On the number of solutions of polynomial equation over $\mathbb{F}_p$*

Ilya Vyugin and Sergey Makarychev

Abstract

We present an upper bound of the number of solutions (x, y) of a polynomial equation $P(x, y) = 0$ over a field $\mathbb{F}_p$, in the case, where $x \in g_1G$, $y \in g_2G$, g_1G, g_2G are cosets by some subgroup G of a multiplicative group $\mathbb{F}_p^*$. Some applications of this bound to hyperelliptic curves and additive energies are obtained.

1 Introduction

We study an algebraic equation

$$P(x, y) = 0 \tag{1}$$

over a field $\mathbb{F}_p$ (or its algebraic closure $\overline{\mathbb{F}}_p$), where p is a prime number. Suppose that $P \in \mathbb{F}_p[x, y]$ is an irreducible polynomial of two variables x and y. Let G be a subgroup of $\mathbb{F}_p^*$ (multiplicative group of $\mathbb{F}_p$).

We estimate the number of solutions (x, y) of the equation (1) which are belong to a subgroup G, ($x \in G$ and $y \in G$) or a product of some cosets $(x, y) \in g_1G \times g_2G$, where $g_1, g_2 \in \mathbb{F}_p^*$.

The first result of such a kind belongs to the A. Garcia and J.F. Voloch [1]. Their result was improved by D.R. Heath-Brown and S.V. Konyagin [2]. They proved using Stepanov method (see [2],[5]) that for any subgroup $G \subset \mathbb{F}_p^*$, such that $|G| < (p-1)/((p-1)^{1/4} + 1)$ and an arbitrary nonzero μ the number of solutions of linear equation

$$y = x + \mu \tag{2}$$

such that $(x, y) \in G \times G$, does not exceed $4|G|^{2/3}$. In the other words they have studied such a problem for linear equations (1). The case of such systems is studied in [6],[4].

Suppose that the polynomial (1) can be rewritten in the form

$$P(x, y) = y^n + f_{n-1}(x)y^{n-1} + \ldots + f_1(x)y + f_0(x). \tag{3}$$

The main result of the paper is Theorem 2. It gives us an upper bound of a number of solutions $(x, y) \in g_1G \times g_2G$ of an equation (1),(3).

Theorem 1. *Let $P(x, y)$ be a polynomial of the form (1),(3), and $\deg_x P(x, y) = m$, $\deg_y P(x, y) = n$, $P(0, 0) \neq 0$, $m + n < p$, G is a subgroup of $\mathbb{F}_p^*$, $100(mn)^{3/2} < |G| < \frac{1}{3}p^{3/4}$, $g_1, g_2 \in \mathbb{F}_p^*$, then the cardinality of the set*

$$M_1 = \{(x, y) \mid P(x, y) = 0,\ x \in g_1G,\ y \in g_2G\} \tag{4}$$

does not exceed $16mn(m + n)|G|^{2/3}$.

*The research was carried out at the IITP RAS at the expense of the Russian Foundation for Sciences (project N 14-50-00150).

For any number $x \in \overline{\mathbb{F}}_p$, there is a set of n numbers $y_1, \dots, y_n \in \overline{\mathbb{F}}_p$, which can be the same, such that $P(x, y_i) = 0$, $i = 1, \dots, n$. We will call such roots $y_1, \dots, y_n$ roots of an equation (1) corresponding to x.

The second result gives us an upper bound for a number of $x \in G$ such that all corresponding roots $y_1, \dots, y_n$ belong to G. We obtain the following theorem.

Theorem 2. *Let $P(x, y)$ be a polynomial of the form (1),(3), and $\deg_y P(x, y) = n$, $\deg f_0(x) = m$, $f_0(0) \neq 0$, G be a subgroup of $\mathbb{F}_p^*$, $64m^3 < |G| < \frac{1}{3}p^{3/4}$, $g_0, h \in \mathbb{F}_p^*$, $m + n < p$, then the cardinality of the set*

$$M_2 = \{x | x \in g_0 G,\ y_1 \dots y_n \in hG,\ y_1, \dots, y_n \text{ – roots of (1) corresponding to } x\} \tag{5}$$

does not exceed $3m^2|G|^{2/3}$ (if $m \geqslant 2$) and $6|G|^{2/3}$ (if $m = 1$).

