UDC 512.624.3

Quantities of points on some Edwards curves

O. V. Rybak[1, a]

[1] *National Technical University of Ukraine «Igor Sikorsky Kiev Polytechnic Institute», Educational and Research Institute of Physics and Technology*

Abstract

The Edwards curves of the form $x^2 + y^2 = 1 + dx^2y^2$ are investigated in this article. An exact formula for the quantity of points on $x^2+y^2 = 1+dx^2y^2$ over a field F_p is obtained for odd prime numbers p. The special attention is paid to the curves with exactly $p+1$ points over the field F_p. These curves are called supersingular. They are not recommended for usage in cryptography, because their structure is relatively simple. The supersingularity of the curve $x^2 + y^2 \equiv 1 + 2x^2y^2 \pmod p$ is proved for any prime $p = 4m + 3$. Also some other values of d, for which $x^2 + y^2 \equiv 1 + dx^2y^2 \pmod p$ is supersingular, are found. For example, it is true for $d = 17 \pm 12\sqrt{2}$ and $p = 8k + 7$, where $\sqrt{2}$ is an element of F_p with the property $(\sqrt{2})^2 \equiv 2 \pmod p$.

Keywords: Edwards curve, elliptic curve, equation over a finite field, supersingularity.

Introduction

Determining the quantity of solutions of an equation over a finite field is an interesting task of the number theory. This task contains the independent mathematical interest, because its solution allows to study the properties of certain Diophantine equations. Also, the data about the quantity of the points on the curve over a finite field help to reveal some algebraic properties of the mentioned curve. For example, some values of the quantity of the points on a curve of the type $R(x, y) = 0$, where R is a polynomial, may tell about the simple algebraic structure of that curve.

One more application of determining the quantity of points of an algebraic curve has relation to the cryptography. Some modern coding systems are based on actions in certain algebraic group, which consists of pairs (x, y), where x and y are elements from a finite field and x, y satisfy certain equality in that field. A well-known example of such systems is a system on some elliptic curve of kind $y^2 \equiv x^3 + ax^2 + bx + c \pmod p$, where p is a sufficiently large prime number. Also we may use the systems, which are based on biquadratic curves $x^2+y^2 \equiv 1+dx^2y^2 \pmod p$. [1] For the creating and for the analysis of the systems, which are connected with the mentioned curves, we need to determine the quantity of points, which satisfy the equation of the curve. It is important for this quantity to be not equal to some values, for which the system is not reliable.

Let us remember some basic concepts. A field F_p is a set of residues from division by a prime number p, where the actions of addition and multiplication are defined. That is, the elements of this field are the residues 0, 1, ..., $p - 1$. The sum, the difference and the product of the elements a and b are such c, d and e from the set 0, 1, ..., $p - 1$, that $a + b \equiv c \pmod p$, $a-b \equiv d \pmod p$ and $ab \equiv e \pmod p$ respectively. Also we may perform division in the field F_p. The notation $a/b = f$ (where $b \neq 0$) means, that f is such an element of the set 0, 1, ..., $p - 1$, that $a \equiv bf \pmod p$. For example, the equality $2/3 = 4$ is correct in the field F_5, because $2 \equiv 3 \cdot 4 \pmod 5$.

The element a from the field F_p is a *quadratic residue*, if there is such an element b in F_p, for which $b^2 = a$. In the opposite case the element a is called a *quadratic non-residue*. For example, in the field F_7 the quadratic residues are 0, 1, 2 and 4, because $0^2 = 0$, $1^2 = 1$, $3^2 = 2$ and $2^2 = 4$. Let's notice, that the equality $3^2 = 2$ is true in the field F_7, because $3^2 = 9 \equiv 2 \pmod 7$.

Let us give an example of connection between the quantity of the points on a curve and its structure. Consider an equation $x^2 + y^2 = 1$ over F_p. One of the solutions of this equation is $x = -1$, $y = 0$. Let's find other solutions in the form $y = a(x + 1)$. We may understand the coefficient a as the slope of the secant line, which passes through the points $(-1, 0)$ and (x, y). For each $a \in F_p$ there is a unique solution, which is different from $(-1, 0)$, namely: $\left(\frac{1-a^2}{a^2+1}, \frac{2a}{a^2+1}\right)$.

If -1 is a quadratic non-residue respectively to the modulo p, then the equation $x^2 + y^2 = 1$ has $p + 1$ solutions in F_p. If -1 is a quadratic residue, then $p - 1$ solutions exist, because for those two $a \in F_p$, which satisfy the condition $a^2 = -1$, there is division by zero in the corresponding solution.

Let's show, how to build two more special solutions of this equation in the case, when there is such $b \in F_p$, for which $b^2 = -1$. Let $v = 1/x$ and $w = y/x$. The equation will be rewritten as $1/v^2 + w^2/v^2 = 1$, or $1 + w^2 = v^2$. Then the pairs $(v, w) = (0, -b)$ and $(v, w) = (0, b)$ are the solutions of the equation $1+w^2 = v^2$. If we would try to recover the pair (x, y) by the pair (v, w), then for the solutions $(0, -b)$ and $(0, b)$ we would get division by zero. That's why these solution are special. They don't belong to the field F_p, but they could be placed in the space of values, which is

[a] E-mail: semperfi@ukr.net

analogous to the Riemann's sphere for the complex numbers. With taking such expansion into account we have $p+1$ solutions.

