

# Elliptic and Edwards curves order counting method

Ruslan Skuratovskii  
 Interregional Academy of Personnel Management,  
 Kiev, Ukraine

Volodymyr Osadchyy  
 Dept. of computer science UCF,  
 Florida, USA

Received: January 26, 2021. Revised: March 26, 2021. Accepted: March 30, 2021. Published: April 5, 2021.

**Abstract**—We consider the algebraic affine and projective curves of Edwards over the finite field  $\mathbb{F}_{p^n}$ . It is well known that many modern cryptosystems can be naturally transformed into elliptic curves. In this paper, we extend our previous research into those Edwards algebraic curves over a finite field. We propose a novel effective method of point counting for both Edwards and elliptic curves. In addition to finding a specific set of coefficients with corresponding field characteristics for which these curves are supersingular, we also find a general formula by which one can determine whether or not a curve  $E_d[\mathbb{F}_p]$  is supersingular over this field. The method proposed has complexity  $\mathcal{O}(p \log_2^2 p)$ . This is an improvement over both Schoof's basic algorithm and the variant which makes use of fast arithmetic (suitable for only the Elkis or Atkin primes numbers) with complexities  $\mathcal{O}(\log_2^8 p^n)$  and  $\mathcal{O}(\log_2^4 p^n)$  respectively. The embedding degree of the supersingular curve of Edwards over  $\mathbb{F}_{p^n}$  in a finite field is additionally investigated. Due existing the birational isomorphism between twisted Edwards curve and elliptic curve in Weierstrass normal form the result about order of curve over finite field is extended on cubic in Weierstrass normal form.

**Keywords:** finite field, elliptic curve, Edwards curve, group of points of an elliptic curve

## I. INTRODUCTION

In order to construct a cryptosystem based on an elliptic curve, we need to firstly analyze the order of a group of elliptic curve (EC) points. We provides an approach to construct Edwards curves of determined order, which are important within the cryptography and coding theory domains. It should be noted that it was accepted in 1999 as an ANSI standard and in 2000 as an IEEE and NIST standard. One of the fundamental problems in EC cryptography regards the generation of cryptographically secure ECs over prime fields, suitable for use in various cryptographic applications. Because supersingular elliptic curves are vulnerable to pairing-based attacks, we find a criterion for Edwards curve supersingularity [11]. The method of finding the order of an algebraic curve over a finite field  $\mathbb{F}_{p^n}$  is of huge interest currently and is at the center of many mathematical studies connected with the use of groups of points of curves of genus 1. In this article, this critical problem is solved. All proofs and analytical results belong to Skuratovskii R. and computational examples, confirming statements, are made by other authors.

Our algorithm has improved complexity for algebraic extensions with a large degree over finite fields. This is because upon choosing sufficiently large values  $n$ , we ob-

tain  $\mathcal{O}(\log_2^8 p^n)$ , which has a much larger complexity than  $\mathcal{O}(p \log_2^2 p)$  for some fixed  $p$ .

## II. MATERIALS AND METHODS

The method of finding the order of an algebraic curve over a finite field  $\mathbb{F}_{p^n}$  is clearly related with constructing curves of a given order. We propose a method for counting points from Edwards and elliptic curves in direct response to a paper by Schoof [9]. To calculate the sum of the squares of binomial coefficients in a finite modulus, we make use of the recursive calculation of the factorial by multiplication. The method we propose has improved complexity over both Schoof's basic algorithm and the variant which makes use of fast arithmetic (suitable only for Elkis or Atkin primes numbers) with complexities  $\mathcal{O}(\log_2^8 p^n)$  and  $\mathcal{O}(\log_2^4 p^n)$  respectively.

In particular, our method yields a vastly improved complexity for algebraic extensions with large degree  $n$  of finite fields. This occurs because when choosing sufficiently large values  $n$ , Schoof's algorithm has complexity  $\mathcal{O}(\log_2^8 p^n)$  [9], which clearly is much larger than  $\mathcal{O}(p \log_2^2 p)$  for fixed  $p$ .

Let  $d$  denote some large number. The method of Karatsuba multiplication is used to calculate all the values  $d^j \pmod{p}$ . In this task, it is optimally applying recursive multiplication  $d^{j-1}$  upon  $d$  and for this we utilise the Karatsuba multiplication method, which requires  $\mathcal{O}(\log_2^{\log_2 3} p)$ , rather than apply the Barrett method of modular multiplication. The complexity of computing the entire tuple of degrees  $d^j$ ,  $j = 1, \dots, n$  is therefore  $\mathcal{O}(\frac{p-1}{2} \log_2^{\log_2 3} p)$ .

## III. REVIEW OF PREVIOUS RESULTS

It is known that the theoretical results of S. Stepanov [14] and P. Deligne provide both upper and lower bounds for the number of curve points, that is  $p^n + 1 - \omega_1^n - \omega_2^n$  [23]. The complexity of the fastest algorithms known are Schoof's basic algorithm [9], which yields  $\mathcal{O}(\log_2^8 p^n)$ , as well as a variant that makes use of fast arithmetic (suitable only for Elkis or Atkin primes), which has complexity  $\mathcal{O}(\log_2^4 p^n)$ . Our method is faster than the approach to order curve determination by counting of a longest chain of points using dividing of a point on 2 [21].

IV. SYSTEMATIC ALGEBRAIC ANALYSIS OF THE CURVE AND CURVE ORDER CALCULATION METHOD

The twisted Edwards curve with coefficients  $a, d \in F_p^*$ , is the curve  $E_{a,d}$  :

$$ax^2 + y^2 = 1 + dx^2y^2,$$

where  $ad(a - d) \neq 0, d \neq 1, p \neq 2$  and  $a \neq d$ . It should be noted that a twisted Edwards curve is simply called an Edwards curve when  $a = 1$ . By  $E_d$ , we denote the Edwards curve with coefficient  $d \in F_p^*$  defined as

$$x^2 + y^2 = 1 + dx^2y^2,$$

over  $F_p$ . The projective curve has the form

$$F(x, y, z) = ax^2z^2 + y^2z^2 = z^4 + dx^2y^2.$$

The special points are the infinitely distant points  $(1, 0, 0)$  and  $(0, 1, 0)$  and we find its singularities at infinity in the corresponding affine components  $A^1 := az^2 + y^2z^2 = z^4 + dy^2$  and  $A^2 := ax^2z^2 + z^2 = z^4 + dx^2$ . These are entitled the simple singularities.

We describe the structure of the local ring at the point  $p_1$ , whose elements are quotients of functions with the form  $F(x, y, z) = \frac{f(x,y,z)}{g(x,y,z)}$ , where the denominator cannot take value 0 at the singular point  $p_1$ . In particular, it should be noted that a local ring with two singularities consists of those functions with denominators which are not divisible by  $(x - 1)(y - 1)$ .

