] An elliptic divisibility sequence (h_n) with $h_2h_3 \neq 0$ is a Lucas sequence with parameter α if and only if it is a singular solution with $r = \alpha$ and $s = 1$ in Theorem 1.1.

If (h_n) is a singular elliptic divisibility sequence with $s \neq 1$ then we have the following result:

Theorem 1.3: [12] Let (h_n) be a singular EDS, and let $\alpha = \frac{r\sqrt{s}}{s^2}$ and $\theta^2 = s$, where r and s are the integers given in Theorem 1.1. Let (l_n) be a Lucas sequence then $h_n = \theta^{n^2-1}l_n$ for all $n \in \mathbf{Z}$

This theorem tells us that every singular EDS is a Lucas sequence or is equivalent to a Lucas sequence.

We will now give a short account of material that we need about elliptic curves, all of the theory of elliptic curves can be found in [6, 8]. Consider an elliptic curve defined over the rational numbers determined by a generalized Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with the coefficients $a_1, \dots, a_6 \in \mathbf{Z}$. Define quantities by

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{aligned}$$

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.

Theorem 1.4: [5] Let (h_n) be an elliptic divisibility sequence with initial values

$$[1 \ h_2 \ h_3 \ h_4].$$

Then there exists an elliptic curve

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x,$$

where $a_1, \dots, a_4 \in \mathbf{Z}$, 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 $n \in \mathbf{Z}$,

where ψ_n is the n -th polynomial of E . Define quantities when $a_1 = 0$,

$$\begin{aligned} a_3 &= h_2, \\ a_4 &= \frac{h_4 + h_2^5}{2h_2h_3}, \\ a_2 &= \frac{h_3 + a_4^2}{h_2^2} \end{aligned} \quad (2)$$

and when $a_1 = 1$,

$$\begin{aligned} a_4 &= \frac{h_4 - h_2^2h_3 + h_2^5}{2h_2h_3}, \\ a_2 &= \frac{h_3 + a_1a_3a_4 + a_4^2}{h_2^2}. \end{aligned} \quad (3)$$

Ward showed that the discriminant of the elliptic divisibility sequence is equal to discriminant of elliptic curve associated to this sequence in the following theorem.

Theorem 1.5: [12] Let (h_n) be an elliptic divisibility sequence in which $h_2h_3 \neq 0$, and let E be an associated elliptic curve with (h_n) . Then the discriminant of (h_n) is equal to discriminant of elliptic curve E .

Ward also showed that there is a similar relation between singular EDSs and the singular curves.

Theorem 1.6: [5, 12] Let (h_n) be a singular elliptic divisibility sequence with $h_2h_3 \neq 0$, in the notation Theorem 1.1, then elliptic curve

$$E : y^2 + ry = x^3 + 3sx^2 + 3s^2x$$

has a cusp and

$$a_3 = r, a_2 = 3s, a_4 = 3s^2 \Leftrightarrow r^2 = 4s^3.$$

II. THE NUMBER OF THE ELLIPTIC DIVISIBILITY SEQUENCES, EQUIVALENT SEQUENCES AND SINGULAR SEQUENCES OVER \mathbf{F}_p .

In this section we will consider the elliptic divisibility sequences over a finite field. Firstly, we define the elliptic sequences and then elliptic divisibility sequences over \mathbf{F}_p , where $p > 3$ is a prime.

Definition 2.1: An elliptic sequence over \mathbf{F}_p is a sequence of elements of \mathbf{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 \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 . Let (h_n) be an EDS over \mathbf{F}_p then we denote this sequence by $(h_n(p))$.

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

Lemma 2.1: Let $(h_n(p))$ be an elliptic divisibility sequence with rank ρ over \mathbf{F}_p . Then $h_{\rho n} \equiv 0(p)$.

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

Now, we will give some basic facts about EDSs over finite fields. We consider the number of the elliptic divisibility sequences over \mathbf{F}_p and then we determine singular elliptic divisibility sequences and number of these sequences.

Theorem 2.1: The number of the elliptic divisibility sequences over \mathbf{F}_p is $p^3 - p^2 + p$.

