The Order of Edwards and Montgomery Curves

RUSLAN SKURATOVBKII
Department of Computer Science
University Igor Sikorsky Kiev Polytechnic Institute, National Technical University of Ukraine
Peremogy 37
UKRAINE

VOLODYMYR OSADCHYY
CEO IT-GRAVITY-VO, Inc.
Orlando, Florida, Edgewater Sr, Suite 1888, Orlando, FL, 32804,
USA

Abstract: - The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the Digital Signature Algorithm (DSA) [2]. It is well known that the problem of discrete logarithm is NP-hard on group on elliptic curve (EC) [5]. The orders of groups of an algebraic affine and projective curves of Edwards [3, 9] over the finite field $F_p$ is studied by us. We research Edwards algebraic curves over a finite field, which are one of the most promising supports of sets of points which are used for fast group operations [1]. We construct a new method for counting the order of an Edwards curve $E_d(F_p)$ over a finite field $F_p$. It should be noted that this method can be applied to the order of elliptic curves due to the birational equivalence between elliptic curves and Edwards curves. The method we have proposed has much less complexity $O(p \log^2 p)$ at not large values $p$ in comparison with the best Schoof basic algorithm with complexity $O(\log^4 p)$, as well as a variant of the Schoof algorithm that uses fast arithmetic, which has complexity $O(\log^4 p^*)$, but works only for Elkis or Atkin primes. We not only find a specific set of coefficients with corresponding field characteristics for which these curves are 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. The symmetric of the Edwards curve form and the parity of all degrees made it possible to represent the shape curves and apply the method of calculating the residual coincidences.

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 established. The criterion of supersingularity for Edwards curves is found over $F_p$.

Key-Words: - finite field, elliptic curve, Edwards curve, algorithm of order counting of group of points of an elliptic curve.


1 Introduction
The method of finding the order of an algebraic curve over a finite field $F_p$ are related with constructing of curves of given order. To construct cryptosystem based on elliptic curve we need to analyze the order of a group of elliptic curve points. Our method gives an approach to construct Edwards curves of determined order that is very important if cryptography and coding theory. It was accepted in 1999 as an ANSI standard and in 2000 as IEEE and NIST standards.

One of the fundamental problems in EC cryptography is the generation of cryptographically secure ECs over prime fields, suitable for use in various cryptographic applications. A typical requirement of all such applications is that the order of the EC [22]. One of essential requirement for EC is its order (number of elements in the algebraic structure induced by the EC) possesses certain properties (e.g., robustness against known attacks [23], small prime factors [22, 24], etc), which gives rise to the problem of how such EC can be generated. One of good decision of this task is curve of big prime order [24]. Also very important for this goal is avoidance curve of order $p + 1$ because of it is tractable by to pairing-based attacks. As we have discussed before, supersingular elliptic curves are vulnerable to pairing-based attacks. Therefore we find a criterion of Edwards curve supersingularity [25]. The method of finding the order of a n
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 our article, this problem is solved.

Our algorithm has much less complexity for algebraic extensions with a large degree of finite fields. This is so because choosing sufficiently large values $n$, we obtain $O(\log p \cdot p^n)$ the value is much larger than $O(\log \log p)$ for a fixed value $p$. The criterion of supersingularity of the Edw ards curves is found over $F_p$. We additionally propose a method for counting the points from Edwards curves and elliptic curves in response to an earlier paper by Schoof [8]. We consider the algebraic affine and projective Edwards curves over a finite field. We not only find a specific set of coefficients with corresponding field characteristics for which the curve $E_d/F_p$ is supersingular over this field or not. All proofs and analytical results belong to Skuratovskii R. and computational examples, confirming statements, are made by Osadchyy V.

2 Algebraic analyses of the curve and Curve Order Calculation Method

We recall that the twisted Edwards curve with coefficients $a, d \in F_p^*$, $d \neq 1, p \neq 2, a \neq d, \text{ is the curve } E_{a,d}$:

$$ax^2 + y^2 = 1 + dx^2y^2, \quad a, d \in F_p^*, \quad ad(a-d) \neq 0.$$ 

It should be noted that a twisted Edwards curve is called an Edwards curve when $a = 1$. We denote by $E_d$ 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 form $F(x, y, z) = ax^2z^2 + y^2z^2 = z^4 + dx^2y^2z^2$. 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 $A' : ax^2 + y^2z^2 = z^4 + dy^2$, $A' : ax^2z^2 + z^2 = z^4 + dx^2z^2$. 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 $\delta_p = \dim \mathcal{O}_p$, where $\mathcal{O}_p$ denotes the local ring at the singular point $p$. We calculate the genus of the curve according to Fulton [4].

$$\rho^*(C) = \rho_+(C) - \sum_{p \in E} \delta_p - \sum_{p \in E} \delta_p = 3 - 2 = 1,$$

where $\rho_+(C)$ 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]. 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 $E_{a,d}$. Koblitz [4,5] tells us that one can detect if a curve is supersingular 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 $F_q$ is called supersingular if for every finite extension $F_{q^r}$ there are no points in the group $E(F_{q^r})$ 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

$$\{x, y\} \mapsto \left(x, \frac{1}{y}\right).$$

We recall an important result from Vinogradov [13] which will act as criterion for supersingularity.

