Algebra and Discrete Mathematics RESEARCH ARTICLE
Volume 11 **(2011)**. Number 2. pp. 82 – 91

Norm Kloosterman sums over $\mathbb{Z}[i]$

O. Savastru and S. Varbanets

Communicated by V. V. Kirichenko

Abstract. n-dimensional norm Kloosterman sums over the ring of the Gaussian numbers investigate. Nontrivial estimates of these sums were obtained.

Introduction

The classical Kloosterman sums $K(a, b\,; q)$ and their n-dimensional analogue $K_n(a_0, a_1, \ldots, a_n\,; q)$ are important ingradients in problems contained with a distribution of arithmetic functions on the arithmetic progressions (see, [5], [6] and etc.). The sums of the Kloosterman sums studied in the works N.V. Kuznetsov [12], H. Iwaniec and I.-M. Deshouillers [7] and etc., have allowed to improve the error terms in additive problems of number theory. The same problems arise at the decision of the asymptotic tasks over the ring of integer numbers of the finite expansions of the rational field. For example, U. Zanbyrbaeva [11] obtained a nontivial estimate of error term in the problem of divisors of the Gaussian integers in an arithmetical progressions (see. also [9]), and in 2003 Bruggeman and Y. Motohashi [2] obtained the lower estimate for fourth moment of the zeta–function Hecke of the Gaussian field $\mathbb{Q}[i]$.

In 2008 was considered the norm Kloosterman sum over the ring of the Gaussian integers $\mathbb{Z}[i]$ (see. [8]). It permitted to find non–trivial asymptotic formula for the divisor function $\tau(\alpha)$ with norm in an arithmetical progression.

In present paper we study n–dimensional norm Kloosterman sums over the ring of the Gaussian integers.

2000 Mathematics Subject Classification: *11L05.*
Key words and phrases: *Kloosterman sum, Gaussian numbers.*

1. Preliminaries

In this section we fix some notations and gather some necessary facts that will be used in the sequel.
In the following, greek letters $\alpha, \beta, \ldots$ we denote the Gaussian integers; p denotes a prime rational number;
$Sp(\alpha)$ is a trace α from $\mathbb{Q}[i]$ in $\mathbb{Q}$, i.e. $Sp(\alpha) = 2\Re\alpha$;
$N(\alpha)$ is a norm α, $N(\alpha) = \alpha\overline{\alpha} = |\alpha|^2$;
$\mathbb{Z}_q$ (respectively,$\mathbb{Z}_q^*$) is complete (respectively, reduced) system of residues modulo q in $\mathbb{Z}$;
$R(q)$ (respectively,$R^*(q)$) is complete (respectively, reduced) system of residues modulo q in $\mathbb{Z}[i]$;
notation $\sum\limits_{S(C)}$ means, that summation passes under the condition C, which we describe separately;
(a, b) means the greatest common divisor a and b in $\mathbb{Z}$ (or in $\mathbb{Z}[i]$);
$e^{2\pi i \frac{x}{q}} := e_q(x),\ x \in \mathbb{R}$.

Let $q = p^a$, $a \in \mathbb{N}$. By $\mathbf{k}_m$ denote the field with q^m elements, $m = 1, 2, \ldots$; $\mathbf{k}_1 := \mathbf{k}$. Let X is N-dimensional vector $\in \mathbf{k}^N$. Denote by $\mathbf{V}_r$ is an algebraic variety defined by polynomial $f(X) \in \mathbf{k}[X]$, i.e.

$$\mathbf{V}_r = \left\{ X \in \mathbf{k}_r^N \mid f(X) = 0 \right\}.$$

Let yet $Tr(x)$, $x \in \mathbf{k}_n$, be the trace transformation $\mathbf{k}_n \to \mathbf{k}$ defined by the Frobenius automorphism:

$$Tr(x) := x + x^q + \ldots + x^{q^{n-1}},\ x \in \mathbf{k}_n.$$

Obviously that $Tr(x) \in \mathbf{k}$. Put for $a \in \mathbf{k}^*$, $\mathbf{k}^* = \mathbf{k} \setminus \{0\}$,

$$S_r(f) = \sum_{X \in \mathbf{V}_r} e_p\left(a\, Tr\left(f(X)\right)\right). \qquad (1)$$

Introduce the function

$$\zeta(\mathbf{V}, t, f) := \exp\left(\sum_{r=1}^{\infty} \frac{S_r(f)}{r} t^r\right), \qquad (2)$$

which we call the zeta-function of an algebraic variety $\mathbf{V}$ over the finite field $\mathbf{k}$.