The set of the points, whose coordinates are the solutions of the equation $x^2+y^2=1$ over the field F_p, is organized rather simply. And this set contains $p+1$ points, taking into account the special ones. It was revealed, that the curves of higher order, which contain $p+1$ points, are relatively simple too, so they don't fit well for coding. [3] Such curves are called supersingular.

Farther we shall regard the equation $x^2+y^2=1+dx^2y^2$ over the field F_p, where p is an odd prime number, $d \in F_p$, $d \neq 0$ and $d \neq 1$. The set of the solutions of this equation is called an Edwards curve. The curves of such form are studied, for example, in [1], where the connection between them and the elliptic curves of the form $y^2=x^3+ax^2+bx+c$ is shown. Also the properties of the Edwards curves are analysed in the works of Ukrainian authors in [2], [3] and [4].

A method of counting the points on an Edwards curve

An important tool for the next researches is the Legendre's symbol $\left(\frac{a}{p}\right)$. If a is a quadratic residue in the field F_p and is not divisible by p, then $\left(\frac{a}{p}\right)=1$. If a is a quadratic non-residue in the field F_p and is not divisible by p, then $\left(\frac{a}{p}\right)=-1$. If a is divisible by p, then $\left(\frac{a}{p}\right)=0$. For the Legendre's symbol the following formula is true.

Euler's formula. For all integers a and odd primes p the formula $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$ is correct.

The proof of this formula may be found, for example, in [5]. Due to Euler's formula it is easy to see the multiplicativity of the Legendre's symbol: for arbitrary integer a, b the equality $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{a}{p}\right)$ is fulfilled.

For determining the quantity of points, which are situated on a certain curve, we shall need the following lemma.

Lemma about powers. For an arbitrary natural n and any prime p there is a relation $\sum\limits_{k=0}^{p-1} k^n \equiv -1 \pmod p$, if $n \vdots (p-1)$, and $\sum\limits_{k=0}^{p-1} k^n \equiv 0 \pmod p$, if $n \not\vdots (p-1)$.

Proof. Let's notice, that $\sum\limits_{k=0}^{p-1} k^n = \sum\limits_{k=1}^{p-1} k^n$. That's why it is sufficient to prove, that $\sum\limits_{k=1}^{p-1} k^n \equiv -1 \pmod p$ for $n \vdots p-1$, and $\sum\limits_{k=1}^{p-1} k^n \equiv 0 \pmod p$ for $n \not\vdots p-1$. Let m and r are such integer numbers, that $n=m(p-1)+r$ and $0 \leq r \leq p-2$.

Firstly let's consider the case $n \vdots p-1$. Then $n=m(p-1)$. If $1 \leq k \leq p-1$, then Fermat's little theorem implies: $k^n \equiv (k^{p-1})^m \equiv 1^m \equiv 1 \pmod p$. So, $\sum\limits_{k=1}^{p-1} k^n \equiv (p-1)\cdot 1 \equiv -1 \pmod p$.

Let's $n \not\vdots p-1$ now. In this case $1 \leq r \leq p-2$. By Fermat's little theorem, $\sum\limits_{k=1}^{p-1} k^n \equiv \sum\limits_{k=1}^{p-1} (k^{p-1})^m k^r \equiv \sum\limits_{k=1}^{p-1} k^r \pmod p$. Consider an arbitrary integer a, which is not divisible by p. For all integer k $(1 \leq k \leq p-1)$ the number ka is not divisible by p, because p is a prime number. Also for all integer j, k $(1 \leq j < k \leq p-1)$ the numbers ja and ka give distinct residues from division by p. Otherwise $a(k-j)$ would be divisible by p, but it is impossible due to the inequality $1 \leq k-j \leq p-2$. So, if we consider the set $\{a,\ 2a,\ ...,\ (p-1)a\}$ as the set of elements of the field F_p, then this set would contain $p-1$ distinct elements, which are not equal to zero. Hence $\{a,\ 2a,\ ...,\ (p-1)a\}$ coincides with $\{1,\ 2,\ ...,\ p-1\}$. Then the sums $\sum\limits_{k=1}^{p-1} k^n$ and $\sum\limits_{k=1}^{p-1} (ka)^n$ coincide in the field F_p. So, the relation $\sum\limits_{k=1}^{p-1} k^r \equiv \sum\limits_{k=1}^{p-1} (ka)^r \equiv a^r \sum\limits_{k=1}^{p-1} k^r \pmod p$ is correct. Let's choose such a, that $1 \leq a \leq p-1$ and $a^r \not\equiv 1 \pmod p$. The mentioned number a always exists: otherwise the polynomial x^r-1 would have $p-1$ roots in the field F_p, what is impossible, because $r<p-1$. From the relation $\sum\limits_{k=1}^{p-1} k^r \equiv a^r \sum\limits_{k=1}^{p-1} k^r \pmod p$ we get $(a^r-1)\sum\limits_{k=1}^{p-1} k^r \equiv 0 \pmod p$. By the choice of a, the condition $a^r-1 \not\equiv 0 \pmod p$ is true. So, $\sum\limits_{k=1}^{p-1} k^r \equiv 0 \pmod p$. That's why the relation $\sum\limits_{k=1}^{p-1} k^n \equiv 0 \pmod p$ is true, what was needed to prove.

The lemma about powers is proved.

Now let's prove the theorem, which gives us the possibility of counting the points on the curve $x^2+y^2=1+dx^2y^2$.

