Edwards curve points counting method and supersingular Edwards and Montgomery curves
(Cryptosystems, Cryptology and Theoretical Computer Science)

RUSLAN SKURATOVSIIK, 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 \(E_p(F_p)\) 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.

Received: January 5, 2020. Revised: April 12, 2020. Re-revised: April 21, 2020. Accepted: April 28, 2020.
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 counting 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 \(E_p(F_p)\) is supersingular over this field or not.

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 \(E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2\), \(a, d \in F_p, ad(a-d) \neq 0\).

It should be noted that a twisted Edwards curve is called an Edwards curve when \(a = 1\).

We denote by \(E_p\) the Edwards curve with coefficient \(d \in F_p\) which is defined as \(x^2 + y^2 = 1 + dx^2y^2\) over \(F_p\). The projective curve has the form \(F(x,y,z) = ax^2z^2 + y^2z^2 + z^4 + dx^2y^2 = 0\). 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

\[A^1: ax^2z^2 + z^4 = 0\]

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 \(\delta_p = \dim O_p / O_p\), where \(O_p\) denotes the local ring at the singular point \(p\) which is generated by the relations of regular functions

\[O_p = \left\{ \frac{f}{g} : (g, (x-1)(y-1)) = 1 \right\}\]

and \(O_p\) denotes the whole closure of the local ring at the singular point \(p\).
We find that $\delta_y = \dim( \mathcal{O}/\mathcal{O}_y ) = 1$ is the dimension of the factor as a vector space. Because the basis of extension $\mathcal{O}/\mathcal{O}_y$ 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],

$$\rho'(C) = \rho_y(C) - \sum_{p \in \mathbb{P}} \delta_y = \frac{(n-1)(n-2)}{2},$$

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 $E_M$. Koblitz [4,5] proves that one can detect if a curve is supersingular points were discovered in [10]. We denote the number of points with a neutral element of an affine Edwards curve over the finite field $F_p$ 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 $p = 3(\mod\ 4)$ is prime and the following condition of supersingularity

$$\sum_{j=0}^{p-1} \left( C_{p-1}^{\frac{p-1}{2}} \right)^3 \frac{d}{j} \equiv 0(\mod\ p),$$

is true then 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

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

**Proof.** Consider the curve $E_j$:

$$x^2 + y^2 = 1 + dx^2 y^2.$$  \hspace{1cm} (2)

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

For our analysis we transform it into the curve

$$y^2 = (x^2 - 1)(dx^2 - 1).$$  \hspace{1cm} (3)

We denote the number of points from an affine Edwards curve over the finite field $F_p$ by $M_{d(p)}$. This curve (3) has $M_{d(p)} = N_{d(p)} + \left( \frac{d}{p} \right) + 1$ points, which is precisely $\left( \frac{d}{p} \right) + 1$ greater than the number of points of curve $E_j$. Note 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 $a_0 + a_1 x + \ldots + a_{p-2} x^{p-2}$, which was obtained from $(x^2 - 1)^{\frac{p-1}{2}} (dx^2 - 1)^{\frac{p-1}{2}}$ after opening the brackets. Thus, summing over all $x$ yields

$$M_{d(p)} = \sum_{x=0}^{p-1} ((x^2 - 1)(dx^2 - 1))^{\frac{p-1}{2}} = p + \sum_{x=0}^{p-1} (x^2 - 1)^{\frac{p-1}{2}}.$$  \hspace{1cm} (4)

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

$$a_{p-2} = (-1)^{\frac{p-1}{2}} \cdot d^{\frac{p-1}{2}} \left( \frac{d}{p} \right) (\mod\ p).$$

So, using Lemma 2.1 we have

$$M_{d(p)} = - \left( \frac{d}{p} \right) \cdot a_{p-1} (\mod\ p).$$  \hspace{1cm} (4)

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

$$M_{d(p)} = - \left( \frac{d}{p} \right) \cdot a_{p-1} (\mod\ p) \quad \text{for} \quad p = 3(\mod\ 4) \quad \text{if} \quad \sum_{j=0}^{p-1} \left( C_{p-1}^{\frac{p-1}{2}} \right)^3 \frac{d}{j} \equiv 0(\mod\ p).$$

