

Mathematical Subject Classification: 11N25, 11S40  
UDC 511.33

**L. Balyas, P. Varbanets**

I. I. Mechnikov Odesa National University

**EXPONENTIAL SUMS OVER  $G_{p^m}^n[x, y, z]$**

**Баляс Л., Варбанець П. Тригонометричні суми над  $G_{p^m}^n[x, y, z]$ .** Розглядається застосування методу С. Хулі для побудови оцінок тригонометричних сум на алгебраїчному многовиді над кінцевим полем. Отримана нетривіальна оцінка тригонометричної суми з раціональною функцією від трьох змінних над кільцем класів вичетів за модулем  $p^m$  в кільці цілих гауссових чисел.

**Ключові слова:** кінцеве поле, алгебраїчний многовид, тригонометричні суми.

**Баляс Л., Варбанець П. Тригонометрические суммы над  $G_{p^m}^n[x, y, z]$ .** Рассматривается применение метода С. Хули для построения оценок тригонометрических сумм на алгебраическом многообразии над конечным полем. Получена нетривиальная оценка тригонометрической суммы с рациональной функцией от трёх переменных над кольцом классов вычетов по модулю  $p^m$  в кольце целых гауссовых чисел.

**Ключевые слова:** конечное поле, алгебраическое многообразие, тригонометрические суммы.

**Balyas L., Varbanets P. Exponential sums over  $G_{p^m}^n[x, y, z]$ .** There is considered the application of C. Hooley method to construct the estimates of exponential sums on algebraic variety over the finite field. We obtained a nontrivial estimate with the rational function on three variables over the ring of residue classes modulo  $p^m$  in the ring of Gaussian integers.

**Key words:** finite field, algebraic variate, exponential sum.

**INTRODUCTION.** Analytical number theory has enormously profited from the estimates of exponential sums of the form

$$\sum_{\substack{x \in \mathbb{F}_q^n \\ f(x)=0}} \frac{2\pi i \text{Tr}(f(x))}{p}, \quad (1)$$

where  $\mathbb{F}_q$  is a finite field with  $q$  elements,  $q = p^m$ ,  $p$  is an odd prime number,  $f(x)$  and  $g(x)$  are polynomials from  $\mathbb{F}_q[x]$ .  $\text{Tr}$  as it usually is the absolute trace mapping from  $\mathbb{F}_q$  into  $\mathbb{F}_p$ , i. e.

$$\text{Tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \dots + \alpha^{p^{m-1}} \in \mathbb{F}_p.$$

The exponential sums (1) are related to special sums associated with zeta- or L-function. The last ones are determined by algebraic variates  $V$ , defined by polynomial  $\varphi(x)$  over the finite field. In particular, for

$$f(x) = \alpha \cdot x = \alpha_1 x_1 + \dots + \alpha_n x_n, \quad \alpha_i \in \mathbb{F}_q,$$

the corresponding zeta-function  $\zeta(t, V)$  has the following form

$$\zeta(t, V) = \sum_{\ell=1}^{\infty} \frac{S_{\ell}(\alpha)}{\ell} t^{\ell}.$$

B. Dwork [6] proved that  $\zeta(t, V)$  is a rational function  $\frac{h(t)}{g(t)}$ , where  $h, g \in P[t]$ ,  $P = \mathbb{Q}\left(e^{\frac{2\pi i}{p}}\right)$ . Moreover,

$$S_{\ell}(\alpha) := \sum_{x \in V_{\ell}} e^{\frac{\text{Tr}_{\ell}(\text{Tr}(\alpha x))}{p}} = \omega_1^{\ell} + \dots + \omega_{k_1}^{\ell} - \omega_{k_1+1}^{\ell} - \dots - \omega_{k_1+k_2}^{\ell}, \quad (2)$$

where  $\text{Tr}_{\ell}$  is the trace from  $\mathbb{F}_{q^{\ell}}$  into  $\mathbb{F}_q$ ,  $\omega_i^{-1}$ ,  $i = 1, \dots, k_1$  (respectively,  $\omega_{k_1+j}^{-1}$ ,  $j = 1, \dots, k_2$ ) are the roots of  $g(t)$  (respectively, of  $h(t)$ ).

The complex numbers  $\omega_j$  are called the characteristic roots of the sum  $S_1$ .

In 1948 A. Weil [10] showed for  $n = 2$  that  $k_1 + k_2 \leq d - 1$  with  $d = \deg \varphi(x)$  and  $|\omega_j| = q^{\frac{1}{2}}$ .