We denote by  $\delta_p = \dim \frac{\overline{\mathcal{O}_p}}{\mathcal{O}_p}$ , where  $\mathcal{O}_p$  denotes the local ring at the singular point  $p$  generated by the relations of regular functions

$$\mathcal{O}_p = \left\{ \frac{f}{g} : (g, (x - 1)(y - 1)) = 1 \right\}$$

and  $\overline{\mathcal{O}_p}$  denotes the whole closure of the local ring at the singular point  $p$ .

We find that  $\delta_p = 1$  is the dimension of the factor as a vector space because the basis of extension  $\frac{\overline{\mathcal{O}_p}}{\mathcal{O}_p}$  consists of just one element at each distinct point. We then calculate the genus of the curve according to Fulton [4], namely

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

$$\rho^*(C) = 3 - 2 = 1,$$

where  $\rho_\alpha(C)$  denotes the arithmetic genus of the curve  $C$  with parameter  $n = \deg(C) = 4$ . It should be noted for completeness that the supersingular points were discovered in [11]. Recall that the curve has a genus of 1 and in consequence, it is known to be isomorphic to a flat cubic curve. Despite this, 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.

Koblitz [4], [6] 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. In addition, 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  $p$  [18]. It is known [1] that the transition from an Edwards curve to the related torsion curve is determined by the reflection  $(\bar{x}, \bar{y}) \mapsto (x, y) = \left(\bar{x}, \frac{1}{\bar{y}}\right)$ .

We now recall an important result from Vinogradov [15] which will act as criterion for supersingularity.

**Lemma 1:** Let  $k \in \mathbb{N}$  and  $p \in \mathbb{P}$ . Then

$$\sum_{k=1}^{p-1} k^n \equiv \begin{cases} 0 \pmod{p}, & n \not\equiv (p-1), \\ -1 \pmod{p}, & n \equiv (p-1), \end{cases}$$

where  $n \equiv (p - 1)$  means 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.

We will now strengthen an existing result given in [11]–[14], [22]. Let  $N_{d[p]}$  denote the number of points with a neutral element of an affine Edwards curve over the finite field  $F_p$  and let  $\overline{N}_{d[p]}$  denote the number of points on the projective curve over the same field.

**Theorem 1:** If  $p \equiv 3 \pmod{4}$  is prime and

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

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

$$N_{d[p]} = p + 1,$$

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

$$N_{d[p]} = p - 3,$$

if  $\left(\frac{d}{p}\right) = 1$ .

*Proof:* Consider the Edwards curve  $E_d$ , namely

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

We transform (2) into the form  $y^2(1 - dx^2y^2) = 1 - x^2$  and then we express  $y^2$  by applying a rational transformation, which leads to  $y^2 = \frac{1-x^2}{1-dx^2y^2}$ . For technical reasons, we transform this into the curve

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

Let  $M_{d[p]}$  denote the number of points from an affine Edwards curve over the finite field  $F_p$ . The curve (3) has precisely  $M_{d[p]} = N_{d[p]} + \left(\frac{d}{p}\right) + 1$  points. This is exactly  $\left(\frac{d}{p}\right) + 1$  greater than the number of points of  $E_d$ , where  $\left(\frac{d}{p}\right)$  denote

the Legendre Symbol. Let  $a_0, a_1, \dots, a_{2p-2}$  be the coefficients of the polynomial  $a_0 + a_1x + \dots + a_{2p-2}x^{2p-2}$ , which was obtained from  $(x^2 - 1)^{\frac{p-1}{2}}(dx^2 - 1)^{\frac{p-1}{2}}$  after opening the brackets.

Upon summing over all  $x$ , we yield that

$$\begin{aligned} M_{d[p]} &= \sum_{x=0}^{p-1} 1 + ((x^2 - 1)(dx^2 - 1))^{\frac{p-1}{2}} = \\ &= p + \sum_{x=0}^{p-1} (x^2 - 1)^{\frac{p-1}{2}} (dx^2 - 1)^{\frac{p-1}{2}} \equiv \\ &\equiv \sum_{x=0}^{p-1} (x^2 - 1)^{\frac{p-1}{2}} (dx^2 - 1)^{\frac{p-1}{2}} \pmod{p}. \end{aligned}$$

By opening the brackets in  $(x^2 - 1)^{\frac{p-1}{2}}(dx^2 - 1)^{\frac{p-1}{2}}$ , we have that  $a_{2p-2} = (-1)^{\frac{p-1}{2}} \cdot d^{\frac{p-1}{2}} \equiv \left(\frac{d}{p}\right) \pmod{p}$ . In light of Lemma IV, we have

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

Recall that we need to prove that  $M_{d[p]} \equiv 1 \pmod{p}$  if  $p \equiv 3 \pmod{8}$  and  $M_{d[p]} \equiv -1 \pmod{p}$  if  $p \equiv 7 \pmod{8}$ . Therefore, we have to show that  $M_{d[p]} \equiv -\left(\frac{d}{p}\right) - a_{p-1} \pmod{p}$  for  $p \equiv 3 \pmod{4}$  if  $\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 d^j \equiv 0 \pmod{p}$ . It should be noted that if we prove that  $a_{p-1} \equiv 0 \pmod{p}$ , then the result will follow from (3). We now determine  $a_{p-1}$  using Newton's binomial formula. In particular, the coefficient of  $x^{p-1}$  in the polynomial, namely  $a_{p-1}$ , is obtained from the product  $(x^2 - 1)^{\frac{p-1}{2}}(dx^2 - 1)^{\frac{p-1}{2}}$ . Therefore,  $a_{p-1} = (-1)^{\frac{p-1}{2}} \sum_{j=0}^{\frac{p-1}{2}} d^j (C_{\frac{p-1}{2}}^j)^2$ . Instead of this equality, we notice that the following equality holds:

$$\begin{aligned} &\sum_{j=0}^{\frac{p-1}{2}} d^j (C_{\frac{p-1}{2}}^{\frac{p-1}{2}-j}) (-1)^{\frac{p-1}{2} - (\frac{p-1}{2}-j)} \cdot d^j (C_{\frac{p-1}{2}}^j)^2 (-1)^{\frac{p-1}{2}-j} \\ &= (-1)^{\frac{p-1}{2}} \sum_{j=0}^{\frac{p-1}{2}} d^j C_{\frac{p-1}{2}}^{\frac{p-1}{2}-j} \cdot C_{\frac{p-1}{2}}^j = (-1)^{\frac{p-1}{2}} \sum_{j=0}^{\frac{p-1}{2}} d^j (C_{\frac{p-1}{2}}^j)^2. \end{aligned}$$

