Журнал обчислювальної та прикладної математики **2020, № 1 (133)** Journal of Numerical & Applied Mathematics

УДК 512.7, 519.6
MSC 11G07, 97U99, 97N30

SUPERSINGULAR EDWARDS CURVES AND EDWARDS CURVE POINTS COUNTING METHOD OVER FINITE FIELD

Ruslan Skuratovskii
National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», V.M. Glushkov Institute of Cybernetics of the NAS of Ukraine, Kyiv, Ukraine,
E-mail: r.skuratovskii@kpi.ua, ruslcomp@mail.ru

СУПЕРСИНГУЛЯРНІ КРИВІ ЕДВАРДСА І МЕТОД ПІДРАХУНКУ ПОРЯДКУ КРИВОЇ ЕДВАРДСА НАД СКІНЧЕННИМ ПОЛЕМ

Р. В. Скуратовський
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Інститут кібернетики імені В.М. Глушкова НАНУ, Київ, Україна,
E-mail: r.skuratovskii@kpi.ua, ruslcomp@mail.ru

Abstract. We consider problem of order counting of algebraic affine and projective curves of Edwards [2, 8] over the finite field $\mathbb{F}_{p^n}$. The complexity of the discrete logarithm problem in the group of points of an elliptic curve depends on the order of this curve (ECDLP) [4, 20] depends on the order of this curve [10]. 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 over a finite field. 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. 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 $E_d[\mathbb{F}_p]$ is supersingular over this field or not. The embedding degree of the supersingular curve of Edwards over $\mathbb{F}_{p^n}$ in a finite field is investigated and the field characteristic, where this degree is minimal, is found. A birational isomorphism between the Montgomery curve and the Edwards curve is also constructed. A one-to-one correspondence between the Edwards supersingular curves and Montgomery supersingular curves is established. The criterion of supersingularity for Edwards curves is found over $\mathbb{F}_{p^n}$.
Keywords: finite field, elliptic curve, Edwards curve, group of points of an elliptic curve.

Анотація. Ми розглядаємо алгебраїчні аффінні і проективні криві Едвардса [2, 8] над скінченним полем $\mathbb{F}_{p^n}$. Складність проблеми дискретного логарифму в групі точок еліптичної кривої (ECDLP) [4] залежить від порядку цієї кривої [10]. Досліджуємо алгебраїчні криві Едвардса над скінченним полем, які є одним з найбільш преспективних носіїв множин точок, які використовуються для швидких групових операцій [1]. Будуємо новий метод підрахунку порядку кривої Едвардса над скінченним полем. Слід зазначити, що цей метод може бути застосований до визначення порядку еліптичних кривих через бірaціональні еквівалентності між еліптичними кривими і кривими Едвардса. Ми не тільки знаходимо набір коефіцієнтів з відповідними характеристиками поля, для яких ці криві є суперсингулярними, ми також додатково знаходимо загальну формулу, згідно з якою можна визначити, чи є крива $E_d[\mathbb{F}_p]$ суперсингулярною над цим полем чи ні. Досліджується ступінь вкладення суперсингулярної кривої Едвардса над $\mathbb{F}_{p^n}$ в скінченне поле. Також знайдена характеристика поля, де цей ступінь мінімальний. У статті знайдено критерій суперсингулярності кривої Едвардса над $\mathbb{F}_{p^n}$. Встановлено взаємно-однозначна відповідність між суперсингулярними кривими Едвардса і суперсингулярними кривими Монтгомері. Побудований бірaціональних ізоморфізм між кривою Монтгомері та кривою Едвардса. Вказані образи спеціальних точок кривої Едвардса на сфері Рімана при бірaціональному ізоморфізмі.
Ключові слова: скінченне поле, еліптична крива, крива Едвардса, група точок на еліптичній кривій.

Introduction

The problem of finding the order of an algebraic curve over a finite field $\mathbb{F}_{p^n}$ 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 cryptography. In our article, this problem is solved for the Edwards and Montgomery curves.

The criterion of supersingularity of the Edwards curves is found over $\mathbb{F}_{p^n}$. We additionally propose a method for counting the points from Edwards curves and elliptic curves in response to an earlier paper by Schoof [19].

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 these curves are supersingular, but we additionally find a general formula by which one can determine whether a curve $E_d[\mathbb{F}_p]$ is supersingular over this field or not.