Proof: If $(h_n(p))$ is an EDS with $h_0 = 0$ and $h_1 = 1$, then there are p alternatives for choosing the terms h_2, h_3 and h_4 . Therefore, we may think there are p^3 elliptic divisibility sequences over \mathbf{F}_p , but we know that h_2 is a divisor of h_4 . So, if $h_2 = 0$, then we may have $h_4 = 0$. Thus we must subtract the sequences with $h_2 = 0$ and $h_4 \neq 0$. Similarly we find number of this sequences is $p(p-1)$. So we have

$$p^3 - p(p-1) = p^3 - p^2 + p$$

sequences over \mathbf{F}_p . ■

Theorem 2.2: The number of the improper elliptic divisibility sequences over \mathbf{F}_p is p^2 .

Proof: If $h_2 \neq 0$, then there are $p-1$ alternatives for the second term and since the third term may equals to zero there are p alternatives for choosing the term h_3 for every h_2 with $h_2 \neq 0$. Therefore there are $p(p-1)$ alternatives for the pairs $h_2 \neq 0$ and h_3 . On the other hand, if $h_2 = 0$ and $h_3 \neq 0$, then there are $p-1$ alternatives for choosing these pairs. Finally considering the case where $h_2 = 0$ and $h_3 = 0$ we see that there are

$$(p-1)p + (p-1) + 1 = p^2$$

improper elliptic divisibility sequences over \mathbf{F}_p . ■

Theorem 2.3: The number of the proper elliptic divisibility sequences over \mathbf{F}_p is $(p-1)^2 p$.

Proof: If $(h_n(p))$ is a proper EDS, then we know that $h_2 \neq 0$ and $h_3 \neq 0$. So there are $p-1$ alternatives for choosing the terms $h_2 = 0$ and h_3 . Thus we have $(p-1)^2$ sequences only considering these terms. Considering that h_2 is a divisor of h_4 and there are p alternatives for choosing the term h_4 we see that the number of the proper elliptic divisibility sequences over \mathbf{F}_p is $(p-1)^2 p$. ■

From now on, we will call *singular curves of first type* if these curves have cusp the case where $c_4 = 0$, and *singular curves of second type* if the curves have node where $c_4 \neq 0$.

Theorem 2.4: For every prime $p > 3$ the sequence [1 2 3 4] is associated to curve $E : y^2 + 2y = x^3 + 3x^2 + 3x$ and all singular sequences equivalent to [1 2 3 4] are associated to first type singular curve and they are birationally equivalent to singular curve $E : y^2 = x^3$. Moreover the number of such sequences is $p-1$.

Proof: If we substitute $h_2 = 2, h_3 = 3$ and $h_4 = 4$ in the equations (1), (3), then we have the singular curve $E : y^2 + 2y = x^3 + 3x^2 + 3x$. Now we find the curve associated to the sequence to equivalent to [1 2 3 4]. So, putting $\theta = 1, 2, \dots, p-1$ in the equation

$$h'_n(p) = \theta^{n^2-1} h_n(p)$$

we see that all sequences $(h'_n(p))$ are associated to first type curves and they are birationally equivalent to singular curve $E : y^2 = x^3$.

We know that the sequence [1 2 3 4] is singular then there exist integers r and s such that

$$h_2 = r = 2, h_3 = s(r^2 - s^3) = 3, h_4 = r s^3 (r^2 - 2s^3) = 4.$$

Similarly since $(h'_n(p))$ is a singular sequence we want to show that there exists r' and s' such that

$$h'_2 = r', h'_3 = s'(r'^2 - s'^3), h'_4 = r' s'^3 (r'^2 - 2s'^3).$$

Since $h'_2 = \theta^3 h_2$ we have $r' = r\theta^3$ and so $r' = 2\theta^3$. Now we determine the number s' . To do this we use the fact that $r' = 4s'^3$. If we substitute $r' = 2\theta^3$ in this equation we find that $s' = \theta^2$.

