UDC 511.19

S. P. Varbanets (Odessa I. I. Mechnikov Nat. Univ.)

GENERAL KLOOSTERMAN SUMS OVER RING OF GAUSSIAN INTEGERS

УЗАГАЛЬНЕНІ СУМИ КЛОСТЕРМАНА НАД КІЛЬЦЕМ ЦІЛИХ ГАУССОВИХ ЧИСЕЛ

The general Kloosterman sum $K(m,n;k;q)$ over $\mathbb{Z}$ was studied by S. Kanemitsu, Y. Tanigawa, Yi. Yuan, Zhang Wenpeng in their research of problem of D. H. Lehmer. In this paper, we obtain the similar estimations of $K(\alpha,\beta;k;\gamma)$ over $\mathbb{Z}[i]$. We also consider the sum $\widetilde{K}(\alpha,\beta;h,q;k)$ which has not an analogue in the ring $\mathbb{Z}$ but it can be used for the inversigation of the second moment of the Hecke zeta-function of field $\mathbb{Q}(i)$.

Узагальнену суму Клостермана $K(m,n;k;q)$ над $\mathbb{Z}$ вивчали S. Kanemitsu, Y. Tanigawa, Yi. Yuan, Zhang Wenpeng в їх дослідженні проблеми D. H. Lehmer. У цій статті отримано подібні оцінки $K(\alpha,\beta;k;\gamma)$ над $\mathbb{Z}[i]$. Також розглянуто суму $\widetilde{K}(\alpha,\beta;h,q;k)$, що не має аналога в кільці $\mathbb{Z}$, але може бути використана при дослідженні другого моменту дзета-функції Геке поля $\mathbb{Q}(i)$.

1. Introduction. The classic Kloosterman sums appeared first in the work of Kloosterman [1] in connection with the representation of natural numbers by binary quadratic forms. The Kloosterman sum is an exponential sum over a reduced residue system modulo q:

$$K(a,b;q) := \sum_{\substack{x=1\\(x,q)=1}}^{q} e^{2\pi i \frac{ax+bx'}{q}}, \quad a,\ b\in\mathbb{Z}, \quad q>1 \quad \text{is natural},$$

here and in seque x' denote the reciprocal to x modulo q, i.e., $xx'\equiv 1 \pmod q$. By the relation for $q=q_1q_2$, $(q_1,q_2)=1$,

$$K(a,b;q)=K(aq_2',bq_2';q_1)K(aq_1',bq_1';q_2)$$

follows that suffices to obtain the estimations $K(a,b;q)$ only for a case $q=p^n$, p be a prime, $n\in\mathbb{N}$.

The greatest difficultly in an estimation of the Kloosterman sums provides the case $q=p$. The estimation $K(a,b;p)\ll p^{\frac{3}{4}}$ under a condition $(a,b,p)=1$ was obtained in the named work of Kloosterman, and then Davenport [2] improved on it up to $\ll p^{\frac{2}{3}}$. A. Weill [3] proved the Riemann hypothesis for algebraic curves of over finite field and obtained the best possible estimation $\ll p^{\frac{1}{2}}$.

Davenport [2] studies the general Kloosterman sums over finite field with the multiplicative character ψ of this field

$$K_\psi(a,b;p)=\sum_{x\in\mathbb{F}_p^*}\psi(x)e^{2\pi i\frac{ax+bx'}{p}}.$$

The further generalization of the Kloosterman sums concerned with a substitution of a prime field $\mathbb{F}_p$ on it a finite expansion $\mathbb{F}_q$, $q=p^n$, $n\in\mathbb{N}$. The generalization of the Kloosterman sums concerned with theory of modular forms studies in the works Kuznetsov [4, 5], Bruggeman [6], Deshoillers, Iwaniec [7], Proskurin [8]. In last years in connection with the investigation of the D. H. Lemer problem was studied others generalizations of the Kloosterman sums (see [9, 10]):

$$K(a,b;q,k,\psi)=\sum_{x\in\mathbb{R}^*(q)}\psi(x)e^{2\pi i\frac{ax^k+bx'^{\,k}}{q}}, \quad xx'\equiv 1 \pmod q,$$

where ψ is a multiplicative character modulo q.

