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 \( F_p, p > 3 \) is a prime.

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

I. PRELIMINARIES.

A divisibility 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 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

\[
h_{m+n}h_{m-n} = h_{m+1}h_{m-1} - h_{m+1}h_{m-1} - h_m^2
\]

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 \(Z\)

\[
0, 1, 2, 3, 4, 5, 6, \ldots
\]

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

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

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 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 \(h_0 = 0, h_1 = 1, h_2h_3 \neq 0\). 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 \(p\) is an integer such that \(m|h_p\) and there is no integer \(j\) such that \(j\) is a divisor of \(p\) with \(m|h_j\) then \(p\) 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 \(\alpha\) be a rational number, and let \(\alpha\) 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 \(n \in \mathbb{Z}\). If \(a = b\) define

\[
l_n = n a^{n-1}.
\]

Then \((l_n)\) is called a Lucas sequence with parameter \(\alpha\). Ward said that the Lucas sequence \((l_n)\) is an EDS if and only if \(\alpha\) 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

\[
\Delta(h_2, h_3, h_4) = \frac{1}{h_2h_3} \left[ \frac{(h_2^4 + 3h_2^2h_3^2 + (3h_2^2 + 8h_3^2)h_4^2)}{h_3^2} \right].
\]

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 \(\theta\) such that

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

for all \(n \in \mathbb{Z}\).
Then there exists an elliptic curve $E$ such that $E_{a,y} + a_2 y^2 + a_4 y = x^3 + a_6 x^2 + a_8 x$.

Ward proved that EDS arise as values of the division polynomials of an elliptic curve. We will write $\psi_n(E)$ for $\psi_n$.

In this section we will consider the elliptic divisibility sequences over a finite field. First, we define the elliptic divisibility sequence over $\mathbb{F}_p$, then we denote this sequence by $(\lambda_n(p))$. In particular, if $(\lambda_n)$ is an elliptic divisibility sequence over $\mathbb{F}_p$, then we denote it by $(\lambda_n(p))$. In this paper, we will deal with non-singular elliptic curves over finite fields.

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

$$E_{a,y} + a_2 y^2 + a_4 y = x^3 + a_6 x^2 + a_8 x.$$

II. THE NUMBER OF THE ELLIPTIC DIVISIBILITY SEQUENCES EQUIVALENT TO $\mathbb{F}_p$ AND SINGULAR CURVES

We also showed that there is a relation between singular elliptic curves and the elliptic divisibility sequences. If $h_0$ is a singular elliptic divisibility sequence, then $h_n$ is equal to the discriminant of the elliptic curve associated to this sequence in the following theorem.

If $h_0$ is a singular elliptic divisibility sequence, then $h_n$ is equal to the discriminant of the elliptic curve associated to this sequence in the following theorem.

This theorem tells us that every singular EDS is a Lucas sequence. We will now give a short account of material that we need to know about elliptic curves. All of the theory of elliptic curves can be found in [8].

Theorem 1.6: Let $(\lambda_n)$ be a Lucas sequence over $\mathbb{F}_p$. Then, the following theorem is proved by Ward.

If $h_0$ is a singular elliptic divisibility sequence, then $h_n$ is equal to the discriminant of the elliptic curve associated to this sequence in the following theorem.

$$h_n = \lambda_n^2 - \lambda_{n+1} \lambda_{n-1}.$$
Note that as in the integral sequences, elliptic divisibility sequences over \( F_p \) satisfy the further conditions that \( h_0 = 0, h_1 = 1 \) and two consecutive terms of \( (h_n) \) cannot vanish over \( F_p \) 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 \( n \in \mathbb{N} \). This relation is shown below:

**Lemma 2.1:** Let \((h_n(p))\) be an elliptic divisibility sequence with rank \( \rho \) over \( F_p \). Then \( h_{\rho n} \equiv 0(p) \).

**Proof:** Let \((h_n(p))\) be an elliptic divisibility sequence over \( F_p \). If \((h_n(p))\) has rank \( \rho \), then \( h_{\rho n} \equiv 0(p) \) since \( h_{\rho} \) divides \( h_{\rho n} \) for \( \rho \) divides \( \rho n \).

Now, we will give some basic facts about EDSs over finite fields. We consider the number of the elliptic divisibility sequences over \( F_p \) and then we determine singular elliptic divisibility sequences and number of these sequences.

**Theorem 2.1:** The number of the elliptic divisibility sequences over \( F_p \) 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 \( p^2 \) elliptic divisibility sequences over \( F_p \), but we know that \( h_2 \) is a divisor of \( h_1 \). So, if \( h_2 = 0 \), then we may have \( h_4 = 0 \). Thus we must substract the sequences with \( h_2 = 0 \) and \( h_4 = 0 \). 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 \( F_p \).

**Theorem 2.2:** The number of the improper elliptic divisibility sequences over \( F_p \) 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 \( F_p \).