Corollary 1. *In the conditions of Theorem 2 consider a set*

$$M_2' = \{x | x \in g_0 G,\ y_1 \in g_1 G, \dots, y_n \in g_n G,\ y_1, \dots, y_n \text{ – roots of (1) corresponding to } x\}, \tag{6}$$

where $g_0, g_1, \dots, g_n \in \mathbb{F}_p^*$. The cardinality of the set M_2' does not exceed $3m^2|G|^{2/3}$ (if $m \geqslant 2$) and $6|G|^{2/3}$ (if $m = 1$).

Corollary 2. *Consider an equation*

$$y = f(x), \qquad f \in \mathbb{F}_p[x], \quad \deg f = m, \quad f(0) \neq 0, \tag{7}$$

such that the polynomial $P(x, y) = y - f(x)$ satisfy to conditions of Theorem 2. Then the number of solutions (x, y) of (7) such that $(x, y) \in g_1 G \times g_2 G$, $g_1, g_2 \in \mathbb{F}_p^*$ does not exceed of $3m^2|G|^{2/3}$ (if $m \geqslant 2$) and $4|G|^{2/3}$ (if $m = 1$).

The numbers of points of an elliptic and a hyperelliptic curves have the great interest for applications. Consider a curve

$$y^2 = f(x), \qquad f \in \mathbb{F}_p[x], \quad \deg f = m, \quad f(0) \neq 0. \tag{8}$$

Corollary 3. *The number of solutions (x, y) of an equation (8) such that $(x, y) \in g_1 G \times g_2 G$, $g_1, g_2 \in \mathbb{F}_p^*$ does not exceed $6m^2|G|^{2/3}$, if $m \geqslant 2$ and a polynomial $P(x, y) = y - f(x)$ satisfy to conditions of Theorem 2.*

Proof. We obtain by Theorem 2 that the number of solutions $(x, \tilde{y})$ of the equation $P(x, \tilde{y}) = f(x) - \tilde{y}$ (7) , such that $(x, \tilde{y}) \in g_1 G \times g_2^2 G$, does not exceed $3m^2|G|^{2/3}$. Consequently, the number of pairs (x, y^2) does not exceed $6m^2|G|^{2/3}$, because there exists at least two numbers $y \in \mathbb{F}_p$ such that $y^2 = \tilde{y}$. $\square$

Corollary 4. *If conditions of Theorem 1 hold, then the number of solutions (x, y, z, w) of an equation*

$$P(x, y) = P(z, w)$$

such that $x, y, z, y \in G$, does not exceed $17mn(m + n)|G|^{8/3}$.

Proof. Let us fix two variables, for example, z and w. Then Theorem 1 gives us that the number of solutions (x, y) of the equation $P(x, y) = P(z, w)$ does not exceed $16mn(m + n)|G|^{\frac{2}{3}}$ if $P(0, 0) - P(z, w) \neq 0$. The condition $P(0, 0) - P(z, w) \neq 0$ can be not satisfied only for $n|G|$ pairs $(z, w) \in G \times G$. Note that for each fixed z and t the number of solutions does not exceed $16mn(m + n)|G|^{2/3}$ if $P(0, 0) - P(z, w) \neq 0$. So obtain that the number of solutions of polynomial equation

$$P(x, y) = P(z, t)$$

does not exceed $16mn(m + n)|G||G|^{2/3} + n^2|G|^2 \leqslant 17mn(m + n)|G|^{8/3}$. $\square$

2 Proof of Theorem 2

We would like to estimate a cardinality of the set M_2 (see (6)). Vieta's theorem gives us that

$$y_1 \dots y_n = f_0(x),$$

where $y_1, \dots, y_n$ are roots of the equation (1) of variable y with a given x. A set M_2 can be defined as following

$$M_2 = \{x \mid x \in g_0 G, \;\; f_0(x) \in hG\}.$$

The cardinality $|M_2|$ is equal to a number of solutions (x, y) of an equation $y = f_0(x)$, such that $x \in g_0 G$, $y \in hG$. We obtain that Corollary 3 is equivalent to Theorem 2.