Theorem 1. Let p be an odd prime number, and let d be an element of the field F_p. Let d be different from 0 and 1. Let's denote by N_d the quantity of pairs (x,y), for which $x^2+y^2=1+dx^2y^2$ and $x,y \in F_p$. Also let q be such a number, that $p=2q+1$. Then $N_d \equiv (-1)^{q+1} \sum\limits_{k=0}^{q} (C_q^k)^2 d^k - 1 - 2\left(\frac{d}{p}\right) \pmod p$.

Proof. Let's transform the equation of the curve to $y^2(1-dx^2)=1-x^2$ and let's multiply both parts by $1-dx^2$. We shall get $y^2(1-dx^2)^2=(1-x^2)(1-dx^2)$. Let's perform the substitution $z=y(1-dx^2)$, after which the equation will transform to $z^2=(1-x^2)(1-dx^2)$. For each pair (x,z), which is the solution of this equation and for which $1-dx^2 \neq 0$, there is a pair (x,y) with $y=z/(1-dx^2)$, which is a solution of $y^2(1-dx^2)=1-x^2$. If $1-dx^2=0$, then there is no corresponding solution of the equation $y^2(1-dx^2)=1-x^2$, because in the case $d \neq 1$ the elements $1-dx^2$

and $1-x^2$ cannot be equal to 0 at the same time. So, if we

denote the quantity of the solutions of the equation $z^2=(1-x^2)(1-dx^2)$ by M_d, then the difference M_d-N_d is equal to the quantity of such x, that $1-dx^2=0$. Hence $M_d-N_d=1+\left(\frac{d}{p}\right)$, which could be transformed to $N_d=M_d-1-\left(\frac{d}{p}\right)$.

For determining M_d let's use the following method. Let $S(x)$ be a polynomial with integer coefficients. Let's assume, that an equation $z^2=S(x)$ is defined over the field F_p. Then for a fixed element x the quantity of such $z\in F_p$, that satisfy the given relation, is equal to $\left(\frac{S(x)}{p}\right)+1$. Let's apply this observation to the equation $z^2=(1-x^2)(1-dx^2)$. Regarding all $x\in F_p$, we shall add the quantities of such meanings of z, which satisfy the condition $z^2=(1-x^2)(1-dx^2)$ for the given x. We get $M_d=\sum\limits_{x=0}^{p-1}\left(1+\left(\frac{(1-x^2)(1-dx^2)}{p}\right)\right)$. So, by Euler's formula: $M_d\equiv\sum\limits_{x=0}^{p-1}(1-x^2)^{\frac{p-1}{2}}(1-dx^2)^{\frac{p-1}{2}}\pmod p$.

The polynomial $(1-x^2)^{\frac{p-1}{2}}(1-dx^2)^{\frac{p-1}{2}}$ is equal to $1+a_1x+a_2x^2+...+a_{2p-2}x^{2p-2}$ for some integer coefficients a_1, a_2, ..., a_{2p-2}. So, $M_d\equiv\sum\limits_{x=0}^{p-1}\left(1+\sum\limits_{k=1}^{2p-2}a_kx^k\right)\equiv p+\sum\limits_{k=1}^{2p-2}\sum\limits_{x=0}^{p-1}a_kx^k\pmod p$, whence $M_d\equiv\sum\limits_{k=1}^{2p-2}\left(a_k\sum\limits_{x=0}^{p-1}x^k\right)\pmod p$. By the lemma about powers, only $k=p-1$ and $k=2p-2$ make a non-zero input to the last expression. That is, $M_d\equiv-a_{p-1}-a_{2p-2}\pmod p$. Let's determine a_{p-1} and a_{2p-2}. Let's remember, that $q=\frac{p-1}{2}$. The product $(1-x^2)^{\frac{p-1}{2}}(1-dx^2)^{\frac{p-1}{2}}$ is equal to $\left(\sum\limits_{k=0}^{q}C_q^k(-1)^kx^{2k}\right)\cdot\left(\sum\limits_{k=0}^{q}C_q^k(-1)^kd^kx^{2k}\right)$.

The monomials with the multiplier x^{p-1} are obtained, when the summands $C_q^{q-k}(-1)^{q-k}x^{2q-2k}$ and $C_q^k(-1)^kx^{2k}$ multiply between each other. That is, $a_{p-1}=(-1)^q\sum\limits_{k=0}^{q}C_q^{q-k}C_q^kd^k$. So, $a_{p-1}=(-1)^q\sum\limits_{k=0}^{q}(C_q^k)^2d^k$. We obtain the monomial with the multiplier x^{2p-2}, only when we multiply the summands with the maximal powers of x. So, $a_{2p-2}=(-1)^{2q}d^q=d^{\frac{p-1}{2}}\equiv\left(\frac{d}{p}\right)\pmod p$.

From the expressions for a_{p-1} and a_{2p-2} we obtain the equality

$$M_d\equiv(-1)^{q+1}\sum_{k=0}^{q}(C_q^k)^2d^k-\left(\frac{d}{p}\right)\pmod p.$$

Because of $N_d=M_d-1-\left(\frac{d}{p}\right)$, we get

$$N_d\equiv(-1)^{q+1}\sum_{k=0}^{q}(C_q^k)^2d^k-1-2\left(\frac{d}{p}\right)\pmod p.$$

The theorem 1 is proved.