By Theorem 1.6 we know that " $(h_n(p))$ is a singular elliptic divisibility sequence then $(h_n(p))$ is associated to curve $E : y^2 + ry = x^3 + 3sx^2 + 3s^2x$ if and only if $r^2 = 4s^3$ " and since $4 \in \mathbf{Q}_p$ (where \mathbf{Q}_p denotes the set of quadratic residues in modulo p) we have

$$4s^3 \in \mathbf{Q}_p \Leftrightarrow s^3 \in \mathbf{Q}_p$$

and so $s \in \mathbf{Q}_p$. Thus there are two y values for every s and so there are $2|\mathbf{Q}_p| = p-1$ sequences. ■

Example 2.1: Consider the sequence [1 2 3 4] in \mathbf{F}_5 . Then for $\theta = 1, 2, 3, 4$ we have the equivalent sequences

$$[1 \ 2 \ 3 \ 4], [1 \ 1 \ 3 \ 2], [1 \ 4 \ 3 \ 3], [1 \ 3 \ 3 \ 1]$$

and these sequences are associated to singular curves

$$E_1 : y^2 + 2y = x^3 + 3x^2 + 3x$$

$$E_2 : y^2 + y = x^3 + 2x^2 + 3x$$

$$E_3 : y^2 + 4y = x^3 + 2x^2 + 3x$$

$$E_4 : y^2 + 3y = x^3 + 3x^2 + 3x$$

respectively, by using the equations (2) and (3). Notice that these curves are birationally equivalent to $E : y^2 = x^3$.

Remark 2.5: Note that we give these result for every prime $p > 3$ this is because we do not use the equations (2) and (3) when $p = 2$ or 3.

First we give the number of the singular proper EDSs over \mathbf{F}_p in the following theorem:

Theorem 2.6: The number of the proper singular elliptic divisibility sequences (h_n) over \mathbf{F}_p is $(p-1)(p-2)$.

Proof: If $(h_n(p))$ is a proper EDS, then we know that $h_2h_3 \neq 0$ and so $r, s \in \mathbf{F}_p^*$. Since there are $p-1$ alternatives for the numbers r and s . So there are $(p-1)^2$ pairs (r, s) . Therefore there are $(p-1)^2$ alternatives for the pairs (r, s) . On the other hand since $s(r^2 - s^3) \neq 0$ we have $r^2 \neq s^3$. First we find the number of pairs (r, s) , where $r^2 = s^3$. So consider two cases either $p \equiv 1(6)$ or $p \equiv 5(6)$.

i) Let $p \equiv 1(6)$. Then since $r^2 = s^3 \in \mathbf{K}_p^*$ (where \mathbf{K}_p denotes the set of cubic residues in modulo p and $\mathbf{K}_p^* = \mathbf{K}_p \setminus \{0\}$) we have $\frac{p-1}{3}$ alternatives for the numbers r . On the other hand the numbers s which satisfies the equation $r^2 = s^3$ are $r^2, r^2\omega, r^2\omega^2$ (where $\omega = \frac{-1+\sqrt{3}}{2}$ is the cubic root of unity) for every r . Therefore there are $3 \cdot \frac{p-1}{3} = p-1$ pairs (r, s) which satisfies the equation $r^2 = s^3$.

ii) Let $p \equiv 5(6)$. Then since $r^2 = s^3 \in \mathbf{K}_p^*$ we have $p-1$ alternatives for the numbers r . On the other hand the numbers s which satisfies the equation $r^2 = s^3$ is only $s = r^2$ for every r .

Therefore there are $p-1$ pairs. Thus there are

$$(p-1)^2 - (p-1) = (p-1)(p-2)$$

singular sequences in both cases. ■

Corollary 2.7: The number of the first type sequences is $(p-1)$ and the number of the second type is $(p-1)(p-3)$.

Proof: By Theorem 2.4 we know that there are $p-1$ first type sequences. Subtracting these sequences from all singular sequences we have desired result. ■

Now we give a theorem to determine equivalence classes of singular EDSs.

Theorem 2.8: Let $(h_n(p))$ and $(h'_n(p))$ be two singular elliptic divisibility sequences. Then $(h_n(p))$ and $(h'_n(p))$ are equivalent if and only if $s \in \mathbf{Q}_p$, s as in Theorem 1.1.