Noting that  $a_{p-1} = -\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 d^j$  means that the exact number of affine points on a non-supersingular curve is

$$M_{d[p]} \equiv -a_{2p-2} - a_{p-1} \equiv -\left(\frac{d}{p}\right) + \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 d^j \pmod{p}. \quad (5)$$

In accordance with the condition of this theorem, we have  $a_{p-1} = 0$  and therefore  $M_{d[p]} \equiv -a_{2p-2} \pmod{p}$ . In

consequence, if  $p$  is a prime such that  $p \equiv 3 \pmod{4}$  and  $\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 d^j \equiv 0 \pmod{p}$  holds, then the curve  $E_d$  has

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

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

The exact number of the points yields an upper bound of  $2p + 1$  since each  $x \neq 0$  corresponds two values of  $y$ , while, for  $x = 0$ , we have only that  $y = 0$ . Taking into account that  $x \in F_p$ , we have exactly  $p$  values of  $x$ . In addition, there are 4 pairs  $(\pm 1, 0)$  and  $(0, \pm 1)$ , which are points of  $E_d$ , thus  $N_{d[p]} > 1$ . In consequence,  $N_{d[p]} = p + 1$ , which completes the proof.

**Corollary 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

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

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

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

if  $\left(\frac{d}{p}\right) = 1$ , if and only if  $p$  is a prime with  $p \equiv 3 \pmod{4}$  and

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

**Theorem 2:** If the coefficient  $d = 2$  or  $d = 2^{-1}$  and  $p \equiv 3 \pmod{4}$ , then

$$\sum_{j=0}^{\frac{p-1}{2}} d^j (C_{\frac{p-1}{2}}^j)^2 \equiv 0 \pmod{p} \text{ and } \overline{N}_{d[p]} = p + 1.$$

*Proof:* When  $p \equiv 3 \pmod{4}$ , we firstly shall show that  $\sum_{j=0}^{\frac{p-1}{2}} d^j (C_{\frac{p-1}{2}}^j)^2 \equiv 0 \pmod{p}$ . We multiply each binomial coefficient in this sum by  $(\frac{p-1}{2})!$  to obtain after some algebraic manipulation  $(\frac{p-1}{2})! C_{\frac{p-1}{2}}^j = \frac{(\frac{p-1}{2})(\frac{p-1}{2}-1)\dots(\frac{p-1}{2}-j+1)(\frac{p-1}{2})!}{1 \cdot 2 \cdot \dots \cdot j} = (\frac{p-1}{2})(\frac{p-1}{2}-1)\dots(\frac{p-1}{2}-j+1)[(\frac{p-1}{2})(\frac{p-1}{2}-1)\dots(j+1)]$ . After applying the congruence  $(\frac{p-1}{2} - k)^2 \equiv (\frac{p-1}{2} + 1 + k)^2 \pmod{p}$  with  $0 \leq k \leq \frac{p-1}{2}$  to the multipliers in previous parentheses, we obtain  $[(\frac{p-1}{2})(\frac{p-1}{2}-1)\dots(j+1)]$ . It yields

$$\begin{aligned} &\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}-1\right)\dots\left(\frac{p-1}{2}-j+1\right)\left[\left(\frac{p-1}{2}+1\right)\dots\right. \\ &\quad \left.\dots\left(\frac{p-1}{2}+\frac{p-1}{2}-j\right)\right](-1)^{\frac{p-1}{2}-j}. \end{aligned}$$

Thus, as a result of squaring, we have:

$$\left(\left(\frac{p-1}{2}\right)! C_{\frac{p-1}{2}}^j\right)^2 \equiv \left(\frac{p-1}{2} - j + 1\right)^2. \quad (6)$$

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

It remains to prove that

$$\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 2^j \equiv 0 \pmod{p},$$

if  $p \equiv 3 \pmod{4}$ .

Consider the auxillary polynomial

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

We are going to show that  $P(2) = 0$  and therefore  $a_{p-1} \equiv 0 \pmod{p}$ . Using (6) it can be shown that  $a_{p-1} = P(t) = \left(\frac{p-1}{2}!\right)^2 \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 t^j \equiv \sum_{j=0}^{\frac{p-1}{2}} (k+1)^2 (k+2)^2 \cdots \left(\frac{p-1}{2} + k\right)^2 t^k \pmod{p}$  over  $F_p$ .

We replace  $d$  by  $t$  in (1) such that we can research a more generalised problem. It should be noted that  $P(t) = \partial^{\frac{p-1}{2}} \left( \partial^{\frac{p-1}{2}} (Q(t) t^{\frac{p-1}{2}}) \right)$  over  $F_p$ , where  $Q(t) = t^{p-1} + \cdots + t + 1$  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  $Q(t) = \frac{t^p-1}{t-1} \equiv \frac{(t-1)^p}{t-1} \equiv (t-1)^{p-1} \pmod{p}$  and therefore the following equality

$$P(t) = \left( ((t-1)^{p-1} t^{\frac{p-1}{2}})^{\left(\frac{p-1}{2}\right)} t^{\frac{p-1}{2}} \right) \text{ holds over } F_p.$$

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  $\theta$  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

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

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

$$R(1) = \frac{(p-1)!}{\left(\frac{p-1}{2}!\right)^2} \sum_{j=0}^{\frac{p-1}{2}} C_{\frac{p-1}{2}}^j (j+1) \cdots \left(j + \frac{p-1}{2}\right). \quad (7)$$

We now will manipulate with the expression  $\left(\frac{p-1}{2} - j + 1\right) \left(\frac{p-1}{2} - j + 2\right) \cdots \left(\frac{p-1}{2} - j + \frac{p-1}{2}\right)$ . 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  $(5-j+1)(5-j+2) \cdots (5-j+5) = (6-j)(7-j) \cdots (10-j) \equiv ((-5-j)(-4-j) \cdots (-1-j)) \equiv (-1)^5 ((j+1)(j+2) \cdots (j+5)) \pmod{11}$ .

Therefore, for a prime  $p$ , we can rewrite the expression as  $\left(\frac{p-1}{2} - j + 1\right) \left(\frac{p-1}{2} - j + 2\right) \cdots \left(\frac{p-1}{2} - j + \frac{p-1}{2}\right) \equiv (-1)^{\frac{p-1}{2}} (j+1) \cdots \left(j + \frac{p-1}{2}\right) \equiv -1(j+1) \cdots \left(j + \frac{p-1}{2}\right) \pmod{p}$ .

As a result, the symmetrical terms in (7) can be reduced yielding  $a_{p-1} \equiv 0 \pmod{p}$ . 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  $a_{p-1} \equiv 0 \pmod{p}$  as required. Thus,  $\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 \equiv 0 \pmod{p}$ , completing the proof of the theorem.