Let's show, that for any odd prime number p the quantity of the points of the curve $x^2+y^2=1+dx^2y^2$ over the field F_p is divisible by 4. Among the points (x,y), for which $x=0$ or $y=0$, only the points $(0,1)$, $(0,-1)$, $(-1,0)$ and $(1,0)$ get onto our curve. If a point (x_1,y_1) belongs to our curve and both its coordinates are distinct from zero, then (x_1,y_1), $(-x_1,y_1)$, $(x_1,-y_1)$ and $(-x_1,-y_1)$ satisfy the equation of the curve. For an odd p all such four points are distinct. So, the points of the curve split into the groups of 4 points. That's why the quantity of the points is divisible by 4.

Let's rewrite the equation $x^2+y^2=1+dx^2y^2$ as $y^2(dx^2-1)=x^2-1$. If $d\neq1$, then the elements dx^2-1 and x^2-1 cannot be equal to zero simultaneously. That's why for every meaning of x there are no more than two such meanings of y, that the point (x,y) belongs to the curve. So, the quantity of the points of the curve $x^2+y^2=1+dx^2y^2$ over the field F_p lies on the segment $[4,2p]$.

It follows from the theorem 1, that the quantity of the points on the mentioned Edwards curve is equal to $mp-1-2\left(\frac{d}{p}\right)+(-1)^{q+1}\sum\limits_{k=0}^{q}(C_q^k)^2d^k$, where $q=\frac{p-1}{2}$ and m is some integer number. There are at most two numbers of such kind on the segment $[4,2p]$. Among them only one number can be even. Due to this it is possible to compute the unique appropriate meaning of the number m, and together with it – the quantity of the points of the curve.

Detection of the supersingular curves

If $\left(\frac{d}{p}\right)=1$ and the Edwards curve contains $p-1-2\left(\frac{d}{p}\right)$ points, whose coordinates belong to the field F_p, then we may add special solutions to this curve. For this let's do the substitutions $v=1/x$ and $w=1/y$. The equation will transform into $1/v^2+1/w^2=1+d/(v^2w^2)$, that is $w^2+v^2=v^2w^2+d$. Among its solutions there are $(0,c)$, $(0,-c)$, $(c,0)$ and $(-c,0)$, where $c^2\equiv d\pmod p$. The shown variants don't correspond to any pair (x,y), where $x,y\in F_p$. So, together with these solutions the Edwards curve contains exactly $p+1$ point.

It was noticed experimentally, that the curve $x^2+y^2=1+2x^2y^2$ demonstrates the described property for prime numbers of the type $p=4m+3$. The quantity of its points is equal to $p+1$ for $p\equiv3\pmod8$ and is equal to $p-3$ for $p\equiv7\pmod8$. Let's prove the theorem, which confirms these observations.

Theorem 2. For an arbitrary prime p of the type $4m+3$ and for $q=\frac{p-1}{2}$ the relation $\sum\limits_{k=0}^{q}(C_q^k)^22^k\equiv0\pmod p$ holds.

Proof. Let's prove, that $(q!)^2\cdot\sum\limits_{k=0}^{q}(C_q^k)^22^k\equiv0\pmod p$. The number $(q!)^2$ is relatively prime with p, from where we shall get $\sum\limits_{k=0}^{q}(C_q^k)^22^k\equiv0\pmod p$.

Let's remember, that $C_q^k=\frac{q!}{k!(q-k)!}$. Hence $q!\cdot C_q^k=\frac{q!}{k!}\cdot\frac{q!}{(q-k)!}=\left(\prod\limits_{m=k+1}^{q}m\right)\cdot\left(\prod\limits_{m=1}^{k}(q-k+m)\right)$. Because of $p=2q+1$, for arbitrary k and m the relation

$q-k+m \equiv -(q+k-m+1) \pmod p$ is correct. Applying this fact to the product $\prod_{m=1}^{k}(q-k+m)$, we have $q!\cdot C_q^k \equiv \left(\prod_{m=k+1}^{q} m\right) \cdot \left(\prod_{m=1}^{k}(-(q+k-m+1))\right) \pmod p$. This gives $q! \cdot C_q^k \equiv (-1)^k \cdot \left(\prod_{m=k+1}^{q} m\right) \cdot \left(\prod_{m=1}^{k}(q+k-m+1)\right) \pmod p$. Let's make a substitution $j = q+k-m+1$ in the second product and get $q! \cdot C_q^k \equiv (-1)^k \cdot \left(\prod_{m=k+1}^{q} m\right) \cdot \left(\prod_{j=q+1}^{q+k} j\right) \pmod p$, that is $q! \cdot C_q^k \equiv (-1)^k \cdot (k+1)(k+2) \cdot ... \cdot (k+q) \pmod p$. Taking squares of the both parts, we get

$$(q!)^2 \cdot (C_q^k)^2 \equiv (k+1)^2(k+2)^2 \cdot ... \cdot (k+q)^2 \pmod p.$$

Let $R(x) = \sum_{k=0}^{q}(k+1)^2(k+2)^2 \cdot ... \cdot (k+q)^2 x^k$. We need to prove, that $R(2) \equiv 0 \pmod p$. Let's consider a polynomial

$$B(x) = \frac{d^q}{dx^q}\left(x^q \cdot \frac{d^q}{dx^q}\left(x^q \cdot (x^{p-1} + x^{p+2} + ... + 1)\right)\right).$$

That is, $B(x) = \sum_{k=0}^{p-1}(k+1)^2(k+2)^2 \cdot ... \cdot (k+q)^2 x^k$. For $q < k \le p-1$ the product $(k+1)^2(k+2)^2 \cdot ... \cdot (k+q)^2$ contains a multiplier, which is equal to p. So, $B(x) \equiv \sum_{k=0}^{q}(k+1)^2(k+2)^2 \cdot ... \cdot (k+q)^2 x^k \pmod p$, whence $B(x) \equiv R(x) \pmod p$. Let's remark: under the notation $B(x) \equiv R(x) \pmod p$ is meant, that all respective coefficients of $B(x)$ and $R(x)$ coincide modulo p.

