The Order of Edwards and Montgomery Curves

RUSLAN SKURATOVSKII
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^n} 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 $O\left(p\log_2^2 p\right)$ at not large values p in comparison with the best Schoof basic algorithm with complexity $O(\log_2^8 p^n)$, as well as a variant of the Schoof algorithm that uses fast arithmetic, which has complexity $O(\log_2^4 p^n)$, 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^n}.

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

Received: October 19, 2019. Revised: May 7, 2020. Re-revised: May 22, 2020. Accepted: May 26, 2020. Published: May 28, 2020.

1 Introduction

The method of finding the order of an algebraic curve over a finite field F_{p^n} 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 if 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 requirment 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 tusk 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 pairingbased attacks. As we have discussed before, supersingular elliptic curves are vulnerable to pairingbased attacks. Therefore we find a criterion of Edwards curve supersingularity [25]. The method of finding the order of an algebraic curve over a finite field F_{p^n} 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 ontain $O(\log_2^8 p^n)$ the value is much larger than $O\left(p\log_2^2 p\right)$ for a fixed value p. The criterion of supersingularity of the Edwards curves is found over F_{p^n}. 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 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. 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 $a,d \in F_p^*, d \neq 1,\ p \neq 2,\ a \neq d,$ 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_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 $F(x,y,z) = ax^2z^2 + y^2z^2 = z^4 + dx^2y^2$. 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 $A^1 := az^2 + y^2z^2 = z^4 + dy^2$, $A^2 :\ ax^2z^2 + z^2 = z^4 + dx^2.$ These are simple singularities.

We describe the structure of the local ring at the point p_1 whose elements are quotients of functions with the form $F(x,y,z) = \dfrac{f(x,y,z)}{g(x,y,z)}$, where the denominator cannot take the value of 0 at the singular point p_1. 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 $\delta_p = \dim^{\overline{O}_p}/_{O_p}$, where O_p denotes the local ring at the singular point p which is generated by the relations of regular functions $O_p = \left\{\dfrac{f}{g} : (g,(x-1)(y-1)) = 1\right\}$ and $\overline{O}_p$ denotes the whole closure of the local ring at the singular point p.

We find that $\delta_p = \dim^{\overline{O}_p}/_{O_p} = 1$ is the dimension of the factor as a vector space. Because the basis of extension $\overline{O}_p/O_p$ consists of just one element at each distinct point, we obtain that $\delta_p = 1$. We then calculate the genus of the curve according to Fulton [4].

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

where $\rho_\alpha(C)$ 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_M. 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 $\left(\bar{x},\bar{y}\right) \mapsto (x,y) = \left(\bar{x}, \dfrac{1}{\bar{y}}\right).$

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

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

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 $x^2+y^2=1+d^{-1}x^2y^2$ 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 $\overline{N}_{d[p]}$.

Theorem 2.1. If $p \equiv 3 (\bmod\ 4)$ is prime and the following condition of supersingularity

$$\sum_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 d^j \equiv 0 (\bmod\ p), \tag{1}$$

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:

$$x^2+y^2=1+dx^2y^2. \tag{2}$$

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 $y^2=\dfrac{1-x^2}{1-dx^2y^2}$.

For analysis we transform it into the curve

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

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_d. Note that $\left(\frac{d}{p}\right)$ denotes the Legendre Symbol. Let $a_0, a_1, \dots, a_{2p-2}$ 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

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

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

$$M_{d[p]} \equiv -\left(\frac{d}{p}\right)-a_{p-1}(\bmod\ p). \tag{4}$$

We need to prove that $M_{d[p]} \equiv 1(\bmod\ p)$ if $p \equiv 3(\bmod\ 8)$ and $M_{d[p]} \equiv -1(\bmod\ p)$. We therefore have to show that $M_{d[p]} \equiv -(\frac{d}{p})-a_{p-1}(\bmod\ p)$ for $p \equiv 3(\bmod\ 4)$ if $\sum_{j=0}^{\frac{p-1}{2}}(C^j_{\frac{p-1}{2}})^2 d^j \equiv 0(\bmod\ p)$. If we prove that $a_{p-1} \equiv 0(\bmod\ p)$, 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, $a_{p-1}=(-1)^{\frac{p-1}{2}}\sum_{j=0}^{\frac{p-1}{2}} d^j(C^j_{\frac{p-1}{2}})^2$. Actually, the following equality holds:

$$\sum_{j=0}^{\frac{p-1}{2}} d^j (C^{\frac{p-1}{2}-j}_{\frac{p-1}{2}})(-1)^{\frac{p-1}{2}-(\frac{p-1}{2}-j)} \cdot d^j (C^j_{\frac{p-1}{2}})^2 (-1)^{\frac{p-1}{2}-j} =$$

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

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

$$M_{d[p]} \equiv -\left(\frac{d}{p}\right)+\sum_{j=0}^{\frac{p-1}{2}}(C^j_{\frac{p-1}{2}})^2 d^j (\bmod\ p). \tag{5}$$

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

$\sum_{j=0}^{\frac{p-1}{2}}(C^j_{\frac{p-1}{2}})^2 d^j \equiv 0(\bmod p)$, the curve E_d has

$$N_{d[p]} = p-\left(\frac{d}{p}\right)-(\left(\frac{d}{p}\right)+1) = p-1-2\left(\frac{d}{p}\right) \tag{6}$$

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 $N_{d[p]} > 1$. Thus, $N_{d[p]} = p+1$. This completes the proof.