**Corollary 2:** The curve  $E_d$  is supersingular iff  $E_{d-1}$  is supersingular.

*Proof:* Let us recall the proved fact in Theorem IV that  $N_{d[p]} \equiv -a_{2p-2} - a_{p-1} \equiv -\left(\frac{d}{p}\right) + \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 d^j \pmod{p}$ .

Since  $(C_{\frac{p-1}{2}}^j)^2 d^j \equiv 0 \pmod{p}$  by condition, and the congruence  $\left(\frac{d}{p}\right) \equiv \left(\frac{d-1}{p}\right)$  holds, then  $N_{d[p]} \equiv N_{d-1[p]}$ .

Now we estimate the number of points on the curve (3). Let  $M_{d[p]}$  denote the number of solutions to equation (3) over the field  $F_p$ . It should be observed that for  $x = 1$  and  $x = -1$ , the right side of (3) is equal to 0. Due to this the number  $M_{d[p]}$  can therefore be bounded by

$$2 \leq M_{d[p]} \leq 2p - 2, \quad (8)$$

where if  $a_{p-1} \equiv 0 \pmod{p}$  we have  $N_{d[p]} \equiv -\left(\frac{d}{p}\right) \pmod{p}$ . Note that the number of solutions is bounded by  $N_{d[p]} \leq 2p - 2$  because if  $x = 1$  and  $x = -1$  we only have one value of  $y$ , namely  $y = 0$ . For different values of  $x$ , we will have no more than two solutions for  $y$  because the equation (3) is quadratic relative to  $y$ . Thus, the only possible number is  $M_{d[p]} \equiv p - \left(\frac{d}{p}\right) \pmod{p}$ .

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

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

IV as well as from Corollary 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  $T \in \mathbb{Z}$ , such that  $T < 2\sqrt{p}$  and  $N_{d[p]} = p - 1 - 2\left(\frac{d}{p}\right) + T$ .

*Example 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  $N_{7[13]} = 20$ . Moreover, if  $p \equiv 7 \pmod{8}$ , then the order of torsion subgroup of curve is  $N_2 = N_{2-1} = p - 3$ , which is clearly different to  $p + 1$ .

For instance  $p = 31$ , then  $N_{2[31]} = N_{2-1[31]} = 28 = 31 - 3$ , which is clearly not equal to  $p + 1$ . If  $p = 7$ ,  $d = 2^{-1} \equiv (4 \pmod{7})$  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  $d = 2 \pmod{7}$ , 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 3:** Let  $d$  satisfy the condition of supersingularity (1). If  $n \equiv 1 \pmod{2}$  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  $n \equiv 0 \pmod{2}$  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

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

*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  $\mathbb{F}_p$ . To make the proof, we take into account that it is known [14] that the number of solutions to  $y^2 = P(x)$  over  $\mathbb{F}_{p^n}$  will have the form  $p^n + 1 - \omega_1^n - \dots - \omega_{m-1}^n$  where  $\omega_1, \dots, \omega_{m-1} \in \mathbb{C}$ ,  $|\omega_i| = p^{\frac{1}{2}}$ .

In case of our supersingular curve, if  $n \equiv 1 \pmod{2}$  the number of points on projective curve over  $\mathbb{F}_{p^n}$  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 [7], [14] that  $|\omega_i| = p^{\frac{1}{2}}$ . 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 [11] 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  $p \equiv 3 \pmod{8}$ , 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 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 the curve is  $p^n + 1 - \omega_1^n - \omega_2^n$  [25].

For  $n \equiv 0 \pmod{2}$  we always have, that every  $d \in F_p$  is a quadratic residue in  $F_{p^n}$ . 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.  $N_{d[p^n]} = p^n - 1 - 2\left(\frac{d}{p}\right) - 2(-p)^{\frac{n}{2}} = p^n - 3 - 2(-p)^{\frac{n}{2}}$ . In more details  $\omega_1, \omega_2$  are eigen values of the Frobenius operator  $F$  endomorphism on étale cohomology over the finite field  $\mathbb{F}_{p^n}$ , where  $F$  acts of  $H^i(X)$ . The number of points, in general case, are determined by Lefschitz formula:

$$\#X(\mathbb{F}_{p^n}) = \sum (-1)^i \text{tr}(F^n | H^i(X)),$$

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

**Lemma 2:** There exists birational isomorphism of  $E_d$  with  $E_M$  and with elliptic curve in canonical Weierstrass form  $E_{a,b}$ , which is determined by correspondent mappings  $x = \frac{1+u}{1-u}$ ,  $y = \frac{2u}{v}$  and Velu formulas [24], over finite field  $F_{p^n}$ .

*Proof:* To verify this statement in both the supersingular case and the non-supersingular case and in also for both values of the quadratic residue  $\frac{d}{p}$  we the birational equivalence  $(u, v) \mapsto (2u/v, (u-1)/(u+1)) = (x, y)$  between  $E_M$  and  $E_d$ . 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  $F_p$ .

In non-supersingular case the curve  $E_d$  has order

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

if  $n \equiv 1 \pmod{2}$  and  $p$  is prime and the order of curve is equal to If  $n \equiv 0 \pmod{2}$  and  $p$  is prime, then the order of curve

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

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 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  $p + 1 - 2 + 1 = p$ . The table of correspondence between points is the following.

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

TABLE I  
 SPECIAL POINTS OF BIRATIONAL MAPPING

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  $v^2 = (d-1)u^3 + 2(d+1)u^2 + (d-1)u$ . Therefore the corresponding point  $(u, v)$  will not be a solution to the equation  $v^2 = (d-1)u^3 + 2(d+1)u^2 + (d-1)u$ , since there will be an element on the left side, different from 0, and on the right will be 0. That is a contradiction as required, therefore  $(x, y) = (1, 0)$  is the special point having not image on  $E_M$ .

If  $y = 0$  then in equality  $y = \frac{2u}{v}$  appear zeros in numerator and denominator and transformation is not correct.

The points  $\left(\frac{-(d+1)-2\sqrt{d}}{d-1}, 0\right)$ ,  $\left(\frac{-(d+1)+2\sqrt{d}}{d-1}, 0\right)$ ,  $(1, -2\sqrt{d})$ ,  $(1, 2\sqrt{d})$  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  $F_q$ . The points  $(1, -2\sqrt{d})$ ,  $(1, 2\sqrt{d})$  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  $\left(\frac{-(d+1)-2\sqrt{d}}{d-1}, 0\right)$ ,  $\left(\frac{-(d+1)+2\sqrt{d}}{d-1}, 0\right)$  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  $E_M$  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 an Montgomery curve. Thus, the order of  $E_M$  is equal  $p + 1$  in this case as supersingular curve has.

