Edwards curve points counting method and supersingular Edwards and Montgomery curves

(Cryptosystems, Cryptology and Theoretical Computer Science)

RUSLAN SKURATOVSKII, MYKOLA BOHDANENKO,
Department of Computer Science,
National Technical University of Ukraine, Kiev,
UKRAINE

Abstract: — In this paper, an algebraic affine and projective Edwards curves [3, 9] over the finite field \( F_p \) is considered. It is well known, in the theory of Cryptosystems, Cryptology and Theoretical Computer Science, that many modern cryptosystems [11] can be naturally transformed into elliptic curves [5]. In this paper, Edwards algebraic curves over a finite field are studied which are one of the most promising supports of sets of points that are used for fast group operations [1]. In this paper, a new method for counting the order of an Edwards curve over a finite field is presented. This method can be applied in the order of elliptic curves due to the birational equivalence between elliptic curves and Edwards curves. We do not find only a specific set of coefficients with corresponding field characteristics for which these curves are supersingular, but we find also a general formula by which one can determine whether a curve \( E_{d}[F_p] \) is supersingular over this field or not. The embedding degree of the supersingular Edwards curve over \( F_p \) in a finite field is investigated and the field characteristic, where this degree is minimal, is found. A birational isomorphism between the Montgomery curve and the Edwards curve is also constructed. A one-to-one correspondence between the Edwards supersingular curves and Montgomery supersingular curves is presented. The criterion of supersingularity for Edwards curves is found over \( F_p \).

Keywords: — Cryptosystems, Cryptology, Theoretical Computer Science, Infinite fields, Elliptic curve, Edwards curves, order of group of points of an elliptic curve.


Published: April 30, 2020.

1. Introduction
It is well known, in the theory of Cryptosystems, Cryptology and Theoretical Computer Science that many modern cryptosystems [11] can be naturally transformed into elliptic curves [5]. The task of finding the order of an algebraic curve over a finite field \( F_p \) is now very relevant and is at the center of many mathematical studies in connection with the use of groups of points of curves of genus 1 in cryptography. In this study, this problem is solved for the Edwards and Montgomery curves.

The criterion of supersingularity of the Edwards curves is found over \( F_p \). We propose also a method for determining the points from Edwards curves and elliptic curves in response to an earlier paper by Schoof [8].

The algebraic affine and projective Edwards curves over a finite field is considered. We do not find only a specific set of coefficients with corresponding field characteristics for which supersingular, but we additionally find a general formula by which one can determine whether a curve \( E_{d}[F_p] \) is supersingular over this field or not.

We denote by \( E_{d} \) the Edwards curve with coefficient \( d \in F_p^{*} \) which is defined as \( x^2 + y^2 = 1 + dx^2 y^2 \) over \( F_p \).

The projective curve has form 
\[
F(x, y, z) = ax^2 z^2 + y^2 z^2 = z^4 + dx^2 y^2.
\]

The special points are the infinitely distant points \((1,0,0)\) and \((0,1,0)\) and therefore we find its singularities at infinity in the corresponding affine components 
\[
A' := ax^2 + y^2 z^2 = z^4 + dy^2 \
\text{and } A'' := ax^2 z^2 + z^2 = z^4 + dx^2.
\]

These are simple singularities.

We describe the structure of the local ring at the point \( p \), whose elements are quotients of functions with the form \( F(x, y, z) = f(x, y, z) / g(x, y, z) \), where the denominator cannot take the value of 0 at the singular point \( p \). In particular, we note that a local ring which has two singularities consists of functions with the denominators are not divisible by \((x - 1)(y - 1)\).

We denote by \( \delta_p = \dim (\overline{O}_p) \), where \( O_p \) denotes the local ring at the singular point \( p \). We denote by \( \overline{O}_p \) the whole closure of the local ring at the singular point \( p \).

2. Main Result
The twisted Edwards curve with coefficients \( a, d \in F_p^{*}, d \neq 1, p \neq 2, a \neq d \), is the curve \( E_{a,d} \):
\[
ax^2 + y^2 = 1 + dx^2 y^2, \quad a, d \in F_p^{*}, \quad ad(a - d) \neq 0.
\]

It should be noted that a twisted Edwards curve is called an Edwards curve when \( a = 1 \).
We find that \( \delta_y = \dim \mathcal{O}_y/\mathcal{O}_y = 1 \) is the dimension of the factor as a vector space. Because the basis of extension \( \mathcal{O}_y/\mathcal{O}_y \) consists of just one element at each distinct point, we obtain that \( \delta_y = 1 \). We calculate then the genus of the curve according to Fulton [4],

\[
\rho(C) = \rho_y(C) - \sum_{p \in \mathcal{P}} \delta_p = \frac{(n-1)(n-2)}{2}, \\
- \sum_{p \in \mathcal{P}} \delta_p = 3 - 2 = 1,
\]

where \( \rho_y(C) \) denotes the arithmetic genus of the curve \( C \) with parameter \( n = \deg(C) = 4 \). It should be noted that the supersingular points were discovered in [10]. We recall the curve has a genus of 1 and as such it is known to be isomorphic to a flat cubic curve, however, the curve is importantly not elliptic because of its singularity in the projective part. Both the Edwards curve and the twisted Edwards curve are isomorphic to some affine part of the elliptic curve. The Edwards curve after normalization is precisely a curve in the Weierstrass normal form, which was proposed by Montgomery [1] and will be denoted by \( E_0 \).