In case, when  $n \geq 3$ , P. Deligne [4] proved that for every  $j = 1, 2, \dots, k_1 + k_2$ , the following equation

$$|\omega_j| = p^{\frac{m_j}{2}}, \quad m_j \in \mathbb{N} \cup \{0\}$$

takes place. Furthermore, for every  $\omega_j$  all its conjugates over  $\mathbb{Q}$  have the same modulus.

E. Bombieri [2] (see, also C. Hooley [8]) got an estimate for the number of characteristic roots in terms of a degree of the variety  $V$  and  $\deg \varphi(x)$ . But the hardest problem in the estimation of the sum (1) is a problem of a determination of  $\max_{1 \leq j \leq k_1+k_2} m_j$ .

For  $n = 3$  C. Hooley [8] (see, also B. Birch and E. Bombieri [1], O. Hunyavy and P. Varbanets [7]) obtained the valuations of  $\max_j m_j$  in certain cases.

In this paper we get the estimate of the sum (1) for  $n = 3$  in special case. Our main methods in the construction of the estimate of (2) are based on the work of C. Hooley [8].

We proved the following theorem.

**Theorem 1.** *Let  $f_1(x, y, z), f_2(x, y, z) \in \mathbb{F}_q[x, y, z]$ ,  $q = p^m$ . Let us define the variety  $V$  by the polynomial  $f_1(x, y, z)$ . And all the solutions of the equation  $f_2(x, y, z) = \tau$ ,  $\tau \in \mathbb{F}_q$ , relative to  $z$ , belong to the field of rational functions  $F_q(x, y, z)$ , i.e.  $z_j = \frac{f_{3j}(x, y, \tau)}{f_{4j}(x, y, \tau)}$ ,  $j = 1, \dots, \ell$ . If for all  $\tau \in \mathbb{F}_q$ , except  $O(1)$  of their values, the polynomials  $f_{3j}(x, y, z)$  are absolutely irreducible polynomials modulo  $p$ , we obtain the estimate*

$$\sum_{(x, y, z) \in V} e^{2\pi i \frac{\text{Tr}(f_2(x, y, z))}{p}} \ll q$$

with constant in the symbol " $\ll$ " depending only on the degree of the polynomials  $f_1$  and  $f_2$ .

In particular, for  $q = p^2$ ,  $p \equiv 3 \pmod{4}$ , we take into account that a residue class ring mod  $p$  in  $G$  forms the field  $G_p$  with  $p^2$  elements, moreover,  $\text{Tr}(u) = \text{Sp}(u)$  for

$u \in G$ . Therefore, we can apply Theorem 1 for the construction of estimates of the exponential sums of the form

$$\sum_{\substack{x, y, z \in G_p \\ \varphi(x, y, z) \equiv 0 \pmod{p}}} e^{2\pi i \frac{Sp(F(x, y) + \gamma z)}{p}},$$

where  $F(x, y)$  is a rational function over  $G_p$ .

In this work we get the estimate of the sum

$$S(\alpha, \beta, \gamma; p^m) = \sum_{\substack{x, y, z \in G_{p^m} \\ xyz \equiv 1 \pmod{p^m}}} e^{2\pi i \frac{Sp(\alpha x + \beta^2 y + \gamma xz)}{p^m}} \quad (3)$$

with the help of Theorem 1.

**Theorem 2.** *Let  $\alpha, \beta, \gamma \in G_{p^m}$ ,  $p \equiv 3 \pmod{4}$ ,  $m \in \mathbb{N}$ ,  $(\gamma, p) = 1$ . Then*

$$S(\alpha, \beta, \gamma; p^m) \ll \begin{cases} p^2 & \text{if } m = 1, \\ N(p^m)^{\frac{3}{2}} & \text{if } m = 2m_0, \\ N(p^m)^{\frac{3}{2}} & \text{if } m = 2m_0 + 1 \\ & \text{and } \alpha \equiv 0 \pmod{p^m}, \\ N(p^m)N(p^{\nu_0}) & \text{if } m = 2m_0 + 1, \nu_p(\alpha) = m_0 + \nu_0 < m \end{cases}$$

with the constants in the symbol " $\ll$ ", which doesn't depend on  $p$  and  $m$ .