**Lemma 2.1.** Let $k \in \mathbb{N}$ and $p \in \mathbb{P}$. Then

$$\sum_{i=1}^{k} k^i \equiv 0 \pmod{p}, \quad n \equiv (p-1),$$

$$\sum_{i=1}^{k} k^i \equiv -1 \pmod{p}, \quad n \equiv (p-1).$$
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 \( x^2 + y^2 = 1 + d^{-1}x^2y^2 \) over \( F_p \). 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 \( F_p \) by \( N_{d[p]} \) and the number of points on the projective curve over the same field by \( \tilde{N}_{d[p]} \).

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

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

(1)
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 \( F_p \) are equal to \( N_{d[p]} = p + 1 \), when \( \left( \frac{d}{p} \right) = -1 \), and \( N_{d[p]} = p - 3 \), when \( \left( \frac{d}{p} \right) = 1 \).

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

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

(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 leads us to the curve \( y^2 = \frac{1 - x^2}{1 - dx^2y^2} \).

For analysis we transform it into the curve

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

(3)

We denote the number of points of 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 \( E_d \). Note that \( \left( \frac{d}{p} \right) \) denotes the Legendre Symbol. Let \( a_0, a_1, \ldots, a_{2p-2} \) be the coefficients of the polynomial \( a_0 + a_1x + \ldots + a_{2p-2}x^{2p-2} \), 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

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

By opening the brackets in \( (x^2 - 1)^{\frac{p-1}{2}}(dx^2 - 1)^{\frac{p-1}{2}} (\pmod{p}) \), we have \( a_{2p-2} = (-1)^{\frac{p-1}{2}}d^2 \equiv \left( \frac{d}{p} \right) (\pmod{p}) \). So, using Lemma 2.1 we have

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

(4)

We need to prove that \( M_{d[p]} = l(\pmod{p}) \) if \( p = 3(\pmod{8}) \) and \( M_{d[p]} = -l(\pmod{p}) \). We therefore have to show that \( M_{d[p]} = -\left( \frac{d}{p} \right) - a_{p-1} (\pmod{p}) \) for \( p = 3(\pmod{4}) \) if \( \sum_{j=0}^{p-1} \left( C_j' \right)^2 d^j = 0(\pmod{p}) \). If we 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 \( (x^2 - 1)^{\frac{p-1}{2}}(dx^2 - 1)^{\frac{p-1}{2}} \). So,

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

Actually, the following equality holds:

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

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

Since \( a_{p-1} = -\sum_{j=0}^{p-1} \left( C_j' \right)^2 d^j \), then exact number of affine points on non supersingular curve (3) is the following \( M_{d[p]} = -a_{2p-2} - a_{p-1} \) exactly:

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

(5)

According to the condition of this theorem \( a_{p-1} = 0 \), therefore \( M_{d[p]} = -a_{2p-2} (\pmod{p}) \). Consequently, in the case when \( p = 3(\pmod{4}) \), where \( p \) is prime and
\[
\sum_{j=0}^{p-1} (C_j^{\ell_2})^2 d^j = 0 (\text{mod } p),
\]
the curve \( E_d \) has affine points and a group of points of the curve completed by singular points has \( p+1 \) points.

Exact number of the points has upper bound \( 2p+1 \) because for every \( x \neq 0 \) corresponds two valuations of \( y \), but for \( x = 0 \) we have only one 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 \( N_{[d]} > 1 \). Thus, \( N_{[d]} = p + 1 \). This completes the proof.

**Corollary 2.1.** The orders of the curves \( x^2 + y^2 + 1 + dx^2 y^2 \) and \( x^2 + y^2 + 1 + dx^2 y^2 \) over \( F_p \) are equal to \( N_{[d]} = p + 1 = \overline{N}_{[d]} \), when \( \left( \frac{d}{p} \right) = -1 \), and \( N_{[d]} = p - 3 = \overline{N}_{[d]} - 4 \), when \( \left( \frac{d}{p} \right) = 1 \) iff

\[ p = 3 \pmod 4 \]
is prime and \( \sum_{j=0}^{p-1} (C_j^{\ell_2})^2 d^j = 0 \pmod p \).