**Theorem 2.3:** The number of the proper elliptic divisibility sequences over \( F_p \) is \( (p - 1)^2p \).

**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 \( h_3 \) and there are \( p \) alternatives for choosing the term \( h_3 \) we see that the number of the proper elliptic divisibility sequences over \( F_p \) is \( (p - 1)^2p \).

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 \( \theta = 1, 2, \ldots, p - 1 \) in the equation

\[
h_\theta(p) = (p^2 - 1)h_n(p)
\]

we see that all sequences \( (h_\theta(p)) \) 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

\[
h_2 = r = 2, \ h_3 = s(r^2 - s^3) = 3, \ h_4 = rs^3(r^2 - 2s^3) = 4.
\]

Similarly since \( (h_\theta(p)) \) 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 \( h_2'^3 = 3h_2' \) 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 \( E : y^2 + ry = x^3 + 3sx^2 + 3x^2x \) if and only if \( r = 4s^3 \). Since there are \( 4s^3 \in \mathbb{Q}_p \) where \( \mathbb{Q}_p \) denotes the set of quadratic residues modulo \( p \) we have

\[
4s^3 \in \mathbb{Q}_p \iff s^3 \in \mathbb{Q}_p.
\]

and so \( s \in \mathbb{Q}_p \). Thus there are two \( y \) values for every \( s \) and so there are \( 2(\mathbb{Q}_p) = p - 1 \) sequences.

**Example 2.1:** Consider the sequence [1 2 3 4] in \( F_5 \). 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 $\mathbb{F}_p$ in the following theorem:

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

**Proof:** If $(h_n(p))$ is a proper EDS, then we know that $h_2 h_3 \neq 0$ and so $r, s \in \mathbb{F}_p^*$. 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 pair $(r, s)$. On the other hand since $s(r^2 - s^2) \neq 0$ we have $r^2 \neq s^2$. First we find the number of pairs $(r, s)$, where $r^2 = s^2$. So consider two cases either $p \equiv 1(6)$ or $p \equiv 5(6)$.

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

ii) Let $p \equiv 5(6)$. Then since $r^2 = s^2 \in \mathbb{F}_p^*$ we have $p-1$ alternatives for the numbers $r$. On the other hand the numbers $s$ which satisfies the equation $r^2 = s^2$ 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 $s \in \mathbb{Q}_p$, $s$ 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 $\theta$ such that $h'_n = \theta^{n} h_n$ for all $n \in \mathbb{Z}$ and by Theorem 1.3 we know that $(h_n)$ and $(h'_n)$ are equivalent singular EDS if and only if there exists $\alpha = \frac{r_s}{r_t}$ and $\theta^2 = s$ such that $h'_n = \theta^{n-1} h_n$ for all $n \in \mathbb{Z}$. Therefore we have $s \in \mathbb{Q}_p$.

**Definition 2.2:** A singular EDS $(h_n(p))$, 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 $h_2 h_3 \neq 0$.

It is clear from the definition that every representative sequence is a sequence of integers or a Lucas sequence. If $s \in \mathbb{Q}_p$, 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 $[(h_n(p))]$. If a singular EDS $(h_n(p))$, with initial values $h_2 = r, \ h_3 = r^2 - 1, \ h_4 = r(r^2 - 2)$ is a representative sequence, then a sequence $(h'_n(p))$, 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 $\mathbb{F}_p$ 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,

$[1 \ 3 \ 1 \ 0] = \{ [1 \ 3 \ 1 \ 0], [1 \ 3 \ 2 \ 0], [1 \ 3 \ 4 \ 0], [1 \ 4 \ 1 \ 0], [1 \ 4 \ 2 \ 0], [1 \ 4 \ 4 \ 0] \}$.

One may choose the sequence $[1 \ 4 \ 1 \ 0]$ as a representative sequence, in this case $[1 \ 3 \ 1 \ 0] = [1 \ 4 \ 1 \ 0]$. 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 $(h_n(p))$ and $(h'_n(p))$, are representative sequences, then they are equivalent, so we can choose one of these as a representative sequence.

**Theorem 2.9:** Let $(h_n(p))$ be an EDS with initial values $h_2 = r, \ h_3 = r^2 - 1, \ h_4 = r(r^2 - 2)$ and let $(h'_n(p))$ 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 $(h_n(p))$ and $(h'_n(p))$, are equivalent sequences.

**Proof:** We now find a constant $\theta$ such that $h_2 = \theta^3 h'_2, \ h_3 = \theta^6 h'_3$ 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 $\theta^3 = -1, \ \theta^6 = 1$ 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 \( \sum_{s=1}^{r-1} \), and there are \( p-1 \) sequences in every equivalence class.

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 \( \sum_{s=1}^{r-1} \) equivalence sequence classes since the sequences \( (h_n(p)) \) and \( ((-1)^{n-1}h_n(p)) \) are equivalent, and there are \( 2|Q_p| = p-1 \) 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

\[
\alpha = \frac{h_4 + h_2^2}{2h_2h_3}
\]

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 \( \alpha = \frac{h_4 + h_2^2}{2h_2h_3} \). 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