It is easy to see that if $h = g_1 \dots g_n$ then $M_2' \subseteq M_2$. We will estimate the cardinality of M_2'. It gives us a proof of Corollary 1.

2.1 Stepanov method

Now we present a Stepanov method scheme. Let G be a subgroup of $\mathbb{F}_p^*$ of the order $t = |G|$ ($t \mid (p-1)$). It is easy to see that

$$G = \{s^{\frac{p-1}{t}} \mid s \in \mathbb{F}_p^*\} = \{s \mid s^t = 1, \;\; s \in \mathbb{F}_p^*\}.$$

Any coset can be defined as a set such that

$$gG = \{s \mid s^t = h, \;\; s \in \mathbb{F}_p^*\},$$

where $h = g^t$.

Consider a polynomial $\Phi \in \mathbb{F}_p[X, Y, Z]$ such that

$$\deg_X \Phi < A, \quad \deg_Y \Phi < B, \quad \deg_Z \Phi < C,$$

or in the other words

$$\Phi(X, Y, Z) = \sum_{a,b,c} \lambda_{a,b,c} X^a Y^b Z^c, \qquad a \in [A], \quad b \in [B], \quad c \in [C],$$

where $[N] = \{0, 1, \dots, N-1\}$. Take the following polynomial

$$\Psi(X) = \Phi(X, X^t, (y_1 \dots y_n)^t),$$

Vieta's theorem and (3),(9) gives us that $(y_1 \dots y_n) = f_0(x)$ where $f_0(x) \in \mathbb{F}_p[x]$ is a polynomial of degree $\leqslant m$. We estimate the number of x such that all corresponding roots $y_1 \in g_1 G, \dots, y_n \in g_n G$. Consequently, the product $(y_1 \dots y_n)$ belongs to hG too ($h = g_1 \dots g_n$).

We will choose constants A, B and C such that

$$\deg \Psi(X) \leqslant (A-1) + (B-1)t + m(C-1)t < p. \tag{9}$$

Now we find the coefficients $\lambda_{a,b,c}$ such that, firstly, the polynomial Ψ is not identically zero, and, secondly, Ψ has a root of an order at least D at every point of the set M_2 (except 0 and roots of a polynomial $f_0(x) = 0$, may be).

Then we obtain the following estimate

$$|M_2| \leqslant \frac{\deg \Psi(x)}{D} < \frac{A + Bt + mCt}{D}. \tag{10}$$

Thus we have to find $\lambda_{a,b,c}$ such that

$$\frac{d^k}{dX^k}\Psi(X)|_{X=x} = 0, \quad \forall k < D, \quad \forall x \in M_2 \setminus \{0, \mu \mid f_0(\mu) = 0\}. \tag{11}$$

and such that

$$\Psi(X) \not\equiv 0. \tag{12}$$

Let us show that if

$$AD + m\frac{D^2}{2} < ABC \tag{13}$$

then there exist coefficients $\lambda_{a,b,c}$ such that (11) and (12) are satisfied.

Note that if $x \neq 0$, $f_0(x) \neq 0$ and $D < p$ then the condition (11) is equivalent to the following

$$\forall k < D, \quad \forall x \in M_2 \setminus \{0, \mu \mid f(\mu) = 0\} \qquad \frac{d^k}{dX^k}\Psi(X)|_{X=x} = 0.$$