Let's show, that $x^{p-1} + x^{p-2} + ... + 1 \equiv (x-1)^{p-1} \pmod p$. According to Newton's binomial, $(x-1)^{p-1} = \sum_{k=0}^{p-1} C_{p-1}^k (-1)^k x^{p-1-k}$. Let's remember, that $C_{p-1}^0 = 1$. For transformation of the other coefficients let's use the equality $C_{p-1}^k = C_p^k - C_{p-1}^{k-1}$ $(1 \le k \le p-1)$. Applying it to k from 1 to $p-1$ consequently, we get $C_{p-1}^k = \sum_{i=0}^{k}(-1)^i C_p^{k-i}$. Because of primeness of the number p, for all $k = 1, 2, ..., p-1$ the number $C_p^k = \frac{p!}{k!(p-k)!}$ is divisible by p. The divisibility has place, because the numerator $p!$ is divisible by p, and the denominator $k!(p-k)!$ is not. Also $C_p^0 = C_p^p = 1$. So, for natural k from 1 to $p-2$ we get: $C_{p-1}^k \equiv \sum_{i=0}^{k}(-1)^i C_p^{k-i} \pmod p$, from where we have $C_{p-1}^k \equiv \sum_{i=0}^{k-1}(-1)^i C_p^{k-i} + (-1)^k C_p^0 \equiv (-1)^k \pmod p$. So, $(x-1)^{p-1} \equiv \sum_{k=0}^{p-1}(-1)^k C_{p-1}^k x^k \equiv \sum_{k=0}^{p-1}(-1)^{2k} x^k \pmod p$. That is,

$$(x-1)^{p-1} \equiv x^{p-1} + x^{p-2} + ... + 1 \pmod p.$$

For arbitrary polynomials $F(x)$ and $G(x)$ from $F(x) \equiv G(x) \pmod p$ the equivalence $\frac{d}{dx}F(x) \equiv \frac{d}{dx}G(x) \pmod p$ follows. That's why we get:

$$B(x) \equiv \frac{d^q}{dx^q}\left(x^q \cdot \frac{d^q}{dx^q}(x^q \cdot (x-1)^{p-1})\right) \pmod p.$$

Let $x = y+1$. Then $B(x)$ may be presented in the form $B(y+1)$. Because of $\frac{dx}{dy} = \frac{d(y+1)}{dy} = 1$, for an arbitrary polynomial $F(x)$ we have $\frac{d}{dy}F(y+1) = \frac{d}{dx}F(x) \cdot \frac{dx}{dy} = \frac{d}{dx}F(x)$. So, the derivative by x could be replaced with the derivative by y: $B(x) \equiv \frac{d^q}{dy^q}\left((y+1)^q \cdot \frac{d^q}{dy^q}((y+1)^q \cdot y^{p-1})\right) \pmod p$. In the polynomial $(y+1)^q y^{p-1} = \sum_{k=0}^{q} C_q^k y^{k+p-1}$ all monomials, except y^{p-1}, will get a coefficient with a multiplier p after the q-th derivation. That's why $\frac{d^q}{dy^q}((y+1)^q \cdot y^{p-1}) \equiv \frac{(p-1)!}{q!} y^q \pmod p$. Taking this relation into account, we get $B(x) \equiv \frac{d^q}{dy^q}\left((y+1)^q \cdot \frac{(p-1)!}{q!} y^q\right) \pmod p$. That is, $B(x) \equiv \frac{(p-1)!}{q!} \cdot \frac{d^q}{dy^q}((y+1)^q y^q) \pmod p$. By Newton's binomial: $\frac{d^q}{dy^q}(y+1)^q y^q = \sum_{k=0}^{q}(k+1) \cdot ... \cdot (k+q) C_q^k y^k$. So,

$$B(x) \equiv \frac{(p-1)!}{q!} \cdot \sum_{k=0}^{q}(k+1) \cdot ... \cdot (k+q) C_q^k y^k \pmod p.$$

Let's show, that for $p = 4m+3$ and $y = 1$ the relation $B(y+1) \equiv 0 \pmod p$ holds. Let $b_k = (k+1) \cdot ... \cdot (k+q) C_q^k$ for all $k = 0, ..., q$. Then $B(y+1) \equiv \frac{(p-1)!}{q!} \cdot \sum_{k=0}^{q} b_k y^k \pmod p$. For every s the relation $k+s \equiv -((q-k)+q+1-s) \pmod p$ is correct, because the right side of this relation is equal to $k+s+2q+1$, that is $k+s+p$. So, $\prod_{s=1}^{q}(k+s) \equiv (-1)^q \cdot \prod_{s=1}^{q}((q-k)+q+1-s) \pmod p$. Taking into account, that $q = \frac{p-1}{2} = 2m+1$ is an odd number, from the previous relation of the products we get $\prod_{s=1}^{q}(k+s) \equiv -\prod_{s=1}^{q}((q-k)+q+1-s) \pmod p$. If the substitution $j = q+1-s$ is performed in the product $\prod_{s=1}^{q}((q-k)+q+1-s)$, then this product will turn into $\prod_{j=1}^{q}((q-k)+j)$, because while s changes its values from 1 to q, the variable $j = q+1-s$ also changes the values from 1 to q in the reversed order. So, $\prod_{s=1}^{q}(k+s) \equiv -\prod_{j=1}^{q}((q-k)+j) \pmod p$. Let's remember, that $C_q^k = C_q^{q-k}$. If j is replaced by s in the second product, then $\prod_{s=1}^{q}(k+s) \equiv -\prod_{s=1}^{q}((q-k)+s) \pmod p$ will be obtained. Let's remember, that $C_q^k = C_q^{q-k}$. That's why $C_q^k \cdot \prod_{s=1}^{q}(k+s) \equiv -C_q^{q-k} \cdot \prod_{s=1}^{q}((q-k)+s) \pmod p$. That is, $b_{q-k} \equiv -b_k \pmod p$. Substituting $y = 1$ into the expression $B(y+1) \equiv \frac{(p-1)!}{q!} \cdot \sum_{k=0}^{q} b_k y^k \pmod p$, we obtain $B(1+1) \equiv \frac{(p-1)!}{q!} \cdot \sum_{k=0}^{q} y^k \pmod p$. So, $B(2) \equiv$