B.Dwork [4] proved, that $\zeta(\mathbf{V}, t, f)$ is a rational function $\frac{h(t)}{g(t)}$, moreover the set of roots $\Omega = \{\omega^{-1}\}$ of the polynomials $h(t), g(t)$ describes the following lemmas:

Lemma 1 (Deligne [3]). *For numbers $\omega_j^{-1} \in \Omega$ we have*

$$|\omega_j| = q^{\frac{m_j}{2}},\ m_j \text{ are nonnegative numbers.}$$

Moreover, for every $\omega_j^{-1} \in \Omega$ all complex conjugate have equal modules. (The numbers call characteristic roots, and numbers m_j call the weights of ω_j, $\omega_j^{-1} \in \Omega$).

Lemma 2. *The cardinality of Ω does not exceed $(4D+5)^{2n+1}$, where $D := \max(1 + deg\mathbf{V}, deg f)$, i.e. depends only on n and f.*

Taking a logarithm from LHS and RHS of (2) and comparing coefficients for the same powers t we obtain

$$S_r := S_r(\mathbf{V}, f) = \sum_{\substack{i \\ h(\omega_i^{-1})=0}} (\omega_i)^r - \sum_{\substack{j \\ g(\omega_j^{-1})=0}} (\omega_j)^r. \tag{3}$$

Lemma 3. *Let q be the number of elements of finite field $\mathbf{k}$. Then for the coefficients S_r associated with the zeta-function of algebraic variety over $\mathbf{k}$ the following assertions:*

(i) $|S_r| = O(q^{\frac{rt}{2}})$ *if* $|S_r| = O(q^{r\theta})$ *for some $\theta > 0$, where $t = [2\theta]$,*

(ii) *if $t \in \mathbb{N}$ and $|S_r| \leqslant cq^{\frac{rt}{2}}$ for all sufficiently large r, then characteristic roots of zeta-function have the weight $m \leqslant t$, and the number of roots does not exceed c^2,*

hold.

Lemmas 2 and 3 were proved by E. Bombieri [1].

Define the algebraic variety $\mathbf{V}$ over $\mathbf{k}$ by the polynomial $x_1 \dots x_N - a$, $a \in \mathbf{k}^*$, and the function f we define as $f = x_1 + \dots + x_N$. In this special case P. Deligne [3] proved that $\zeta(\mathbf{V}, t, f)$ has exactly N characteristic roots of the weight $(N-1)$, and hence

$$|S_r(\mathbf{V}, f)| = |S_r| \leqslant Nq^{\frac{r(N-1)}{2}}. \tag{4}$$

Now we define the N-dimensional Kloosterman sum.
Let $q > 1$ is a positive integer. Then $h \in \mathbb{N}$, $(h,q) = 1$, calls a norm residue modulo q, if there exist $\alpha \in \mathbb{Z}$, such that $N(\alpha) \equiv h \pmod{q}$.

Since for $(h,p) = 1$, $p > 2$ is a prime,

$$\mathcal{J}_{p^n}(h) := \left\{x, y \in \mathbb{Z}_{p^n} :\ x^2 + y^2 \equiv h \pmod{p^n}\right\} = p^n \left(1 - \frac{(-1)^{\frac{p-1}{2}}}{p}\right)$$

we conclude that every $h \in \mathbb{Z}_q^*$ is a norm residue modulo q if $(q, 2) = 1$.

For the Gaussian integers $\alpha_0, \alpha_1, \ldots, \alpha_N$ define the N-dimensional Kloosterman sum for $(h, q) = 1$:

$$\widetilde{K}_N(\alpha_0, \alpha_1, \ldots, \alpha_N\,; q, h) := \sum_{S(C)} e_q\left(\Re(\alpha_0 x_0 + \ldots + \alpha_N x_N)\right), \quad (5)$$

где

$$C : x_i \in \mathbf{R}(q),\ i = 0, 1, \ldots, N;\ N(x_0 x_1 \ldots x_N) \equiv h \pmod{q}.$$