Koblitz [4,5] proves that one can detect if a curve is supersingular. Montgomery [1] proposed by Montgomery [1] and will be denoted by \( E_0 \). Using the search for the curve when that curve has the same number of points as its torsion curve. Also an elliptic curve \( E \) over \( \mathbb{F}_q \) is called supersingular if for every finite extension \( \mathbb{F}_{q^r} \) there are no points in the group \( E(\mathbb{F}_{q^r}) \) of order \( p \) [17]. It is known [1] that the transition from an Edwards curve to the related torsion curve is determined by the reflection \((\overline{x}, \overline{y}) \mapsto (x, y) = (\overline{x}, \frac{1}{\overline{y}}) \). We now recall an important result from Vinogradov [13] which will act as criterion for supersingularity.

**Lemma 2.1.** Let \( k \in \mathbb{Z} \) and \( p \in \mathbb{P} \). Then

\[
\sum_{k=0}^{n} k^r \equiv \begin{cases} 0 \pmod{p} & n \mid (p-1), \\
-1 \pmod{p} & n \mid (p-1),
\end{cases}
\]

where \( n \mid (p-1) \) denotes that \( n \) is divisible by \( p-1 \).

The order of a curve is precisely the number of its affine points with a neutral element, where the group operation is well defined. It is known that the order of \( x^2 + y^2 = 1 + dx^2y^2 \) coincides with the order of the curve \( x^2 + y^2 = 1 + dx^2y^2 \) over \( \mathbb{F}_p \). We will now strengthen an existing result given in [10]. We denote the number of points with a neutral element of an affine Edwards curve over the finite field \( \mathbb{F}_p \) by \( N_{d[p]} \) and the number of points on the projective curve over the same field by \( \overline{N}_{d[p]} \).

**Theorem 2.1.** If \( p = 3 \pmod{4} \) is prime and the following condition of supersingularity

\[
\sum_{j=0}^{p-1} \left( \frac{C_{p-1}^{j}}{2} \right)^2 d^j \equiv 0 \pmod{p},
\]

is true then the orders of the curves \( x^2 + y^2 = 1 + dx^2y^2 \) and \( x^2 + y^2 = 1 + d^{-1}x^2y^2 \) over \( \mathbb{F}_p \) are equal to

\[
N_{d[p]} = p + 1, \quad \text{when} \quad \left( \frac{d}{p} \right) = -1 , \quad \text{and} \quad N_{d[p]} = p - 3, \quad \text{when} \quad \left( \frac{d}{p} \right) = 1.
\]

**Proof.** Consider the curve \( E_d \):

\[
x^2 + y^2 = 1 + dx^2y^2.
\]

Transform it into the form \( y^2(1 - dx^2y^2) = 1 - x^2 \), then we express \( y^2 \) by applying a rational transformation which lead us to the curve \( y^2 = \frac{1 - x^2}{1 - dx^2y^2} \).

For our analysis we transform it into the curve

\[
y^2 = (x^2 - 1)(dx^2 - 1).
\]

We denote the number of points from an affine Edwards curve over the finite field \( \mathbb{F}_p \) by \( M_{d[p]} \). This curve (3) has

\[
M_{d[p]} = N_{d[p]} + \left( \frac{d}{p} \right) + 1 \text{ points, which is precisely } \left( \frac{d}{p} \right) + 1 \text{ greater than the number of points of curve } E_d.
\]

Let that \( \left( \frac{d}{p} \right) \) denotes the Legendre Symbol. Let \( a_0, a_1, \ldots, a_{p-2} \) be the coefficients of the polynomial \( a_0 + a_1x + \ldots + a_{p-2}x^{p-2} \), which was obtained from \( (x^2 - 1)^{p-1} = \frac{p-1}{2} \) after opening the brackets. Thus, summing over all \( x \) yields

\[
M_{d[p]} = \sum_{x=0}^{p-1} (x^2 - 1)(dx^2 - 1)^{p-1} = p + \sum_{x=0}^{p-1} \left( \frac{p-1}{2} \right)^{p-1}.
\]

By opening the brackets in \( (x^2 - 1)^{p-1} = \frac{p-1}{2} (dx^2 - 1)^{p-1} \), we have

\[
a_{p-2} = (-1)^{p-1} \cdot \frac{p-1}{2} \cdot \left( \frac{d}{p} \right) = \left( \frac{d}{p} \right) \pmod{p}.
\]

So, using Lemma 2.1 we have

\[
M_{d[p]} = - \left( \frac{d}{p} \right) - a_{p-1} \pmod{p}.
\]

We need to prove that \( M_{d[p]} = 0 \pmod{p} \) if \( p = 3 \pmod{8} \) and \( M_{d[p]} = -1 \pmod{p} \). We have to show therefore that

\[
\sum_{j=0}^{p-1} \left( \frac{C_{p-1}^{j}}{2} \right)^2 d^j = 0 \pmod{p}.
\]

If we can prove that \( a_{p-1} = 0 \pmod{p} \), then it will follow from (3). Let us determine \( a_{p-1} \) according to Newton’s binomial formula: \( a_{p-1} \) is equal to the coefficient at \( x^{p-1} \) in the polynomial, which is obtained as a product \( (x^2 - 1)^{p-1} \). So,
We replace \( a_{p-1} \equiv \frac{p-1}{2} \sum_{j=0}^{p-1} d^j \left( C_{e_j}^{j} \right)^2 \). Actually, the following equality holds:

\[
\sum_{j=0}^{p-1} d^j \left( C_{e_j}^{j} \right)^2 \equiv \left( \frac{p-1}{2} \right)^2 \sum_{j=0}^{p-1} \left( C_{e_j}^{j} \right)^2 \left( C_{e_j}^{j} \right)^2.
\]