**NOTATION.** We will use the following notations:

- $G := \{a + bi \mid a, b \in \mathbb{Z}, i^2 = -1\}$ ;
- for  $\alpha \in G$  we denote  $Sp(\alpha) = 2\Re(\alpha)$ ,  $N(\alpha) = |\alpha|^2$ ;
- $G_{p^m}$  (respectively,  $G_{p^m}^*$ ) denotes the complete (respectively, reduced) system of residues modulo  $p^m$  in  $G$ ,  $m \geq 1$ ;
- $\sum_{(\ell)}$  (respectively,  $\sum_{(\ell)^*}$ ) means the summation over complete (respectively, reduced) system of residues modulo  $\ell$  in  $G$ ;
- we denote by  $\mathbb{F}_q$  a finite field with  $q$  elements,  $q = p^r$ ,  $r \in \mathbb{N}$ ;
- by  $f \ll g$  ( $f = O(g)$ ) for  $x \in X$ , where  $X$  is an arbitrary set on which  $f$  and  $g$  are defined, we mean that there exists a constant  $C > 0$  such that  $|f(x)| \leq Cg(x)$  for all  $x \in X$ ;
- $\mathbb{F}_q[X]$  (or  $G[X]$ ) denotes the ring of polynomials over  $\mathbb{F}_q$  (or  $G$ );
- $e_{p^m}(t) = e^{2\pi i \frac{\Re(t)}{p^m}}$ ,  $t \in G$ ;
- $\nu_p(\alpha) = \nu$  if  $p^\nu \mid \alpha$ .

**AUXILIARY ARGUMENTS.** We will apply some auxiliary lemmas.

**Lemma 1** (A. Weil [10]). *Let  $I(\varphi)$  be the number of the solutions of the equation  $\varphi(x, y) = 0$  in the field  $\mathbb{F}_q$ ,  $q = p^r$ , where  $\varphi(x, y)$  is an absolutely irreducible polynomial modulo  $p$ ,  $\deg \varphi = \ell$ , with the coefficients from  $\mathbb{F}_q$ . Then we have*

$$|I(\varphi) - p^r| \leq A(\ell)p^{\frac{r}{2}},$$

where a positive constant  $A(\ell)$  doesn't depend on  $p$  and  $z$ .

**Lemma 2** (E. Bombieri – H. Davenport [3]). *Let  $\ell_j$  and  $z_j$  be complex numbers,  $|z_j| = 1$ ,  $z_i \neq \pm z_j$  with  $i \neq j$ ,  $j = 1, \dots, \mu$ . Then the following estimate takes place*

$$\lim_{\substack{z \rightarrow \infty \\ z \equiv 1 \pmod{2}}} \left| \sum_{1 \leq j \leq \mu} \ell_j z_j^2 \right| \leq \left( \sum_{1 \leq j \leq \mu} |\ell_j|^2 \right)^{\frac{1}{2}}.$$

**Lemma 3** (Deligne [4], [5]). *For the characteristic roots  $\omega_j$  we have the equality*

$$|\omega_j| = q^{\frac{m_j}{2}}, \quad m_j \in \mathbb{N} \cup \{0\}, \quad j = 1, \dots, k.$$

Moreover, all conjugates with  $\omega_j$  over  $\mathbb{Q}$  have equal modules (number  $m_j$  is called the weight of root  $\omega_j$ ).

**Lemma 4.** *The following relation is true:*

$$\sum_{x \in G_{p^m}} e^{2\pi i \frac{\text{Tr}(\alpha x)}{p^m}} = \begin{cases} N(p^m), & \text{if } \alpha \equiv 0 \pmod{p^m}, \\ 0 & \text{otherwise.} \end{cases}$$

**Lemma 5.** *Let  $f(x) = A_1x + A_2x^2 + p(A_3x^3 + \dots)$  and  $g(x) = B_1x + p(B_2x^2 + \dots)$  be polynomials over  $\mathbb{Z}$ , and let  $\nu_p(A_2) = \nu > 0$ ,  $\nu_p(A_j) \geq \nu$ ,  $j = 3, 4, \dots$ ;  $(B_1, p) = 1$ . Then for  $\nu \leq m$ ,  $m \geq 2$  the following estimates*

$$\left| \sum_{x \in R_m} e^{2\pi i \frac{f(x)}{p^m}} \right| = \begin{cases} p^{\frac{m+\nu}{2}}, & \text{if } \nu_p(A_1) \geq \nu, \\ 0, & \text{else.} \end{cases}$$

$$\left| \sum_{x \in R_m^*} e^{2\pi i \frac{f(x) + g(x^{-1})}{p^m}} \right| \leq 4p^{\frac{m}{2}}$$

hold.

For the proof see [9].