For $q = q_1 q_2,\ (q_1, q_2) = 1$, we have

$$\begin{gathered}\widetilde{K}_N(\alpha_0, \alpha_1, \ldots, \alpha_N; q, h) = \\ = \widetilde{K}_N(\alpha_0 q_2, \ldots, \alpha_N q_2; q_1, h)\widetilde{K}_N(\alpha_0 q_1, \ldots, \alpha_N q_1; q_2, h).\end{gathered} \quad (6)$$

Therefore in sequel we consider only case $q = p^m$, p is a prime, $m \in \mathbb{N}$. From the definition of norm sum we have the trivial estimate

$$|\widetilde{K}_N(\alpha_0, \alpha_1, \ldots, \alpha_N; p^m, h)| \leqslant (\varphi(p^m))^{2N+1}, \quad (7)$$

where $\varphi(\cdot)$ is the Euler function.

From an estimate of the n-dimensional Kloosterman sum over $\mathbb{Z}[i]$ (see. [10]) we infer

$$|\widetilde{K}_N(\alpha_0, \alpha_1, \ldots, \alpha_N; p^m, h)| \leqslant \epsilon_p \cdot N \cdot (\varphi(p^m))^{2N},$$

where

$$\epsilon_p(N) = \begin{cases} N, & \text{if } m \text{ is even number;} \\ \frac{N(N-1)}{2} \cdot p^{\frac{2-N}{2}}, & \text{if } m \text{ is odd, } p \neq 2, 3; \\ 4N, & \text{if } m \text{ is odd, } p = 2; \\ 3N, & \text{if } m \text{ is odd, } p = 3. \end{cases}$$

From main theorem which will prove below we obtain "the rooted estimate" for $\widetilde{K}_N(\alpha_0, \alpha_1, \ldots, \alpha_N; p^m, h)$ (i.e. an estimate is the square root out of trivial estimate) for the case $(\alpha_0 \ldots \alpha_N, p) = 1)$.

2. Main result

Let $\gamma \in \mathbb{Z}[i]$. Denote $m_\gamma = \max\{m : p^m | \gamma\}$.

Theorem 1. *Let h is a norm residue modulo p. Then*

$$\widetilde{K}_N(\alpha_0, \alpha_1, \ldots, \alpha_N; p^m, h) \leqslant 2(4N-1)p^{2N(m-n)} I(\alpha_1, \ldots, \alpha_N; p^m), \quad (8)$$

where $I(\alpha_1,\dots,\alpha_N;p^m)$ is the number of solutions of the system of congruences (23);
moreover $I(\alpha_1,\dots,\alpha_N;p^m)\leqslant(4N-1)p^{N(2n-m)}$,
if $m_{\alpha_1}=\dots=m_{\alpha_N}=0$.
(Here $n=\left[\frac{m+1}{2}\right]$, $[x]$ denotes the biggest integer $\leqslant x$).

Proof. First let $m=1$. The case $m_{\alpha_0}=\dots=m_{\alpha_N}=1$ is trivial, and so suppose α_i is coprime with p for some number i. Putting
$\alpha_j=a_j+ib_j$, $j=0,1,\dots,N$, infer $(a_0,\dots,a_N,b_0,\dots,b_N,p)=1$.
For $p\equiv 1\,(\mathrm{mod}\ 4)$ we have

$$\widetilde{K}_n(\alpha_0,\dots,\alpha_N;p,h)=\sum_{S(C)}e_p(a_0x_0+\dots+a_Nx_N-b_0y_0-\dots-b_Ny_N),\quad (9)$$

where

$$C:\{x_0,\dots,x_N,y_0,\dots,y_N\in\{0,1,\dots,p-1\};\ \prod_{j=0}^{N}(x_j^2+y_j^2)\equiv h\ (\mathrm{mod}\ p)\}.$$

Let ε_0 is solution of the congruence $x^2\equiv -1\,(\mathrm{mod}\ p)$.
Put

$$u_j=x_j+\varepsilon_0y_j,\ v_j=x_j-\varepsilon_0y_j,\ j=0,1,\dots,N.\quad (10)$$