Since \( a_{p-1} = -\frac{p-1}{2} \sum_{j=0}^{p-1} \left( C_{e_j}^{j} \right)^2 d^j \), then exact number of affine points on non-supersingular curve is the following

\[
M_{d[p]} = -a_{2p-1} - a_{p-1} = -\left( \frac{d}{p} \right) + \sum_{j=0}^{p-1} \left( C_{e_j}^{j} \right)^2 d^j \pmod{p}.
\]  

(5)

According to the condition of this theorem \( a_{p-1} = 0 \), therefore \( M_{d[p]} = -a_{2p-1} \pmod{p} \). Consequently, in the case when \( p = 3 \pmod{4} \), where \( p \) is prime and

\[
\sum_{j=0}^{p-1} \left( C_{e_j}^{j} \right)^2 d^j = 0 \pmod{p},
\]

the curve \( E_d \) has

\[
N_{d[p]} = p - \left( \frac{d}{p} \right) - \left( \frac{d}{p} \right) + 1 = p - 1 - \left( \frac{d}{p} \right)
\]

affine points and a group of points of the curve completed by singular points has \( p + 1 \) points.

The exact number of the points has upper bound \( 2p + 1 \), but for \( x = 0 \) we have only solution \( y = 0 \). Taking into account that \( x \in F_p \) we have exactly \( p \) values of \( x \). Also there are 4 pairs \( (\pm 1, 0) \) and \( (0, \pm 1) \) which are points of \( E_d \) thus \( N_{d[p]}) = 1 \). Thus \( N_{d[p]} = p + 1 \). This completes the proof.

Corollary: The orders of the curves \( x^2 + y^2 = 1 + dx^2 y^2 \) and \( x^2 + y^2 = 1 + d^{-1} x^2 y^2 \) over \( F_p \) are equal to

\[
N_{d[p]} = p + 1 = \overline{N}_{d[p]},
\]

when \( \left( \frac{d}{p} \right) = -1 \), and

\[
N_{d[p]} = p - 3 = \overline{N}_{d[p]} - 4,
\]

when \( \left( \frac{d}{p} \right) = 1 \) if \( p = 3 \pmod{4} \) is prime and

\[
\sum_{j=0}^{p-1} \left( C_{e_j}^{j} \right)^2 d^j = 0 \pmod{p}.
\]

Since all transformations in proof of Theorem 2.1 were equivalent transitions then we obtain the proof of equivalece of conditions.

**Theorem 2.2.** If the coefficient \( d = 2 \) or \( d = 2^{-1} \) and \( p = 3 \pmod{4} \) then \( \sum_{j=0}^{p-1} d^j \left( C_{e_j}^{j} \right)^2 = 0 \pmod{p} \) and

\[
\overline{N}_{d[p]} = p + 1.
\]

Proof. When \( p = 3 \pmod{4} \), we shall show that

\[
\sum_{j=0}^{p-1} d^j \left( C_{e_j}^{j} \right)^2 = 0 \pmod{p}.
\]

We multiply each binomial coefficient in this sum by \( \left( \frac{p-1}{2} \right)! \) to obtain after some algebraic manipulation

\[
\left( \frac{p-1}{2} \right)! C_{e_j}^{j} = \left( \frac{p-1}{2} \right)! \left( \frac{p-1}{2} - j + 1 \right) \left( \frac{p-1}{2} \right) \left( \frac{p-1}{2} - j - 1 \right) \cdots \left( \frac{p-1}{2} - j \right).
\]

After that, by applying the congruence

\[
\left( \frac{p-1}{2} \right)! \left( \frac{p-1}{2} + k \right) \equiv \left( \frac{p-1}{2} + k \right) \pmod{p},
\]

for \( 0 \leq k \leq \frac{p-1}{2} \) to the multipliers in previous parentheses, we obtain

\[
\left( \frac{p-1}{2} \right)! \left( \frac{p-1}{2} \right) \left( \frac{p-1}{2} - j \right) \cdots \left( \frac{p-1}{2} - j - 1 \right) \left( \frac{p-1}{2} - j \right).
\]

Thus, as a result of squaring, we have:

\[
\left( \frac{p-1}{2} \right)! C_{e_j}^{j} = \left( \frac{p-1}{2} - j + 1 \right) \left( \frac{p-1}{2} - j \right) \cdots \left( \frac{p-1}{2} - j - 1 \right) \left( \frac{p-1}{2} - j \right).
\]

(6)

It remains to prove that \( \sum_{j=0}^{p-1} \left( C_{e_j}^{j} \right)^2 d^j = 0 \pmod{p} \) if \( p = 3 \pmod{4} \).