If $x \in \Omega$ then we have

$$x^t = g_0^t, \quad f_0^t(x) = h^t, \tag{14}$$

where g_0^t and h^t are constants, which do not depend on the elements $x \in g_0 G$ and $f_0(x) \in hG$. We obtain from (14) that

$$x^k f_0^k(x)\frac{d^k}{dx^k}x^a x^{bt} f_0^{ct}(x) = x^{bt} f_0^{ct}(x) \cdot P_{a,b,c}(x)|_{x\in M_2} = g_0^t h^t P_{a,b,c}(x),$$

where $P_{a,b,c}(x)$ is a polynomial and $\deg P_k(x) < A + km$. Consequently, we have

$$x^k f_0^k(x)\frac{d^k}{dx^k}\Psi(x)|_{x\in\Omega} = \sum \lambda_{a,b,c} P_{a,b,c}(x) = P_k(x),$$

where $P_k(x)$ is a polynomial and $\deg P_k(x) < A + km$. It is easy to see that the coefficients of polynomials $P_k(x)$ are homogeneous linear forms of coefficients $\lambda_{a,b,c}$ and the condition

$$P_k(x) \equiv 0$$

can be represent as a system of $A + km$ homogeneous linear algebraic equations of variables $\lambda_{a,b,c}$. The system of such a form has a nonzero solution if the number of equations the less than the number of variables. This condition is the condition (13).

Now we obtain the estimate

$$|M_2| \leqslant \frac{\deg \Psi(x)}{D} + m + 1 < \frac{A + tB + tmC}{D}.$$

The proof Theorem 2 will be completed if we define the constants A, B, C and D, which satisfy (13) and prove (12). The next part is devoted to the proof of condition (12).

2.2 Linear independence of products

We would like to prove the condition (12). We will prove a sufficient condition for (12). Let us prove the following lemma.

Lemma 1. *The set of functions*

$$x^a x^{bt} f^{ct}(x), \qquad a \in [A], \quad b \in [B], \quad c \in [C]$$

is linear independent if $f(0) \neq 0$ *and*

$$t \geqslant AB. \tag{15}$$

Proof. Let us consider an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$. We can extend derivative from the field $\mathbb{F}_p$ to its algebraic closure $\overline{\mathbb{F}}_p$. The polynomial $f(x)$ has a form

$$f(x) = (x - \alpha_1) \dots (x - \alpha_m), \qquad \alpha_1, \dots, \alpha_m \in \overline{\mathbb{F}}_p.$$

Suppose there is a combination

$$\sum_{a,b,c} C_{a,b,c} x^a x^{bt} f^{ct}(x) \equiv 0 \tag{16}$$

with nonzero coefficients $C_{a,b,c}$. Let $c_{min} = \min_{a,b,c}\{c \mid C_{a,b,c} \neq 0\}$, then a combination (16) can be represented in the form

$$f^{c_{min}}(x) \left[\sum_{a,b;c \geqslant c_{min}+1} C_{a,b,c} x^a x^{bt} f^{(c-c_{min})t}(x) + \sum_{a,b} C_{a,b,c_{min}} x^a x^{bt} \right] \equiv 0.$$

We obtain that $(x - \alpha_1)^t \mid \sum_{a,b} C_{a,b,c_{min}} x^a x^{bt}$, but the polynomial $\sum_{a,b} C_{a,b,c_{min}} x^a x^{bt}$ can not be divided by $(x - \alpha_1)^t$ if $t \geqslant AB$ (see Lemma 6 of [2]). $\square$

2.3 End of the proof of Theorem 2

Let us suppose that $64m^3 < t < \frac{1}{3}p^{3/4}$ and $m \geqslant 2$. Take the following constants:

$$A = mC^2, \quad B = mC, \quad C = \left[\frac{t^{1/3}}{m} \right], \quad D = C^2$$

which are satisfy the condition (9)

$$(A-1) + t(B-1) + tm(C-1) < p. \tag{17}$$

Obviously, the condition (17) has a form

$$mC^2 + m2Ct \leqslant \frac{t^{2/3}}{m} + 2t^{4/3} < p. \tag{18}$$

The condition (13):

$$AD + m\frac{D^2}{2} = mC^4 + \frac{m}{2}C^4 < m^2C^4 = ABC$$

hold if $m \geqslant 2$. The condition (15)

$$t > t/m > m^2 \left[\frac{t^{1/3}}{m}\right]^3 >= m^2 C^3 = AB$$

holds too. Consequently, the Stepanov method can be applied. Now let us obtain the estimate

$$|M_2| < m+1+\frac{mC^2+2mCt}{C^2} = m+1+\frac{mC+2mt}{C} < m+1+\frac{t^{1/3}+2mt}{\left[\frac{t^{1/3}}{m}\right]} < 3m^2t^{2/3} = 3m^2|G|^{2/3}.$$