By $(h,p)=1$ and $u_jv_j\equiv x_j^2+y_j^2\not\equiv 0\,(\mathrm{mod}\ p)$, $j=0,1,\dots,N$ we obtain that $u_j,v_j\in\mathbb{Z}_p^*$.
Therefore (by (10)):

$$\begin{cases}\widetilde{K}_n(\alpha_0,\dots,\alpha_N;p,h)=\sum\limits_{S(C)}e_p\left(\sum\limits_{j=0}^{N}A_ju_j+\sum\limits_{j=0}^{N}B_jv_j\right),\\ C:\{u_j,v_j\in\mathbb{Z}_p^*,j=0,1,\dots,N:\ \prod\limits_{j=0}^{N}u_jv_j\equiv h\ (\mathrm{mod}\ p)\}.\end{cases}\quad (11)$$

Let among of $\alpha_0,\dots,\alpha_N$ have exactly l nulls modulo p elements (for example, $\alpha_0=\dots=\alpha_{l-1}=0$, $\alpha_{l+1}\dots\alpha_N\not\equiv 0\,(\mathrm{mod}\ p)$.
Then from (11) infer

$$\begin{cases}\widetilde{K}_n(\alpha_0,\dots,\alpha_N;p,h)=\sum\limits_{u_0=1}^{p-1}\dots\sum\limits_{u_{l-1}=1}^{p-1}\sum\limits_{S(C)}e_p(\sum\limits_{j=l}^{N}(A_ju_j+B_jv_j)),\\ C:\{u_j,v_j\in\mathbb{Z}_p^*,j=l,\dots,N;\prod\limits_{j=l}^{N}u_jv_j\equiv h\prod\limits_{j=0}^{l-1}(u_jv_j)^{-1}(\mathrm{mod}\ p)\}.\end{cases}\quad (12)$$

Take into account that for $j=l,\dots,N$.

$$A_j\equiv\frac{1}{2}(a_j-\varepsilon_0^{-1}b_j),\ B_j\equiv\frac{1}{2}(a_j+\varepsilon_0^{-1}b_j),\ \varepsilon_0\varepsilon_0^{-1}\equiv 1\ (\mathrm{mod}\ p);$$

$$A_jB_j \equiv \frac{1}{4}(a_j^2+b_j^2) \equiv \frac{1}{4}N(\alpha_j) \pmod p.$$

Hence $(A_j,p)=(B_j,p)=1$.
Now, the application of the P. Deligne estimate [3] (see, formula (4), the above) gives

$$|\widetilde{K}_N(\alpha_0,\alpha_1,\ldots,\alpha_N;p,h)| \leqslant (N-l+1)p^{2Nl}p^{\frac{2(N-l)-1}{2}} = (N-l+1)p^{N+l+\frac{1}{2}}. \tag{13}$$

In particular, for $l=0$ we obtain "the rooted estimate" $(N+1)p^{\frac{2N+1}{2}}$.

Now consider the case $p\equiv 3 \,(\mathrm{mod}\ 4)$.
Let $\alpha_0,\ldots,\alpha_{l-1}\equiv 0 \,(\mathrm{mod}\ p)$, $\alpha_l\ldots\alpha_N \not\equiv 0 \,(\mathrm{mod}\ p)$.
The complete system of residues modulo p in $\mathbb{Z}[i]$ is field $\mathbf{R}(p)$ from p^2 elements.
Again we consider the algebraic variety $\mathbf{V}$ over $\mathbf{k}=\mathbb{Z}_p$, generated by the polynomial

$$x_0x_1\ldots x_N-h, \quad h\in\mathbf{k}^*$$

and let $f(x_0,\ldots,x_N)=\alpha_0x_0+\ldots+\alpha_Nx_N$.
For $p\equiv 3(\mathrm{mod}\ 4)$ we have

$$(u+vi)^p \equiv u^p - iv^p \equiv u-iv \pmod p, \quad u,v\in\mathbb{Z},$$

and, hence, in the field $\mathbf{R}(p)$:

$$Sp\,(u+iv) \equiv Tr\,(u+iv) \pmod p, \tag{14}$$

where the function $Sp(\cdot)$ (respectively, $Tr(\cdot)$) we consider as a function of trace from the quadratic expansion $\mathbb{Q}[i]$ (respectively, from $\mathbf{k}_2=\mathbf{R}(p)$) in Q (respectively, in $\mathbf{k}=\mathbb{Z}_p$).
Hence, denoting by l the number of α_i, congruented with 0 modulo p, we can estimate $S_2(\mathbf{V},f)$ by formula (4). And so we have

$$S_2(\mathbf{V},f) \leqslant (N+1-l)p^{\frac{2(2N+2-2l-1)}{2}}p^{4l} = (N+1-l)p^{2N+2l+1}. \tag{15}$$

Now from (3) follows that

$$S_1^2(\mathbf{V},f) \sim NS_2(\mathbf{V},f). \tag{16}$$

Thereby in the case $p\equiv 3 \,(\mathrm{mod}\ 4)$ the assertion of theorem proved also.
Since, the case $p=2$ is trivial we obtain the proof of theorem for $m=1$.