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 [8], [14], to the case  $y^2 = P(x)$ , where  $\deg P(x) = m$ ,  $m = 3$ . The order  $N_{M[p^n]}$  of the curve  $E_M$  over  $F_{p^k}$  can be evaluated due to Stepanov [14]. The research tells us that the order is  $\bar{N}_{M[p^n]} = p^n + 1 - \omega_1^n - \omega_2^n$ , 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  $n \equiv 1 \pmod{2}$ , 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  $\mathbb{F}_{p^n}$  are determined by the expression  $p^n + 1 - \omega_1^n - \omega_2^n$  if  $n \equiv 1 \pmod{2}$ .

Consider a more general case, namely the transition from a twisted Edwards curve to  $E_M$ .

Firstly the Edwards curve by a rational transformation

$$\psi_1(x, y) = \left( (a-d)\frac{1+u}{1-v}, (a-d)\frac{2u}{y} \right) = \left( (a-d)x, (a-d)y \right) = (u, v). \tag{9}$$

is transformed into the birationally equivalent Montgomery form

$$v^2 = u^3 - 2(a+d)u^2 + (a-d)u. \tag{10}$$

The point  $(0,0)$  is the second-order point of this curve, which, together with the point at infinity as a neutral element of the group, forms the kernel of the 2-isogeny. It is required to find parameters  $\bar{a}$  and  $\bar{d}$  of the isogenous curve with equation (10) and the rational function  $2(x, y) = (X, Y)$ . For the Montgomery curve in the general form

$$M_{cb} : y^2 = x^3 + cx^2 + bx, \tag{11}$$

finding 2-isogeny is well known [24]. Based on the Velu formulas, using the laws of the addition of the points of the curve in the general Weierstrass form, for the curve (11) one can obtain the 2-isogeny ( [24]. the example 12.4)

$$\psi_2(u, v) = \left( \frac{u^2+cu+b}{u}, \frac{u^2-b}{u^2}v \right) = (X, Y) \tag{12}$$

as a result the equation of the isogenous curve is the following:

$$Y^2 = X^3 - 2cX^2 + (c^2 - 4b)X. \quad (13)$$

The discriminant of the quadratic equation on the right-hand side of (13) is  $\delta = 16b$ , and depending on the meaning of (b), the curve (11) has one or three points of the  $2^{nd}$  order. In the first case, one can construct one 2-isogeny. in the two-three points (for three kernels as subgroups of the second-order). The main aim of this work is the goal of the existence of correspondence of orders via birational equivalence in two classes of Edwards curves where values of the quadratic residue  $\left(\frac{d}{p}\right)$  1 and -1.

For twisted Edwards curve  $E_{a,d}$  as follows from equations of  $E_M$  and  $E_{a,b}$ , only those curves  $E_{a,d}$  of general (canonical) form can be reduced to the Montgomery form (1) (and, accordingly, to the Edwards form), the parameter  $b$  of which is the quadratis square  $\left(\frac{b}{p}\right) = 1$ ). This is connected with the existence on the curve canonical elliptic curve  $E_{a,b}$  the points of the  $4^{th}$  order  $F = (u_1, v_1)$ , such that  $2F = (0, 0)$ . Then, taking  $b = u_1^2$ , equation (11) after replacement  $c \rightarrow Cu_1$  is reduced to the form

$$v^2 = u^3 + Cu_1u^2 + u_1^2u. \quad (14)$$

The inverse transformation of isogenous curves after the substitution  $c \rightarrow Cx_1$  in  $E_{a,d}$  in the Montgomery form into the Edwards form  $E_{a,ad}$  is performed based on rational functions this Lemma taking into account different values of coordinates of points of the  $4^{th}$  order  $\pm X_1 \in 4a\sqrt{d}, 4a\sqrt{1-d}, 4a\sqrt{d(d-1)}$  or  $\pm X_1 = \bar{a} - \bar{d}$  with the help of rational function.

*Example:* 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 4.:** If  $d = 2$ ,  $n \equiv 1(\text{mod } 2)$  and  $p \equiv 3(\text{mod } 8)$ , then the order of curve  $E_d$  and order of the projective curve are the following:

$$\bar{N}_{d[p^n]} = p^n + 1.$$

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

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

and the number of points on affine curve  $E_d$  is also

$$N_{d[p^n]} = p^n - 3.$$

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

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

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

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

*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 [7] as  $N_{M[p^n]} = p^n + 1 - \omega_1^n - \omega_2^n$ , where  $\omega_i^n \in \mathbb{C}$  and  $\omega_1^n = -\omega_2^n$ ,  $|\omega_i| = \sqrt{p}$  with  $i \in \{1, 2\}$ . For the finite algebraic extension of degree  $n$ , we will consider  $p^n - \omega_1^n - \omega_2^n = p^n$  if  $n \equiv 1(\text{mod } 2)$ . Therefore, for  $n \equiv 1(\text{mod } 2)$ , 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  $\omega_1 = \bar{\omega}_2$  by [6], 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  $\bar{N}_{d[p^2]} = p^2 + 1 + 2p = (p + 1)^2$  with respect to Lagrange theorem have to be divisible on  $\bar{N}_{d[p]}$ . Because a group of  $E_d(F_{p^2})$  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  $E_d(F_{p^2})$  holds because in our case  $p = 7$  thus  $\bar{N}_{E_d} = 8^2$  and  $p + 1 = 8 = N_{d[7]}$  [17].

The following two examples exemplify Corollary 4.

*Example:* If  $p \equiv 3(\text{mod } 8)$  and  $n = 2k$  then we have when  $d = 2$ ,  $n = 2$ ,  $p = 3$  that the number of affine points equals to

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

and the number of projective points is equal to

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

*Example:* If  $p \equiv 7(\text{mod } 8)$  and  $n = 2k$  then we have when  $d = 2$ ,  $n = 2$ ,  $p = 7$  that the number of affine points equals to

$$N_{2[7]} = p^n - 3 - 2(-p)^{\frac{n}{2}} = 7^2 - 3 - 2 \cdot (-7) = 60,$$

and the number of projective points is equal to

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

**Proposition 1:**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  $2\left(\frac{d}{p}\right) + 2$ .

*Proof:* The singular points were discovered in [11] and hence if the curve is free of singular points then the group order is  $p + 1$ .