Consider the case $m = 1$. Suppose that $64 < t < \frac{1}{3}p^{3/4}$. Take the following constants:

$$A = C^2, \quad B = C, \quad C = \left[t^{1/3}\right], \quad D = \frac{1}{2}C^2$$

which satisfy the condition (9):

$$\left[t^{1/3}\right]^2 - 1 + t\left(\left[t^{1/3}\right] - 1\right) + t\left(\left[t^{1/3}\right] - 1\right) < t^{2/3} + t^{4/3} + t^{4/3} < 3t^{4/3} < p.$$

The condition (13)

$$AD + m\frac{D^2}{2} = \frac{1}{2}C^4 + \frac{1}{8}C^4 < C^4 = ABC$$

hold. The condition (15)

$$t \geqslant \left[t^{1/3}\right]^3 = C^3 = AB$$

hold too. Now let us obtain the estimate

$$|M_2| < 2 + \frac{C^2+2Ct}{\frac{1}{2}C^2} = 2 + 2\frac{C+2t}{C} < 2 + 2\frac{t^{1/3}+2t}{\left[t^{1/3}\right]} < 6t^{2/3} = 6|G|^{2/3}.$$

Theorem 2 is proved. □

3 Proof of Theorem 1

3.1 Stepanov method with polynomials of two variables

Consider a polynomial $\Phi \in \mathbb{F}_p[X, Y, Z]$ such that

$$\deg_X \Phi < A, \quad \deg_Y \Phi < B, \quad \deg_Z \Phi < C,$$

or in the other words

$$\Phi(X, Y, Z) = \sum_{a,b,c} \lambda_{a,b,c} X^a Y^b Z^c, \qquad a \in [A], \quad b \in [B], \quad c \in [C],$$

where $[N] = \{0, 1, \ldots, N-1\}$. Take the following polynomial

$$\Psi(x, y) = \Phi(x, x^t, y^t), \tag{19}$$

such that it satisfy to the following conditions:

1) all roots (x, y), such that $x \in g_1 G, y \in g_2 G$, of an equation (1) are zeros of system

$$\begin{cases} \Psi(x, y) = 0 \\ P(x, y) = 0 \end{cases} \tag{20}$$

of an order at least D.

2) the greatest common divisor of polynomials $\Psi(x, y)$ and $P(x, y)$ is equal to 1.

Then the generalized Bézout's theorem gives us an upper bound of the number N of roots (x, y) such that $x \in g_1 G$, $y \in g_2 G$:

$$N \leqslant \frac{\deg \Psi(x, y) \cdot \deg P(x, y)}{D} \leqslant \frac{(m + n) \deg \Psi(x, y)}{D}. \tag{21}$$

Lemma 2. *Let $Q(x, y)$ be a polynomial and*

$$\deg_x Q(x, y) \leqslant \mu, \quad \deg_y Q(x, y) \leqslant \nu$$

and $P(x, y)$ such that

$$\deg_x P(x, y) \leqslant m, \quad \deg_y P(x, y) \leqslant n,$$

then the condition

$$P(x, y) \mid Q(x, y)$$

can be given by $n((\nu - n + 2)m + \mu) \leqslant (\mu + \nu + 1)mn$ homogeneous linear algebraic equations.