**MAIN RESULTS.** In this section we will prove Theorem 1 and Theorem 2.

**Proof.** 1Let us prove Theorem 1.

Without restricting the generality, we may put  $f_j(x, y, \tau) = \ell \neq 0$ , where  $\ell$  is a constant. Let  $N_k(\tau)$  be the number of the solutions of the system of equations for  $(\xi, \eta, \zeta) \in \mathbb{F}_{q^k}^3$  so that

$$f_1(\xi, \eta, \zeta) - \tau = 0, \quad f_2(\xi, \eta, \zeta) = 0.$$

We put

$$\bar{N}_k = \frac{1}{q^k} \sum_{\tau \in \mathbb{F}_{q^k}} N_k(\tau).$$

For a nontrivial additive character  $\psi$  from the field  $\mathbb{F}_{q^k}$  we have

$$\sum_{\mu \in \mathbb{F}_{q^k}} \psi(\mu) = 0.$$

Thus, for  $i = 1, 2$

$$S_k(f_1, f_2) := \sum_{\substack{x, y, z \in \mathbb{F}_{q^k} \\ f_2(x, y, z) = 0}} e^{\frac{2\pi i \text{Tr}(f_2(x, y, z))}{p}},$$

where  $\text{Tr}$  is an absolute trace from  $\mathbb{F}_{q^k}$  into  $\mathbb{F}_p$ .

That is why for every  $\mu \in \mathbb{F}_{q^k}^*$  the following relation is true

$$S_k(\mu f_1, f_2) = \sum_{\tau \in \mathbb{F}_{q^k}} N_k(\tau) \psi(\mu \tau) = \sum_{\tau \in \mathbb{F}_{q^k}} (N_k(\tau) - \bar{N}_k) \psi(\mu \tau).$$

So, for the second moment of  $S_k$  we get

$$\begin{aligned} M_k = M(f_1, f_2) &:= \sum_{\mu \in \mathbb{F}_{q^k}^*} |S(\mu f_1, f_2)|^2 = \\ &= \sum_{\mu \in \mathbb{F}_{q^k}^*} \sum_{\tau_1, \tau_2 \in \mathbb{F}_{q^k}} (N_k(\tau_1) - \bar{N}_k)(N_k(\tau_2) - \bar{N}_k) e^{\frac{2\pi i \text{Tr}(\mu(\tau_1 - \tau_2))}{p}} = \\ &= (q^k - 1) \sum_{\tau \in \mathbb{F}_{q^k}} (N_k(\tau) - \bar{N}_k)^2 - \sum_{\tau_1 \neq \tau_2} (N_k(\tau_1) - \bar{N}_k)(N_k(\tau_2) - \bar{N}_k) \times \\ &\quad \times \sum_{\mu \in \mathbb{F}_{q^k}^*} e^{\frac{2\pi i \text{Tr}(\mu(\tau_1 - \tau_2))}{p}} = \\ &= q^k \sum_{\tau \in \mathbb{F}_{q^k}} (N_k(\tau) - \bar{N}_k)^2 - \sum_{\tau_1, \tau_2 \in \mathbb{F}_{q^k}} (N_k(\tau_1) - \bar{N}_k)(N_k(\tau_2) - \bar{N}_k) = \\ &= q^k \sum_{\tau \in \mathbb{F}_{q^k}} (N_k(\tau) - \bar{N}_k)^2 - \left( \sum_{\tau \in \mathbb{F}_{q^k}} (N_k(\tau) - \bar{N}_k) \right)^2 = \\ &= q^k \sum_{\tau \in \mathbb{F}_{q^k}} (N_k(\tau) - \bar{N}_k)^2 = \\ &= q^k \sum_{\tau \in \mathbb{F}_{q^k}} (N_k(\tau) - q^k)^2 - q^{2k} (\bar{N}_k - q^k)^2 \leq q^k \sum_{\tau \in \mathbb{F}_{q^k}} (N_k(\tau) - q^k)^2. \end{aligned}$$

It is obvious that  $N_k(\tau) = \sum_{j=1}^{\ell} N_{k_{ij}}(\tau) + O(q^k)$ , where  $N_{k_{ij}}(\tau)$  is the number of the solutions of the equation

$$f_2(\xi, \eta, z_j(\xi, \eta, \zeta)) = 0.$$

Indeed, let us put

$$V = \left\{ (x, y, z) \in \mathbb{F}_{q^k}^3 \mid f_2(x, y, z) = 0 \right\} = \bigcup_{j=1}^{\ell} V_j,$$

where  $V_j = \left\{ (x, y, z) \in \mathbb{F}_{q^k}^3 \mid f_2(x, y, z_j) = 0 \right\}$ .