$\frac{(p-1)!}{q!}\cdot\left(\sum\limits_{k=0}^{(q-1)/2}b_k+\sum\limits_{l=(q+1)/2}^{q}b_l\right)\pmod p$. Let's do a substitution $l=q-k$ in the second sum. The result of this transformation is the formula $B(2)\equiv\frac{(p-1)!}{q!}\cdot\left(\sum\limits_{k=0}^{(q-1)/2}b_k+\sum\limits_{k=0}^{(q-1)/2}b_{q-k}\right)\pmod p$. That is, $B(2)\equiv\frac{(p-1)!}{q!}\cdot\left(\sum\limits_{k=0}^{(q-1)/2}b_k+\sum\limits_{k=0}^{(q-1)/2}(-b_k)\right)\equiv 0\pmod p$, what was needed to show.

And then $(q!)^2\cdot\sum\limits_{k=0}^{q}(C_q^k)^2 2^k\equiv R(2)\equiv B(2)\equiv 0\pmod p$, what implies $\sum\limits_{k=0}^{q}(C_q^k)^2 2^k\equiv 0\pmod p$.

The theorem 2 is proved.

From theorem 2 follows, that in the case $p\equiv 3\pmod 4$ the curve $x^2+y^2=1+2x^2y^2$ contains $p-1-2\left(\frac{2}{p}\right)$ points over the field F_p. The cases, when the quantity of the points is equal to $-1-2\left(\frac{2}{p}\right)$ or $2p-1-2\left(\frac{2}{p}\right)$, are impossible, because these numbers are odd. Other variants of the form $mp-1-2\left(\frac{2}{p}\right)$ don't get onto the segment $[4,2p]$.

As it is known, $\left(\frac{2}{p}\right)=(-1)^{\left[\frac{p+1}{4}\right]}$. [5] In particular, the equalities $\left(\frac{2}{p}\right)=-1$ for $p\equiv 3\pmod 8$ and $\left(\frac{2}{p}\right)=1$ for $p\equiv 7\pmod 8$ hold. That's why for a prime $p=8m+3$ the curve $x^2+y^2=1+2x^2y^2$ contains $p+1$ points over the field F_p, and for $p=8m+7$ it contains $p-3$ points. In the case $p=8m+7$ it is possible to add 4 virtual points to the mentioned curve by the substitutions $v=1/x$ and $w=1/y$, as was shown earlier.

So, in the cases $p=8m+3$ and $p=8m+7$ the curve $x^2+y^2=1+2x^2y^2$ contains exactly $p+1$ points together with special ones. That is, for $p\equiv 3\pmod 4$ the curve $x^2+y^2=1+2x^2y^2$ over the field F_p is supersingular.

It is interesting to explore, for which other values of d the curve $x^2+y^2=1+dx^2y^2$ demonstrates supersingularity for some series of prime numbers. From theorem 1 we get, that it will be observed for those and only those d, for which $\sum\limits_{k=0}^{q}(C_q^k)^2 d^k\equiv 0\pmod p$, where $q=\frac{p-1}{2}$.

For example, let's note, that together with an arbitrary $d\neq 0$ this condition will be satisfied by d^{-1} – the element, which is equal to $1/d$ in the field F_p. Really, $\sum\limits_{k=0}^{q}(C_q^k)^2 d^{-k}\equiv d^{-q}\cdot\sum\limits_{k=0}^{q}(C_q^k)^2 d^{q-k}\pmod p$. Due to the equality $C_q^k=C_q^{q-k}$ we have $\sum\limits_{k=0}^{q}(C_q^k)^2 d^{-k}\equiv d^{-q}\cdot\sum\limits_{k=0}^{q}(C_q^{q-k})^2 d^{q-k}\pmod p$. This gives

$$\sum_{k=0}^{q}(C_q^k)^2 d^{-k}\equiv d^{-q}\cdot\sum_{s=0}^{q}(C_q^s)^2 d^s\pmod p,$$

after the substitution $s=q-k$ in the right part. So, from $\sum\limits_{k=0}^{q}(C_q^k)^2 d^k\equiv 0\pmod p$ the relation $\sum\limits_{k=0}^{q}(C_q^k)^2(d^{-1})^k\equiv 0\pmod p$ follows.

One more similar result is stated as a theorem.