Proof: We know that “ (h_n) and (h'_n) are equivalent if and only if there exists a rational constant θ such that $h'_n = \theta^{n^2-1}h_n$ for all $n \in \mathbf{Z}$ ” and by Theorem 1.3 we know that “ (h_n) and (h'_n) are equivalent singular EDS if and only if there exists $\alpha = \frac{r\sqrt{s}}{s^2}$ and $\theta^2 = s$ such that $h'_n = \theta^{n^2-1}h_n$ for all $n \in \mathbf{Z}$ ”. Therefore we have $s \in \mathbf{Q}_p$. ■

Definition 2.2: A singular EDS $(h_n(p))_s$ with initial values

$$h_2 = r, h_3 = r^2 - 1, h_4 = r(r^2 - 2)$$

is called representative sequence of singular EDSs, where $h_2h_3 \neq 0$

It is clear from the definition that every representative sequence is a sequence of integers or a Lucas sequence. If $s \in \mathbf{Q}_p$, then every singular EDS is equivalent to a representative sequence and so we can classify all singular EDSs by using these representative sequences. We denote this equivalence sequence classes by $\overline{[(h_n(p))]}$. If a singular EDS $(h_n(p))_s$ with initial values

$$h_2 = r, h_3 = r^2 - 1, h_4 = r(r^2 - 2)$$

is a representative sequence, then a sequence $(h'_n(p))_s$ with initial values

$$h'_2 = -r = -h_2, h'_3 = r^2 - 1 = h_3, h'_4 = -r(r^2 - 2) = -h_4$$

is also a representative sequence.

Example 2.2: An EDS with initial values $[1 \ 3 \ 1 \ 0]$ is a representative sequence in \mathbf{F}_7 and sequences which are equivalent to this can be find as

$$[1 \ 3 \ 2 \ 0], [1 \ 3 \ 4 \ 0], [1 \ 4 \ 1 \ 0], [1 \ 4 \ 2 \ 0], [1 \ 4 \ 4 \ 0].$$

Therefore,

$$\overline{[1 \ 3 \ 1 \ 0]} = \left\{ \begin{array}{l} [1 \ 3 \ 1 \ 0], [1 \ 3 \ 2 \ 0], [1 \ 3 \ 4 \ 0], \\ [1 \ 4 \ 1 \ 0], [1 \ 4 \ 2 \ 0], [1 \ 4 \ 4 \ 0] \end{array} \right\}.$$

One may choose the sequence $[1 \ 4 \ 1 \ 0]$ as a representative sequence, in this case $\overline{[1 \ 3 \ 1 \ 0]} = \overline{[1 \ 4 \ 1 \ 0]}$. The next theorem will show us that sequences $[1 \ 3 \ 1 \ 0]$ and $[1 \ 4 \ 1 \ 0]$ are equivalent. All of these sequences are associated to singular curve which has node and they are birationally equivalent to singular curve

$$E : y^2 = x^3 + 2x + 2.$$

Now we see that if the sequences $(h_n(p))_s$ and $(h'_n(p))_s$ are representative sequences, then they are equivalent, so we can choose one of these as a representative sequence.

Theorem 2.9: Let $(h_n(p))_s$ be an EDS with initial values

$$h_2 = r, h_3 = r^2 - 1, h_4 = r(r^2 - 2)$$

and let $(h'_n(p))_s$ be an EDS with initial values

$$h'_2 = -r = -h_2, h'_3 = r^2 - 1 = h_3, h'_4 = -r(r^2 - 2) = -h_4,$$

then $(h_n(p))_s$ and $(h'_n(p))_s$ are equivalent sequences.

Proof: We now find a constant θ such that $h_2 = \theta^3h'_2$, $h_3 = \theta^8h'_3$ and $h_4 = \theta^{15}h'_4$. If we substitute $h'_2 = -h_2$, $h'_3 = h_3$ and $h'_4 = -h_4$ in these equations we have $\theta^3 = -1$, $\theta^8 = 1$ and $\theta^{15} = -1$. Therefore $\theta = -1$. ■

From now on we will call the sequence $((-1)^{n-1}h_n(p))$ inverse sequence of $(h_n(p))$ and we give results about $((-1)^{n-1}h_n(p))$.

Theorem 2.10: If $(h_n(p))$ is a singular EDS then its inverse $((-1)^{n-1}h_n(p))$ is also a singular EDS.

Proof: If (h_n) is a singular EDS, then $\Delta(h_2, h_3, h_4) = 0$. Putting $-h_2$ and $-h_4$ instead of h_2 and h_4 gives that

$$\Delta(-h_2, h_3, -h_4) = 0.$$

This shows us that $((-1)^{n-1}h_n(p))$ is a singular EDS. ■

Theorem 2.11: Let $(h_n(p))$ be an elliptic divisibility sequence with $h_2h_3 \neq 0$, then the number of the representative sequences so the number of the equivalence sequence classes is $\frac{p-3}{2}$, and there are $p-1$ sequences in every equivalence classes.