In more details conditions \( N_{[d]} = p - 3 = \overline{N}_{[d]} - 4 \), when \( \left( \frac{d}{p} \right) = 1 \) and \( N_{[d]} = p + 1 = \overline{N}_{[d]} \), when

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

imply (1), due to the formula of number of points (5) and deduced from (5) formula (6) of affine points number of curve (2)

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

Since all transformations in proof of (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 \( p = 3 \pmod 4 \) then \( \sum_{j=0}^{p-1} d^j (C_j^{\ell_2})^2 = 0 \pmod p \) and \( \overline{N}_{[d]} = p + 1 \).

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

\[ \sum_{j=0}^{p-1} d^j (C_j^{\ell_2})^2 = 0 \pmod p. \]

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

some algebraic manipulation

\[
\frac{(p-1)^2}{2} = \frac{(p-1)!}{2^{(p-1)/2}} \cdot \frac{1 \cdot 2 \cdot \cdots \cdot (p-1)}{2^{(p-1)/2}} = \left( \frac{p-1}{2} \right)(p-1)! = (p-1)(p-1)!(p-1)! \cdots (p-1)!
\]

After applying the congruence

\[
\left( \frac{p-1}{2} \right)^2 = \left( \frac{p-1}{2} + 1 \right)^2 \pmod p
\]

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

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

Thus, as a result of squaring, we have:

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

(7)

It remains to prove that \( \sum_{j=0}^{p-1} d^j (C_j^{\ell_2})^2 = 0 \pmod p \) if \( p = 3 \pmod 4 \).

Consider the auxiliary polynomial

\[
P(t) = \left( \frac{p-1}{2} \right)^2 \sum_{j=0}^{p-1} (C_j^{\ell_2})^2 t^j.
\]

We are going to show that \( P(2) = 0 \) and therefore \( a_{p-1} = 0 \pmod p \). Using (7) it can be shown that

\[
a_{p-1} = P(t) = \left( \frac{p-1}{2} \right)^2 \sum_{j=0}^{p-1} (C_j^{\ell_2})^2 t^j = \sum_{j=0}^{p-1} (k+1)^2.
\]

(\( k+2 \)) \cdots (\( p-1 \)) \cdots (\( p-1 \)) \pmod p

over \( F_p \). We replace \( d \) by \( t \) in (1) such that we can research a more generalised problem. It should be noted that \( t P(t) = \left( \frac{p-1}{2} \right)^2 \left( \left( \frac{p-1}{2} \right)^2 \left( \left( \frac{p-1}{2} \right)^2 \right) \right) \pmod p
\]

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

\[
Q(t) = t^{p-1} - \frac{t(t-1)^p}{t-1} = (t-1)^{p-1} \pmod p \]

and

\[
E-ISSN: 2224-2880
\]

Volume 19, 2020

256
then the equality \[ P(i) = \left( \left( (t-1)^{t-1} \right)^{\frac{p-1}{2}} \right) \left( (t+1)^{t+1} \right)^{\frac{p-1}{2}} \] holds over \( F_p \).

In order to simplify notation we let \( 0 = t-1 \) and \( R(0) = P(0+1) \). For the case \( t = 2 \) we have \( 0 = 1 \).

Performing this substitution leads the polynomial \( P(i) \) of \( 2 \) to \( t \) the polynomial \( R(t-1) \) of \( 1 \). Taking \( g \) into account the linear nature of the substitution \( 0 = t-1 \), it can be seen that that derivation by \( 0 \) and \( t \) coincide. Derivat ion leads us to the transformation of polynomial \( R(0) \) to form where it has the necessary ar y coefficient \( a_{p+1} \). Then

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

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

We now will manipulate the expression \[ \frac{p-1}{2} \left( \frac{p-1}{2} \right) \left( 0^{p-1} + 1 \right) \left( 0^{p-1} + 1 \right)^{\frac{p-1}{2}}. \] In order to illustrate the simplification we now consider the scenario when \( p = 11 \) and hence \( \frac{p-1}{2} = 5 \).

The expression reads \[ \frac{p-1}{2} \left( \frac{p-1}{2} \right) \left( 0^{p-1} + 1 \right) \left( 0^{p-1} + 1 \right)^{\frac{p-1}{2}}. \] In order to illustrate the simplification we now consider the scenario when \( p = 11 \) and hence \( \frac{p-1}{2} = 5 \).

The expression reads \[ \frac{p-1}{2} \left( \frac{p-1}{2} \right) \left( 0^{p-1} + 1 \right) \left( 0^{p-1} + 1 \right)^{\frac{p-1}{2}}. \]

Therefore, for a prime \( p \), we can rewrite the expression as \[ \left( \frac{p-1}{2} \right) \left( j+1 \right) \cdots \left( j + \frac{p-1}{2} \right). \] As a result, the symmetrical terms in (7) can be reduced yielding \( a_{p+1} = 0 \mod p \).