Furthermore, we obtain inequality

$$\left| S(V, f_2) - \sum_{j=1}^{\ell} S(V_j, f_2) \right| \leq \sum_{1 \leq j_1 < j_2 \leq \ell} S(V_{j_1} \cap V_{j_2}, 0) = O(q^k)$$

with the constant in the symbol "O", which depends on  $\ell$ . Here,

$$V_j = \left\{ (\xi, \eta) \in \mathbb{F}_{q^k} \mid f_2(\xi, \eta, z_j(\tau)) = 0 \right\}.$$

But under the hypothesis of theorem the polynomial  $f_2(\xi, \eta, z_j(\xi, \eta, \tau)) := f_3(\xi, \eta, \tau)$  is absolutely irreducible modulo  $p$  for all  $\tau \in \mathbb{F}_{q^k}$ , except  $O(1)$  of their values.

As far as  $N_k(\tau) = O(q^k)$  in all cases (the constant in the symbol "O" depends only on the degree of  $f_2(x, y, z)$ ) we use Lemma 1 (separating exceptional values of  $\tau$ ) and get

$$M_k = q^k \sum_{\tau \in \mathbb{F}_{q^k}}' (O(q^{\frac{k}{2}}))^2 + q^k \cdot O(1) \cdot O(q^{2k}) = O(q^{3k}). \quad (4)$$

Now, if

$$S_k(\mu\alpha, \mu\beta, \mu\gamma) = \omega_{1,\mu}^k + \dots - \omega_{\ell,\mu}^k, \quad \mu \in \mathbb{F}_{q^k}^*$$

the characteristic roots  $\omega_{j,\mu}$  and  $\omega_{j,\nu}$ ,  $\mu\nu \in \mathbb{F}_{q^k}^*$ , are conjugated over  $\mathbb{Q}(\sqrt[\ell]{1})$ . In view of Lemma 3 their modules are equal and don't depend on  $\mu$  and  $\nu$ .

Let  $q^{\frac{N}{2}}$ , with  $N \geq 0$ ,  $N \in \mathbb{Z}$ , be the maximum of  $|\omega_j|$ ,  $j = 1, \dots, \ell$ .

If  $N \leq 2$ , it immediately follows that  $S_k(\alpha, \beta, \gamma) \ll q^k$ , and, in particular,  $S(\alpha, \beta, \gamma) \ll q$ . In this case the theorem is proved.

That is why we suppose that  $N > 3$ . Let  $\ell_0$  be the number of  $\omega_j$ ,  $j = 1, \dots, \ell$ , for which  $|\omega_j| = q^{\frac{N}{2}}$ . Thus we have

$$S_k(\mu\alpha, \mu\beta, \mu\gamma) = \ell_1 \omega_{1,\mu}^k + \dots + \ell_{\ell_0} \omega_{\ell_0,\mu}^k + O\left(q^{\frac{k(N-1)}{2}}\right),$$

where  $|\omega_{j_1,\mu}| = q^{\frac{N}{2}}$  and  $\omega_{j_1,\mu} \neq \pm \omega_{j_2,\mu}$  for  $j_1 \neq j_2$ ,  $\ell_1, \dots, \ell_{\ell_0}$  are integers and on of them at least isn't equal to zero. If this is not true, we consider such  $\omega_j$ , for which  $|\omega_j| = q^{\frac{N-1}{2}}$ , and so on. (It is known the contribution of  $\omega_j$  with  $|\omega_j| = q^{\frac{N}{2}}$  has the value of zero).

It is clear that

$$S_k(\mu\alpha, \mu\beta, \mu\gamma) = q^{\frac{kN}{2}} (\ell_1 z_{1,\mu}^k + \dots + \ell_{\ell_0} z_{\ell_0,\mu}^k) + O\left(q^{\frac{k(N-1)}{2}}\right), \quad (5)$$

where  $z_{j,\mu}$  are complex numbers,  $|z_{j,\mu}| = 1$  and  $z_{j_1,\mu} \neq \pm z_{j_2,\mu}$  for  $j_1 \neq j_2$ .

Now it follows from (5)

$$\begin{aligned} q^{-kN} M_k(\alpha, \beta, \gamma) &= q^{-kN} \sum_{\mu \in \mathbb{F}_q^{*k}} |S_k(\mu\alpha, \mu\beta, \mu\gamma)|^2 \geq \\ &\geq q^{-kN} \sum_{\mu \in \mathbb{F}_q^{*k}} |S_k(\mu\alpha, \mu\beta, \mu\gamma)|^2 = \sum_{\mu \in \mathbb{F}_q^*} |\ell_1 z_{1,\mu}^k + \dots + \ell_{\ell_0} z_{\ell_0,\mu}^k|^2 + O\left(q^{1-\frac{k}{2}}\right). \end{aligned}$$