Consider the auxiliary polynomial

\[
P(t) = \left( \frac{p-1}{2} \right)! \sum_{j=0}^{p-1} \left( C_{e_j}^{j} \right)^2 t^j.
\]

We are going to show that

\[
P(t) = 0 \pmod{p},
\]

and therefore \( a_{p-1} = 0 \pmod{p} \). Using (6) it can be shown that

\[
a_{p-1} = P(t) = \left( \frac{p-1}{2} \right)! \sum_{j=0}^{p-1} \left( C_{e_j}^{j} \right)^2 t^j = \sum_{j=0}^{p-1} \left( C_{e_j}^{j} \right)^2 t^j = \sum_{i=0}^{p-1} \left( 1 + k \right) t^j.
\]

over \( F_p \). We replace \( d \) by \( t \) in (1) such that we can research a more generalized problem. It should be noted that

\[
P(t) = t^0 + \cdots + t^p \pmod{p}
\]

for \( t = new variable but not a coordinate of curve. Observe that
$Q(t) = t^p - t^{-1} = (t - 1)^p (t + 1)^{-1} \pmod{p}$ and therefore the equality $P(t) = \left(\left((t - 1)^p - t^{-1}\right)\left(\frac{p-1}{2}\right)\right)$ holds over $\mathbb{F}_p$.

In order to simplify the notation, we let $\theta = t - 1$ and $R(\theta) = P(\theta + 1)$. For the case $t = 2$ we have $\theta = 1$.

Performing this substitution leads the polynomial $P(t)$ of 2 to the polynomial $R(t)$ of 1. Taking into account the linear nature of the substitution $\theta = t - 1$, it can be seen that that derivation by $\theta$ and $t$ coincide. Derivation leads us to the transformation of polynomial $R(\theta)$ to form where it has the necessary coefficient $a_{p-1}$. Then

$$R(\theta) = P(\theta + 1) = \frac{p-1}{2}\left(\frac{p-1}{2}\right)\left(\theta^{-1}(\theta + 1)\right)(\theta + 1) = \frac{p-1}{2}\left(\frac{p-1}{2}\theta^{-1} + 1\right) = \frac{p-1}{2}\left(\frac{p-1}{2}\right).$$

In order to prove that $a_{p-1} = 0 \pmod{p}$, it is now sufficient to show that $R(\theta) = 0$ if $\theta = 0$ over $\mathbb{F}_p$. We obtain

$$R(\theta) = \frac{p-1}{2}\left(\frac{p-1}{2}\right)(j + 1) \cdots (j + p^{-1} - 1).$$

We will manipulate now the expression

$$\frac{p-1}{2}(j + 1)(j + 2) \cdots (j + p^{-1} - 1).$$

In order to illustrate the simplification we now consider the scenario when $p = 11$ and hence $\frac{p-1}{2} = 5$.

The expression gets the form

$$(5 - j + 1)(5 - j + 2) \cdots (5 - j + 5) = (6 - j)(7 - j) \cdots (10 - j) = (-1)^5 (j + 1)(j + 2) \cdots (j + 5) \pmod{11}.$$ 

Therefore, for a prime $p$, we can rewrite the expression as

$$\frac{p-1}{2}(j + 1)(j + 2) \cdots (j + p^{-1} - 1) = (-1)^5 (j + 1)(j + 2) \cdots (j + p^{-1} - 1) \pmod{p}.$$

As a result, the symmetrical terms in (7 ) can be reduced yielding $a_{p-1} = 0 \pmod{p}$ . It should be noted that

$$(-1)^5 (j + 1)(j + 2) \cdots (j + p^{-1} - 1) = -1 \pmod{p}.$$ 

Consequently, we have $P(2) = R(1) = 0$ and hence $a_{p-1} = 0 \pmod{p}$ as required. Thus,

$$\sum_{j=0}^{p-1}(C_j^{\theta})^2 = 0 \pmod{p},$$

completing the proof of the corollary.

**Corollary 2.2.** The curve $E_d$ is supersingular i f $E_{d^*}$ is supersingular.

**Proof.** Let us recall the proved fact in Theorem 2.1 that

$$N_{d[p]} = -a_{d-2} - a_{d-1} = -\left(\frac{d}{p}\right) + \sum_{j=0}^{d-1}(C_j^{\theta})^2 \pmod{p}.$$ 

Since $(C_j^{\theta})^2 \pmod{p}$ by condition, and the congruence $\frac{d}{p} \pmod{p}$, holds then $N_{d[p]} = N_{d^*[p]}$.

**Corollary 2.3.** If $p \equiv 3 \pmod{4}$, is prime then there exists some $T$ such that $T = \sum_{j=0}^{d-1}(C_j^{\theta})^2 \pmod{p}$ and $N_{d[p]} = p - 1 - 2\left(\frac{d}{p}\right) + T$.

**Proof.** Due to equality (5) and the bounds (8) as well as according to generalized Hasse-Weil theorem $|N_{d[p]} - (p + 1) - 2\left(\frac{d}{p}\right)| \leq 2g\sqrt{p}$, where $g$ is genus of curve, we obtain exact number $N_{d[p]}$ as we showed, $g = 1$.

From Theorem 2.1 as well as from Corollary 2.2 we get, that

$$\sum_{j=0}^{d-1}(C_j^{\theta})^2 = -N_{d[p]} - (p + 1) - 2\left(\frac{d}{p}\right)$$

so there exists $T \in \mathbb{Q}$, such that $T < 2\sqrt{p}$ and $N_{d[p]} = p - 1 - 2\left(\frac{d}{p}\right) + T$.

**Example 2.1.** If $p = 13$, $d = 2$ gives $N_{d[1]} = 8$ and $p = 13$, $d^{-1} = 7$ gives that the number of points of $E_7$ is $N_{7[1]} = 20$, which is in contradiction to the results suggested by Bessalov and Thsigankova.

Moreover, if $p \equiv 7 \pmod{8}$, then the order of torsion subgroup of curve is $N_2 = N_{2^t[1]} = 31 - 3$, which is clearly different to $p + 1$.