We can prove that $a_{p-1} \equiv 0(\mod\ p)$, 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 $(x^2 - 1)^{\frac{p-1}{2}} (dx^2 - 1)^{\frac{p-1}{2}}$. So,
\[ a_{p-1} = (-1)^{\frac{p+1}{2}} \sum_{j=0}^{\frac{p-1}{2}} d^j (C_{\frac{p}{2}})^2. \]

Actually, the following equality holds:

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

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

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

(5)

According to the condition of this theorem, \( a_{p-1} = 0 \), therefore \( M_{d(p)} = -a_{p-1}(p \pmod p) \). Consequently, in the case when \( p \equiv 3 \pmod 4 \), where \( p \) is prime and \( \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p}{2}})^2 d^j = 0 \pmod p \), the curve \( E_d \) has \( p+1 \) 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 \( 2p+1 \) for every \( x \neq 0 \) corresponds to two valuations of \( y \), but for \( x = 0 \) we have only one solution \( y = 0 \).

Taking into account that \( x \in \mathbb{F}_p \), 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 \( N_{d(p)} > 1 \). 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 \( \mathbb{F}_p \) are equal to \( N_{d(p)} = p + 1 \) when \( \frac{d}{p} = -1 \), and \( N_{d(p)} = p - 3 = \overline{N}_{d(p)} + 4 \), when \( \frac{d}{p} = 1 \) if

\[ p \equiv 3 \pmod 4 \] is prime and \( \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p}{2}})^2 d^j = 0 \pmod p \).

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

**Theorem 2.2.** If the coefficient \( d = 2 \) or \( d = 2^{-1} \) and \( p \equiv 3 \pmod 4 \) then \( \sum_{j=0}^{\frac{p-1}{2}} d^j (C_{\frac{p}{2}})^2 = 0 \pmod p \) and \( \overline{N}_{d(p)} = p + 1 \).

Proof: When \( p \equiv 3 \pmod 4 \), we shall show that

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

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

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

After that, by applying the congruence \( \left( \frac{p-1}{2} - k \right)^2 \equiv \left( \frac{p-1}{2} - k + j \right)^2 \pmod p \) with \( 0 \leq k \leq \frac{p-1}{2} \) to the multipliers in previous parentheses, we obtain \( \left( \frac{p-1}{2} \right) \left( \frac{p-1}{2} - 1 \right) \cdots (j + 1) \). It yields

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

Thus, as a result of squaring, we have:

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

(6)

It remains to prove that \( \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p}{2}})^2 d^j = 0 \pmod p \) if

\[ p \equiv 3 \pmod 4 \]

Consider the auxiliary polynomial

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

We are going to show that \( P(2) = 0 \) and therefore \( a_{p-1} = 0 \pmod p \). Using (6) it can be shown that

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

\[ (k + 2)^2 \cdots \left( \frac{p-1}{2} - k \right)^2 t^j \pmod p \]

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

\[ P(t) = \frac{\partial^{\frac{p-1}{2}}}{\partial t^{\frac{p-1}{2}}} \left( Q(t) \left( \frac{p-1}{2} \right) \right) \]

over \( F_p \), where \( Q(t) = t^{-1} + \cdots + t + 1 \) and \( \frac{\partial^{\frac{p-1}{2}}}{\partial t^{\frac{p-1}{2}}} \) denotes the \( \frac{p-1}{2} \)-th derivative by \( t \), where \( t \) is new variable but not a coordinate of curve. Observe that

\[ EISSN: 2224-3402 81 Volume 17, 2020 \]
In order to simplify the notation, we let $\theta = t-1$ and $R(0) = P(0+1)$. For the case $t = 2$ we have $\theta = 0$. Performing this substitution leads the polynomial $P(t)$ of 2 to the polynomial $R(\theta)$ 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

$$R(\theta) = P(\theta+1) = \frac{n-1}{2} \left( (p-1)(0 + (0 + \frac{n-1}{2}) (0 + \frac{n-1}{2}) \right) =$$

$$= \frac{\frac{n-1}{2}}{2} \left( \frac{p-1}{2} \right) (0 + (0 + \frac{n-1}{2}) (0 + \frac{n-1}{2}) \right).$$