1. Review of Previous Results

It is known that the theoretical results of S. Stepanov [11] and P. Deligne provide both upper and lower bounds for the number of curve points, that is $p^n + 1 - \omega_1^n - \omega_2^n$ [18]. The complexity of the fastest algorithms known are Schoof's basic algorithm [19], 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 [17].

2. Main Result

The twisted Edwards curve with coefficients $a, d \in \mathbb{F}_p{}^*$ 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 called an Edwards curve when $a = 1$. We denote by E_d the Edwards curve with coefficient $d \in \mathbb{F}_p{}^*$ which is defined as

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

over $\mathbb{F}_p$. 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 $A^1 := az^2 + y^2z^2 = z^4 + dy^2$ and $A^2 := \ ax^2z^2 + z^2 = z^4 + dx^2$. 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

$$F(x, y, z) = \frac{f(x, y, z)}{g(x, y, z)},$$

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 $\delta_{\mathrm{p}} = \dim \overline{\mathcal{O}}_{\mathrm{p}}/_{\mathcal{O}_p}$, where $\mathcal{O}_{\mathrm{p}}$ denotes the local ring at the singular point p which is generated by the relations of regular functions $\mathcal{O}_{\mathrm{p}} = \left\{ \frac{f}{g} : \ (g, (x-1)(y-1)) = 1 \right\}$ and $\overline{\mathcal{O}}_{\mathrm{p}}$ denotes the whole closure of the local ring at the singular point p.

We find that $\delta_p = \dim \overline{\mathcal{O}}_p/_{\mathcal{O}_p} = 1$ is the dimension of the factor as a vector space. Because the basis of extension $\overline{\mathcal{O}}_p/_{\mathcal{O}_p}$ 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 [3]

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

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 [9]. 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, 3] 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 $\mathbb{F}_q$ is called supersingular if for every finite extension $\mathbb{F}_{q^r}$ there are no points in the group $E(\mathbb{F}_{q^r})$ of order p [16]. It is known [1] that the transition from an Edwards curve to the related torsion curve is determined by the reflection $(\overline{x}, \overline{y}) \mapsto (x, y) = \left(\overline{x}, \frac{1}{\overline{y}}\right)$.

We now recall an important result from Vinogradov [12] which will act as criterion for supersingularity.

Lemma 1 (Vinogradov [12])**.** *Let $k \in \mathbb{N}$ and $p \in \mathbb{P}$. Then*

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

where $n|(p-1)$ 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 finite field $\mathbb{F}_p$.

We will now strengthen an existing result given in [9]. We denote the *number of points with a neutral element of an affine Edwards* curve over the finite field $\mathbb{F}_p$ by $N_{d[p]}$ and the *number of points on the projective curve* over the same field by $\overline{N}_{d[p]}$.

Theorem 1. *If $p \equiv 3 (\mathrm{mod}\ 4)$ is prime and the following condition of supersingularity*

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

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 $\mathbb{F}_p$ 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 $y^2 = \frac{1-x^2}{1-dx^2y^2}$. 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 $\mathbb{F}_p$ by $M_{d[p]}$. This curve (3) has $M_{d[p]} = N_{d[p]} + \left(\frac{d}{p}\right) + 1$ points, which is precisely $\left(\frac{d}{p}\right) + 1$ greater than the number of points of curve E_d. Note that $\left(\frac{d}{p}\right)$ denotes the Legendre Symbol. Let $a_0, a_1, \ldots, a_{2p-2}$ be the coefficients of the polynomial $a_0 + a_1 x + \cdots + a_{2p-2}x^{2p-2}$, 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

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

$$= p + \sum_{x=0}^{p-1} (x^2-1)^{\frac{p-1}{2}}(dx^2-1)^{\frac{p-1}{2}} \equiv \sum\nolimits_{x=0}^{p-1} (x^2-1)^{\frac{p-1}{2}}(dx^2-1)^{\frac{p-1}{2}} (\text{mod } p).$$

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

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

We need to prove that $M_{d[p]} \equiv 1 (\text{mod } p)$ if $p \equiv 3 (\text{mod } 8)$ and $M_{d[p]} \equiv -1 (\text{mod } p)$ if $p \equiv 7 (\text{mod } 8)$. We therefore have to show that $M_{d[p]} \equiv -(\frac{d}{p}) - a_{p-1} (\text{mod } p)$ for $p \equiv 3 (\text{mod } 4)$ if $\sum\limits_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 d^j \equiv 0 (\text{mod } p)$. If we prove that $a_{p-1} \equiv 0 (\text{mod } p)$, then it will follow from (3). Let us determine a_{p-1} according to Newton's binomial formula: a_{p-1} is equal to the coefficient at x^{p-1} in the polynomial, which is obtained as a product $(x^2-1)^{\frac{p-1}{2}}(dx^2-1)^{\frac{p-1}{2}}$. So, $a_{p-1} = (-1)^{\frac{p-1}{2}} \sum\limits_{j=0}^{\frac{p-1}{2}} d^j (C^j_{\frac{p-1}{2}})^2$. 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 $a_{p-1} = -\sum\limits_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 d^j$, then exact number of affine points on non supersingular curve is the following