Corollary 2.1. 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 $N_{d[p]} = p+1 = \overline{N}_{d[p]}$, when $(\frac{d}{p}) = -1$, and $N_{d[p]} = p-3 = \overline{N}_{d[p]}-4$, when $(\frac{d}{p}) = 1$ iff $p \equiv 3(\bmod\ 4)$ is prime and $\sum_{j=0}^{\frac{p-1}{2}}(C^j_{\frac{p-1}{2}})^2 d^j \equiv 0(\bmod p)$.

In more details conditions $N_{d[p]} = p-3 = \overline{N}_{d[p]}-4$, when $(\frac{d}{p}) = 1$ and $N_{d[p]} = p+1 = \overline{N}_{d[p]}$, when $(\frac{d}{p}) = -1$, imply (1), due to the formula of number of points (5) and deduced from (5) formula (6) of affine points number of curve (2) $N_{d[p]} = p-\left(\frac{d}{p}\right)-(\left(\frac{d}{p}\right)+1) = p-1-2\left(\frac{d}{p}\right)$. Since all transformations in prof 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 $p \equiv 3(\bmod 4)$ then $\sum_{j=0}^{\frac{p-1}{2}} d^j (C^j_{\frac{p-1}{d}})^2 \equiv 0(\bmod p)$ and $\overline{N}_{d[p]} = p+1$.

Proof. When $p \equiv 3(\bmod\ 4)$, we shall show that $\sum_{j=0}^{\frac{p-1}{2}} d^j (C^j_{\frac{p-1}{d}})^2 \equiv 0(\bmod p)$. We multiply each binomial coefficient in this sum by $(\frac{p-1}{2})!$ to obtain after some algebraic manipulation

$$(\frac{p-1}{2})! C^j_{\frac{p-1}{2}} = \frac{(\frac{p-1}{2})(\frac{p-1}{2}-1)\cdots(\frac{p-1}{2}-j+1)(\frac{p-1}{2})!}{1\cdot 2\cdots j} =$$
$$= (\frac{p-1}{2})(\frac{p-1}{2}-1)\cdots(\frac{p-1}{2}-j+1)[(\frac{p-1}{2})(\frac{p-1}{2}-1)\cdot ...$$
$$\cdot(j+1)].$$

After applying the congruence $(\frac{p-1}{2}-k)^2 \equiv (\frac{p-1}{2}+1+k)^2 (\bmod p)$ with $0 \le k \le \frac{p-1}{2}$ to the multipliers in previous parentheses, we obtain $[(\frac{p-1}{2})(\frac{p-1}{2}-1)\cdots(j+1)]$.

It yields $\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}-1\right)\cdots\left(\frac{p-1}{2}-j+1\right)\cdot$

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

Thus, as a result of squaring, we have:

$$((\frac{p-1}{2})!\ C^j_{\frac{p-1}{2}})^2 \equiv (\frac{p-1}{2}-j+1)^2(\frac{p-1}{2}-j+2)^2\cdot$$
$$\cdots(p-j-1)^2(\bmod p). \tag{7}$$

It remains to prove that $\sum_{j=0}^{\frac{p-1}{2}}(C^j_{\frac{p-1}{2}})^2 2^j \equiv 0(\bmod p)$ if $p \equiv 3(\bmod\ 4)$.

Consider the auxillary polynomial $P(t) = (\frac{p-1}{2}!)^2 \sum_{j=0}^{\frac{p-1}{2}}(C^j_{\frac{p-1}{2}})^2 t^j$. We are going to show that $P(2) = 0$ and therefore $a_{p-1} \equiv 0(\bmod p)$. Using (7) it can be shown that

$$a_{p-1} = P(t) = (\frac{p-1}{2}!)^2 \sum_{j=0}^{\frac{p-1}{2}}(C^j_{\frac{p-1}{2}})^2 t^j \equiv \sum_{j=0}^{\frac{p-1}{2}}(k+1)^2\cdot$$
$$\cdot(k+2)^2 ... (\frac{p-1}{2}+k)^2 t^k (\bmod p)$$

over F_p. We replace d by t in (1) such that we can research a more generalised problem. It should be noted that $P(t) = \partial^{\frac{p-1}{2}}\left(\partial^{\frac{p-1}{2}}\left(Q(t)\, t^{\frac{p-1}{2}}\right)t^{\frac{p-1}{2}}\right)$ over F_p, where $Q(t) = t^{p-1}+...+t+1$ and $\partial^{\frac{p-1}{2}}$ denotes the $\frac{p-1}{2}$-th derivative by t, where t is new variable but not a coordinate of curve. Observe that $Q(t) = \frac{t^p-1}{t-1} \equiv \frac{(t-1)^p}{t-1} \equiv (t-1)^{p-1}(\bmod p)$ and therefore the equality $P(t) = \left(\left((t-1)^{p-1} t^{\frac{p-1}{2}}\right)^{(\frac{p-1}{2})} t^{\frac{p-1}{2}}\right)^{(\frac{p-1}{2})}$ holds over F_p.