It should be noted that \( \left( \frac{p-1}{2} \right)^{\frac{p-1}{2}} = -1 \) since \( p = Mk+3 \) 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, \( \sum_{j=0}^{p-1} C_{\frac{p-1}{2}}^j \left( j+1 \right) \cdots \left( j + \frac{p-1}{2} \right) = 0 \mod p \), completing the proof of the of the theorem. The complexity of calculating of (1) is \( O(p \log^2 p) \) that will be proved in Theorem 2.4.

**Corollary 2.2.** The curve \( E_j \) is supersingular iff \( E_{p^j} \) is supersingular. 

**Proof.** Let us recall the proved fact in Theorem 2.1 that \( N_{dp^j} = -a_{2p^j-2} - a_{p^j-1} = -\left( \frac{d}{p} \right) + \sum_{j=0}^{p-1} (C_{\frac{p-1}{2}}^j)^2 d^j \mod p \).

Since \( (C_{\frac{p-1}{2}}^j)^2 d^j = 0 \mod p \) by condition, and the congruence \( \left( \frac{d}{p} \right) = (\frac{d}{p}) \mod p \), holds, then according to (6) the number of points on \( E_d \) is \( N_{dp^j} = -a_{2p^j-2} - a_{p^j-1} = -\left( \frac{d}{p} \right) = \left( \frac{d}{p} \right) \mod p \), also \( N_{dp^j} = N_{dp^j} \).

**Corollary 2.3.** If \( p = 3 \mod 4 \), is prime then \( N_{dp^j} = p - 2 \left( \frac{d}{p} \right) + T \), where \( T \) is such that

\[ T = \sum_{j=0}^{p-1} (C_{\frac{p-1}{2}}^j)^2 d^j \mod p \] and \( T \leq 2\sqrt{p} \).

**Proof.** Due to equality (5) and the bounds (8) as well as accordingly to generalized Hasse-Weil theorem \( |N_{dp^j} - (p+1) - 2 \left( \frac{d}{p} \right)| \leq 2g\sqrt{p} \), where \( g \) is genus of curve, we obtain exact number \( N_{dp^j} \). As we showed, \( g \leq 1 \). From Theorem 2.1 as well as from Corollary 2.2 we get, that \( T = \sum_{j=0}^{p-1} (C_{\frac{p-1}{2}}^j)^2 d^j = -N_{dp^j} - (p+1) - 2 \left( \frac{d}{p} \right) \) so there exists \( T \in Z \), such that \( T < 2\sqrt{p} \) and \( N_{dp^j} = p - 2 \left( \frac{d}{p} \right) + T \).

**Example 2.1.** If \( p = 13 \), \( d = 2 \) gives \( N_{2[13]} = 8 \) and \( p = 13 \), \( d = 4 \) gives that the number of points of \( E_j \) is \( N_{7[13]} = 20 \), which is in contradiction to that suggested by A. Bessalov and O. Tsishganka. 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 \( p + 1 \) as suggested by A. Bessalov and O. Tsishganka.

For instance \( p = 31 \), then \( N_{2[31]} = N_{2[31]} = 28 = 31 - 3 \), which is clearly not equal to \( p + 1 \). If \( p = 7 \), \( d = 2 \) gives \( 4 \mod 7 \) then the curve \( E_{2^i} \) has four points, namely \((0,1); (0,6); (1,0); (6,0)\), and in the case \( p = 7 \) with
Theorem 2.3. Let $d$ satisfy the condition of supersingularity (1). If $n \equiv 1 \pmod{2}$ and $p$ is prime, then $\overline{N}_{d[p]} = p^n + 1$ and the order of curve is equal to $N_{d[p]} = p^n + 1 - 2(-p)^{\frac{n}{2}}$.

If $n \equiv 0 \pmod{2}$ and $p$ is prime, then the order of projective curve is equal to $\overline{N}_{d[p]} = p^n - 2(-p)^{\frac{n}{2}}$, and the order of affine curve is equal to $N_{d[p]} = p^n + 1 - 2(-p)^{\frac{n}{2}}$.

Proof. We consider the extension of the base field $F_p$ to $F_{p^2}$ in order to determine the number of the points on the curve $x^2 + y^2 = 1 + dx^2 y^2$. 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 [12] that the number of solutions to $y^2 = P(x)$ over $F_{p^2}$ will have the form $p^n + 1 - \omega_1^x - \cdots - \omega_{m-1}^x$, where $\omega_1, \ldots, \omega_{m-1} \in \overline{F}$, $|\omega| = \frac{1}{p}$.