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

According to the condition of this theorem $a_{p-1} = 0$, therefore $M_{d[p]} \equiv -a_{2p-2}(\text{mod}p)$. Consequently, in the case when $p \equiv 3(\text{mod } 4)$, where p is prime and $\sum\limits_{j=0}^{\frac{p-1}{2}} \left(C^j_{\frac{p-1}{2}}\right)^2 d^j \equiv 0(\text{ mod } p)$, 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.

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 $x \in \mathbb{F}_p$ we have exactly p values of x. Also there are 4 pairs $(\pm 1, 0)$ and $(0, \pm 1)$ which are points of E_d thus $N_{d[p]} > 1$. Thus $N_{d[p]} = p + 1$. This 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* $\mathbb{F}_p$ *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* $p \equiv 3(\text{mod } 4)$ *is prime and* $\sum\limits_{j=0}^{\frac{p-1}{2}} \left(C^j_{\frac{p-1}{2}}\right)^2 d^j \equiv 0(\text{mod } p)$.

Since all transformations in proof of Theorem 1 were equivalent transitions then we obtain the proof of equivalence of conditions.

Theorem 2. *If the coefficient* $d = 2$ *or* $d = 2^{-1}$ *and* $p \equiv 3(\text{mod}4)$ *then* $\sum\limits_{j=0}^{\frac{p-1}{2}} d^j \left(C^j_{\frac{p-1}{d}}\right)^2 \equiv 0\,(\text{mod}p)$ *and* $\overline{N}_{d[p]} = p + 1$.

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

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

$$= (\frac{p-1}{2})(\frac{p-1}{2} - 1)\cdots(\frac{p-1}{2} - j + 1)[(\frac{p-1}{2})(\frac{p-1}{2} - 1)\cdots(j+1)].$$

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

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

Thus, as a result of squaring, we have:

$$\Big(\Big(\frac{p-1}{2}\Big)!\, C^{j}_{\frac{p-1}{2}}\Big)^2 \equiv$$

$$\equiv \Big(\frac{p-1}{2}-j+1\Big)^2\Big(\frac{p-1}{2}-j+2\Big)^2\cdots\Big(p-j-1\Big)^2(\text{mod } p). \quad (6)$$

It remains to prove that $\sum\limits_{j=0}^{\frac{p-1}{2}} (C^{j}_{\frac{p-1}{2}})^2 2^j \equiv 0(\text{mod } p)$ if $p \equiv 3(\text{mod } 4)$. Consider the auxillary polynomial

$$P(t) = (\frac{p-1}{2}!)^2 \sum\nolimits_{j=0}^{\frac{p-1}{2}} (C^{j}_{\frac{p-1}{2}})^2 t^j.$$

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

$$a_{p-1} = P(t) = (\frac{p-1}{2}!)^2 \sum\nolimits_{j=0}^{\frac{p-1}{2}} (C^{j}_{\frac{p-1}{2}})^2 t^j \equiv$$

$$\equiv \sum\nolimits_{j=0}^{\frac{p-1}{2}} (k+1)^2(k+2)^2...(\frac{p-1}{2}+k)^2 t^k (\text{mod } p)$$

over $\mathbb{F}_p$.

We replace d by t in (1) such that we can research a more generalised problem. It should be noted that $P(t) = \partial^{\frac{p-1}{2}}\Big(\partial^{\frac{p-1}{2}}\big(Q(t)\ t^{\frac{p-1}{2}}\big)t^{\frac{p-1}{2}}\Big)$ over $\mathbb{F}_p$, 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 $Q(t) = \frac{t^p-1}{t-1} \equiv \frac{(t-1)^p}{t-1} \equiv (t-1)^{p-1}(\text{mod } p)$ and therefore the equality $P(t) = \Big(\big((t-1)^{p-1}t^{\frac{p-1}{2}}\big)^{(\frac{p-1}{2})}t^{\frac{p-1}{2}}\Big)^{(\frac{p-1}{2})}$ holds over $\mathbb{F}_p$.