For instance $p = 31$, then $N_{d[1]} = N_{2^t[1]} = 28 = 31 - 3$, which is clearly not equal to $p + 1$.

If $p = 7$, $d = 2^{-1} = 4 \pmod{7}$ then the curve $E_{2^{-1}}$ has four points, namely $\{0,1\} \cup \{(0,6), (1,0),(6,0)\}$, and the in case $p = 7$ with $d = 2 \pmod{7}$, the curve $E_{2^t}$ also has four points: $\{0,1\} \cup \{(0,6), (1,0),(6,0)\}$, demonstrating the order in this scenario is $p - 3$.

The following theorem shows that the total number of affine points upon the Edwards curves $E_d$ and $E_{d^*}$, are equal under certain assumptions. This theorem provides us additionally with a formula for enumerating the number of affine points upon the birationally isomorphic Montgomery curve $N_m$. 

**Theorem 2.4.**
**Theorem 2.3.** Let \( d \) satisfy the condition of supersingularity (1). If \( n = l(\text{mod } 2) \) and \( p \) is prime, then \( N_{d(p')} = p^n + 1 \) and the order of curve is equal to

\[
N_{d(p')} = p^n + 1 - 2\left(\frac{d}{p}\right).
\]

If \( n = 0(\text{mod } 2) \) and \( p \) is prime, then the order of curve

\[
N_{d(p')} = p^n - 2(-p)^{\frac{n}{2}},
\]

and the order of projective curve is equal to \( N_{d(p')} = p^n + 1 - 2(-p)^{\frac{n}{2}} \).

If \( n = 0(\text{mod } 2) \) and \( p \) is prime, then the order of projective curve is equal to \( N_{d(p')} = p^n + 2(-p)^{\frac{n}{2}} \), and The order of curve is equal to \( N_{d(p')} = p^n + 2(-p)^{\frac{n}{2}} \).

**Proof.** We consider the extension of the base field \( F_p \) to \( F_p' \) in order to determine the number of the points on the curve \( x^2 + y^2 = 1 + dx^2y^2 \). Let \( P(x) \) denotes a polynomial with degree \( m > 2 \) whose coefficients are from \( F_p \). To make the proof, we take into account that it is known that the number of solutions to \( y^2 = P(x) \) over \( F_p' \) will have the form \( p^n + 1 - \omega^e_1 - \cdots - \omega^e_{m-1} \) where \( \omega_1, \ldots, \omega_{m-1} \in \mathbb{F}_p \), \( |\omega| = \frac{1}{p^2} \).

In case of the supersingular curve, if \( n = l(\text{mod } 2) \) the number of points on projective curve over \( F_p' \) is determined by the expression \( p^n + 1 - \omega^e_1 - \omega^e_2 \), where \( \omega^e_1 \) and \( \omega^e_2 \) are the eigenvalues of Frobenius operator \( F_p' \) composition of the Frobenius operator. Consequently, because of \( P(x) = 1 \) four singular points appear on the curve. Thus, the number of affine points is less by \( 4 \), i.e.

\[
N_{d(p')} = p^n - 2\left(\frac{d}{p}\right) - 2(-p)^{\frac{n}{2}} = p^n - 3 - 2(-p)^{\frac{n}{2}}.
\]

**Lemma 2.2.** There exists birational isomorphism between \( E_d \) and \( E_{d'\mu} \), which is determined by correspondent mappings \( x = \frac{1+u}{1-u} \) and \( y = \frac{2u}{v} \).

**Proof.** To verify this statement in supersingular case we suppose that the curve \( x^2 + y^2 = 1 + dx^2y^2 \) contains \( p - 1 - 2\left(\frac{d}{p}\right) \) points \((x, y)\), with coordinates over prime field \( F_p \). Consider the transformation of the curve \( x^2 + y^2 = 1 + dx^2y^2 \), into the following form

\[
y^2(dx^2 - 1) = x^2 - 1.
\]

Make the substitution \( x = \frac{1+u}{1-u} \) and \( y = \frac{2u}{v} \). We will call the special points of this transformations the points in which these transformations or inverse transformations are not determined. As a result the equation of curve the equation of the curve takes the form

\[
y^2 = (d-1)u^2 + 2(d+1)u + (d-1)u^2 - (1-u)^2.
\]

Multiply the equation of the curve by \( \frac{y^2(1-u)^2}{4u} \). As a result of the reduction, we obtain the equation

\[
y^2 = (d-1)u^2 + 2(d+1)u + (d-1)u.
\]

We analyze what new solutions appeared in the resulting equation in comparing
\[ Q(t) = \frac{t^p - 1}{p - 1} = \frac{(t - 1)^p}{t - 1} = (t - 1)^{p-1} \mod p \] 
and therefore the equality \( P(t) = \left( \left( 1-t \right)^{p-1} \right)^{\frac{p-1}{2}} = \left( \left( 1-t \right)^{p-1} \right)^{\frac{p-1}{2}} \mod p \) holds over \( F_p \).

In order to simplify the notation, we let \( \theta = t - 1 \) and \( R(\theta) = P(t) \mod (t-1) \). For the case \( t = 2 \) we have \( \theta = 1 \). Performing this substitution leads the polynomial \( P(t) \) to the polynomial \( R(t) \) of \( t = 1 \). Taking into account the linear nature of the substitution \( \theta = t - 1 \), it can be seen that that derivation by \( \theta \) and \( t \) coincide. Derivation leads us to the transformation of polynomial \( R(\theta) \) to form where it has the necessary coefficient \( a_{p-1} \).