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 $F_p$. We obtain

$$R(\theta) = \frac{n-1}{2} \left( \left( \frac{p-1}{2} \right) (0 + (0 + \frac{n-1}{2}) (0 + \frac{n-1}{2}) \right).$$

We will manipulate now the expression

$$(p-1)(2-2j)(p-1)(2-2j-2j-2j-2j-2j) 

\text{In order to illustrate the simplification we now consider the scenario when } p \text{ = 11 and hence } \frac{p-1}{2} = 5.$$
Theorem 2.3. Let $d$ satisfy the condition of supersingularity (1). If $n = 1(\text{mod} \ 2)$ and $p$ is prime, then
\[ N_{d[p]} = p^* + 1 \] and the order of curve is equal to
\[ N_{d[p]} = p^* - 1 - 2 \left( \frac{d}{p} \right). \]
If $n = 0(\text{mod} \ 2)$ and $p$ is prime, then the order of curve
\[ N_{d[p]} = p^* - 3 - 2(-p)\frac{n}{2}, \] and the order of projective curve is equal to $N_{d[p]} = p^* + 1 - 2(-p)^{\frac{n}{2}}$.
If $n = 0(\text{mod} \ 2)$ and $p$ is prime, then the order of projective curve is equal to $N_{d[p]} = p^* + 1 - 2(-p)^{\frac{n}{2}}$.

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

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 $p^* + 1 - \alpha_1^* - \cdots - \alpha_{m-1}^*$ where $\alpha_1, \ldots, \alpha_{m-1} \in \mathbb{F}_p$, $|\alpha_i| = p^\frac{1}{2}$.

In case of our supersingular curve, if $n = 1(\text{mod} \ 2)$ the number of points on projective curve over $F_p^*$ is determined by the expression $p^* - 1 - \alpha_1^* - \cdots - \alpha_{m-1}^*$, where $\alpha_i \in \mathbb{F}_p$ and $|\alpha_i| = \sqrt{p}$ that's why $\alpha_i = \pm \sqrt{p}$ or $\alpha_i = -i\sqrt{p}$ with $i \in \{1, 2\}$. In the general case, it is known that $|\alpha_i| = \frac{1}{2}$. The order of the projective curve is therefore $p^* + 1$.

If $p = 7(\text{mod} \ 8)$, then it is known from a result of Skuratovskii [10] that $E_d$ has in its projective closure of the curve singular points which are not affine and therefore
\[ N_{d[p]} = p^* - 3. \]
If $p = 3(\text{mod} \ 8)$, then there are no singular points, hence
\[ N_{d[p]} = N_{d[p]} = p^* + 1. \]

Consequently the number of points on the Edwards curve depends on $\left( \frac{d}{p} \right)$ and is equal to $N_{d[p]} = p^* - 3$ if $p = 7(\text{mod} \ 8)$ and $N_{d[p]} = p^* + 1$ if $p = 3(\text{mod} \ 8)$ where $n = 1(\text{mod} \ 2)$. We note that this is because the transformation of (3) in $E_d$ depends upon the denominator $(dx^2 - 1)$.

If $n = 1(\text{mod} \ 2)$ then, with respect to the sum of the root of the characteristic equation for the Frobenius endomorphism $\alpha_1^* + \alpha_2^*$, which in this case have the same signs, we obtain that the number of points in the group of points of the curve is $p^* + 1 - \alpha_1^* - \alpha_2^*$ [19]. In more details $\alpha_1, \alpha_2$ are eigenvalues of Frobenius operator $F$ endomorphism on etale cohomology over the finite field $F_p^*$, where $F$ acts of $H'(X)$. The number of points, in general case, are determined by Lifshitz formula:
\[ \#X(F_p^*) = \sum (-1)^{\text{tr}(F^\infty|H'(X))} \]
where $\#X(F_p^*)$ is a number of points in the manifold $X$ over $F$, $F^\infty$ is composition of the Frobenius operator. In our case, $E_d$ is considered as the manifold $X$ over $F_p^*$.