Using Lemma 2, we get

$$\sum_{\mu \in \mathbb{F}_q^*} \frac{1}{R} \sum_{\substack{k < 2R \\ k \equiv 1 \pmod{2}}} |\ell_1 z_{1,\mu}^k + \dots + \ell_{\ell_0} z_{\ell_0,\mu}^k|^2 = O(1) + O\left(\frac{1}{R} q^{\frac{1}{2}}\right),$$

and it means

$$\begin{aligned} (q-1)(\ell_1^2 + \dots + \ell_{\ell_0}^2) &= \sum_{\mu \in \mathbb{F}_q^*} \lim_{\substack{k \rightarrow \infty \\ k \equiv 1 \pmod{2}}} |\ell_1 z_{1,\mu}^k + \dots + \ell_{\ell_0} z_{\ell_0,\mu}^k|^2 = \\ &= \sum_{\mu \in \mathbb{F}_q^*} \overline{\lim}_{R \rightarrow \infty} \frac{1}{R} \sum_{\substack{k \leq 2R \\ k \equiv 1 \pmod{2}}} |\ell_1 z_{1,\mu}^k + \dots + \ell_{\ell_0} z_{\ell_0,\mu}^k|^2 = O(1). \end{aligned}$$

Finally,

$$(q-1)(\ell_1^2 + \dots + \ell_{\ell_0}^2) = O(1) \quad (6)$$

But the last equality is true only in the case, when  $q = O(1)$ . So, for all  $q \geq K$ ,  $K$  is an enough large constant, the maximum of  $|\omega_j|$  is equal to  $q$  or less than  $q$ . It immediately follows that

$$S_k(\alpha, \beta, \gamma) \ll q^k,$$

and, in particular,  $S(\alpha, \beta, \gamma) \ll q$ .

The theorem 1 is proved. ■

**Proof.** We will use Theorem 1. with the conditions

$$\begin{aligned} f_1(x, y, z) &= \alpha x + \beta y^2 + \gamma xz, \\ f_2(x, y, z) &= xyz - 1, \\ \alpha, \beta, \gamma &\in G, \quad (\gamma, p) = 1. \end{aligned}$$

In view of the fact that residue classes modulo  $p$ ,  $p \equiv 3 \pmod{4}$ , in the ring of Gaussian integers form the field  $G_p$  with  $p^2$  elements, we will verify feasibility of conditions of Theorem 1 for  $q = p^2$ .

From the equation  $\alpha x + \beta y + \gamma xz = \tau$  we have

$$z = \frac{\tau - \alpha x - \beta y^2}{\gamma x} \quad \text{and} \quad f_2(x, y, z) = \gamma^{-1} y (\tau - \alpha x - \beta \gamma^{-1}).$$

If we want to demonstrate the fact of absolute irreducibility of  $\varphi\tau(x, y) = \gamma^{-1} y (\tau - \alpha x - \beta \gamma^{-1})$ , it suffices to show that the system of algebraic equations

$$\frac{\partial F}{\partial x} = 0, \quad \frac{\partial F}{\partial y} = 0, \quad \frac{\partial F}{\partial \omega} = 0$$

has no solutions. Here  $F(x, y, \omega) = \omega^3 \left( \gamma^{-1} \tau \frac{y}{\omega} - \alpha \gamma^{-1} \frac{xy}{\omega^2} - \gamma^{-1} \beta \frac{y^3}{\omega^3} \right)$ .

We have the system of equations

$$\begin{cases} \gamma^{-1} \omega^2 - \alpha \gamma^{-1} x \omega - 3 \gamma^{-1} \beta y^2 = 0, \\ \alpha \gamma^{-1} y \omega = 0, \\ 2 \tau \gamma^{-1} y \omega - \alpha \gamma^{-1} x y = 0 \end{cases}$$

with the condition  $x, y \in \mathbb{F}_{p^2}^*$ .

It follows that for  $\alpha = 0$  this system has no solutions, i.e. exceptional values of doesn't.

Let us  $\alpha \neq 0$ . Then from the second equation of system it follows that for  $y \neq 0$  this system also has no solutions.

So, we can apply Theorem 1. Hence, for  $m = 1$  the statement of Theorem 2 proved.

For  $m > 1$  we will consider two cases:

- i)  $m = 2m_0, m_0 \in \mathbb{N}$ ,
- ii)  $m = 2m_0 + 1, m_0 \in \mathbb{N}$ .