In order to simplify 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 $R(t-1)$ of 1. Taking into account the linear nature of the substitution $\theta = t-1$, it can be seen that that derivation by θ 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

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

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

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

We now will manipulate with the expression $(\frac{p-1}{2}-j+1)(\frac{p-1}{2}-j+2)\cdots(\frac{p-1}{2}-j+\frac{p-1}{2})$. In order to illustrate the simplification we now consider the scenario when $p=11$ and hence $\frac{p-1}{2}=5$. The expression gets the form

$$(5-j+1)(5-j+2)\cdots(5-j+5) = (6-j)(7-j)\cdots(10-j) \equiv$$
$$\equiv \left((-5-j)(-4-j)\cdots(-1-j)\right) \equiv$$
$$\equiv (-1)^5\left((j+1)(j+2)\cdots(j+5)\right)(\bmod\ 11).$$

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

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

As a result, the symmetrical terms in (7) can be reduced yielding $a_{p-1} \equiv 0(\bmod p)$. It should be noted that $(-1)^{\frac{p-1}{2}} = -1$ since $p = Mk+3$ and $\frac{p-1}{2} = 2k+1$. Consequently, we have $P(2) = R(1) = 0$ and hence $a_{p-1} \equiv 0(\bmod p)$ as required. Thus, $\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^{j})^2 \equiv 0(\bmod p)$, completing the proof of the of the theorem. The complexity of calculating of (1) is $O\left(p\log_2^2 p\right)$ that will be proved in Theorem 2.4.

Corollary 2.2. The curve E_d is supersingular iff $E_{d^{-1}}$ is supersingular.

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

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

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

Corollary 2.3. If $p \equiv 3(\bmod 4)$, is prime then $N_{d[p]} = p-1-2\left(\frac{d}{p}\right)+T$, where T is such that $T \equiv \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^{j})^2 d^j \bmod p$ and $T \le 2\sqrt{p}$ **.**

Proof. Due to equality (5) and the bounds (8) as well as according to generalized Hasse-Weil theorem $| N_{d[p]} - (p+1) - 2\left(\frac{d}{p}\right)| \le 2g\sqrt{p}$, 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 $\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^{j})^2 d^j \equiv -N_{d[p]} - (p+1) - 2\left(\frac{d}{p}\right)$ so there exists $T \in Z$, 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 $N_{2[13]} = 8$ and $p=13$, $d^{-1}=7$ gives that the number of points of E_7 is $N_{7[13]} = 20$, which is in contradiction to that suggested by A. Bessalov and O. Thsigankova. Moreover, if $p \equiv 7(\bmod\ 8)$, then the order of torsion subgroup of curve is $N_2 = N_{2^{-1}} = p-3$, which is clearly different to $p+1$ as suggested by A. Bessalov and O. Thsigankova.

For instance $p=31$, then $N_{2[31]} = N_{2^{-1}[31]} = 28 = 31-3$, which is clearly not equal to $p+1$. If $p=7, d = 2^{-1} \equiv (4 \bmod\ 7)$ then the curve $E_{2^{-1}}$ has four points, namely $(0,1)$; $(0,6)$; $(1,0)$; $(6,0)$, and the in case $p=7$ with

$d = 2(\bmod\ 7)$, the curve $E_{2^{-1}}$ 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 $E_{d^{-1}}$ are equal under certain assumptions. This theorem additionally provides us with a formula for enumerating the number of affine points upon the birationally isomorphic Montgomery curve N_M.

Theorem 2.3. Let d satisfy the condition of supersingularity (1). If $n \equiv 1(\bmod\ 2)$ and p is prime, then $\overline{N}_{d[p^n]} = p^n + 1$ and the order of curve is equal to $N_{d[p^n]} = p^n - 1 - 2\left(\frac{d}{p}\right)$.

If $n \equiv 0(\bmod\ 2)$ and p is prime, then the order of curve

$N_{d[p^n]} = p^n - 3 - 2(-p)^{\frac{n}{2}}$, and the order of projective curve is equal to $\overline{N}_{d[p^n]} = p^n + 1 - 2(-p)^{\frac{n}{2}}$.

If $n \equiv 0(\bmod\ 2)$ and p is prime, then the order of projective curve is equal to $\overline{N}_{d[p^n]} = p^n + 1 - 2(-p)^{n/2}$, and the order of affine curve is equal to $N_{d[p^n]} = p^n + 3 - 2(-p)^{n/2}$.

Proof. We consider the extension of the base field F_p to F_{p^n} 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 [12] that the number of solutions to $y^2 = P(x)$ over F_{p^n} will have the form $p^n + 1 - \omega_1^n - \ldots - \omega_{m-1}^n$, where $\omega_1, \ldots, \omega_{m-1} \in \mathbb{C}$, $|\omega_i| = p^{\frac{1}{2}}$.

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

If $p \equiv 7(\bmod\ 8)$, 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 $N_{d[p]} = p^n - 3$.