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

$$R(\theta) = P(\theta+1) = \partial^{\frac{p-1}{2}}\Big(\partial^{\frac{p-1}{2}}\big(\theta^{p-1}(\theta+1)^{\frac{p-1}{2}}\big)(\theta+1)^{\frac{p-1}{2}}\Big) =$$

$$= \partial^{\frac{p-1}{2}}\Big(\frac{(p-1)!}{((p-1)/2)!}\theta^{\frac{p-1}{2}}(\theta+1)^{\frac{p-1}{2}}\Big).$$

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

$$R(1) = \frac{(p-1)!}{(\frac{p-1}{2})!}\sum\nolimits_{j=0}^{\frac{p-1}{2}} C^{j}_{\frac{p-1}{2}}(j+1)\cdots(j+\tfrac{p-1}{2}). \quad (7)$$

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 $(5-j+1)(5-j+2)\cdots(5-j+5) = (6-j)(7-j)\cdots(10-j) \equiv \big((-5-j)(-4-j)\cdots(-1-j)\big) \equiv (-1)^5\big((j+1)(j+2)\cdots(j+5)\big) (\mathrm{mod}\ 11)$.

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

As a result, the symmetrical terms in (7) can be reduced yielding $a_{p-1} \equiv 0(\mathrm{mod}\ p)$. 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 $a_{p-1} \equiv 0(\mathrm{mod}\ p)$ as required. Thus, $\sum_{j=0}^{\frac{p-1}{2}} \left(C^j_{\frac{p-1}{2}}\right)^2 \equiv 0(\mathrm{mod}\ p)$, completing the proof of the 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 1 that

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

Since $\left(C^j_{\frac{p-1}{2}}\right)^2 d^j \equiv 0(\mathrm{mod}\ p)$ by condition, and the congruence $(\frac{d}{p}) \equiv (\frac{d^{-1}}{p})$ holds, then according to shown in the proof of Theorem 1 the curve E_d has $N_{d[p]} = p - \left(\frac{d}{p}\right) - (\left(\frac{d}{p}\right)+1) = p - 1 - 2\left(\frac{d}{p}\right)$ affine points. So the number of points on E_d is $N_{d[p]} \equiv -a_{2p-2} - a_{p-1} \equiv -\left(\frac{d}{p}\right) \equiv \left(\frac{d}{p}\right) (\mathrm{mod} p)$, therefore $N_{d[p]} \equiv N_{d^{-1}[p]}$. □

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 $\mathbb{F}_p$. 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

$$2 \le M_{d[p]} \le 2p - 2, \tag{8}$$

where if $a_{p-1} \equiv 0(\mathrm{mod}\ p)$ we have $N_{d[p]} \equiv -\left(\frac{d}{p}\right)(\mathrm{mod}\ p)$. The number of solutions is bounded by $N_{d[p]} \le 2p-2$ 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 $M_{d[p]} \equiv p - \left(\frac{d}{p}\right)(\mathrm{mod}\ p)$.

Corollary 3. *If $p \equiv 3(\mathrm{mod}\ 4)$ is prime, then $N_{d[p]} = p-1-2\left(\frac{d}{p}\right)+T$, where T is such that $T \equiv \sum\limits_{j=0}^{\frac{p-1}{2}} \left(C^j_{\frac{p-1}{2}}\right)^2 d^j \le 2\sqrt{q}$ 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 $|N_{d[p]} - (p+1) - 2\left(\frac{d}{p}\right)| \le 2g\sqrt{p}$, where g is genus of curve,

we obtain exact number $N_{d[p]}$. As we showed, $g = 1$. From Theorem 1 as well as from Corollary 2 we get, that $\sum_{j=0}^{\frac{p-1}{2}} \left(C_{\frac{p-1}{2}}^{j}\right)^2 d^j \equiv -N_{d[p]} - (p+1) - 2\left(\frac{d}{p}\right)$ 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 $N_{7[13]} = 20$, which is in contradiction to that suggested by A. Bessalov and O. Thsigankova. Moreover, if $p \equiv 7 (\mathrm{mod}\ 8)$, 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 them.