In case  $m = 2m_0$  we put

$$X = X_0(1 + p^{m_0} X_1), \quad Y = Y_0(1 + p^{m_0} Y_1), \quad X_0, Y_0 \in G_{p^{m_0}}^*, \quad X_1, Y_1 \in G_{p^{m_0}}.$$

Then the condition  $XYZ \equiv 1 \pmod{p^m}$  gives

$$Z \equiv X^{-1} Y^{-1} \equiv X_0^{-1} Y_0^{-1} (1 - p^{m_0} (X_1 + Y_1)) \pmod{p^{2m_0}}.$$

So,

$$f_1(X, Y, Z) \equiv \alpha X_0 (1 + p^{m_0} X_1) + \beta Y_0^2 (1 + 2p^{m_0} Y_1) + \gamma Y_0^{-1} (1 - p^{m_0} Y_1) \pmod{p^{2m_0}}.$$

From the definition  $S(\alpha, \beta, \gamma; p^m)$  we infer

$$\begin{aligned} & |S(\alpha, \beta, \gamma; p^{2m_0})| = \\ & = \left| \sum_{X_0, Y_0 \in G_{p^{m_0}}^*} e^{2\pi i \frac{\text{Tr}(\alpha X_0 + \beta Y_0^2 + \gamma Y_0^{-1})}{p^{2m_0}}} \sum_{X_1, Y_1 \in G_{p^{m_0}}} e^{2\pi i \frac{\text{Tr}(\alpha X_0 X_1 + (2\beta Y_0^2 - \gamma Y_0^{-1}) Y_1)}{p^{m_0}}} \right| = \\ & = \begin{cases} 0 & \text{if } \alpha \not\equiv 0 \pmod{p^{m_0}}, \\ p^{6m_0} \left(1 - \frac{1}{p^2}\right) \left| \sum_{\substack{Y_0 \in G_{p^{m_0}}^* \\ 2\beta Y_0^2 \equiv \gamma Y_0^{-1} \pmod{p^{m_0}}} } e^{2\pi i \frac{\text{Tr}(\beta Y_0^2 + \gamma Y_0^{-1})}{p^{m_0}}} \right| & \leq 3p^{3m} = \\ & = 3(N(p^m))^{\frac{3}{2}}. \end{cases} \end{aligned}$$

Now let  $m = 2m_0 + 1$ . As above we have

$$\begin{aligned}
S(\alpha, \beta, \gamma; p^{2m_0+1}) &= \\
&= \sum_{X_0, Y_0 \in G_{p^{m_0+1}}^*} e^{2\pi i \frac{\text{Tr}(\alpha X_0 + \beta Y_0^2 + \gamma Y_0^{-1})}{p^{2m_0+1}}} \times \\
&\times \sum_{X_1, Y_1 \in G_{p^{m_0}}} e^{2\pi i \frac{\text{Tr}(\alpha X_0 X_1 + (2\beta Y_0^2 + \gamma Y_0^{-1}) Y_1)}{p^{m_0}}} = \\
&= \begin{cases} 0, & \text{if } \alpha \not\equiv 0 \pmod{p^{m_0}}, \\ N(p^{2m_0}) \sum_1 \cdot \sum_2, & \text{if } \alpha = \alpha_0 p^{m_0}, \end{cases} \tag{7}
\end{aligned}$$

where

$$\begin{aligned}
\sum_1 &= \sum_{X_0 \in G_{p^{m_0+1}}^*} e^{2\pi i \frac{\text{Tr}(\alpha_0 X_0)}{p^{m_0+1}}}, \\
\sum_2 &= \sum_{\substack{Y_0 \in G_{p^{m_0+1}}^* \\ 2\beta Y_0^3 \equiv \gamma \pmod{p^{m_0}}}} e^{2\pi i \frac{\text{Tr}(\beta Y_0^2 + \gamma Y_0^{-1})}{p^{2m_0+1}}}.
\end{aligned}$$

It is evident that  $\sum_1$  is the Ramanujan sum over  $G$  and it is equal to

$$\begin{cases} N(p^{\nu_0}) \mu(p^{m_0+1-\nu_0}), & \text{if } \nu_p(\alpha_0) = \nu_0 < m_0 + 1, \\ N(p^{m_0+1}), & \text{if } \nu_p(\alpha_0) \geq m_0 + 1. \end{cases} \tag{8}$$

Further, in sum  $\sum_2$  we take into account that the congruence  $2\beta Y_0^3 \equiv \gamma \pmod{p^{m_0}}$  has at most three solutions. Denote  $\Xi$  the set of solutions of this congruence. If  $\Xi = \emptyset$ , we have  $S(\alpha, \beta, \gamma; p^{2m_0+1}) = 0$ . Otherwise, let  $Y_{0j}$  is one of the impliable solutions. Put  $Y_0 = Y_{0j} + p^{m_0}y$ ,  $y \in G_p$ .