Then \( R(\theta) = P(\theta) + 1 = \frac{p-1}{2} \theta \left( \frac{(p-1)!}{2} \theta + 1 \right) \left( 0 + 1 + \frac{p-1}{2} \right) \).

In order to prove that \( a_{p-1} \neq 0 \mod p \), it is now sufficient to show that \( R(\theta) = 0 \) if \( \theta = 1 \) over \( F_p \). We obtain

\[ R(\theta) = (\frac{p-1}{2} \theta + 1) \theta + 1 \left( 0 + 1 + \frac{p-1}{2} \right) \]

We will manipulate now the expression

\[ \frac{p-1}{2} \theta + 1 \theta \left( 0 + 1 + \frac{p-1}{2} \right) \]

In order to illustrate the simplification we now consider the scenario when \( p = 11 \) and hence \( \frac{p-1}{2} = 5 \).

The expression gets the form

\[ (5 - j + 1)(5 - j + 2) \cdots (5 - j + 5) = (6 - j)(7 - j) \cdots (10 - j) = \]

\[ = \left( (-5 - j)(-4 - j) \cdots (-j - 1) \right) \]

\[ = (-1)^j \left( (j + 2)(j + 3) \cdots (j + 5) \right) \mod 11. \]

Therefore, for a prime \( p \), we can rewrite the expression as

\[ \frac{p-1}{2} \theta + 1 \theta \left( 0 + 1 + \frac{p-1}{2} \right) \]

\[ = (j + 1)(j + 2) \cdots (j + 5) \mod (p). \]

As a result, the symmetrical terms in \( \theta \) can be reduced yielding \( a_{p-1} = 0 \mod p \). It should be noted that

\[ (-1)^j \left( (j + 2)(j + 3) \cdots (j + 5) \right) = -1 \]

Consequently, we have \( P(2) = R(1) = 0 \) and hence \( a_{p-1} = 0 \mod p \).

Thus, \( \sum_{j=0}^{p-1} (C_j^{p-1})^2 \equiv 0 \mod p \), completing the proof of the theorem.

**Corollary 2.2.** The curve \( E_d \) is supersingular iff \( E_{d'} \) is supersingular.

Proof. Let us recall the proved fact in Theorem 2.1 that

\[ N_{d[p]} = -a_{d-2} - a_{d-1} = -\left( \frac{d}{p} \right) + \sum_{j=0}^{p-1} (C_j^{p-1})^2 d' \mod p. \]

Since \( (C_j^{p-1})^2 d' \equiv 0 \mod p \) by condition, and the congruence \( \frac{d}{p} = d' \) holds, then \( N_{d[p]} = N_{d'[p]} \).

**Corollary 2.3.** If \( p \equiv 3 \mod 4 \), is prime then there exists some \( T \) such that \( T < 2 \sqrt{p} \) and \( N_{d[p]} = p - 1 - 2 \left( \frac{d}{p} \right) + T \).

Proof. Due to equality (5) and the bounds (8) as well as according to generalized Hasse-Weil theorem

\[ |N_{d[p]}| = (p+1) - 2 \left( \frac{d}{p} \right) \leq 2g \sqrt{p} \], where \( g \) is genus of the curve, we obtain exact number \( N_{d[p]} \) as we showed, \( g = 1 \).

From Theorem 2.1 as well as from Corollary 2.2 we get,

\[ \sum_{j=0}^{p-1} (C_j^{p-1})^2 d' = -N_{d[p]} - p - 1 - 2 \left( \frac{d}{p} \right) \]

there exists \( T \in \mathbb{N} \), such that \( T < 2 \sqrt{p} \) and \( N_{d[p]} = p - 1 - 2 \left( \frac{d}{p} \right) + T \).

**Example 2.1.** If \( p = 13 \), \( d = 2 \) gives \( N_{[13]} = 8 \) and \( p = 13 \), \( d = 7 \) gives that the number of points of \( E_7 \) is \( N_{[13]} = 20 \), which is in contradiction to that suggested by Bessalov and Thsigankova.

Moreover, if \( p = 7 \mod 8 \), then the order of torsion subgroup of curve is \( N_2 = N_2', = p - 3 \), which is clearly different to \( p + 1 \)

For instance \( p = 31 \), then \( N_{[31]} = N_{[31]}' = 28 = 31 - 3 \), which is clearly not equal to \( p + 1 \). If \( p = 7 \), \( d = 2 \mod 4 \) then the curve \( E_{d'} \) has four points, namely \( (0, 1); (0, 6); (1, 0); (6, 0) \), and the in case \( p = 7 \) with \( d = 2 \mod 7 \), the curve \( E_{d'} \) also has four points: \( (0, 1); (0, 6); (1, 0); (6, 0) \), demonstrating the order in this scenario is \( p - 3 \).

The following theorem shows that the total number of affine points upon the Edwards curves \( E_d \) and \( E_{d'} \) are equal under certain assumptions. This theorem provides us additionally with a formula for enumerating the number of affine points upon the birationally isomorphic Montgomery curve \( N_{M} \).
algebraic extension of degree \( n \), we will consider 
\[ p^s - \alpha_1^n - \alpha_2^n = p^s \] if \( n = 1 \mod 2 \). Therefore, for 
\( n = 1 \mod 2 \), the order of the Montgomery curve is precisely given by 
\[ N_{M[p]} = p^s + 1 \]. Here’s one infinitely remote point as a neutral element of the group of points of
the curve.