Put further $m>1$.
Without loss of generality, we can suppose that
$(p^{m_{\alpha_0}},\, p^{m_{\alpha_1}},\ldots,\, p^{m_{\alpha_N}},\, p^m)=1$. Consequently, though one from numbers a_j, $j=0,1,\ldots,N$ is coprime whith p. Let$(\alpha_0,p)=1$. Hence, $(a_0,b_0,p)=$

1, where $\alpha_0 = a_0 + ib_0$.
Denote $\xi_j = x_j + iy_j$, $j = 0, 1, \dots, N$. We have

$$
\begin{aligned}
&\widetilde{K}_N(\alpha_0, \dots, \alpha_N; p^m, h) = \\
&= \frac{1}{p^m} \sum_{\substack{\xi_j \in \mathbf{R}(p^m) \\ j=0,\dots,N}} \sum_{k=0}^{p^m-1} e_{p^m}\left(k(N(\xi_0 \dots \xi_N) - h) + \sum_{j=0}^{N} \Re(\alpha_j \xi_j)\right) = \\
&= \frac{1}{p^m} \sum_{S(C)} e_{p^m}\left(k \prod_{j=0}^{N} (x_j^2 + y_j^2) - h) + \sum_{j=0}^{N} a_j x_j - \sum_{j=0}^{N} b_j y_j\right), \\
&C : \{k \in \mathbb{Z}_{p^m},\ x_j, y_j \in \mathbb{Z}_{p^m},\ j = 0, 1, \dots, N\}.
\end{aligned} \tag{17}
$$

We can suppose that $\xi_j \in \mathbf{R}^*(p^m)$, $j = 1, \dots, N$, (else, the summation over k gives zero).
Next, for every $k \equiv 0 \,(\mathrm{mod}\ p)$ the summation over x_0, y_0 (by $(a_0, b_0, p) = 1$) gives zero.
Hence, from (14) obtain

$$
\begin{aligned}
&\widetilde{K}_N(\alpha_0, \dots, \alpha_N; p^m, h) = \frac{1}{p^m} \sum_{k \in \mathbb{Z}^*_{p^m}} \sum_{\substack{\xi_j \in \mathbf{R}^*(p^m) \\ j=1,\dots,N}} e_{p^m}(-kh) \times \\
&\times \sum_{\xi_0 \in \mathbf{R}(p^m)} e_{p^m}\left(kN(\xi_0) \prod_{j=1}^{N} N(\xi_j) + \Re(\alpha_0 \xi_0) + \sum_{j=1}^{N} \Re(\alpha_j \xi_j)\right) = \\
&= \frac{1}{p^m} \sum_{k \in \mathbb{Z}^*_{p^m}} e_{p^m}(-kh) \times \\
&\times \sum_{\substack{\xi_j \in \mathbf{R}^*(p^m) \\ j=1,\dots,N}} \sum_{x_0, y_0 \in \mathbb{Z}_{p^m}} e_{p^m}\left(k \prod_{j=1}^{N} N(\xi_j)(x_0^2 + y_0^2) + a_0 x_0 - b_0 y_0\right) = \\
&= \sum_{k \in \mathbb{Z}^*_{p^m}} e_{p^m}(-kh) \sum_{\substack{\xi_j \in \mathbf{R}^*(p^m) \\ j=1,\dots,N}} e_{p^m}\left(\Re(\alpha_j \xi_j) - 4' k' \prod_{j=1}^{N} N(\xi_j)'(a_0^2 + b_0^2)\right),
\end{aligned} \tag{18}
$$

where $4 \cdot 4' \equiv 1 (\mathrm{mod}\ p^m)$, $k \cdot k' \equiv 1 (\mathrm{mod}\ p^m)$, $N(\xi_j) \cdot N(\xi_j)' \equiv 1 (\mathrm{mod}\ p^m)$, $j = 1, \dots, N$.
(We estimated the sums over x_0, y_0 as the classical Gaussian sums).