Theorem 3. Let $d\neq 1$ be a quadratic residue by the prime modulo $p=2q+1$. Let $\sqrt{d}$ denote an arbitrary element $c\in F_p$, for which $c^2=d$. Then from the relation $\sum\limits_{k=0}^{q}(C_q^k)^2 d^k\equiv 0\pmod p$ the equivalence $\sum\limits_{k=0}^{q}(C_q^k)^2 g^k\equiv 0\pmod p$ follows for $g=\left(\frac{\sqrt{d}-1}{\sqrt{d}+1}\right)^2$.

Proof. By the theorem 1, if the condition $\sum\limits_{k=0}^{q}(C_q^k)^2 d^k\equiv 0\pmod p$ holds, then the curve $x^2+y^2=1+dx^2y^2$ contains exactly $p-1-2\left(\frac{d}{p}\right)$ points (x,y), whose coordinates belong to the field F_p. Let's rewrite the equation of the curve in the form $y^2(dx^2-1)=x^2-1$. Now let's perform the substitutions $x=\frac{1+u}{1-u}$ and $y=\frac{2u}{v}$. The equation will take the form $\frac{4u^2}{v^2}\cdot\frac{(d-1)u^2+2(d+1)u+(d-1)}{(1-u)^2}=\frac{4u}{(1-u)^2}$. Let's multiply both parts by $\frac{v^2(1-u)^2}{4u}$. We shall get the relation

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

Now our task is to analyse, which new solutions of the given equation appeared relatively to $y^2(dx^2-1)=x^2-1$, and which solutions disappeared.

At the beginning let's describe the solutions (u,v), where $v=0$. A solution of such type cannot correspond to any pair (x,y), because for the evaluation of the needed coordinates (x,y) we would divide by zero in the formula $y=\frac{2u}{v}$. For $v=0$ the equation transforms into $(d-1)u^3+2(d+1)u^2+(d-1)u=0$. Let's find its solutions. Firstly, the variant $u=0$ fits. Secondly, the needed solutions are the roots of the equation $(d-1)u^2+2(d+1)u+(d-1)=0$. They can be found by the formula $u=\frac{-b\pm\sqrt{b^2-ac}}{a}$ for roots of an equation $au^2+2bu+c=0$, where $a\neq 0$. The formula acts in an arbitrary field, so in F_p too. We have $u=\frac{-(d+1)\pm 2\sqrt{d}}{d-1}$. So, if d is a quadratic residue by modulo p, then the solutions $u=\frac{-(d+1)-2\sqrt{d}}{d-1}$ and $u=\frac{-(d+1)+2\sqrt{d}}{d-1}$ are added. That is, in the case $\left(\frac{d}{p}\right)=-1$ exactly one additional solution, which satisfies the condition $v=0$, appears: it is $(u,v)=(0,0)$. In the case $\left(\frac{d}{p}\right)=1$ three additional solutions of such form appear. Uniting these cases, we obtain $2+\left(\frac{d}{p}\right)$ additional solutions (u,v), for which $v=0$.

Also no pairs (x,y) correspond the solutions (u,v), where $u=1$.

The correspondent pairs (x,y) are absent because of division by zero in the expression $x=\frac{1+u}{1-u}$. For $u=1$ our equation transforms into $v^2=4d$. If d is a quadratic residue by modulo p, then new solutions $(u,v)=(1,-2\sqrt{d})$ and $(u,v)=(1,2\sqrt{d})$ appear. We have $1+\left(\frac{d}{p}\right)$ solutions more.

On the other side, the reverse substitutions have the form $u = \frac{x-1}{x+1}$ and $v = \frac{2(x-1)}{y(x+1)}$. So, the solutions with $x = -1$ or $y = 0$ disappear, because they don't correspond to pairs (u, v). Substituting $x = -1$ and $y = 0$ to the equation $y^2(dx^2-1)x^2-1$ separately, we get two disappearing solutions: $(x, y) = (-1, 0)$ and $(x, y) = (1, 0)$.

Let L_d denote the quantity of the points (u, v), for which $v^2 = (d-1)u^3+2(d+1)u^2+(d-1)u$ and $u, v \in F_p$. According to the described properties of the solutions (u, v) and (x, y), if the curve $x^2+y^2 = 1+dx^2y^2$ contains exactly $p-1-2\left(\frac{d}{p}\right)$ points (x, y) with coordinates in the field F_p, then the equality $L_d = p-1-2\left(\frac{d}{p}\right)+2+\left(\frac{d}{p}\right)+1+\left(\frac{d}{p}\right)-2 = p$ holds.

Now let's apply the technique of evaluation of the quantity of the points by the modulo p, which was in the proof of the theorem 1. We have $L_d \equiv \sum\limits_{u=0}^{p-1}\left(\frac{(d-1)u^3+2(d+1)u^2+(p-1)u}{p}\right) \pmod p$, that is

$$L_d \equiv \sum_{u=0}^{p-1}((d-1)u^3+2(d+1)u^2+(p-1)u)^{\frac{p-1}{2}} \pmod p.$$

By condition, the element $\sqrt{d}$ exists in F_p. We can check directly the equality $(d-1)u^3+2(d+1)u^2+(p-1)u = (d-1)u\left(u+\frac{\sqrt{d}-1}{\sqrt{d}+1}\right)\left(u+\frac{\sqrt{d}+1}{\sqrt{d}-1}\right)$. So, $L_d \equiv (d-1)^q\sum\limits_{u=0}^{p-1}u^q\left(u+\frac{\sqrt{d}-1}{\sqrt{d}+1}\right)^q\left(u+\frac{\sqrt{d}+1}{\sqrt{d}-1}\right)^q \pmod p$, where $q = \frac{p-1}{2}$.