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 $d = 2 (\mathrm{mod}\ 7)$, 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 $n \equiv 1 (\mathrm{mod}\ 2)$ and p is prime, then the order of projective curve $\overline{N}_{d[p^n]} = p^n + 1$, and the order of curve is equal to $N_{d[p^n]} = p^n - 1 - 2\left(\frac{d}{p}\right)$. If $n \equiv 0 (\mathrm{mod}\ 2)$ 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 $\mathbb{F}_p$ to $\mathbb{F}_{p^n}$ 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 [11] that the number of solutions to $y^2 = P(x)$ over $\mathbb{F}_{p^n}$ will have the form $p^n + 1 - \omega_1^n - ... - \omega_{m-1}^n$ where $\omega_1, ..., \omega_{m-1} \in \mathbb{C}$, $|\omega_i| = p^{\frac{1}{2}}$.

In case of our supersingular curve, if $n \equiv 1 (\mathrm{mod}\ 2)$ 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 [11, 14, 5] that $|\omega_i| = p^{\frac{1}{2}}$. The order of the projective curve is therefore $p^n + 1$.

If $p \equiv 7 (\mathrm{mod}\ 8)$, then it is known from a result of Skuratovskii [9] 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 $p \equiv 3 (\mathrm{mod}\ 8)$, 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 $p \equiv 7(\mathrm{mod}\ 8)$ and $N_{d[p]} = p^n + 1$ if $p \equiv 3(\mathrm{mod}\ 8)$ where $n \equiv 1(\mathrm{mod}\ 2)$. We note that this is because the transformation of (3) in E_d depends upon the denominator $(dx^2 - 1)$.

If $n \equiv 1(\mathrm{mod}\ 2)$ 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 points of the curve is $p^n + 1 - \omega_1^n - \omega_2^n$ [18].

For $n \equiv 0(\mathrm{mod}\ 2)$ we always have, that every $d \in \mathbb{F}_p$ is a quadratic residue in $\mathbb{F}_{p^n}$. 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. $N_{d[p^n]} = p^n - 1 - 2\left(\frac{d}{p}\right) - 2(-p)^{\frac{n}{2}} = p^n - 3 - 2(-p)^{\frac{n}{2}}$. In more details $\omega_1,\ \omega_2$ are eigen values of the Frobenius operator F endomorphism on etale 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 Lefshitz formula:

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

where $\#X\left(\mathbb{F}_{p^n}\right)$ 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 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 $\mathbb{F}_p$. 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 solutions appear

$$(u_1, v_1) = \left(\frac{-(d+1) - 2\sqrt{d}}{d-1},\ 0 \right), \quad (u_2, v_2) = \left(\frac{-(d+1) + 2\sqrt{d}}{d-1},\ 0 \right).$$

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.

Table 1. Special points of birational maping

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

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

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 $\mathbb{F}_q$. 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 $(\frac{-(d+1)-2\sqrt{d}}{d-1}, 0)$, $(\frac{-(d+1)+2\sqrt{d}}{d-1}, 0)$ 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 an Montgomery curve. Thus, the order of E_M is equal $p+1$ in this case as supersingular curve has. The images of special points after projectivization have an image on the Riemann sphere or on the projective plane. □

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 [11, 6], 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 $\mathbb{F}_{p^k}$ can be evaluated due to Stepanov [11, 14]. 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 $n \equiv 1 (\mathrm{mod}\ 2)$, 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 $n \equiv 1 (\mathrm{mod}\ 2)$. □

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

Corollary 4. *If $d = 2$, $n \equiv 1 (\mathrm{mod}\ 2)$ and $p \equiv 3 (\mathrm{mod}\ 8)$, 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 $d = 2$, $n \equiv 1 (\mathrm{mod}\ 2)$ and $p \equiv 7 (\mathrm{mod}\ 8)$, 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 $N_{d[p^n]} = p^n - 3$.

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

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

The general formula for $n \equiv 0 (\mathrm{mod}\ 2)$ 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 $\mathbb{F}_{p^n}$. The order $N_{M[p^n]}$ of E_M over $\mathbb{F}_{p^n}$ can be evaluated [5] 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 $n \equiv 1(\mathrm{mod}\ 2)$. Therefore, for $n \equiv 1(\mathrm{mod}2)$, 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 [4], 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 $\bar{N}_{d[p]}$. Because a group of $E_d(\mathbb{F}_{p^2})$ over square extension of $\mathbb{F}_p$ contains the group $E_d(\mathbb{F}_p)$ as a proper subgroup. In fact, according to Theorem 1 the order $E_d(\mathbb{F}_p)$ is $p + 1$ therefore divisibility of order $E_d(\mathbb{F}_{p^2})$ holds because in our case $p = 7$ thus $\overline{N}_{E_d} = 8^2$ and $p + 1 = 8 = N_{d[7]}$ [15].