Considering now an elliptic curve, we have 
\( \omega_i = \delta_i \) by [5], which leads to \( \omega_1 + \omega_2 = 0 \). For \( n = 1 \), it is

The singular points were discovered in [10] and hence if the
the curve is free of singular points then the group order is \( p + 1 \).

**Example 2.3.** If \( p = 3 \mod 8 \) and \( n = 2k \) then we have
when \( d = 2 \), \( n = 2 \), \( p = 3 \) that the number of affine points
equals to 
\[ N_{2[3]} = p^s - 3 - 2(-p)^{\frac{n}{2}} = 3^2 - 3 - 2(-3) = 12 \],
and the number of projective points is equal to 
\[ N_{2[3]} = p^s + 1 - 2(-p)^{\frac{n}{2}} = 3^2 + 1 - 2(-3) = 16 \].

**Example 2.4.** If \( p = 7 \mod 8 \) and \( n = 2k \) then we have
when \( d = 2 \), \( n = 2 \), \( p = 7 \) that the number of affine points
equals to 
\[ N_{2[7]} = p^s - 3 - 2(-p)^{\frac{n}{2}} = 7^2 - 3 - 2(-7) = 60 \],
and the number of projective points is equal to 
\[ N_{2[7]} = p^s + 1 - 2(-p)^{\frac{n}{2}} = 7^2 + 1 - 2(-7) = 64 \].

The group of points of the supersingular curve \( E_d \) contains
\( p - 1 - 2 \left( \frac{d}{p} \right) \) affine points and the affine singular points
whose number is 
\[ 2 \left( \frac{d}{p} \right) + 2 \].

The singular points were discovered in [10] and hence if the
curve is free of singular points then the group order is \( p + 1 \).

**Theorem 2.24.** The order of Edwards curve over \( F_p \) is congruent to
\[ N_{d[p]} = (p - 1 - 2 \left( \frac{d}{p} \right) + (-1)^{\frac{p-1}{2}} \sum_{j=0}^{p-1} (C_{j,x}^1)^2 d^j) = \]
\[ = (-1)^{\frac{p-1}{2}} \sum_{j=0}^{p-1} (C_{j,x}^1)^2 d^j - 1 - 2 \left( \frac{d}{p} \right) (\mod p). \]

The true value of \( N_{d[p]} \) lies in \([4; 2p]\) and is even.

**Proof.** This result follows from the number of solutions of the equation 
\( y^2 = (x^2 - 1)(dx^2 - 1) \) over \( F_p \) which equals to
\[ \sum_{x=0}^{p-1} \left( \frac{(x^2 - 1)(dx^2 - 1) + 1}{p} \right) = \sum_{x=0}^{p-1} \left( \frac{(x^2 - 1)(dx^2 - 1)}{p} \right) + p = \]
\[ = \left( \sum_{x=0}^{p-1} \left( \frac{p-1}{2} \right)^3 (dx^2 - 1)^2 d^j - \left( \frac{d}{p} \right) (\mod p) \right) = \]
\[ = (-1)^{\frac{p-1}{2}} \sum_{j=0}^{p-1} (C_{j,x}^1)^2 d^j - \left( \frac{d}{p} \right) (\mod p). \]

The quantity of solutions for \( x^2 + y^2 = 1 + dx^2 y^2 \) differs from the quantity of \( y^2 = (dx^2 - 1)(x^2 - 1) \) by
\( \left( \frac{d}{p} \right) + 1 \) due to new solutions in the form \((\sqrt{d}, 0), (-\sqrt{d}, 0)\).
So this quantity is such
\[ \sum_{x=0}^{p-1} \left( \frac{(x^2 - 1)(dx^2 - 1)}{p} \right) + \left( \frac{d}{p} \right) = \]
\[ = \left( \sum_{x=0}^{p-1} \left( \frac{p-1}{2} \right)^3 (dx^2 - 1)^2 d^j - (\frac{d}{p} + 1) (\mod p) \right) = \]
\[ = (-1)^{\frac{p-1}{2}} \sum_{j=0}^{p-1} (C_{j,x}^1)^2 d^j - (2 \left( \frac{d}{p} \right) + 1) (\mod p). \]

According to Lemma 1 the last sum
\[ \left( \sum_{x=0}^{p-1} \left( \frac{p-1}{2} \right)^3 (dx^2 - 1)^2 d^j \right) (\mod p) \]

is congruent to \( -a_{p-1} - a_{2p-1} (\mod p) \), where \( a_i \) are the coefficients from
presentation
\( (x^2 - 1)^{\frac{p-1}{2}} (dx^2 - 1)^{\frac{p-1}{2}} = a_0 + a_1 x + ... + a_{2p-2} x^{2p-2}. \)
The exact order is not less than 4 because cofactor of this curve is 4. To determine the order is uniquely enough to take into account that $p$ and $2p$ have different parity. Taking into account that the order is even we chose a term $p$ or $2p$, for the sum which define the order.

**Theorem 2.5.3** If $\left(\frac{d}{p}\right) = 1$, then the orders of the curves $E_d$ and $E_{d^{-1}}$, satisfies to the following relation

$$|E_d| = |E_{d^{-1}}|.$$
That $\frac{y^2}{d} = \frac{d^{-1} \left(\frac{1}{x_0} \right)^2 - 1}{\left(\frac{1}{x_0} \right)^2 - 1}$ is a root of $\pm \sqrt{d} + \sqrt{d} - 1$. Therefore last transformations $(x_0, y_0) \mapsto \left(\frac{1}{x_0}, \frac{y_0}{\sqrt{d}}\right) = (x, y)$ determines isomorphism and bijection.