If $p \equiv 3(\bmod\ 8)$, 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 $(\frac{d}{p})$ and is equal to $N_{d[p]} = p^n - 3$ if $p \equiv 7(\bmod\ 8)$ and $N_{d[p]} = p^n + 1$ if $p \equiv 3(\bmod\ 8)$ where $n \equiv 1(\bmod\ 2)$. We note that this is because the transformation of (3) in E_d depends upon the denominator $(dx^2 - 1)$. If $n \equiv 1(\bmod\ 2)$ then, with respect to the sum of root of the characteristic equation for the Frobenius endomorphism $\omega_1^n + \omega_2^n$, which in this case have the same signs, we obtain that the number of points in the group of points of the curve is $p^n + 1 - \omega_1^n - \omega_2^n$ [19]. In more details ω_1, ω_2 are eigen values of Frobenius operator F endomorphism on etale cohomology over the finite field F_{p^n}, where F acts of $H^i(X)$. The number of points, in general case, are determined by Lefshitz formula:

$$\#X\left(\mathrm{F}_{p^n}\right) = \sum (-1)^i tr(\mathrm{F}^n \left| H^i(X)\right.)$$

where $\#X\left(\mathrm{F}_{p^n}\right)$ is a number of points in the manifold X over F_{p^n}, F^n is composition of the Frobenius operator. In our case, E_d is considered as the manifold X over F_{p^n}.

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

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

Lemma 2.2. There exists birational isomorphism between E_d and E_M, 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 substitutions $x=\frac{1+u}{1-u}$ and $y=\frac{2u}{v}$. We will call the special points of this 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 $\frac{4u^2}{v^2}\cdot\frac{(d-1)u^2+2(d+1)u+(d-1)}{(1-u)^2}=\frac{4u}{(1-u)^2}$. Multiply the equation of the curve by $\frac{v^2(1-u)^2}{4u}$. As a result of the reduction, we obtain the equation $v^2=(d-1)u^3+2(d+1)u^2+(d-1)u.$ We analyze what new solutions appeared in the resulting equation in comparing with $y^2(dx^2-1)=x^2-1$. 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: $(u_1,v_1)=\left(\frac{-(d+1)-2\sqrt{d}}{d-1},0\right)$, $(u_2,v_2)=\left(\frac{-(d+1)+2\sqrt{d}}{d-1},0\right)$. 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 $(u,0)$ more exact it is point with coordinates $(0,0)$ also two points $((-1;0),(1;0))$ of E_d have not images on E_M in result of action of birational map on E_M. Thus, in this case, number of affine points on E_M is equal to $p+1-2+1=p$.

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_M. 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 $v^2=(d-1)u^3+2(d+1)u^2+(d-1)u$.

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:

Special points of E_M	Special points of E_d
$(0;0)$	–
$(\frac{-(d+1)-2\sqrt{d}}{d-1},0)$	–
$(\frac{-(d+1)+2\sqrt{d}}{d-1},0)$	–
$(1,-2\sqrt{d})$	–
$(1,2\sqrt{d})$	–
–	$(-1,0)$
–	$(1,0)$

Table 1: Special points of birational maping.

The points $(\frac{-(d+1)-2\sqrt{d}}{d-1},0)$, $(\frac{-(d+1)+2\sqrt{d}}{d-1},0)$, $(1,-2\sqrt{d})$, $(1,2\sqrt{d})$ exist on E_M only when $(\frac{d}{p})=1$. These points are elements of group which can be presented on Riemann sphere over F_q. The points $(1,-2\sqrt{d})$, $(1,2\sqrt{d})$ $(1,2\sqrt{d})$ 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 $(\frac{-(d+1)-2\sqrt{d}}{d-1},0)$, $(\frac{-(d+1)+2\sqrt{d}}{d-1},0)$ 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 is equal to p because of 5 additional solutions of equation of E_M appears but 2 points $((-1;0),(1;0))$ of E_d have not images on E_M. These are 5 additional points appointed in tableau above. Also it exists one infinitely distant point on a n 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 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 $N_{d[p]}$. In such way we apply this result [7, 12], to the case $y^2 = P(x)$, where $degP(x) = m$, $m = 3$. The order $N_{M[p^n]}$ of the curve E_M over F_{p^k} can be evaluated due to Stepanov [12, 15]. The research tells us that the order is $\overline{N}_{M[p^n]} = p^n + 1 - \omega_1^n - \omega_2^n$, where $\omega_i^n \in \mathbb{C}$ and $\omega_1^n = -\omega_2^n$, $|\omega_i| = \sqrt{p}$ with $i \in \{1,2\}$. Therefore, we conclude when $n \equiv 1(\bmod\ 2)$, we know the order of Montgomery curve is precisely $N_{M[p^n]} = p^n + 1$.

This result leads us to the conclusion that the number of solutions of $x^2 + y^2 = 1 + dx^2y^2$ as well as $v^2 = (d-1)u^3 + 2(d+1)u^2 + (d-1)u$ over the finite field F_{p^n} are determined by the expression $p^n + 1 - \omega_1^n - \omega_2^n$ if $n \equiv 1(\bmod\ 2)$.