In case of our supersingular curve, if $n \equiv 1 \pmod{2}$, the number of points on projective curve over $F_{p^2}$ is determined by the expression $p^n + 1 - \omega_1^x - \omega_2^x$, where $\omega_1^x \in \overline{F}$ and $\omega_2 = -\omega_1$, $|\omega_1| = \sqrt[p]{p}$ that's why $\omega_1 = i\sqrt[p]{p}$, $\omega_2 = -i\sqrt[p]{p}$ with $i \in \{1, 2\}$. In the general case, it is known [12, 15, 19] that $|\omega| = \frac{1}{p}$. The order of the projective curve is therefore $p^n + 1$.

If $p \equiv 7 \pmod{8}$, 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 $N_{d[p]} = p^n - 1$.

If $p \equiv 3 \pmod{8}$, then there are no singular points, hence $\overline{N}_{d[p]} = N_{d[p]} = p^n + 1$. Consequently the number of points on the Edwards curve depends on $\left(\frac{d}{p}\right)$ and is equal to $N_{d[p]} = p^n - 3$ if $p \equiv 7 \pmod{8}$ and $N_{d[p]} = p^n + 1$ if $p \equiv 3 \pmod{8}$ where $n \equiv 1 \pmod{2}$. We note that this is because the transformation of (3) in $E_d$ depends upon the denominator $(dx^2 - 1)$. If $n \equiv 1 \pmod{2}$ then, with respect to the sum of root of the characteristic equation for the Frobenius endomorphism $\omega_1^x + \omega_2^x$, which in this case have the same signs, we obtain that the number of points in the group of points of the curve is $p^n + 1 - \omega_1^x - \omega_2^x$ [19]. In more details $\omega_1$, $\omega_2$ are eigenvalues of Frobenius operator $F$ endomorphism on etale cohomology over the finite field $F_{p^2}$, where $F$ acts of $H(X)$. The number of points, in general case, are determined by Lefshitz formula:

$$\#X(F_{p^2}) = \sum (-1)^i \text{tr}(F^i|H^i(X))$$

where $\#X(F_{p^2})$ is a number of points in the manifold $X$ over $F_{p^2}$, $F^{\infty}$ is isomorphism of the Frobenius operator. In our case, $E_d$ is considered as the manifold $X$ over $F_{p^2}$.

For $n \equiv 0 \pmod{2}$ we always have, that every $d \in F_p$ is a quadratic residue in $F_{p^2}$. Consequently, because of $\left(\frac{d}{p}\right) = 1$ four singular points appear on the curve. Thus, the number of affine points is less by 4, i.e.

$$N_{d[p]} = p^n - 1 - 2\left(\frac{d}{p}\right) - 2(-p)^{\frac{n}{2}} = p^n - 3 - 2(-p)^{\frac{n}{2}}.$$

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

Proof. To verify this statement in supersingular case we suppose that the curve $x^2 + y^2 = 1 + dx^2 y^2$ 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 $x^2 + y^2 = 1 + dx^2 y^2$ into the following form
The points $M_{12}(0,0)$, $1_{12}(1,0)$ then the following transformations the point 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 

\[ \frac{4u^2}{v^2} = \frac{(d-1)u^2 + 2(d+1)u + (d-1)}{(1-u)^2} = \frac{4u}{(1-u)^2}. \]

Multiply the equation of the curve by $v^2(1-u)^2$. As a result of the reduction, we obtain the equation $v^2 = (d-1)u^2 + 2(d+1)u + (d-1)u$. We analyze what new solutions appeared in the resulting equation in comparison with $v^2(x^2 - 1) = x^2 - 1$. First, there is an additional solution $(u, v) = (0, 0)$. Second, if $d$ is a quadratic residue by modulo $p$, then the following solutions appear:

\[(u_1, v_1) = \left(\frac{-d+1}{d-1}, 0\right), \quad (u_2, v_2) = \left(\frac{-d+1}{d-1}, 0\right).\]

If $\left(\frac{d}{p}\right) = -1$ then as it was shown above the order of $E_d$ is equal to $p+1$. Therefore, in case $\left(\frac{d}{p}\right) = -1$ order of $E_d$ appears one additional solution of from $(0,0)$ more exact it is point with coordinates $(0,0)$ also two points $(-1;0),(1;0)$ of $E_d$ have not images on $E_u$ in result of action of birational map on $E_M$. Thus, in this case, number of affine points on $E_M$ is equal to $p+1 - 2 = p$.

If $x = -1$ then equality $x = \frac{1+u}{1-u}$ transforms to form $-1+u = 1+u$, or $-1=1$ that is impossible for $p>2$. Therefore point $(-1,0)$ have not an image on $E_u$.

Consider the case $x = 1$. As a result of the substitutions $x = (1+u)/(1-u)$, $y = 2u/v$ we get the pair $(x, y)$ corresponding to the pair $(u, v)$ for which $v^2 = (d-1)u^2 + 2(d+1)u^2 + (d-1)u$.