*Example:* 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 4:** The order of projective Edwards curve over  $F_p$  is congruent to

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

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

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

$$y^2 = (dx^2 - 1)(x^2 - 1) \text{ over } F_p \text{ which equals to}$$

$$\begin{aligned} & \sum_{x=0}^{p-1} \left( \frac{(x^2 - 1)(dx^2 - 1)}{p} + 1 \right) \equiv \\ & \equiv \sum_{x=0}^{p-1} \left( \frac{(x^2 - 1)(dx^2 - 1)}{p} \right) + p \equiv \\ & \equiv \left( \sum_{j=0}^{\frac{p-1}{2}} (x^2 - 1)^{\frac{p-1}{2}} (dx^2 - 1)^{\frac{p-1}{2}} \right) \pmod{p} \equiv \\ & \equiv \left( (-1)^{\frac{p+1}{2}} \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 d^j - \left( \frac{d}{p} \right) \right) \pmod{p}. \end{aligned}$$

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

$$\begin{aligned} & \sum_{x=0}^{p-1} \left( \frac{(x^2 - 1)(dx^2 - 1)}{p} + 1 \right) - \left( \left( \frac{d}{p} \right) + 1 \right) \equiv \\ & \sum_{x=0}^{p-1} \left( \frac{(x^2 - 1)(dx^2 - 1)}{p} \right) + p - \left( \left( \frac{d}{p} \right) + 1 \right) \equiv \\ & \equiv \left( \sum_{j=0}^{\frac{p-1}{2}} (x^2 - 1)^{\frac{p-1}{2}} (dx^2 - 1)^{\frac{p-1}{2}} - \left( \frac{d}{p} \right) + 1 \right) \pmod{p} \equiv \\ & \equiv (-1)^{\frac{p+1}{2}} \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 d^j - \left( 2 \left( \frac{d}{p} \right) + 1 \right) \pmod{p}. \end{aligned}$$

According to Lemma 1, the last sum  $\left( \sum_{j=0}^{\frac{p-1}{2}} (x^2 - 1)^{\frac{p-1}{2}} (dx^2 - 1)^{\frac{p-1}{2}} \right) \pmod{p}$  is congruent to  $-a_{p-1} - a_{2p-2} \pmod{p}$ , where  $a_i$  are the coefficients from  $(x^2 - 1)^{\frac{p-1}{2}} (dx^2 - 1)^{\frac{p-1}{2}} = a_0 + a_1x + \dots + a_{2p-2}x^{2p-2}$ .

Last presentation was obtained due to transformation  $(x^2 - 1)^{\frac{p-1}{2}} (dx^2 - 1)^{\frac{p-1}{2}} = \left( \sum_{x=0}^{p-1} C_{\frac{p-1}{2}}^k x^{2k} (-1)^{\frac{p-1}{2}-k} \right) \left( \sum_{x=0}^{p-1} C_{\frac{p-1}{2}}^j d^j x^{2j} (-1)^{\frac{p-1}{2}-j} \right)$ .

Therefore  $a_{2p-2}$  is equal to  $d^{\frac{p-1}{2}} \equiv \left( \frac{d}{p} \right) \pmod{p}$  and  $a_{p-1} = \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 d^j (-1)^{\frac{p-1}{2}}$ .

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

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

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

Indeed, we have equality

$$\begin{aligned} & \sum_{j=0}^{\frac{p-1}{2}} d^j (C_{\frac{p-1}{2}}^{\frac{p-1}{2}-j}) (-1)^{\frac{p-1}{2} - (\frac{p-1}{2}-j)} \cdot (C_{\frac{p-1}{2}}^j)^2 (-1)^{\frac{p-1}{2}-j} = \\ & = (-1)^{\frac{p-1}{2}} \sum_{j=0}^{\frac{p-1}{2}} d^j C_{\frac{p-1}{2}}^{\frac{p-1}{2}-j} \cdot C_{\frac{p-1}{2}}^j = (-1)^{\frac{p-1}{2}} \sum_{j=0}^{\frac{p-1}{2}} d^j (C_{\frac{p-1}{2}}^j)^2. \end{aligned}$$

In form of a sum it is the following

$$\begin{aligned} & \sum_{j=0}^{\frac{p-1}{2}} 2^j (C_{\frac{p-1}{2}}^{\frac{p-1}{2}-j}) (-1)^{\frac{p-1}{2} - (\frac{p-1}{2}-j)} \cdot 2^j (C_{\frac{p-1}{2}}^j)^2 (-1)^{\frac{p-1}{2}-j} = \\ & = (-1)^{\frac{p-1}{2}} \sum_{j=0}^{\frac{p-1}{2}} 2^j C_{\frac{p-1}{2}}^{\frac{p-1}{2}-j} \cdot C_{\frac{p-1}{2}}^j = (-1)^{\frac{p-1}{2}} \sum_{j=0}^{\frac{p-1}{2}} 2^j (C_{\frac{p-1}{2}}^j)^2. \end{aligned}$$

Now, if

$$a_{p-1} = \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 d^j (-1)^{\frac{p-1}{2}} \equiv 0 \pmod{p},$$

then as it was shown by the author in that the curve is supersingular and the number of solutions of the

$$y^2 = (dx^2 - 1)(x^2 - 1)$$

over  $F_p$  equals to

$$p - 1 - 2 \left( \frac{d}{p} \right) + \left( 1 + \left( \frac{d}{p} \right) \right) = p - \left( \frac{d}{p} \right)$$

and differs from the quantity of solutions of

$$x^2 + y^2 = 1 + dx^2y^2$$

by  $\left(\frac{d}{p}\right) + 1$  due to new solutions of

$$y^2 = (dx^2 - 1)(x^2 - 1).$$

Thus, in general case if

$$a_{p-1} = \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 d^j (-1)^{\frac{p-1}{2}} \neq 0,$$

we have

$$N_{E_d} = \left( p - \left( \frac{d}{p} \right) - \left( \left( \frac{d}{p} \right) + 1 \right) - (-1)^{\frac{p-1}{2}} \right).$$



$$\begin{aligned} & \cdot \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^{\frac{p-1}{2}-j} C_{\frac{p-1}{2}}^j)^2 d^j \equiv \\ & \equiv (p-1 - (-1)^{\frac{p-1}{2}} \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 d^j - 2(\frac{d}{p})) \equiv \\ & \equiv ((-1)^{\frac{p+1}{2}} \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 d^j - 1 - 2(\frac{d}{p})) \pmod{p}. \end{aligned}$$

The exact order is not less than 4 because cofactor of this curve is 4. To determine the order is uniquely enough to take into account that  $p$  and  $2p$  have different parity. Taking into account that the order is even we chose a term  $p$  or  $2p$ , for the sum which define the order.

Let us analyze the complexity of calculating the value of

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

Binomial coefficients of the form  $C_{\frac{p-1}{2}}^l$  we calculate recursively having  $C_{\frac{p-1}{2}}^l$  we get  $C_{\frac{p-1}{2}}^{l+1}$ . 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  $\mathcal{O}(\frac{p-1}{2} \log_2^3 p)$ . Squaring the calculated binomial coefficient  $C_{\frac{p-1}{2}}^j$  also does not exceed  $\mathcal{O}(\log_2^2 p)$ .