Example 2.2. The elliptic curve presented in the form of Montgomery $E_M : v^2 = u^3 + 6u^2 + u$ is birationally equivalent [1] to the curve $x^2 + y^2 = 1 + 2x^2y^2$ over the field F_{p^k}.

Corollary 2.4. If $d = 2,\ n \equiv 1(\bmod\ 2)$ and $p \equiv 3(\bmod\ 8)$, then the order of curve E_d and order of the projective curve are the following: $N_{d[p^n]} = p^n + 1, \overline{N}_{d[p^n]} = p^n + 1.$

If $d = 2$, $n \equiv 1(\bmod\ 2)$ and $p \equiv 7(\bmod\ 8)$, then the number of points of projective curve is

$$\overline{N}_{d[p^n]} = p^n + 1,$$

and the number of points on affine curve E_d is also

$$\overline{N}_{d[p^n]} = p^n - 3.$$

In case $d = 2$, $n \equiv 0(\bmod 2)$, $p \equiv 3(\bmod 4)$, the general formula of the curves order is

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

The general formula for $n \equiv 0(\bmod 2)$ and $d = 2$ for the number of points on projective curve for the supersingular case is

$$\overline{N}_{d[p^n]} = p^n + 1 - 2(-p)^{\frac{n}{2}}.$$

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

Note that for $n = 2$ we can express the number as $\overline{N}_{d[p^2]} = p^2 + 1 + 2p = (p+1)^2$ with respect to Lagrange theorem have to be divisible on $\overline{N}_{d[p]}$. Because a group of $E_d(F_{p^2})$ over square extension of F_p contains the group $E_d(\mathrm{F}_p)$ as a proper subgroup. In fact, according to Theorem 1 the order $E_d(\mathrm{F}_p)$ is $p+1$ therefore divisibility of order $E_d(\mathrm{F}_{p^2})$ holds because in our case $p = 7$ thus $\overline{N}_{E_d} = 8^2$ and $p + 1 = 8 = N_{d[7]}$ [16]. The following two examples exemplify Corollary 2.4.

Example 2.3. If $p \equiv 3(\bmod\ 8)$ and $n = 2k$ then we have when $d = 2$, $n = 2$, $p = 3$ that the number of affine points equals to

$$N_{2[3]} = p^n - 3 - 2(-p)^{\frac{n}{2}} = 3^2 - 3 - 2\cdot(-3) = 12,$$

and the number of projective points is equal to

$$\overline{N}_{2[3]} = p^n + 1 - 2(-p)^{\frac{n}{2}} = 3^2 + 1 - 2\cdot(-3) = 16.$$

Example 2.4. If $p \equiv 7(\bmod\ 8)$ and $n = 2k$ then we have when $d = 2$, $n = 2$, $p = 7$ that the number of affine points equals to

$N_{2[7]} = p^n - 3 - 2(-p)^{\frac{n}{2}} = 7^2 - 3 - 2\cdot(-7) = 60,$ and the number of projective points is equal to

$$\overline{N}_{2[7]} = p^n + 1 - 2(-p)^{\frac{n}{2}} = 7^2 + 1 - 2\cdot(-7) = 64.$$

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. *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*

$$\overline{N}_{d[p]} \equiv (p-1-2\left(\frac{d}{p}\right)+(-1)^{\frac{p+1}{2}}\sum_{j=0}^{\frac{p-1}{2}}(C^j_{\frac{p-1}{2}})^2 d^j) \equiv$$

$$\equiv ((-1)^{\frac{p+1}{2}}\sum_{j=0}^{\frac{p-1}{2}}(C^j_{\frac{p-1}{2}})^2 d^j - 1 - 2\left(\frac{d}{p}\right))(\operatorname{mod} p).$$

The true value of $\overline{N}_{d[p]}$ lies in $[4; 2p]$ and is even.

Proof. This result follows fro m the num ber of solutions of the equation $y^2=(x^2-1)(dx^2-1)$ over F_p which equals to

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

$$\equiv (\sum_{j=0}^{\frac{p-1}{2}}(x^2-1)^{\frac{p-1}{2}}(dx^2-1)^{\frac{p-1}{2}})(\operatorname{mod} p) \equiv$$

$$\equiv ((-1)^{\frac{p+1}{2}}\sum_{j=0}^{\frac{p-1}{2}}(C^j_{\frac{p-1}{2}})^2 d^j - (\frac{d}{p}))(\operatorname{mod} p).$$

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 $(\frac{d}{p})+1$ due to new solutions in the from $(\sqrt{d},0),(-\sqrt{d},0)$. So this quantity is such

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

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

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

$$\equiv (-1)^{\frac{p+1}{2}}\sum_{j=0}^{\frac{p-1}{2}}(C^j_{\frac{p-1}{2}})^2 d^j - (2(\frac{d}{p})+1)(\operatorname{mod} p).$$