If it occurs that $y = 0$, then the preimage having coordinates $u = 0$ and $v$ is not equal to 0 is suitable for the birational map $y = \frac{2u}{v}$ which implies that $u = 0$ and $v \neq 0$. But pair $(u, v)$ of such form do not satisfies the equation of obtained in result of mapping equation of Montgomery curve $v^2 = (d-1)u^3 + 2(d+1)u^2 + (d-1)u$. The table of correspondence between points is the following:

<table>
<thead>
<tr>
<th>$E_M$</th>
<th>$E_d$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(0, 0)$</td>
<td>$\left(\frac{-d+1}{d-1}, 0\right)$</td>
</tr>
<tr>
<td>$\left(\frac{-d+1}{d-1}, 0\right)$</td>
<td>$\left(\frac{-d+1}{d-1}, 0\right)$</td>
</tr>
<tr>
<td>$(1, -2\sqrt{d})$</td>
<td>$\left(\frac{-d+1}{d-1}, 0\right)$</td>
</tr>
<tr>
<td>$(1, 2\sqrt{d})$</td>
<td>$\left(\frac{-d+1}{d-1}, 0\right)$</td>
</tr>
<tr>
<td>$(-1, 0)$</td>
<td>$\left(\frac{-d+1}{d-1}, 0\right)$</td>
</tr>
<tr>
<td>$(1, 0)$</td>
<td>$\left(\frac{-d+1}{d-1}, 0\right)$</td>
</tr>
</tbody>
</table>

Table 1: Special points of birational mapping.

The points $\left(\frac{-d+1}{d-1}, 0\right)$, $\left(\frac{-d+1}{d-1}, 0\right)$, $(1, -2\sqrt{d})$, $(1, 2\sqrt{d})$ exist on $E_M$ only when $\left(\frac{d}{p}\right) = 1$.

These points are elements of group which can be presented on Riemann sphere over $F_p$. The points $\left(\frac{-d+1}{d-1}, 0\right)$, $(1, 2\sqrt{d})$, $(1, 2\sqrt{d})$ have not images on $E_d$ because of in denominator of transformations $x = \frac{1+u}{1-u}$ appears zero. By the same reason points $\left(\frac{-d+1}{d-1}, 0\right)$, $\left(\frac{-d+1}{d-1}, 0\right)$ have not an images on $E_d$. If $\left(\frac{d}{p}\right) = 1$ then as it was shown above the order of $E_d$ is equal to $p-3$. Therefore order of $E_M$ equal to $p$ because of 5 additional solutions of equation of $E_u$ appears but 2 points $(-1;0),(1;0)$ of $E_d$ have not images on $E_M$. These are 5 additional points ap pointed in the table above. Also exist one infinitely distant point on an Montgomery curve. Thus, the order of $E_M$ is equal $p+1$ in this case as supersingular curve has.

The proof if complicated. It should be noted that the supersingular curve $E_d$ is birationally equivalent to the supersingular elliptic curve which may be presented in Montgomery form $v^2 = (d-1)u^3 + 2(d+1)u^2 + (d-1)u$. As well 1 as exceptional points [1] for the birational equivalence $(u, v) \mapsto (2u/v, (u-1)/(u+1)) = (x, y)$ are in one to one correspondence to the affine point of order 2 on $E_d$ and to the points in projective closure of $E_d$. Since the formula for number of affine points on $E_M$ can be applied to counting $N_{[u,v]}$. In such way
we apply this result [7, 12], to the case \( y^2 = P(x) \), where \( \deg P(x) = m \), \( m = 3 \). The order \( N_{M(|p|)} \) of the curve \( E_M \) over \( F_p \) can be evaluated due to Stepanov [12, 15]. The research tells us that the order is \( \overline{N}_{M(|p|)} = p^r + 1 - \omega_1^r - \omega_2^r \), where \( \omega_1^r \in \mathbb{C} \) and \( \omega_2^r = - \omega_3^r \), \( |\omega_i| = \sqrt{p} \) with \( i \in \{1, 2\} \). Therefore, we conclude when \( n = 1(\mod \, 2) \), we know the order of Montgomery curve is precisely \( N_{M(|p|)} = p^r + 1 \).

This result leads us to the conclusion that the number of solutions of \( x^2 + y^2 = 1 + dx^2 y^2 \) as well as \( y^2 = (d-1)u + 2(d+1)u^2 + (d-1)u \) over the finite field \( F_p \) are determined by the expression \( p^r + 1 - \omega_1^r - \omega_2^r \) if \( n = 1(\mod \, 2) \).