Let $n := [\frac{m+1}{2}]$. Put for $j = 1, 2, \dots, N$:

$$\xi_j = \eta_j + p^n \zeta_j \qquad \eta_j \in \mathbf{R}^*(p^n), \qquad \zeta_j \in \mathbf{R}(p^{m-n}). \tag{19}$$

Then

$$N(\xi_j)' = N(\eta_j)'(1 - 2p^n(x_j u_j + y_j v_j) N(\zeta_\eta)'), \tag{20}$$

if we set

$$\eta_j = x_j + iy_j, \quad \zeta_j = u_j + iv_j, \quad x_j, y_j \in \mathbb{Z}_{p^m}, \quad u_j, v_j \in \mathbb{Z}_{p^{m-n}} \tag{21}$$

And so, from (18) we find

$$|\widetilde{K}(\alpha_0,\dots,\alpha_N;p^m,h)| = $$
$$= |\sum_{k\in\mathbb{Z}_{p^m}^*} e_{p^m}(-kh) \sum_{j=1}^{N} \sum_{\substack{x_j,y_j\in\mathbb{Z}_{p^n}\\ (x_j^2+y_j^2,p)=1}} e_{p^m}(\Re(\alpha_j\eta_j)) \sum_{u_j,v_j\in\mathbb{Z}_{p^{m-n}}} e_{p^m}(G+p^nH)|, \tag{22}$$

where

$$G = 4'k'(a_0^2+b_0^2)\prod_{j=1}^{N}(x_j^2+y_j^2)' := 4'k'(a_0^2+b_0^2)D.$$

$$H = \sum_{j=1}^{N}\left\{-2'k'(a_0^2+b_0^2)\cdot D\cdot(x_ju_j+y_jv_j)+a_ju_j-b_jv_j\right\}.$$

Note that now the summation over u_j, v_j gives zero if the system of congruences

$$\begin{cases} a_j - 2D^2N(\eta_j)'x_j \equiv 0 \pmod{p^{m-n}}, \\ b_j + 2D^2N(\eta_j)'y_j \equiv 0 \pmod{p^{m-n}}, \end{cases} \tag{23}$$

disturbs though for one j, $j=1,2,\dots,N$. This system is equivalent to the system

$$\begin{cases} a_jy_j + b_jx_j \equiv 0 \,(\mathrm{mod}\; p^{m-n}), \\ 2'k'\prod_{j=1}^{N}\left((x_j^2+y_j^2)^2\right)'(a_0^2+b_0^2)x_j + a_j \equiv 0 \,(\mathrm{mod}\; p^{m-n}), \\ \qquad\qquad \text{if } a_j\not\equiv 0,\ b_j\not\equiv 0 \,(\mathrm{mod}\; p^{m-n}); \\ y_j\equiv 0, \qquad \text{if } b_j\equiv 0 \,(\mathrm{mod}\; p^{m-n}); \\ x_j\equiv 0, \qquad \text{if } a_j\equiv 0 \,(\mathrm{mod}\; p^{m-n}), \\ (j=1,2,\dots,N). \end{cases} \tag{24}$$

Let t is the number of α_j, $j=1,\dots,N$, which are coprime with p. If $t=N$, then from (23)-(24) we see that every x_j defines the single y_j modulo p^{m-n}, and, hence, there does not exceed $p^{n-(m-n)}=p^{2n-m}$ the value y_j, corresponding to x_j modulo p^n.
Moreover the secondary congruence in (24) gives

$$x_j \equiv a_1'a_jx_1 \pmod{p^{m-n}}, \quad \text{if}\,(a_1,p)=1,$$

or

$$y_j \equiv b_1'b_jy_1 \pmod{p^{m-n}}, \quad \text{if}\,(b_1,p)=1.$$

Consequently, the value x_1 (or y_1, if $a_1\equiv 0(\mathrm{mod}\; p)$) defines the single y_1 and the pairs (x_j,y_j) modulo $p^{n-m}, j=2,\dots N$. Moreover, N-tuple