By the lemma about powers, $L_d \equiv -(d-1)^q b_{p-1} \pmod p$, where b_0, b_1, ..., b_{3q} are such numbers, for which $u^q\left(u+\frac{\sqrt{d}-1}{\sqrt{d}+1}\right)^q\left(u+\frac{\sqrt{d}+1}{\sqrt{d}-1}\right)^q = b_{3q}u^{3q}+...+b_1u+b_0$. Because of $p = 2q+1$, we have the equality $b_{p-1} = \sum\limits_{k=0}^{q}(C_q^k)^2\left(\frac{\sqrt{d}-1}{\sqrt{d}+1}\right)^k\left(\frac{\sqrt{d}+1}{\sqrt{d}-1}\right)^{q-k}$, whence

$$b_{p-1} = \left(\frac{\sqrt{d}+1}{\sqrt{d}-1}\right)^q \cdot \sum_{k=0}^{q}(C_q^k)^2\left(\frac{\sqrt{d}-1}{\sqrt{d}+1}\right)^{2k}.$$

So,

$$L_d \equiv (-1)^q(\sqrt{d}+1)^{2q}\sum_{k=0}^{q}(C_q^k)^2\left(\frac{\sqrt{d}-1}{\sqrt{d}+1}\right)^{2k} \pmod p.$$

We have already proved the equality $L_d = p$. That's why $L_d \equiv 0 \pmod p$. We get

$$\sum_{k=0}^{q}(C_q^k)^2\left(\frac{\sqrt{d}-1}{\sqrt{d}+1}\right)^{2k} \equiv 0 \pmod p,$$

what was needed to prove.

The theorem 3 is proved.

For example, if $p \equiv 7 \pmod 8$, than 2 is a quadratic residue by modulo p. So, from the theorems 2 and 3 we have, that for $g = \left(\frac{\sqrt{2}-1}{\sqrt{2}+1}\right)^2$ the curve $x^2+y^2 \equiv 1+gx^2y^2 \pmod p$ is supersingular. Multiplying the numerator and the denominator in the expression for g by $\sqrt{2}-1$, we get

$$g = \left(\frac{(\sqrt{2}-1)^2}{(\sqrt{2}+1)(\sqrt{2}-1)}\right)^2 = 17-12\sqrt{2}.$$

In such a way, the curve $x^2+y^2 \equiv 1+(17-12\sqrt{2})x^2y^2 \pmod p$ is supersingular for an arbitrary prime $p \equiv 7 \pmod 8$. The same is correct for the coefficient $g = 17+12\sqrt{2}$, because $17+12\sqrt{2} = (17-12\sqrt{2})^{-1}$.

Conclusions

The formula for the quantity of points of a biquadratic Edward's curve $x^2+y^2 = 1+dx^2y^2$ over the field F_p for an odd prime p and $d \neq 1$ is obtained. The quantity of the points, whose coordinates belong to the field, is equal to some $mp-1-2\left(\frac{d}{p}\right)+(-1)^{q+1}\sum\limits_{k=0}^{q}(C_q^k)^2d^k$, where $q = \frac{p-1}{2}$ and m is an integer number. This quantity belongs to the segment $[4, 2p]$ and is even, that's why is determined unambiguously. If we take into account the special points, then the general quantity of the points of the curve equals $mp+1+(-1)^{q+1}\sum\limits_{k=0}^{q}(C_q^k)^2d^k$.

If the condition $\sum\limits_{k=0}^{q}(C_q^k)^2d^k \equiv 0 \pmod p$ holds, then the curve $x^2+y^2 = 1+dx^2y^2$ is supersingular, that means it contains exactly $p+1$ points.

We proved, that for $p \equiv 3 \pmod 4$ the curve $x^2+y^2 = 1+2x^2y^2$ is supersingular over the field F_p.

Also it is shown, that the supersingularity of the curve $x^2+y^2 = 1+dx^2y^2$ implies the supersingularity of the curves of the form $x^2+y^2 = 1+gx^2y^2$ for $g = d^{-1}$, $g = \left(\frac{\sqrt{d}-1}{\sqrt{d}+1}\right)^2$ and $g = \left(\frac{\sqrt{d}+1}{\sqrt{d}-1}\right)^2$.

Analogous results have place for the elliptic curve $v^2 = (d-1)u^3+2(d+1)u^2+(d-1)u$, because there are the same quantity of the points on it, as on $x^2+y^2 = 1+dx^2y^2$, if we take into account the special points.

References

[1] H. M. Edwards, "A normal form for elliptic curves", *Bulletin of the American Mathematical Society*, vol. 44, N 3, p. 393–422, 2007.

[2] 2. А. В. Бессалов, "Число изоморфизмов и пар кручения кривых Эдвардса над простым полем", *Радиотехника*, вып. 167, с. 203–208, 2011.

[3] А. В. Бессалов, А. А. Дихтенко, "Криптостойкие кривые Эдвардса над простыми полями", *Прикладная радиоэлектроника*, вып. 12, № 2, с. 285–291, 2013.

[4] А. В. Бессалов, О. В. Цыганкова, "Новые свойства эллиптической кривой в форме Эдвардса над простым полем", *Радиотехника*, вып. 180, с. 137–143, 2015.

[5] И. М. Виноградов, "Основы теории чисел", 180 с., М.–Л.: *Гостехиздат*, 1952.