Proof: There are p alternatives for the number r since $s = 1$ where r and s as in Theorem 1.1. r can not be zero since $h_2 \neq 0$ and $h_2 = r$, and r can not be 1 or -1 since $h_3 = r^2 - 1$ and $h_3 \neq 0$. So there are $\frac{p-3}{2}$ equivalence sequence classes since the sequences $(h_n(p))$ and $((-1)^{n-1}h_n(p))$ are equivalent, and there are $2|\mathbf{Q}_p| = p-1$ sequences since $\theta^2 = s$. ■

Theorem 2.12: Let $(h_n(p))$ be a singular sequence. Then $(h_n(p))$ and its inverse $((-1)^{n-1}h_n(p))$ are associated to singular curves

$$E_1 : y^2 + h_2y = x^3 + \frac{h_3 + \alpha^2}{h_2^2}x^2 + \alpha x$$

and

$$E_2 : y^2 - h_2y = x^3 + \frac{h_3 + \alpha^2}{h_2^2}x^2 + \alpha x,$$

respectively, where

$$\alpha = \frac{h_4 + h_2^5}{2h_2h_3}$$

and they are birationally equivalent to the same singular curve E .

Proof: A singular EDS with initial values $[1 \ h_2 \ h_3 \ h_4]$ is associated to the singular curve

$$E_1 : y^2 + h_2y = x^3 + \frac{h_3 + \alpha^2}{h_2^2}x^2 + \alpha x$$

where $\alpha = \frac{h_4 + h_2^5}{2h_2h_3}$. Putting $-h_2$ and $-h_4$ instead of h_2 and h_4 in the last equation we have

$$E_2 : y^2 - h_2y = x^3 + \frac{h_3 + \alpha^2}{h_2^2}x^2 + \alpha x.$$

■

Theorem 2.13: If $(h_n(p))$ is associated to first type singular curve $E : y^2 + 2y = x^3 + 3x^2 + 3x$, then representative sequences of $(h_n(p))$ is sequence of integers $[1 \ 2 \ 3 \ 4]$ and other one can be chosen the Lucas sequence $[1 \ -2 \ 3 \ -4]$ which is inverse of $[1 \ 2 \ 3 \ 4]$.

Proof: By Theorem 1.6, we know that if $(h_n(p))$ is associated to a first type singular curve $E : y^2 + 2y = x^3 + 3x^2 + 3x$, then $r^2 = 4s^3$. Since sequences with $s = 1$ are representative sequences we have $r = \pm 2$. So for $r = -2$, $(h_n(p))$ is associated to first type singular curve $E : y^2 - 2y = x^3 + 3x^2 + 3x$ and these two curves are birationally equivalent to $E : y^2 = x^3$. Hence we have $[1 \ 2 \ 3 \ 4]$ and $[1 \ -2 \ 3 \ -4]$ are representative sequences. ■

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** (1986), 385–434.
- [2] Einsiedler M., Everest G., Ward T. *Primes in elliptic divisibility sequences*. LMS J. Comput. Math. **4** (2001), 1–13, electronic.
- [3] Everest G., Van der Poorten A., Shparlinski I., 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**(2001), 245–259.
- [5] Shipsey R. *Elliptic Divisibility Sequences*. Dissertation, 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 sequences*. Journal of Ramanujan Math. Soc. **21** (2006), 1–17.
- [8] Silverman J. and Tate J. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics, Springer, 1992.
- [9] Swart, C.S. *Elliptic Curves and Related Sequences*. Dissertation, University of London, 2003.
- [10] Tekcan A., Gezer B. and Bizim O. *Some relations on Lucas numbers and their sums*. Advanced Studies in Contemporary Mathematics **15**(2)(2007), 195–211.
- [11] Ward M. *The law of repetition of primes in an elliptic divisibility sequences*. Duke Math. J. **15**(1948), 941–946.
- [12] Ward M. *Memoir on elliptic divisibility sequences*. Amer. J. Math. **70** (1948), 31–74.