Calculate all values of  $d^j \pmod{p}$  optimally applying recursive multiplication  $d^{j-1}$  on  $d$ . For this we make use of the Karatsuba multiplication method, which requires  $\mathcal{O}(\log_2^{\log_2^3 p})$ , rather than applying the Barrett method of modular multiplication. Therefore, the complexity of computing the entire tuple of degrees  $d^j, j = 1, \dots, n$  is  $\mathcal{O}(\frac{p-1}{2} \log_2^{\log_2^3 p})$ . Therefore, we obtain  $\mathcal{O}(\frac{p-1}{2} \log_2^2 p)$ .

*Example:* Number of curve points for  $d = 2$  and  $p = 31$  equals  $N_{2[p]} = N_{2^{-1}[p]} = p - 3 = 28$ .

**Theorem 5:** If  $(\frac{d}{p}) = 1$ , then the orders of the curves  $E_d$  and  $E_{d-1}$ , satisfies to the following equality

$$|E_d| = |E_{d-1}|.$$

If  $(\frac{d}{p}) = -1$ , 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

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

*Proof:* Let the curve be defined by  $x^2 + y^2 = 1 + dx^2y^2 \pmod{p}$ , then we can express  $y^2$  in such way:

$$y^2 \equiv \frac{x^2 - 1}{dx^2 - 1} \pmod{p}. \tag{15}$$

For  $x^2 + y^2 = 1 + d^{-1}x^2y^2 \pmod{p}$  we could obtain that

$$y^2 \equiv \frac{x^2 - 1}{d^{-1}x^2 - 1} \pmod{p} \tag{16}$$

Consider the case when  $(\frac{d}{p}) = 1$  the case  $(\frac{d}{p}) = -1$  proves analogously. if  $(\frac{d}{p}) = 1$ , then for the fixed  $x_0$  a quantity of  $y$  over  $F_p$  can be calculated by the formula  $(\frac{x^2-1}{d^{-1}x^2-1}) + 1$  for  $x$  such that  $d^{-1}x^2 + 1 \equiv 0 \pmod{p}$ . For solution  $(x_0, y_0)$  to (2), we have the equality  $y_0^2 \equiv \frac{x_0^2-1}{dx_0^2-1} \pmod{p}$  and we express  $y_0^2 \equiv \frac{1 - \frac{1}{x_0^2}}{1 - \frac{1}{dx_0^2}} d^{-1} \equiv \frac{(\frac{1}{x_0})^2 - 1}{\frac{1}{d}(\frac{1}{x_0})^2 - 1} d^{-1} \equiv \frac{(\frac{1}{x_0})^2 - 1}{d^{-1}(\frac{1}{x_0})^2 - 1} d^{-1}$ . Observe that

$$\begin{aligned} y^2 &= \frac{x^2 - 1}{d^{-1}x^2 - 1} = \frac{1 - x^2}{1 - d^{-1}x^2} = \frac{(\frac{1}{x^2} - 1)x^2}{((\frac{d}{x^2}) - 1)d^{-1}x^2} = \\ &= \frac{(\frac{1}{x^2} - 1)}{((\frac{d}{x^2}) - 1)} d. \end{aligned} \tag{17}$$

Thus, if  $(x_0, y_0)$  is solution of (2), then  $(\frac{1}{x_0}, \frac{y_0}{\sqrt{d}})$  is a solution to (16) because last transformations determines that  $\frac{y_0^2}{d} \equiv \frac{d^{-1}(\frac{1}{x_0})^2 - 1}{(\frac{1}{x_0})^2 - 1} \pmod{p}$ . Therefore last transformations  $(x_0, y_0) \rightarrow (\frac{1}{x_0}, \frac{y_0}{\sqrt{d}}) = (x, y)$  determines isomorphism and bijection.

*Example:* The number of points on  $E_d$  for  $d = 2$  and  $d^{-1} = 2$  with  $p = 31$  is equal to  $N_{2[31]} = N_{E_2^{-1}[31]} = p - 3 = 28$ .

*Example:* 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* 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  $\mathbb{F}_{p^k}$ .

Let us obtain conditions of embedding [16] for the group of supersingular curves  $E_d[\mathbb{F}_p]$  of order  $p$  in the multiplicative group of field  $\mathbb{F}_{p^k}$  whose embedding degree is  $k = 12$  [16]. We now utilise the Zsigmondy theorem which implies that a suitable characteristic of field  $\mathbb{F}_p$  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  $(x^n - 1) \not\equiv 0 \pmod{p}$  for an arbitrary  $n = 1, \dots, 11$ .

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

The proof is based on the fact that the order of the group of a supersingular curve  $E_d$  is equal to  $p^k + 1$  and will be detailed in our next article.

Consider  $E_2$  over  $F_{p^2}$ , for instance we assume  $p = 3$ . We define  $F_9$  as  $F_3(\alpha)$ , where  $\alpha$  is a root of  $x^2 + 1 = 0$  over  $F_9$ . Therefore elements of  $F_9$  have form:  $a + b\alpha$ , where  $a, b \in F_3$ .

So we assume that  $x \in \{\pm(\alpha + 1), \pm(\alpha - 1), \pm\alpha\}$  and check its belonging to  $E_2$ . For instance if  $x = \pm(\alpha + 1)$  then  $x^2 = \alpha^2 + 2\alpha + 1 = 2\alpha = -\alpha$ . 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 similar computations lead us to full the following list of curves points.

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

TABLE II  
 POINTS OF EDWARDS CURVE OVER SQUARE EXTENSION.

The total amount is 12 affine points that confirms Corollary IV and Theorem IV because of  $p^n - 3 - 2(-p)^{\frac{n}{2}} = 3^2 - 3 - 2(-3) = 12$ .

### V. RESULTS

Our method for determining the order of a curve is valuable in itself and, in addition, provides a way to solve the inverse problem, that is, construct a curve of a given order. The conditions on a coefficients determining pairs of twisted curves of Edwards was found by us. We found a degree of embedding for the group of a supersingular curve in finite field with a minimal degree of extension. Due to Theorem 5. we obtain method to calculate the order of twisted curve for any Edwards curve. Let the first number denotes the quotient  $p$  (i.e. mod  $p$ ). The second number is the number of points for  $d = 2$  and the third number is the number solution for  $d = 2^{-1} = (p + 1)/2$ .