The following two examples exemplify Corollary 4.

Example 3. If $p \equiv 3(\mathrm{mod}\ 8)$ 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

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

Example 4. If $p \equiv 7(\mathrm{mod}\ 8)$ 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

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

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 [9] and hence if the curve is free of singular points then the group order is $p + 1$. □

Example 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 4. *The order of Edwards curve over $\mathbb{F}_p$ is congruent to*

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

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

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

Proof. This result follows from the number of solutions of the equation

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

over $\mathbb{F}_p$ which equals to

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

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

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

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

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

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

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

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

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

$$(x^2-1)^{\frac{p-1}{2}} (dx^2-1)^{\frac{p-1}{2}} = a_0 + a_1 x + ... + a_{2p-2} x^{2p-2}.$$

Last presentation was obtained due to transformation

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

Therefore a_{2p-2} is equal to $d^{\frac{p-1}{2}} \equiv (\frac{d}{p})(\mathrm{mod} p)$ and

$$a_{p-1} = \sum\nolimits_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 d^j (-1)^{\frac{p-1}{2}}.$$

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

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

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

Indeed, we have equality

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

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

In form of a sum it is the following

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

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

If

$$a_{p-1} = \sum\nolimits_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 d^j (-1)^{\frac{p-1}{2}} \equiv 0(\mathrm{mod} p),$$

then as it is was shown by the author in [9] this curve is supersingular and the number of solutions of the $y^2 = (dx^2-1)(x^2-1)$ over $\mathbb{F}_p$ equals to $p - 1 - 2\left(\frac{d}{p}\right) + \left(1 + (\frac{d}{p})\right) = p - \left(\frac{d}{p}\right)$ and differs from 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 case if $a_{p-1} = \sum_{j=0}^{\frac{p-1}{2}} \left(C^j_{\frac{p-1}{2}}\right)^2 d^j (-1)^{\frac{p-1}{2}} \neq 0$ we have

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

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

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

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. □

Example 6. Number of curve points for $d = 2$ and $p = 31$ equals $N_{2[p]} = N_{2^{-1}[p]} = p - 3 = 28$.

Theorem 5. *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*

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

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

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

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

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

If $\left(\frac{d}{p}\right) = 1$, then for the fixed x_0 a quantity of y over $\mathbb{F}_p$ can be calculated by the formula $(\frac{\frac{x^2-1}{d^{-1}x^2-1}}{p}) + 1$ for x such that $d^{-1}x^2 + 1 \equiv 0(\mathrm{mod} p)$. For solution (x_0, y_0) to (2), we have the equality $y_0^2 \equiv \ \frac{x_0^2-1}{dx_0^2-1} \, (mod \ p)$ and we express

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

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

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 $\frac{y_0^2}{d} \equiv \frac{d^{-1}\left(\frac{1}{x_0}\right)^2-1}{\left(\frac{1}{x_0}\right)^2-1} mod p$. Therefore last transformations $(x_0,\ y_0) \to (\frac{1}{x_0},\ \frac{y_0}{\sqrt{d}}) = (x,\ y)$ determines isomorphism and bijection.

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

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

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 solutions 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 7. 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 8. The number of points of E_d over $\mathbb{F}_p$ 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 $\mathbb{F}_{13}$ 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 9. If $p = 7$ and $d = 2^{-1} \equiv 4(\text{mod } 7)$, 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 $d = 2(\text{mod } 7)$, the curve $E_{2^{-1}}$ also has four points which are $(0, 1); (0, 6); (1, 0); (6, 0)$.

Definition 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 $\mathbb{F}_{p^k}$.

Let us obtain conditions of embedding [13] 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 $k = 12$ [13]. 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 $q \,|\mathrm{P}_{12}(p)$, where $\mathrm{P}_{12}(x)$ is the cyclotomic polynomial. This p will satisfy the necessary conditions $(x^n - 1) \not| \; p$ for an arbitrary $n \in \{1, ..., 11\}$.

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

The order of the group of a supersingular curve E_d is equal to p^k+1. It should 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 work 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 the definition to conclude that the degree of immersion must be 2, confirming the proposition.

Consider E_2 over $\mathbb{F}_{p^2}$, for instance we assume $p = 3$. We define $\mathbb{F}_9$ as $\mathbb{F}_3(\alpha)$, where α is a root of $x^2 + 1 = 0$ over $\mathbb{F}_9$. Therefore elements of $\mathbb{F}_9$ have form: $a + b\alpha$, where $a,\ b \in \mathbb{F}_3$. 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.