By virtue,

$$\beta Y_0^2 + \gamma Y_0^{-1} = \beta Y_{0j}^2 + 2\beta p^{m_0} Y_{0j} y + p^{2m_0} \beta y^2 + \gamma Y_{0j}^{-1} (1 - p^{m_0} Y_{0j}^{-1} y + p^{2m_0} Y_{0j}^{-2} y^2),$$

we, by Lemma 5, infer

$$\sum_2 = \sum_{Y_{0j} \in \Xi} e^{2\pi i \frac{\text{Tr}(\beta Y_{0j}^2)}{p^{2m_0+1}}} \sum_{y \in G_p} e^{2\pi i \frac{\text{Tr}\left(\frac{Y_{0j}(2\beta Y_{0j}^2 - \gamma Y_{0j}^{-1})}{p^{m_0}} y + \beta y^2\right)}{p}}. \tag{9}$$

The inner sum over  $y$  estimates similarly of the Gauss sum if  $(\beta, p) = 1$ , and, for  $\beta \equiv 0 \pmod{p}$ , it is equal to 0.

Finally, note, that for  $\nu_p(\alpha_0) \geq m_0 + 1$  we have  $\alpha \equiv 0 \pmod{p^m}$  and then being

investigated exponential sum  $S(\alpha, \beta, \gamma; p^m)$  take on form

$$\begin{aligned}
 S(0, \beta, \gamma; p^m) &= \sum_{\substack{X, Y, Z \in G_{p^m}^* \\ XYZ \equiv 1 \pmod{p^m}}} e^{2\pi i \frac{\text{Tr}(\beta Y^2 + \gamma XY)}{p}} = \\
 &= \sum_{X, Y \in G_{p^m}^*} e^{2\pi i \frac{\text{Tr}(\beta Y^2 + \gamma Y^{-1})}{p}} = \\
 &= N(p^m) \left(1 - \frac{1}{p^2}\right) \sum_{Y \in G_{p^m}^*} e^{2\pi i \frac{\text{Tr}(\beta Y^2 + \gamma Y^{-1})}{p}},
 \end{aligned} \tag{10}$$

and last sum estimates, by Lemma 5, as  $N(p^m)^{\frac{1}{2}}$  if  $(\beta, p) = 1$ , and as  $-1$  if  $\beta \equiv 0 \pmod{p}$ ,  $(\gamma, p) = 1$ . From (7)-(10) we obtain the assertion of Theorem 2. ■

The scheme of reasoning used in the proof of Theorem 2 can be applied to investigations of various generalizations of the Kloosterman sums.

**CONCLUSION.** We considered the application of C. Hooley method for construction of the estimates of exponential sums on algebraic variety over the finite field. It was obtained a nontrivial estimate with the rational function on three variables over the ring of residue classes modulo  $p^m$  in the ring of Gaussian integers.

1. **Birch B.** On some exponential sums [text] / Birch B., Bombieri E. // Ann. Math. – 1985. – V. 121. – P. 345–350.
2. **Bombieri E.** On exponential sums in finite fields [text] / Bombieri E. // Invent. Math. – 1978. – V. 47. – P. 29–39.
3. **Bombieri E.** On two problems of Mordell [text] / Bombieri E., Davenport H. // Amer. J. Math. – 1966. – V. 88. – P. 67–70.
4. **Deligne P.** La conjecture de Weil I [text] / Deligne P. // Inst. Hautes. Etudes Sci. Publ. Math. – 1974. – V. 43. – P. 273–307.
5. **Deligne P.** La conjecture de Weil II [text] / Deligne P. // Inst. Hautes. Etudes Sci. Publ. Math. – 1980. – V. 52. – P. 137–252.
6. **Dwork B.** On the rationality of the zeta function of an algebraic variety [text] / Dwork B. // Amer. J. Math. – 1960. – V. 82. – P. 631–648.
7. **Gunyavy O.** Exponential sum on algebraic variety  $\frac{\alpha}{f_1(x,y)} + \frac{\beta}{f_2(x,y)} = 1$  [text] / Gunyavy O., Varbanets P. // Annales Univ. Sci. Budapest, Sect. Comp. – 2008. – V. 28. – P. 283–301.
8. **Hooley C.** On the numbers that are representable as the sum of two cubes [text] / Hooley C. // J. Reine Angew. Math. – 1980. – V. 314. – P. 145–173.
9. **Varbanets P.** On inversive congruential generator with a variable shift with prime power modulus [text] / Varbanets P., Varbanets S. // Annales Univ. Sci. Budapest, Sect. Comp. – 2010. – V. 32. – P. 151–176.
10. **Weil A.** On the exponential sums [text] / Weil A. // J. London Math. Soc.(2). – 1948. – V. 3. – P. 204–207.

Received 08.12.2014