Proof. Consider a polynomial

$$P(x, y) = f_n(x)y^n + \ldots + f_1(x)y + f_0(x), \qquad \deg f_i(x) \leqslant m$$

and a polynomial

$$Q_0(x, y) = Q(x, y)f_n(x) = g_{0,\nu}(x)y^\nu + \ldots + g_{0,1}(x)y + g_{0,0}(x).$$

Let construct polynomials $Q_i(x, y) = g_{i,\nu-i}(x)y^{\nu-i} + \ldots + g_{i,1}(x)y + g_{i,0}(x)$, $i = 1, \ldots, \nu - n + 1$ such that

$$Q_i(x, y) = Q_{i-1}(x, y) - \frac{g_{i-1,\nu-i+1}(x)}{f_n(x)} P(x, y).$$

It is easy to see that $\deg_y Q_i(x, y) < \deg_y Q_{i-1}(x, y)$, $\frac{g_{i-1,\nu-i+1}(x)}{f_n(x)}$ — is a polynomial, because $f_n(x) \mid g_{i-1,\nu-i+1}(x)$ and $\deg g_{i,j}(x) \leqslant \mu + (i + 1)m$.

Consequently, $P(x, y) \mid Q(x, y)$ if and only if $Q_{\nu-n+1}(x, y) \equiv 0$. The polynomial $Q_{\nu-n+1}(x, y)$ has $n((\mu + (\nu - n + 2)m)$ coefficients which are homogeneous linear forms of coefficients of polynomial $Q(x, y)$. We have $n((\nu - n + 2)m + \mu)$ homogeneous linear algebraic equations. □

Lemma 3. *Let*

$$\Psi(x, y) = \sum_{a,b,c} \lambda_{a,b,c} x^a x^{bt} y^{ct}, \qquad a \in [A], \quad b \in [B], \quad c \in [C],$$

be a polynomial with $AB \leqslant t$, and coefficients $\lambda_{a,b,c}$ do not vanish simultaneously, $P(x, y)$ be an irreducible polynomial, $P(0, 0) \neq 0$, then there are x and y, such that $P(x, y) = 0$ and $\Psi(x, y) \neq 0$.

Proof. Let $c_{min} = \min_{a,b,c:\lambda_{a,b,c}\neq 0} c$. Consider a polynomial Ψ in the form

$$\Psi(x,y) = y^{c_{min}t}\left(\sum_{a,b,c:c>c_{min}} \lambda_{a,b,c}x^a x^{bt} y^{(c-c_{min})t} + \sum_{a,b} \lambda_{a,b,c_{min}} x^a x^{bt}\right), \quad a \in [A],\, b \in [B],\, c \in [C],$$

Let us suppose that for any x and y, such that $P(x,y) = 0$, $\Psi(x,y)$ vanish. Then for any $x \in \mathbb{F}_p$ and $y_1, \ldots, y_n \in \overline{\mathbb{F}}_p$ such $P(x,y_i) = 0$, $i = 1, \ldots, n$ the following holds

$$(y_1 \ldots y_n) \mid \Psi(x,0)$$

(Bézout's theorem). It is easy to see that the polynomial $\psi(y) = \Psi(x, x^t, y^t)$ depends only on y^t and we have the following

$$(y_1 \ldots y_n)^t \mid \Psi(x,0).$$

The term $(y_1 \ldots y_n)^t$ is a symmetric polynomial of variables $y_1 \ldots y_n$, it can be expressed as a polynomial of x by means coefficients of polynomial $P'(y) = P(x,y)$. In the other words

$$(y_1 \ldots y_n)^t = (P(x,0))^t.$$

Then we have the following

$$(P(x,0))^t \mid \Psi(x,0).$$

It can not be true if $P(x,0)$ has at least one nonzero root and the number of members of polynomial $\Psi(x,0)$ does not exceed t ($t \geqslant AB$). □

3.2 Derivatives and differential operators

We have a condition $P(x,y) = 0$. Let us consider the following formal derivatives $\frac{d^k}{dx^k}y$.