Table 2. Points of Edwards curve over square extension.

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

The total amount is 12 affine points that confirms Corollary 4 and Theorem 3 because of $p^n - 3 - 2(-p)^{\frac{n}{2}} = 3^2 - 3 - 2(-3) = 12$.

3. Complexity

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 our theorem 5 we obtain method to calculate the order of twisted curve for any Edwards curve. The computations confirming Theorem 5 are presented in table below. 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 of points for $d = 2^{-1} = (p + 1)/2$.

Table 2. The twisted pairs of Edwards curves

3: 4, 4	47: 44, 44	103: 100, 100	167: 164, 164	233: 204, 204
5: 8, 4	53: 40, 68	107: 108, 108	173: 200, 148	239: 236, 236
11: 12, 12	59: 60, 60	109: 104, 116	179: 180, 180	241: 268, 268
13: 8, 20	61: 72, 52	113: 124, 124	181: 200, 164	251: 252, 252
17: 12, 12	67: 68, 68	127: 124, 124	191: 188, 188	257: 252, 252
19: 20, 20	71: 68, 68	131: 132, 132	193: 204, 204	263: 260, 260
23: 20, 20	73: 76, 76	137: 156, 156	197: 200, 196	269: 296, 244
29: 40, 20	79: 76, 76	139: 140, 140	199: 196, 196	271: 268, 268
31: 28, 28	83: 84, 84	149: 136, 164	211: 212, 212	277: 296, 260
37: 40, 36	89: 76, 76	151: 148, 148	223: 220, 220	281: 268, 268
41: 28, 28	97: 76, 76	157: 136, 180	227: 228, 228	283: 284, 284

It is very important to avoid of curves of order $p+1$ because of it is tractable to the pairingbased attacks [4]. Our Theorems 1 and 2 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.

Consider the the complexity of our method. The calculating of $\sum\limits_{j=0}^{\frac{p-1}{2}} \left(C^j_{\frac{p-1}{2}}\right)^2 d^j$, where $C^l_{\frac{p-1}{2}}$ can be calculated recursively, is performed by *modp*. We have $C^l_{\frac{p-1}{2}}$ then we calculate $C^{l+1}_{\frac{p-1}{2}}$. 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 both cases, the complexity of calculating all the coefficients 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 $O\left(\log_2^2 p\right)$.

Compute all values of $d^j \bmod p$ optimally applying recursive multiplication d^{j-1} on d for this we use the Karatsuba multiplication method requiring $O(log_2^{\log_2 3} p)$, than apply the Barrett method of modular multiplication. Therefore, the complexity of computing the entire tuple of degrees d^j, $j = 1, ..., n$ is $O(\frac{p-1}{2} log_2^{\log_2 3} p)$. Totally we obtain $O(\frac{p-1}{2}\log_2^2 p)$.

Conclusion

The new method for order curve counting was founded for Edwards and elliptic curves. The criterion for supersingularity was additionally obtained.

Our method of order curve determination has complexity $O\left(p\log_2^2 p\right)$ that for sufficiently large n is less then Schoof algorithm has $O(log_2^8 p^n)$.