For $n = 0(\text{mod} \ 2)$ we always have, that every $d \in F_p^*$ is a quadratic residue in $F_p^*$. Consequently, because of $(\frac{2}{p}) = 1$

four singular points appear on the curve. Thus, the number of affine points is less by 4, i.e.
\[ N_{d[p]} = p^* - 1 - 2 \left( \frac{d}{p} \right) - 2(-p)^{\frac{n}{2}} = p^* - 3 - 2(-p)^{\frac{n}{2}}. \]

Lemma 2.2. There exists birational isomorphism between $E_d$ and $E_m$, which is determined by correspondent mappings $x = 1 + u$ 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
\[ y^2(dx^2 - 1) = x^2 - 1. \]

Make the substitutions $x = \frac{1 + u}{1 - u}$ 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
\[ 4u^2 \left( (d - 1)u^2 + 2(d + 1)u + (d - 1) \right) = 4u \left( 1 - u \right)^2. \]

Multiply the equation of the curve by $\frac{v^2(1 - u)}{4u}$. As a result of the reduction, we obtain the equation
\[ v^2 = (d - 1)u^2 + 2(d + 1)u^2 + (d - 1)u. \]
We analyze what new solutions appeared in the resulting equation in comparison
In order to prove that $10 \equiv \mod{p}$, the theorem.

We will manipulate now the expression

$$\frac{(p-1)!}{(p-1)2!} \cdot \left( \frac{p-1}{2} \right) \cdot \left( \frac{p-1}{2} \right) \cdot \left( \frac{p-1}{2} \right) \cdot \left( \frac{p-1}{2} \right).$$

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

$$R(1) = \frac{(p-1)!}{(p-1)2!} \cdot \sum_{j=0}^{p-1} \frac{p-1}{2} \cdot \left( \frac{p-1}{2} \right) \cdot \left( \frac{p-1}{2} \right) \cdot \left( \frac{p-1}{2} \right).$$

We will manipulate now the expression

$$\frac{(p-1)!}{(p-1)2!} \cdot \left( \frac{p-1}{2} \right) \cdot \left( \frac{p-1}{2} \right) \cdot \left( \frac{p-1}{2} \right) \cdot \left( \frac{p-1}{2} \right).$$

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

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

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

$$\frac{(p-1)!}{(p-1)2!} \cdot \sum_{j=0}^{p-1} \frac{p-1}{2} \cdot \left( \frac{p-1}{2} \right) \cdot \left( \frac{p-1}{2} \right) \cdot \left( \frac{p-1}{2} \right).$$

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

$$(-1)^5 = -1 \text{ since } p = M + 3 \text{ and } \frac{p-1}{2} = 2k + 1.$$ 

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

$$\sum_{j=0}^{p-1} \frac{p-1}{2} \cdot \left( \frac{p-1}{2} \right) \cdot \left( \frac{p-1}{2} \right) \cdot \left( \frac{p-1}{2} \right) = 0(\mod{p}),$$

completing the proof of the theorem.

**Corollary 2.2.** The curve $E_d$ is supersingular iff $E_{d^1}$ is supersingular.
algebraic extension of degree \( n \), we will consider 
\[ p^r - \omega_y \omega_x^2 = p^s \] if \( n = 1 \mod (2) \). Therefore, for \( n = 1 \mod (2) \), the order of the Montgomery curve is precisely given by \( N_{M[p^r]} = p^s + 1 \). 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 
\[ \omega_x = \bar{\omega}_x \] by [5], which leads to \( \omega_x + \omega_y = 0 \). For \( n = 1 \), it is clear that \( N_{M[p]} = p \). When \( n \) is odd, we have \( \omega_x + \omega_y = 0 \) and therefore \( N_{M[p^r]} = p^s + 1 \). Because \( n \) is even by initial assumption, we shall show that \( N_{M[p^r]} = p^s + 2(p-2)^2 \) holds as required.

Note that for \( n = 2 \) we can express the number as 
\[ \overline{N}_{M[p^r]} = p^2 + 1 + 2p = (p + 1)^2 \] with respect to Lagrange theorem have to be divisible on \( \overline{N}_{M[p]} \). Because a group of \( E_d(F_p) \) over square extension of \( F_p \) contains the group \( E_d(F_p) \) as a proper subgroup. In fact, according to Theorem 1 the order \( E_d(F_p) \) is \( p + 1 \) therefore divisibility of order \( E_d(F_p) \) holds because in our case \( p = 7 \) thus \( N_{E_d} = 8^2 \) and \( p + 1 = 8 = N_{M[p]} \) [16].