According to Lemma 1 the last sum $(\sum_{j=0}^{\frac{p-1}{2}}(x^2-1)^{\frac{p-1}{2}}(dx^2-1)^{\frac{p-1}{2}})(\operatorname{mod} p)$ is congruent to $-a_{p-1}-a_{2p-2}(mod\ p)$, where a_i are the coefficients from presentation

$$(x^2-1)^{\frac{p-1}{2}}(dx^2-1)^{\frac{p-1}{2}} = a_0 + a_1x + ... + a_{2p-2}x^{2p-2}.$$

Last presentation was obtained due t o transformation

$$(x^2-1)^{\frac{p-1}{2}}(dx^2-1)^{\frac{p-1}{2}} = (\sum_{x=0}^{p-1}C^k_{\frac{p-1}{2}}x^{2k}(-1)^{\frac{p-1}{2}-k})$$

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

Therefore a_{2p-2} is equal to $d^{\frac{p-1}{2}} \equiv (\frac{d}{p})(\operatorname{mod} p)$ and $a_{p-1}=\sum_{j=0}^{\frac{p-1}{2}}(C^j_{\frac{p-1}{2}})^2 d^j(-1)^{\frac{p-1}{2}}$.

According to Newton's binom ial formula a_{p-1} equal to the coefficient at x^{p-1} in the product of two brackets and when substituting this d instead of 2 is such

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

that is, it has the form o f the poly nomial with inverse order of coef ficients. Indeed, we have equality

$$\sum_{j=0}^{\frac{p-1}{2}}d^j(C^{\frac{p-1}{2}-j}_{\frac{p-1}{2}})(-1)^{\frac{p-1}{2}-(\frac{p-1}{2}-j)}\cdot(C^j_{\frac{p-1}{2}})^2(-1)^{\frac{p-1}{2}-j} =$$

$$=(-1)^{\frac{p-1}{2}}\sum_{j=0}^{\frac{p-1}{2}}d^jC^{\frac{p-1}{2}-j}_{\frac{p-1}{2}}\cdot C^j_{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}\sum_{j=0}^{\frac{p-1}{2}}d^j(C^j_{\frac{p-1}{2}})^2.$$

In form of a su m it is the following

$$\sum_{j=0}^{\frac{p-1}{2}}2^j(C^{\frac{p-1}{2}-j}_{\frac{p-1}{2}})(-1)^{\frac{p-1}{2}-(\frac{p-1}{2}-j)}\cdot 2^j(C^j_{\frac{p-1}{2}})^2(-1)^{\frac{p-1}{2}-j} =$$

$$=(-1)^{\frac{p-1}{2}}\sum_{j=0}^{\frac{p-1}{2}}2^jC^{\frac{p-1}{2}-j}_{\frac{p-1}{2}}\cdot C^j_{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}\sum_{j=0}^{\frac{p-1}{2}}2^j(C^j_{\frac{p-1}{2}})^2.$$

over F_p equals to $p-1-2\left(\frac{d}{p}\right)+\left(1+(\frac{d}{p})\right)=p-\left(\frac{d}{p}\right)$ and differs fro m the quantity of solutions of $x^2+y^2=1+dx^2y^2$ by $(\frac{d}{p})+1$ due to new solutions of $y^2=(dx^2-1)(x^2-1)$. Thus, in general c ase if $a_{p-1}=\sum_{j=0}^{\frac{p-1}{2}}(C^j_{\frac{p-1}{2}})^2d^j(-1)^{\frac{p-1}{2}} \neq 0$ we have

$$N_{E_d} = (p-(\frac{d}{p})-((\frac{d}{p})+1)-(-1)^{\frac{p-1}{2}}\sum_{j=0}^{\frac{p-1}{2}}(C^{\frac{p-1}{2}-j}_{\frac{p-1}{2}}C^j_{\frac{p-1}{2}})^2d^j) \equiv$$

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

$$\equiv ((-1)^{\frac{p+1}{2}}\sum_{j=0}^{\frac{p-1}{2}}(C^j_{\frac{p-1}{2}})^2d^j-1-2(\frac{d}{p}))(\operatorname{mod} p).$$

The exact or der is not les s than 4 beca use cofactor of this curve is 4. To determine the order is uniquely enough to take into acco unt that p and $2p$ have different parity. Taking into account that the order is even we chose a term p or $2p$, for the su m which define the order.

Let us analyze the complexity of calculating the value of $\sum_{j=0}^{\frac{p-1}{2}}(C^j_{\frac{p-1}{2}})^2 d^j$. Binomial coefficients of the form $C^l_{\frac{p-1}{2}}$ we calculate recursively having $C^l_{\frac{p-1}{2}}$ we get $C^{l+1}_{\frac{p-1}{2}}$. 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 b oth cases, the co mplexity of calculating all the coeffici ents from the sum (3) is equal to $O(\frac{p-1}{2}\log_2^2 p)$. Squaring the calculated binomial coefficient $C^j_{\frac{p-1}{2}}$ also does not exceed $O\left(\log_2^2 p\right)$. Calculate all values of $d^j \bmod p$ optimally applying recursive multiplication d^{j-1} on d for thi s we use the Ka ratsuba multiplication method requiring $O(\log_2^{\log_2 3} p)$, than apply the Barrett method of modular multip lication. Therefore, the com plexity of computing th e entire tuple of degrees d^j, $j=1,....,n$ is $O(\frac{p-1}{2}\log_2^{\log_2 3} p)$. T otally we obtai n $O(\frac{p-1}{2}\log_2^2 p)$.