In case $\left(\frac{d}{p}\right) = -1$, then every $x \in F_p$ is such that $dx^2 - 1 \neq 0$ and $d^{-1}x^2 - 1 \neq 0$. If $x_0 \neq 0$, then $x_0$ generate 2 solutions of (2) iff $x_0^{-1}$ gives 0 solutions of (10) because of (11) yields the following relation

$$\frac{x^2 - 1}{d^{-1}x^2 - 1} = \frac{x^2 - 1}{p} = \frac{d^{-1}x^2 - 1}{p} = \frac{x^2 - 1}{p}, \quad (12)$$

Analogous reasons give us that $x_0$ gives exactly one solution of (2) iff $x_0^{-1}$ gives 1 solutions of (10). Consider the set $x \in \{1, 2, \ldots, p - 1\}$ we obtain that the total amount of solutions of form $(x_0, y_0)$ that represent point of (2) and pairs of form $(x_0, y_0)$ that represent point of curve (10) is $2p - 2$. Also we have two solutions of (2) of form $(0, 1)$ and $(0, -1)$ and two solutions of (10) that has form $(0, 1)$ and $(0, -1)$. The proof is fully completed.

**Example 2.6.** The number of points of $E_d$ over $F_p$ for $p = 13$ and $d = 2$ is given by $N_{2(13)} = 8$. In the case when $p = 13$ and $d^{-1} = 7$ we have that the number of points of $E_d$ is $N_{2(13)} = 20$. Therefore, we have that the sum of orders for these curve is equal to $28 = 2 \cdot 13 + 2$ which confirms our theorem. The set of points over $F_{13}$ when $d = 2$ are precisely $\{(0,1);(0,12);(1,0);(4,4);(4,9);(9,4);(9,9);(12,0)\}$. 

While for $d = 7$, we have the set $\{(0,1);(0,12);(1,0);(2,4);(2,9);(4,2);(4,11);(5,6);(5,7);(6,5);(6,8);(7,5);(7,8);(8,6);(8,7);(9,2);(9,11);(11,4);(11,9);(12,0)\}$.

**Example 2.7.** If $p = 7$ and $d = 2^{-1} = 4 (mod 7)$, then we have $\left(\frac{d}{p}\right) = 1$ and the curve $E_{2^{-1}}$ has four points which are $(0,1);(0,6);(1,0);(6,0)$. and the in case $p = 7$ for $d = 2 (mod 7)$, the curve $E_{2^{-1}}$ also has four points which are $(0,1);(0,6);(1,0);(6,0)$.

**Definition 2.1.** We call the embedding degree a minimal power $k$ of a finite field extension such that the group of points of the curve can be embedded in the multiplicative group of $F_{p^k}$.

Let us obtain conditions of embedding [14] for the group of supersingular curves $E_d[F_p^k]$ of order $p$ in the multiplicative group of field $F_{p^k}$ whose embedding degree is $k = 12$ [14]. We now utilise the Zsigmondy theorem which implies that a suitable characteristic of field $F_p$ is an arbitrary prime $p$ which do not divide 12 and satisfies the condition $q \mid P_2(p)$, where $P_2(x)$ is the cyclotomic polynomial. This $p$ will satisfy the necessary conditions $(x^2 - 1) \not\equiv p$ for an arbitrary $n = 1, \ldots, 11$.

**Proposition 2.2.7** The degree of embedding for the group of a supersingular curve $E_d$ is equal to 2.

**Proof.** The order of the group of a supersingular curve $E_d$ is equal to $p^4 + 1$. It should be observed that $p^4 + 1$ divides $p^{12} - 1$, but $p^4 + 1$ does not divide expressions of the form $p^{12} - 1$ with $l \leq k$. This division does not work for smaller values of $l$ due to the decomposition of the expression $p^{12} - 1 = (p^4 - 1)(p^4 + 1)$. Therefore, we can use the definition to conclude that the degree of immersion must be 2, confirming the proposition.

Consider $E_2$ over $F_{p^k}$, for instance we assume $p = 3$. We define $F_9$ as $F_3(\sqrt{-1})$, where $\alpha$ is a root of $x^2 + 1 = 0$ over $F_3$. Therefore elements of $F_9$ have form: $a + b\alpha$, where $a, b \in F_3$. So we assume that $x \in \{\pm(\alpha + 1), \pm(\alpha - 1), \pm\alpha\}$ and check its belonging to $E_2$. For instance if $x = \pm(\alpha + 1)$ then $x^2 = \alpha^2 + 2\alpha + 1 = \alpha^2 - \alpha$. Also in this case $y^2 = \frac{\alpha^2 - 1}{\alpha - 1} = \frac{\alpha - 1}{\alpha - 1} = 1$. Therefore the correspondent second coordinate is $y = \pm(\alpha - 1)$. The similar computations lead us to full the following list of curves points.

Points of Edwards curve over square extension. The total amount is 12 affine points that confirms Corollary 2.4. and Theorem 2.3. because of $p^4 - 3 - 2(-p) = 3^2 - 2(3) = 12$.

**3. Conclusion**

A new method for the order curve counting for Edwards and elliptic curves has been presented. The criterion for supersingularity of these curves was also obtained.

**Acknowledgement:** We thanks to Alexandr Rybak for interesting discussion.

**References**