The following two examples exemplify Corollary 2.4.

**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 \( N_{[2]} = p^x - 3 - 2(-p)^{\frac{2}{3}} - 3 - 2 \cdot (-3) = 12 \), and the number of projective points is equal to 
\[ \overline{N}_{[2]} = p^x + 2(-p)^{\frac{2}{3}} = 3^2 + 2 \cdot (-3) = 16. \]

**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 \( N_{[2]} = p^x - 3 - 2(-p)^{\frac{2}{3}} = 7^2 - 3 - 2 \cdot (-7) = 60 \), and the number of projective points is equal to 
\[ \overline{N}_{[2]} = p^x + 2(-p)^{\frac{2}{3}} = 7^2 + 2 \cdot (-7) = 64. \]

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 \( p + 1 \).

**Example 2.5.1** The number of curve points over finite field when \( d = 2 \) and \( p = 31 \) is equal to 
\[ N_{[2]} = N_{[2]} = p - 3 = 28. \]

**Theorem 2.4.** The order of Edwards curve over \( F_p \) is congruent to 
\[ N_{d[p]} = (p - 1 - 2 \left( \frac{d}{p} \right) + (-1)^{\frac{p-1}{2}} \sum_{j=0}^{p-1} C_{\frac{d}{j}}^2 d^j) \]
\[ = ((-1)^{\frac{p-1}{2}} \sum_{j=0}^{p-1} C_{\frac{d}{j}}^2 d^j - (\frac{d}{p}) (mod p)). \]

The true value of \( \overline{N}_{d[p]} \) 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 
\[ \sum_{x=0}^{p-1} (x^2 - 1)(dx^2 - 1) + 1 = \sum_{x=0}^{p-1} (x^2 - 1)(dx^2 - 1)) + p = \]
\[ = (\sum_{x=0}^{p-1} (x^2 - 1)(dx^2 - 1)) (mod p) = \]
\[ = (\sum_{x=0}^{p-1} (x^2 - 1)(dx^2 - 1)) (mod p). \]

The quantity of solutions for \( x^2 + y^2 = 1 \) differs from the quantity of \( y^2 = (dx^2 - 1)(x^2 - 1) \) by \((\frac{d}{p}) + 1 \) due to new solutions in the from \((\sqrt{d}, 0), (-\sqrt{d}, 0)) \).

So this quantity is such
\[ \sum_{x=0}^{p-1} (x^2 - 1)(dx^2 - 1) + 1 = \left( \frac{d}{p} \right) + 1 \]
\[ \sum_{x=0}^{p-1} (x^2 - 1)(dx^2 - 1)) + p = \left( \frac{d}{p} \right) - 1 = \]
\[ = (\sum_{x=0}^{p-1} (x^2 - 1)(dx^2 - 1)) (mod p) = \]
\[ = (\sum_{x=0}^{p-1} (x^2 - 1)(dx^2 - 1)) (mod p). \]

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

is congruent to 
\[ -a_{p+1} - a_{p-1} (mod p), \] where \( a_i \) are the coefficients from presentation
\[ (x^2 - 1)(dx^2 - 1) = a_0 + a_1 x + \ldots + a_{2p-2} x^{2p-2}. \]
Due to the product of two brackets and when substituting it to new solutions of $(1) = (1) = (1)$.

According to Newton's binomial formula $(d/dx) = (d/dx) = (d/dx)$.

In form of a sum it is the following:

$$\sum_{j=0}^{p-1} 2^{2j} d^{2j} C^j_{1/2}$$

That is, it has the form of the polynomial with inverse order of coefficients.

Indeed, we have equality:

$$\sum_{j=0}^{p-1} 2^{2j} d^{2j} C^j_{1/2} = (-1)^{p-1} \sum_{j=0}^{p-1} d^{2j} C^j_{1/2}.$$

For $x^2 + y^2 = 1 + dx^2 y^2 (modp)$, we can express $y^2$ in such way:

$$y^2 = x^2 - 1 (mod p)$$

For $x^2 + y^2 = 1 + dx^2 y^2 (modp)$ we could obtain

$$y^2 = x^2 - 1 (mod p)$$

If $(d/p) = 1$, then for the fixed $x_0$ a quantity of $x$ over $F_p$ can be calculated by the formula $(d/p) = (d/p)$.