**Example 2.2.** The elliptic curve presented in the form of Montgomery \( E_M : y^2 = u^3 + 6u^2 + u \) is birationally equivalent \( \{ 1 \} \) to the curve \( x^2 + y^2 = 1 + 2x^2 y^2 \) over the field \( F_p \).

**Corollary 2.4.** If \( d = 2, n = 1(\mod \, 2) \) and \( p = 3(\mod \, 8) \), then the order of curve \( E_d \) and order of the projective curve \( E \) are the following:

- \( N_{d(|p|)} = p^r + 1, \overline{N}_{d(|p|)} = p^r + 1. \)
- When \( n = 1(\mod \, 2) \), then we have \( p^r + 1 - \omega_1^r - \omega_2^r = 1\) and the number of points on affine curve \( E_d \) is also \( N_{d(|p|)} = p^r - 3 \).

In case \( d = 2, n = 0(\mod \, 2) \), \( p = 3(\mod \, 4) \), the general formula of the curve orders is \( N_{d(|p|)} = p^r - 3 - 2(-p)^{\frac{r}{2}} \).

The general formula for \( n = 1(\mod \, 2) \) and \( d = 2 \) for the number of points on projective curve for the supersingular case is \( \overline{N}_{d(|p|)} = p^r + 1 - 2(-p)^{\frac{r}{2}}. \)

**Proof.** We denote by \( N_{M(|p|)} \) the order of the curve \( E_M \) over \( F_p \). The order \( N_{M(|p|)} \) of the curve \( E_M \) over \( F_p \) can be evaluated \( \{ 6 \} \) as \( N_{M(|p|)} = p^r + 1 - \omega_1^r - \omega_2^r \), where \( \omega_1^r \in \mathbb{C} \) and \( \omega_2^r = - \omega_3^r \), \( |\omega_i| = \sqrt{p} \) with \( i \in \{1, 2\} \). For the finite algebraic extension of degree \( n \), we will consider \( p^r - \omega_1^r - \omega_2^r = p^r \) if \( n = 1(\mod \, 2) \). Therefore, for \( n = 1(\mod \, 2) \), the order of the Montgomery curve is precisely given by \( N_{M(|p|)} = p^r + 1 \). 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 \( \omega_1 = \overline{\omega}_2 \) by \( [5] \), which leads to \( \omega_1 + \omega_2 = 0 \). For \( n = 1 \), it is clear that \( N_M = p^r \). When \( n \) is odd, we have \( \omega_1^r + \omega_2^r = 0 \) and therefore \( N_{M,p} = p^r + 1 \). Because \( n \) is even by initial assumption, we shall show that \( N_{M(|p|)} = p^r + 1 - 2(-p)^{\frac{r}{2}} \) holds as required.

Note that for \( n = 2 \) we can express the number as \( \overline{N}_{d(|p|)} = p^r + 1 + 2p = (p + 1)^2 \) with respect to Lagrange theorem to have be divisible on \( \overline{N}_{d(|p|)} \).

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 \( r \) \( E_d(F_p) \) holds because in our case \( p = 7 \) thus \( \overline{N}_{E_d} = 8^2 \) and \( p + 1 = 8 = N_{d10} \)[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 \( N_{2(3)} = p^r - 3 - 2(-p)^{\frac{r}{2}} = 3^2 - 3 - 2(3) = 12 \), and the number of projective points is equal to \( \overline{N}_{2(3)} = p^r - 1 - 2(-p)^{\frac{r}{2}} = 3^2 + 1 - 2(3) = 16 \).

**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 \( N_{2(7)} = p^r - 3 - 2(-p)^{\frac{r}{2}} = 7^2 - 3 - 2(-7) = 60 \), and the number of projective points is equal to \( \overline{N}_{2(7)} = p^r + 1 - 2(-p)^{\frac{r}{2}} = 7^2 + 1 - 2(-7) = 64 \).

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 \( p + 1 \).

**Example 2.5.** The number of curve points over finite field when \( d = 2 \) and \( p = 31 \) is equal to \( N_{2(31)} = N_{2^{-1}(31)} = p - 3 = 28 \).
Theorem 2.4. The order of Edwards curve over $F_p$ is congruent to

$$\mathcal{N}_{d,p} = (p-1-2\left(\frac{d}{p}\right)+\sum_{j=0}^{p-1} (C_{j,p}^d)^2 d^j)$$

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

The true value of $\mathcal{N}_{d,p}$ 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

$$\sum_{j=0}^{p-1} \left(\frac{x^2 - 1}{p}\right) (dx^2 - 1) = \sum_{j=0}^{p-1} (x^2 - 1)(dx^2 - 1) + p =$$

$$\equiv \left(\sum_{j=0}^{p-1} (x^2 - 1)^j d^j\right) - (d/p)(\bmod p) =$$

$$\equiv \left(-1\right)^{p-1} \sum_{j=0}^{p-1} (C_{j,p}^d)^2 d^j - (d/p)(\bmod p).$$