Theorem 2.6. *If* $\left(\frac{d}{p}\right)=1$, *then the orders of the curves* E_d *and* $E_{d^{-1}}$, *satisfies to the following relation* $|E_d|=|E_{d^{-1}}|$.

If $\left(\frac{d}{p}\right)=-1$, then E_d and $E_{d^{-1}}$ are pair of twisted curves i.e. orders of curves E_d and $E_{d^{-1}}$ satisfies to the following relation of duality

$$|E_d|+|E_{d^{-1}}|=2p+2.$$

Let the curve be defined b y $x^2+y^2=1+dx^2y^2(modp)$, then we can express y^2 in such way:

$$y^2 \equiv \frac{x^2-1}{dx^2-1}\left(mod\ p.\right) \tag{9}$$

For $x^2+y^2=1+d^{-1}x^2y^2(modp)$ we could obtai n that

$$y^2 \equiv \frac{x^2-1}{d^{-1}x^2-1}\left(mod\ p\right) \tag{10}$$

If $\left(\frac{d}{p}\right)=1$, then for the fixed x_0 a quantit y of y over F_p can be calcul ated by the for mula $(\frac{\frac{x^2-1}{d^{-1}x^2-1}}{p})+1$ for x such that $d^{-1}x^2+1\equiv 0(\bmod p)$. For solution (x_0,y_0) to (10), we have the equality $y_0^2 \equiv \frac{x_0^2-1}{dx_0^2-1}\left(mod\ p\right)$ and we express

$$y_0^2 \equiv \frac{1-\frac{1}{x_0^2}}{1-\frac{1}{dx_0^2}} d^{-1} \equiv \frac{\left(\frac{1}{x_0}\right)^2-1}{\frac{1}{d}\left(\frac{1}{x_0}\right)^2-1} d^{-1} \equiv \frac{\left(\frac{1}{x_0}\right)^2-1}{d^{-1}\left(\frac{1}{x_0}\right)^2-1} d^{-1}.$$

Observe that

$$y^2=\frac{x^2-1}{d^{-1}x^2-1}=\frac{1-x^2}{1-d^{-1}x^2}=\frac{(\frac{1}{x^2}-1)}{((\frac{d}{x^2})-1)}d. \tag{11}$$

Thus, if (x_0,y_0) is solution of (2), then $\left(\frac{1}{x_0},\frac{y_0}{\sqrt{d}}\right)$ is a solution to (10) because last transformations determines that $\frac{y_0^2}{d} \equiv \frac{d^{-1}\left(\frac{1}{x_0}\right)^2-1}{\left(\frac{1}{x_0}\right)^2-1} modp.$ Therefore last transformations $\left(x_0,y_0\right)\to(\frac{1}{x_0},\frac{y_0}{\sqrt{d}})=\left(x,y\right)$ determines isomorphism and bijection.

In case $\left(\frac{d}{p}\right)=-1$, then every $x\in\mathrm{F}_p$ 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 so lutions of (2) iff x_0^{-1} gives 0 solution s of (10) because of (11) yields the following relation

$$(\frac{\frac{x^2-1}{d^{-1}x^2-1}}{p})=(\frac{\frac{x^{-2}-1}{dx^{-2}-1}}{p})(\frac{d}{p})=-(\frac{\frac{x^{-2}-1}{dx^{-2}-1}}{p}). \tag{12}$$

Analogous reasons give us that x_0 give exactly one solution of (2) iff x_0^{-1} gives 1 solutions of (10). Consider the set $x\in\{1,2,....,p-1\}$ we obtain that the total amount of solution s of form (x_0^{-1},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_7 is $N_{7[13]}=20$. 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 $d=2^{-1}\equiv 4 \pmod 7$, then we have $(\frac{d}{p})=1$ 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 $d=2 \pmod 7$, 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 em bedding [14] for the grou p of supersingular curves $E_d[\mathrm{F}_p]$ 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 no t divide 12 and satisfi es the condition $q|\mathrm{P}_{12}(p)$, where $\mathrm{P}_{12}(x)$ is the cy clotomic polynomial. This p will satisfy the necessary conditions $(x^n-1)\nmid p$ 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 o rder of the group of a supersingular curve E_d is equal to p^k+1. It sho uld be observed that p^k+1 divides $p^{2k}-1$, but p^k+1 does not divide expressions of the form $p^{2l}-1$ with $l<k$. This division does not wo rk for smaller values of l due to the decomposition of the expression $p^{2k}-1=(p^k-1)(p^k+1)$. Therefore, we can use t he definition to conclude that the degree o f embedding must be 2, confirming the proposition.