Consider the polynomials $q_k(x,y)$ and $r_k(x,y)$, $k \in \mathbb{N}$ defined by induction

$$q_1(x,y) = -\frac{\partial}{\partial x}P(x,y), \qquad r_1(x,y) = \frac{\partial}{\partial y}P(x,y),$$

and

$$q_{k+1}(x,y) = \frac{\partial q_k}{\partial x}\left(\frac{\partial P}{\partial y}\right)^2 - \frac{\partial q_k}{\partial y}\frac{\partial P}{\partial x}\frac{\partial P}{\partial y} - (2k-1)q_k(x,y)\frac{\partial^2 P}{\partial x \partial y}\frac{\partial P}{\partial y} + (2k-1)q_k(x,y)\frac{\partial^2 P}{\partial y^2}\frac{\partial P}{\partial x},$$

$$r_{k+1}(x,y) = r_k(x,y)\left(\frac{\partial P}{\partial y}\right)^2 = \left(\frac{\partial P}{\partial y}\right)^{2k+1}, \qquad k = \mathbb{N}.$$

Actually, formal derivatives have the following expressions $\frac{d^k}{dx^k}y = \frac{q_k(x,y)}{r_k(x,y)}$, $k \in \mathbb{N}$.

These derivatives coincide to the derivatives of algebraic function $y(x)$ defined by an equation $P(x,y) = 0$. Actually,

$$\frac{d}{dx}y = \frac{q_1(x,y)}{r_1(x,y)} = -\frac{\frac{\partial}{\partial x}P(x,y)}{\frac{\partial}{\partial y}P(x,y)},$$

$$\frac{d^{k+1}}{dx^{k+1}}y = \frac{q_{k+1}(x,y)}{r_{k+1}(x,y)} = \frac{\frac{\partial q_k}{\partial x}\left(\frac{\partial P}{\partial y}\right)^2 - \frac{\partial q_k}{\partial y}\frac{\partial P}{\partial x}\frac{\partial P}{\partial y} - (2k-1)q_k(x,y)\frac{\partial^2 P}{\partial x \partial y}\frac{\partial P}{\partial y} + (2k-1)q_k(x,y)\frac{\partial^2 P}{\partial y^2}\frac{\partial P}{\partial x}}{r_k(x,y)\left(\frac{\partial P}{\partial y}\right)^2}.$$

We obtain the following lemma.

Lemma 4. *Degrees of polynomials $q_k(x,y)$ and $r_k(x,y)$ satisfy to the following estimates*

$$\deg_x q_k(x,y) \leqslant (2k-1)m-k, \quad \deg_y q_k(x,y) \leqslant (2k-1)n-k+1,$$

$$\deg_x r_k(x,y) \leqslant (2k-1)m, \quad \deg_y r_k(x,y) \leqslant (2k-1)(n-1), \quad k \in \mathbb{N}.$$

Proof. It is easy to see that $\deg_x q_1(x,y) \leqslant m-1$, $\deg_y q_1(x,y) \leqslant n$ and

$$\deg_x q_k(x,y) \leqslant \deg_x q_{k-1}(x,y)+2m-1 \leqslant (2k-1)m-k, \quad \deg_y q_k(x,y) \leqslant \deg_y q_{k-1}(x,y)+2n-1 \leqslant (2k-1)n-k+1$$

For the polynomial $r_k(x,y)$ the statement is obvious. □

Let us define differential operators

$$D_k = \left(\frac{\partial P}{\partial y}\right)^{2k-1} x^k y^k \frac{d^k}{dx^k}, \qquad k = \mathbb{N}.$$

It is easy to see that we have the following relations

$$D_k x^a x^{bt} y^{ct} = R_{k,a,b,c}(x,y) x^a x^{bt} y^{ct},$$

$$D_k \Psi(x,y)|_{x,y\in G} = R_k(x,y)|_{x,y\in G}$$

and the following Lemma 5 holds.