The quantity of solutions for $x^2 + y^2 = 1 + dx^2y^2$ differs from the quantity of $y^2 = (dx^2 - 1)(x^2 - 1)$ by $(d/p) + 1$ due to new solutions in the form $(\sqrt{d}, 0), (\sqrt{d}, 0)$. Hence if this quantity is such

$$\sum_{j=0}^{p-1} \left(\frac{x^2 - 1}{p}\right) (dx^2 - 1) + 1 = \left(\frac{d}{p}\right) + 1 =$$

$$\equiv \left(\sum_{j=0}^{p-1} (x^2 - 1)^j d^j\right) + (d/p) - 1 =$$

$$\equiv \left(-1\right)^{p-1} \sum_{j=0}^{p-1} (C_{j,p}^d)^2 d^j - (2d/p) + 1(\bmod p) =$$

According to Lemma 1 the last sum

$$\sum_{j=0}^{p-1} (x^2 - 1)^j d^j - (2d/p) + 1(\bmod p)$$

is congruent to $-a_{p-1} - a_{2p-2}(\bmod p)$, where $a_j$ are the coefficients from presentation

$$(x^2 - 1)^j d^j = a_0 + a_1 x + \ldots + a_{2p-2} x^{2p-2}.$$
Let us analyze the complexity of calculating the value of $\sum_{j=0}^{2^{e-1}} C_{\frac{p-1}{2}}^j d^j$. Binomial coefficients of the form $C_{\frac{p-1}{2}}^j$ we calculate recursively having $C_{\frac{p-1}{2}}^1$ we get $C_{\frac{p-1}{2}}^{e-1}$. Such a transformation can be done by one multiplication of one division. But division can be avoided by applying the Legendre formula to count the number of occurrences of all prime factors from $2$ to $(p-1)/2$. In both cases, the complexity of calculating all the coefficients from the sum (3) is equal to $O(2^{e-1} \log p)$.

For $(x_0, y_0)$ is solution of $(2)$, then

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

is a solution of $(10)$ because last transformations determines that

$$y_0^2 = \frac{1}{d} \left(\frac{x_0}{\sqrt{d}}\right)^2 - 1 \mod p.$$
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 $p = 3$ and $d = 2$ is given by $N_{213} = 8$. In the case when $p = 3$ and $d^{-1} = 7$ we have that the number of points of $E_d$ is $N_{213} = 20$. 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 $F_3$, 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 $d/p = 1$ and the curve $E_{d^{-1}}$ 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 $E_{d^{-1}}$ 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 $p$ of supersingular curves $E_d[F_p]$ of order $p$ in the multiplicative group of field $F_p$, 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 $q | P_{12}(p)$, where $P_{12}(x)$ is the cyclotomic polynomial. This $p$ will satisfy the necessary conditions $(x^2 - 1) \not| p$ for an arbitrary $n = 1,...,11$.

**Proposition 2.1** 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 $p^2 + 1$. It should be observed that $p^2 + 1$ divides $p^{2k} - 1$, but $p^2 + 1$ does not divide expressions of the form $p^{2k} - 1$ with $l < k$. This division does not work for smaller values of $l$ due to the decomposition of the expression $p^{2k} - 1 = (p^{2l} - 1)(p^{2l} + 1)$. Therefore, we can use the definition to conclude that the degree of embedding must be 2, confirming the proposition.

Consider $E_2$ over $F_2^p$, for instance we assume $p = 3$. We define $F_2$ as $F_2(\alpha)$, where $\alpha$ is a root of $x^2 + 1 = 0$ over $F_2$. Therefore elements of $F_2$ have form $a + b \alpha$, where $a, b \in F_2$. So we assume that $x = \pm (\alpha + 1)$, $\pm (\alpha - 1), \pm \alpha$ and check its belonging to $E_2$. For instance if $x = \pm (\alpha + 1)$ then $x^2 = \alpha^2 + 2\alpha + 1 = 2\alpha = \alpha$. Also in this case $y^2 = 2a - 1 = (2a - 1)(\alpha + 1)$. Therefore the correspondent second coordinate is $y = \pm (\alpha - 1)$. The similar computations lead us to full the following list of curves points.

<table>
<thead>
<tr>
<th>$x$</th>
<th>$y$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\pm 1$</td>
<td>$\pm (\alpha + 1)$</td>
</tr>
</tbody>
</table>

Table 2: 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 $p^2 - 3 - 2(-p)^2 = 3^2 - 3 - 2(-3) = 12$.

**4 Conclusion**

The new effective algorithm for the elliptic and Edwards curves order curve counting was found. The criterion for supersingularity of these curves was additionally obtained.

**References:**