According to GlobalSign, elliptical curve cryptography (ECC) can be used on most of today's modern browsers and operating systems. The list below shows which OS and browser versions are known to be compatible with ECC: Apple OS X, OS X 10.6, Google Android 4.0 Microsoft Windows and many other. 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 is solved due our method. A typical requirement of all such applications is that the order of the EC [6], [8], [16], [20]. 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 [6, 16], small prime factors [6], [16], etc), which

3: 4, 4	47: 44, 44	103: 100, 100	167: 164, 164
5: 8, 4	53: 40, 68	107: 108, 108	173: 200, 148
11: 12, 12	59: 60, 60	109: 104, 116	179: 180, 180
13: 8, 20	61: 72, 52	113: 124, 124	181: 200, 164
17: 12, 12	67: 68, 68	127: 124, 124	191: 188, 188
19: 20, 20	71: 68, 68	131: 132, 132	193: 204, 204
23: 20, 20	73: 76, 76	137: 156, 156	197: 200, 196
29: 40, 20	79: 76, 76	139: 140, 140	199: 196, 196
31: 28, 28	83: 84, 84	149: 136, 164	211: 212, 212
37: 40, 36	89: 76, 76	151: 148, 148	223: 220, 220
41: 28, 28	97: 76, 76	157: 136, 180	227: 228, 228
43: 44, 44	101: 104, 100	163: 164, 164	229: 200, 260

TABLE III  
 THE TWISTED PAIRS OF EDWARDS CURVES

gives rise to the problem of how such EC can be generated. One of good decision of this task is a curve of big prime order [6], [16], [18]. Our method of determination of elliptic and Edwards curve order give one of possible decisions of these problems by analytic expression for the of curves order over a finite field  $F_{p^n}$ .

It is very important to avoid of curves of order  $p+1$  because of it is tractable to the pairingbased attacks [6]. Our Theorems IV and IV establish criterion and sufficient conditions for such curves with order  $p + 1$  therefore, it completely solves this problem. Additionally conditions of embedding of such curves was obtained. That is give rise to using the Edwards curve in the methods of zero knowledge proof such as Zk-Snark and Zk-Stark.

### VI. DISCUSSIONS

The complexity of the discrete logarithm problem in the group of points of an elliptic curve depends on the order of this curve. Therefore, for intelligent control of the security level in the system, it is important to apply our method of determining the order [8], [9], [14],[19] of the curve providing the necessary level of cryptographic stability of the system.

### VII. CONCLUSIONS

In this paper we have found a new effective algorithm for the elliptic and Edwards curves order over a finite field. In addition, the criterion for supersingularity of these curves has been was obtained as a result of this the using of groups of points of curves of genus 1 in cryptography which is intractable to MOV attacks. We have investigated the number of affine and projective points. It should be noted that our results provide a possibility to determine the number of such points in a constructive way, which provides a way for some intelligent control of the security level in the cryptosystem based on EC. The embedding degree for the Edwards and Montgomery curves have also been determined.

We proved using existence of the birational isomorphism between twisted Edwards curve and elliptic curve in Weierstrass normal form that the result about order of curve over finite field can be applied to cubic in Weierstrass normal form.

### REFERENCES

- [1] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted edwards curves. In Serge Vaudenay, editor, *Progress in Cryptology – AFRICACRYPT 2008*, pages 389–405, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.
- [2] A.V Bessalov and O.V. Thsiganhova. Vzaimosvyaz' semeystva tocek bol'shikh poryadkov 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] Harold Edwards. A normal form for elliptic curves. *Bulletin of the American mathematical society*, 44(3):393–422, 2007.
- [6] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.
- [7] Rudolf Lidl and Harald Niederreiter. *Introduction to Finite Fields and their Applications*. Cambridge university press, 1994.
- [8] Peter L Montgomery. Speeding the pollard and elliptic curve methods of factorization. *Mathematics of computation*, 48(177):243–264, 1987.

- [9] René Schoof. Counting points on elliptic curves over finite fields. *Journal de théorie des nombres de Bordeaux*, 7(1):219–254, 1995.
- [10] Ruslan Viacheslavovich Skuratovskii. The order of projective edwards curve over  $\mathbb{F}_{p^n}$  and embedding degree of this curve in finite field. In *Cait 2018, Proceedings of Conferences*, pages 75 – 80, 2018.
- [11] Ruslan Viacheslavovich Skuratovskii. Supersingularity of elliptic curves over  $F_{p^n}$  (in ukrainian). *Research in Mathematics and Mechanics*, 31(1):17–26, 2018.
- [12] Ruslan Viacheslavovich Skuratovskii. Normal high order elements in finite field extensions based on the cyclotomic polynomials. In *Algebra and Discrete Mathematics*, pages 241–248. 29(2), 2020.
- [13] Ruslan Viacheslavovich Skuratovskii, Williams Alled. Irreducible bases and subgroups of a wreath product in applying to diffeomorphism groups acting on the Mebius band *Rendiconti del Circolo Matematico di Palermo*, pages 1–19. Springer, 2020.
- [14] Sergeĭ Aleksandrovich Stepanov. *Arifmetika algebraicheskikh krivyykh (in Russian)*. Nauka, Glav. red. fiziko-matematicheskoi lit-ry, 1991.
- [15] Ivan Matveevich Vinogradov. Elements of number theory. *Courier Dover Publications*, 2016.
- [16] Paulo S. 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.
- [17] P.D Varbanec, P Zarzycki. Divisors of the Gaussian integers in an arithmetic progression. *Journal of Number Theory*. Volume 33, Issue 2, October 1989, Pages 152-169
- [18] Silverman, Joseph, H.; *The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics*, 106, Springer-Verlag, 1986.
- [19] Craig Costello and Benjamin Smith. Montgomery curves and their arithmetic. *Journal of Cryptographic Engineering*, 8(3):227-240, 2018.
- [20] Manoj Gyawali and Daniele Di Tullio. Elliptic curves of nearly prime order. *Cryptology ePrint Archive, Report 2020/001*, 2020. <https://eprint.iacr.org/2020/001>.
- [21] Ruslan Skuratovskii and Aled Williams. A solution of the inverse problem to doubling of twisted edwards curve point over finite field. *Przetwarzanie, transmisja i bezpieczeństwo informacji*, 2:351-358, 2019. *Elliptic curve cryptosystems. Mathematics of computation*.
- [22] Drozd YA., Skuratovskii R.V. Cubic rings and their ideals (in Ukrainian) // *Ukr. Mat. Zh.* - 2010.-V. 62, Á<sup>1</sup>11-P.464-470. (arXiv:1001.0230 [math.AG])
- [23] Pierre Deligne. *La conjecture de weil*. *Publ. Math. IHES*, 52:137-252, 1980.
- [24] Moody, D., Shumow, D. Analogues of Velu’s formulas for isogenies on alternate models of elliptic curves. *Math. Computation* 85(300), 1929-1951 (2015). <https://doi.org/10.1090/mcom/3036>

## Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0

[https://creativecommons.org/licenses/by/4.0/deed.en\\_US](https://creativecommons.org/licenses/by/4.0/deed.en_US)