Lemma 5.

$$\deg_x R_{k,a,b,c}(x,y) \leqslant 2(2k-1)m \leqslant 4km \qquad \deg_y R_{k,a,b,c}(x,y) \leqslant 2(2k-1)(2n-1)+1 \leqslant 4kn$$

$$\deg_x R_k(x,y) \leqslant A+4km \qquad \deg_y R_k(x,y) \leqslant 4kn.$$

3.3 End of the proof of Theorem 1

Let us suppose that $P(x,y)$ is an irreducible polynomial. Give the following parameters

$$A = B^2, \quad C = B, \quad B = [t^{1/3}]$$

$$D = \left[\frac{B^2}{4mn}\right].$$

Consider a polynomial (19) and a system (20). The condition

$$D_k \Psi(x,y) = 0 \quad \text{if } P(x,y) = 0 \text{ and } (x,y) \in g_1 G \times g_2 G,\ k = 0,\dots,D-1 \tag{22}$$

can be calculated by means of Lemmas 5 and 2. The condition (22) is equivalent to the set of

$$\sum_{k=0}^{D-1} (4km+4kn+A+1) = (A+1)Dmn + 2mn(m+n)D(D-1) \leqslant ADmn + 2mn(m+n)D^2$$

homogeneous linear algebraic equations of variables $\lambda_{a,b,c}$. This system has a nonzero solution if

$$2D^2 mn(m+n) + DmnA < ABC. \tag{23}$$

The inequality (23) has a form

$$2D^2mn(m+n)+DmnA<\frac{1}{4}B^4+\frac{1}{4}B^4<B^4=ABC.$$

The conditions of Lemma 3 hold

$$t\geqslant AB=[t^{1/3}]^3,$$

and the conditions

$$\deg\Psi(x,y)<A+Bt+Ct<p,\qquad \deg P(x,y)<m+n<p$$

is hold too.

$$N\leqslant\frac{(m+n)(B^2+2Bt)}{\left[\frac{B^2}{4mn}\right]}\leqslant 16mn(m+n)t^{2/3},$$

because $t>100(mn)^{3/2}$ and, consequently, $\left[\frac{B^2}{4mn}\right]>\frac{B^2}{4mn}-1>\frac{3}{4}\frac{B^2}{4mn}$.

Consider the case of reducible polynomial $P(x,y)$. Represent a polynomial $P(x,y)$ as a product of irreducible polynomials $P_i(x,y)$:

$$P(x,y)=\prod_{i=1}^{s}P_i(x,y).$$

Then $\deg_x P_i(x,y)=m_i$, $\deg_y P_i(x,y)=n_i$, and $m=\sum_{i=1}^s m_i$, $n=\sum_{i=1}^s n_i$. The set $M_1\subseteq\sum_{i=1}^s M_{1,i}$, where

$$M_{1,i}=\{(x,y)\mid P_i(x,y)=0,\ x\in g_1G,\ y\in g_2G\}.$$

Consequently, we have the estimate

$$|M_1|\leqslant\sum_{i=1}^{s}16m_in_i(m_i+n_i)|G|^{2/3}\leqslant 16mn(m+n)|G|^{2/3}.$$

Theorem 1 is proved. □

4 Conclusion

The authors are grateful to Sergey Konyagin, Ilya Shkredov and Ivan Yakovlev for their attention and useful comments. The authors are particularly grateful to Igor Shparlinski for statement of the problem, which is considered in the paper.

References

[1] A. Garcia, J.F. Voloch, *Fermat curves over finite fields* // J. Number Theory 30 (1988), 345–356.

[2] D. R. Heath-Brown, S. Konyagin, *New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum* // Quart. J. Math. 51 (2000), 221–235.

[3] T. Schoen, I. D. Shkredov, *Higher moments of convolutions* J. of Number Theory, **133** (2013), 1693–1737.

[4] I. D. Shkredov, E. V. Solodkova, I. V. Vyugin, *Intersections of multiplicative subgroups and Heilbronn's exponential sum* // arXiv:1302.3839

[5] S.A. Stepanov, *The number of points of a hyperelliptic curve over a prime field*, Izv. Akad. Nauk SSSR Ser. Mat., 33 (1969), 1171-1181.

[6] I.V. Vyugin, I.D. Shkredov, *On additive shifts of multiplicative subgroups,* Math. Sbornik. 203:**6** (2012), 81–100.

Vyugin I.V.
Insitute for Information Transmission Problems RAS,
and
National Research University Higher School of Economics,
vyugin@gmail.com.

Makarychev S.V.
National Research University Higher School of Economics,
sergei-lenin2008@yandex.ru.