References

1. Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted edwards curves. In: Serge Vaudenay (ed.) Progress in Cryptology – AFRICACRYPT 2008, Berlin, Heidelberg, 2008. Springer. P. 389–405.
2. Edwards H. A normal form for elliptic curves. *Bulletin of the American mathematical society*. 2007. 44(3). P. 393–422.
3. Fulton W. Algebraic curves. An Introduction to Algebraic Geometry. Addison-Wesley, 3 edition, 2008.
4. Koblitz N. Elliptic curve cryptosystems. *Mathematics of computation*. 1987. 48(177). P. 203–209.
5. Lidl R., Niederreiter H. Introduction to Finite Fields and their Applications. Cambridge University Press, 1994.
6. Montgomery P. L. Speeding the pollard and elliptic curve methods of factorization. *Mathematics of computation*. 1987. 48(177). P. 243–264.
7. Schoof R. Counting points on elliptic curves over finite fields. *Journal de théorie des nombres de Bordeaux*. 1995. 7(1). P. 219–254.
8. Skuratovskii R. V. 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. 2018. P. 75–80.
9. Skuratovskii R. V. Supersingularity of elliptic curves over F_{p_n}. *Research in Mathematics and Mechanics*. 2018. 31(1). P. 17–26. (in Ukrainian)
10. Skuratovskii R. V. Employment of minimal generating sets and structure of sylow 2-subgroups alternating groups in block ciphers. In: Advances in Computer Communication and Computational Sciences. Springer. 2019. P. 351–364.
11. Stepanov S. A. Arifmetika algebraicheskikh krivykh. Nauka. Glav. red. fiziko-matematicheskoĭ lit-ry. 1991. (in Russian)
12. Vinogradov I. M. Elements of number theory. Courier Dover Publications. 2016.
13. Barreto P. S. L. M., Naehrig M. Pairing-friendly elliptic curves of prime order. In: Bart Preneel and Stafford Tavares (eds.) Selected Areas in Cryptography. Berlin, Heidelberg, 2006. Springer. P. 319–331.
14. Glazunov N. M., Skobelev S. P. Manifolds over the rings. *IAMM National Academy of Sciences of Ukraine*. Donetsk. 2011. P. 323.
15. Varbanec P. D., Zarzycki P. Divisors of the Gaussian integers in an arithmetic progression. *Journal of Number Theory*. 1989. Vol. 33. Iss. 2. P. 152–169
16. Silverman J. H. The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics. Vol. 106. Springer-Verlag. 1986.
17. Skuratovskii R. V., Williams A. A solution of the inverse problem to doubling of twisted Edwards curve point over finite field. Processing, transmission and security of information. 2019. vol. 2. Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Bialej.
18. Deligne P. La conjecture de Weil. *Publications Mathematiques de l'IHES*. 1974. Vol. 43. P. 273–307.
19. René Schoof. Counting points on elliptic curves over finite fields. *Journal de théorie des nombres de Bordeaux*, 7(1):219–254, 1995.
20. R. Skuratovskii. *The Derived Subgroups of Sylow 2-Subgroups of the Alternating Group and Commutator Width of Wreath Product of Groups*. Mathematics, Basel, Switzerland, 2020, 8 (4), pp. 3–22.

Received: 25.12.2019 / Accepted: 20.05.2020

СУПЕРСИНГУЛЯРНЫЕ КРИВЫЕ ЭДВАРДСА И МЕТОД ПОДСЧЕТА ПОРЯДКА КРИВОЙ ЭДВАРДСА НАД КОНЕЧНЫМ ПОЛЕМ

Р. В. Скуратовский

Национальный технический университет Украины «Киевский политехнический институт имени Игоря Сикорского», Институт кибернетики имени В.М. Глушкова НАНУ, Киев, Украина, E-mail: r.skuratovskii@kpi.ua, ruslan@unicyb.kiev.ua

Аннотация. Рассматриваются алгебраические аффинные и проективные кривые Эдвардса [2, 8] над конечным полем $\mathbb{F}_{p^n}$. Сложность проблемы дискретного логарифма в группе точек эллиптической кривой (ECDLP) [4] зависит от порядка этой кривой [10]. Известно, что многие современные криптосистемы [10] могут быть естественным образом построены на эллиптические кривых [4]. Мы исследуем алгебраические кривые Эдвардса над конечным полем, которые являются одним из наиболее многообещающих носителей множеств точек, использующихся для быстрых групповых операций [1]. Нами построен новый метод подсчета порядка кривой Эдвардса над конечным полем. Следует отметить, что этот метод может быть применен к определению порядка эллиптических кривых из-за бирациональной эквивалентности между эллиптическими кривыми и кривыми Эдвардса. Мы не только находим набор коэффициентов с соответствующими характеристиками поля, для которых эти кривые являются суперсингулярными, мы также дополнительно находим общую формулу, по которой можно определить, является ли кривая $E_d[\mathbb{F}_p]$ суперсингулярной над этим полем или нет. Таким образом необходимые и достаточные условия суперсингулярности найдены. В статье исследована степень вложения суперсингулярной кривой Эдвардса над $\mathbb{F}_{p^n}$ в конечное поле. Также найдена характеристика поля, где эта степень минимальна. В статье найден критерий суперсингулярности кривой Эдвардса над $\mathbb{F}_{p^n}$. Установлено взаимнооднозначное соответствие между суперсингулярными кривыми Эдвардса и суперсингулярными кривыми Монтгомери. Построен бирациональный изоморфизм между кривой Монтгомери и кривой Эдвардса. Указаны образы специальных точек, полученных при бирациональном изоморфизме, кривой Эдвардса на сферу Римана.

Ключевые слова: конечное поле, эллиптическая кривая, кривая Эдвардса, группа точек на эллиптической кривой.