$(x_1, y_1, \dots, x_N, y_N)$ is the solution of the congruences (23). Next, from (24) one easily derives that x_1 is the root of the congruence $Ax_1^{4N+1} \equiv B(\text{mod } p^{m-n})$. Consequently, the number of solutions of system (23) does not exceed $(4N-1)p^{N(2n-m)}$.
Hence, by (22) we have

$$|\widetilde{K}_N(\alpha_0, \dots, \alpha_N; p^m, h)| = \sum_{(x_1,\dots,y_N)}{}^{*} \sum_{k\in\mathbb{Z}^*_{p^m}} |e_{p^m}(-kh + k'h_1)|,$$

where the $(*)$ indicates that the summation passes over admissible $2N$-tuples $(x_1, y_1, \dots, x_N, y_N)$; and h_1 is integer, depended from $(x_1, \dots, y_N)$. Hence, using an estimate of the rational Kloosterman sum and the estimate of the number of admissible $2N$-tuples, we obtain

$$\begin{aligned} |\widetilde{K}_N(\alpha_0, \dots, \alpha_N; p^m, h)| \leqslant 2p^{\frac{m}{2}}(4N-1)p^{N(2n-m)}p^{2N(m-n)} = \\ = 2(4N-1)p^{\frac{2N+1}{2}m}. \end{aligned} \tag{25}$$

In general case, from (22)-(23)

$$|\widetilde{K}_N(\alpha_0, \alpha_1, \dots, \alpha_N; p^m, h)| \leqslant 2p^{\frac{m}{2}+2N(m-n)} I(\alpha_1, \dots, \alpha_N; p^m), \tag{26}$$

where $I(\alpha_1, \dots, \alpha_N; p^m)$ is the number of solutions of congruence (23). It is easy to see that

$$I(\alpha_1, \dots, \alpha_N; p^m) \leqslant (4N-1)p^{m_{\alpha_1}+\dots+m_{\alpha_N}}.$$

Conclusion

In conclusion note, that the estimate (25) is "the rooted estimate" and apparently in general case is best possible

References

[1] E. Bombieri, *On exponential sums in finite fields,II*, Invent. math., 47(1),1978, pp. 29-39.

[2] R. Bruggeman, Y. Motohashi, *Sum formula for Kloosterman sums and fourth moment of the Dedekind zeta-function over the Gaussian number field*, Functiones et Approximatio., XXXI(2003), pp. 23-92.

[3] P. Deligne, *La conjecture de Weill, I, II*, Publ. Math. IHES, 43(1974),pp. 273-307; 52(1980), pp. 137-252.

[4] B. Dwork, *In the rationality of the zeta-function of an algebraic variety*, Amer. J. Math. ,82(1960), pp. 631-648.

[5] D.R. Heath-Brown, *The divisor function $d_3(n)$ in arithmetic progressions*, Acta Arith.,XLVII(1986), pp. 59-86.

[6] C. Hooley, *An asymptotic formula in the theory of numbers*, Proc. London Math. Soc. (3), 7(1957), pp. 396-413.

[7] I.-M. Deshouillers, H. Iwaniec, *Kloosterman sums and Fourier coefficients of cusp forms*, Invent. math.,70(1982), pp. 219-288.

[8] S. P. Varbanets, *General Kloosterman sum over ring of Gaussian integers*,Ukr. Math. J., 59 (№ 9), 2007, pp. 1179-1201.

[9] O. Savastru, P. Varbanets, *An additive divisor problem in* $\mathbb{Z}[i]$, Algebra and discrete mathematics, N.1, 2003, pp. 103-110.

[10] S. Varbanets, O. Savastru, *n-dimensional Kloosterman sums over the ring of the gaussian integers*, Vestnik I.I. Mechnikov Odessa National University (to appear).

[11] U.B. Zanbyrbaeva, *Asympotic problems of number theory in sector region*, Dissertation, Odessa, 1993. (in Russian)

[12] N.V. Kuznetsov, *Petterson hypothesis for the form with weight zero and Linnik hypothesis*, Math. Sb., 3 (1980),pp. 334-383. (in Russian)

Contact information

O. Savastru ul.Dvoryanskaya 2, Dept. of computer algebra and discrete mathematics, Odessa national university, Odessa 65026, Ukraine
E-Mail: sav_olga@bk.ru

S. Varbanets ul.Dvoryanskaya 2, Dept. of computer algebra and discrete mathematics, Odessa national university, Odessa 65026, Ukraine
E-Mail: varb@sana.od.ua

Received by the editors: 14.03.2011
and in final form 05.05.2011.