Consider E_2 over F_{p^2}, for instance we assume $p=3$. We define F_9 as $\mathrm{F}_3(\alpha)$, where α is a root of $x^2+1=0$ over F_9. Therefore el ements of F_9 have form: $a+b\alpha$, where $a,b\in\mathrm{F}_3$. 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 $x^2=\alpha^2+2\alpha+1=2\alpha=-\alpha$. Also in this case

$$y^2=\frac{2\alpha-1}{\alpha-1}=\frac{(2\alpha-1)(\alpha+1)}{(\alpha-1)(\alpha+1)}=\frac{(2\alpha-1)(\alpha+1)}{(\alpha-1)(\alpha+1)}=\frac{\alpha}{-2}=\alpha.$$

Therefore the correspondent second coordinate is $y=\pm(\alpha-1)$. The si milar computations lead us to full the following list of curves points.

x	± 1	0	$\pm(\alpha+1)$	$\pm(\alpha-1)$
y	0	± 1	$\pm(\alpha-1)$	$\pm(\alpha+1)$

Table 2: Points of Edwards curve over square extension.

The total amount is 12 affine poin ts that confirms Corollary 2.4. and Theore m 2.3. because of $p^n-3-2(-p)^{\frac{n}{2}}=3^2-3-2(-3)=12$.

4 Conclusion

The new effective algorithm for the elli ptic and Edwards curves order curve counting was founded. The criterion for supersingularit y of t hese curves was additionally obtained.

References:

[1] Daniel J. Be rnstein, Peter Birkner, Marc Joy e, Tanja Lange, and Christ iane Peters. T wisted edwards curves. *Progress in Cryptology* -- AFRICACRYPT 2008 (6,5);(6,8);(7,5);, pp. 389--405, Berlin, Heidelberg, 2008.

[2] Don Johnson, Alfred Menezes, Scott Vanstone. The Elliptic Curve Digital Signature Algorithm. *International Journal of Information Security volume 1*, Springer, 2014, pp. 36–63.

[3] Harold Edwards. A normal form fo r 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.L.

[5] Neal Koblitz. Elliptic curve cryptos ystems. *Mathematics of computation*, 48(177):203--209, 1987.

[6] Rudolf Lidl and Harald Niederreiter. Introduction to Fi nite Fields and t heir Applications. *Cambridge university press*, 1994.

[7] Peter L Montgomery. Speeding the pollard and elliptic curve methods of factorization. *Mathematics of computation*, 48(177):243--264, 1987.

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

[9] Ruslan Viacheslavovich Skuratovskii. The order of projective edwards curve ove r an d embedding degree of this curve in finite field. In Cait 2018, pp. 75 -- 80, 2018.

[10] Ruslan Viacheslavovich Skur atovskii. Supersingularity of elliptic curves. *Research in Mathematics and Mechanics*, 31(1):17--26, 2018.

[11] Ruslan Viacheslavovich Skur atovskii. Employment of m inimal generating sets and structure of sy low 2-subgroups alternating groups in block ciphers. *In Advances in Computer Communication and Computational Sciences*, pages 351--364. Springer, 2019.

[12] Serge Aleksandrovich Stepanov. Arifmetika algebraicheskikh krivykh (in Russian). *Nauka,* Glav. red. fiziko-matematichesko lit-ry, 1991.

[13] Ivan Matveevich Vinogradov. Elements of number theory. Courier Dover Publ ications, 2016.

[14] Paulo S. L. M. Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. Springer, *Selected Areas in Cryptography*, pages 319--331, Berlin, Heidelberg, 2006.

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

[16] P.D Varbanec, P Zarzycki. Divisors of the Gaussian integers in an ar ithmetic progression. *Journal of Number Theory.* Volume 33, Issue 2, October 1989, Pages 152-169

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

[18] R. V. Skuratovskii, Aled William s (2019) "A solution of the inverse problem to doubling of twisted Edwards curve poi nt over finite field", *Processing, transmission and security of information* - 2019 vol. 2,

[19] Deligne, Pierre. La conjecture de Weil, *Publications Mathematiques de l'IHES*. 1974. Vol. 43. pp. 273-307.IEEE

[20] R. V. Skura tovskii, Employment of Minimal Generating Sets and Structure of S ylow 2-Subgroups Alternating Groups in Block Ciphers. Springer, *Advances in Computer Communication and Computational Sciences*, 2019, pp. 351-364.

[21] R. Skuratovskii, The Derived Subgr oups of Sylow 2-Subgroups of the Alternating Group and Comm utator Width of Wreath Pr oduct of Groups. *Mathematics, Basel, Switzerland,* (2020) *№ 8(4),* pp. 1-19.

[22] Craig Costello, Benjam in Smith Montgom ery curves and their arit hmetic. *Journal of Cryptographic Engineering* volume 8 no.3, pp. 227–240 (2018).

[23] Andrea Bandini, Laur a Paladino. Fields generated by torsion poi nts of ellipti c curves 2016 *Journal of Number Theory* 169: pp. 10 3-133.

[24] Daniele di Tullio, Manoj Gy awali. Elliptic curves of nearly prime order. pp. 1-19. [Source: iacr.org], access mode: https://eprint.iacr.org/2020/001.pdf

[25] Craig Costello. Com puting Supersingular Isogenies on Kummer Surfaces. Springer. Advances in Cryptology 24 *International conference in Theory Cryptography*, Part 3.– ASIACRYPT 2018. pp. 428-440.