For $x^2 + y^2 = 1 + dx^2 y^2 (modp)$ and we express

$$y^2 = x^2 - 1 (mod p)$$

Observe that

$$y^2 = x^2 - 1 (mod p)$$

Thus, if $(x_0, y_0)$ is solution of $(2)$, then

$$\left(\frac{1}{x_0}, \frac{y_0}{d}\right)$$

is a solution to $(10)$ because last transformations determine...
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 $q|P_2(p)$, where $P_2(x)$ is the cyclotomic polynomial. This $p$ will satisfy the necessary conditions $(x^m-1)\mid p$ for an arbitrary $m=1, \ldots, 11$.

**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 $p^3 + 1$. It should be observed that $p^3 + 1$ divides $p^{2l} - 1$, but $p^3 + 1$ does not divide expressions of the form $p^{2l} - 1$ with $l < k$. This division does not work for smaller values of $l$ due to the decomposition of the expression $p^{2l} - 1 = (p^3 - 1)(p^3 + 1)$. 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 $F_p$ as $F_p(x)$, where $x$ is a root of the equation $x^2 + 1 = 0$ over $E_p$. Therefore elements of $F_p$ have form: $a + bx$, where $a, b \in F_p$. So we assume that $x \in \{p, \pm (\alpha + 1), \pm (\alpha - 1), \pm \alpha\}$ and check its belonging to $E_2$.

For instance if $x = \pm (\alpha + 1)$ then $x^2 = 2\alpha^2 + 2\alpha + 1 = 2\alpha - 2\alpha = 2\alpha$. Also in this case $y^2 = \frac{2\alpha - 1}{(\alpha - 1)(\alpha + 1)} = \frac{(2\alpha - 1)(\alpha + 1)}{(\alpha - 1)(\alpha + 1)} = \frac{\alpha}{\alpha - 2} = \frac{\alpha}{\alpha - 2}$.

Therefore the correspondent second coordinate is $y = \pm (\alpha - 1)$. The similar computations lead us to fulfill 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 $p^2 - 3 - 2(-p)^{\frac{2}{2}} = 3^2 - 3 - 2(-3) = 12$.

**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**

[1] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted edwards curves. In Serge Vaudenay, editor, Progress in Cryptology --
A.V Bessalov and O.V. Thsigankova. Vzaimosvyaz' semeystva tochek bol'shikh poryadkov krivy krivoy edwardsa nad prostym polem (in russian). Information Security, 17(1):73--80, 2015.

[3] Harold Edwards. A normal form for elliptic curves. Bulletin of the American mathematical society, 44(3):393--422, 2007.

[4] William Fulton. Algebraic curves. An Introduction to Algebraic Geometry. Addison-Wesley, 3 edition, 2008.

[5] Neal Koblitz. Elliptic curve cryptosystems. Mathematics of computation, 48(177):243--264, 1987.

[6] René Schoof. Counting points on elliptic curves over finite fields. Journal de théorie des nombres de Bordeaux, 7(1):219--254, 1995.

[7] Paul Solomon L. M. Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. In Bart Preneel and Stafford Tavares, editors, Selected Areas in Cryptography, pages 319--331, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[8] N.M. Glazunov, Skobelev S.P. Manifolds over the rings. IAMM National Academy of Sciences of Ukraine, Donetsk, 2011. 323 p.

[9] P.D Varbanee, P Zarzycki. Divisors of the Gaussian integers in an arithmetic progression. Journal of Number Theory. Volume 33, Issue 2, October 1989, Pages 152-169

[10] Silverman, Joseph H.; The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, 106, Springer-Verlag, 1986.

[11] Deligne, Pierre. La conjecture de Weil, Publications Mathématiques de l'IHÉS. 1974. Vol. 43. pp. 273-307,IEEE

[12] R. V. Skuratovskii, Employment of Minimal Generating Sets and Structure of Sylow 2-subgroups Alternating Groups in Block Ciphers. Springer, Advances in Computer Communication and Computational Sciences, 2019, pp. 351-364.