The multiple Kloosterman sums introduced Mordell [11]:

$$K(a_1,\ldots,a_n;q)=\sum_{\substack{x_1,\ldots,x_n\in\mathbb{F}_q^*\\ x1\ldots x_n=1}} e^{2\pi i\frac{\sigma_m(a_1x_1+\ldots+a_nx_n)}{p}},$$

where $a_1,\ldots,a_n\in\mathbb{F}_q^*$, $q=p^m$, $\sigma_m(c)$ is a trace from $\mathbb{F}_q$ into $\mathbb{F}_p$.

The multiple Kloosterman sums are a particular case of the trigonometric sums on an algebraic variate over a finite field. By virtue of the investigations Dwork [12] (which has proved a rationality of the zeta-function of an algebraic variate over finite field), Deligne [13] (which has proved the Riemann hypothesis for an algebraic variate over $\mathbb{F}_q$) and Bombieri [14] (which has estimated in terms of a generative polynomial the number of characteristic roots of the zeta-function) was obtained the final estimation (see Deligne [15], Bombieri [14])

$$K(a_1,\ldots,a_n;q)\le nq^{\frac{n-1}{2}}.$$

In this paper we obtain the estimations of general Kloosterman sums over the ring of the Gaussian integers.

Notations. We denote $\mathbb{Z}[i]$ the ring of the Gaussian integers

$$\mathbb{Z}[i]:=\big\{a+bi\big|a,\ b\in\mathbb{Z},\ i^2=-1\big\}.$$

For the designation of the Gaussian integers we shall use the Greek letters α, β, γ, ξ, η; a Gaussian prime number denote through $\mathfrak{p}$ if $\mathfrak{p}\notin\mathbb{Z}$. For $\alpha\in\mathbb{Z}[i]$ we put $\mathrm{Sp}(\alpha)=\alpha+\overline{\alpha}$, $N(\alpha)=\alpha\overline{\alpha}$, where $\overline{\alpha}$ denotes a complex conjugate with α; $Sp(\alpha)$ and $N(\alpha)$ we name a trace and a norm (accordingly) of α from $\mathbb{Q}(i)$ into $\mathbb{Q}$. $\mathbb{F}_q$ denotes a field which contain just q an element, $q=p^n$, $n\in\mathbb{N}$.

For $x\in\mathbb{F}_q$ we denote through $\sigma_n(x)$ a trace x from $\mathbb{F}_q$ into $\mathbb{F}_p$, i.e.,

$$\sigma_n(x):=x+x^p+\ldots+x^{p^{n-1}},\qquad \sigma_1(x)=\sigma(x)=x.$$

The writing $a\in R(q)$ (accordingly, $a\in R(q,i)$) denotes that $a\in\mathbb{Z}$ (accordingly, $a\in\mathbb{Z}[i]$) and a runs a complete residue system modulo q. Analogous, $a\in R^*(q)$ (accordingly, $a\in R^*(q,i)$) denotes $a\in\mathbb{Z}$ (accordingly $a\in\mathbb{Z}[i]$) and runs a reduced residue system modulo q.

The writing $\sum_{(U)}$ denotes that the summation runs over the region U which describe extra. Moreover, $\exp(z)=e^z$, $e_q(z)=e^{2\pi i\frac{z}{q}}$ for $q\in\mathbb{N}$; the Vinogradov symbol as in $f(x)\ll g(x)$ means that $f(x)=O(g(x))$.

For Gaussian integers α, β, γ we define the Kloosterman sum

$$K(\alpha,\beta;\gamma)=\sum_{x\in R^*(\gamma,i)}\exp\left(\pi i\,\mathrm{Sp}\frac{\alpha x+\beta x'}{\gamma}\right).$$

Zanbyrbaeva [16] obtained the estimation

$$K(\alpha,\beta;\gamma)\ll 2^{\nu(\gamma)}N(\gamma)^{\frac12}N((\alpha,\beta,\gamma))^{\frac12},$$

where $\nu(\gamma)$ is the number distinct prime divisors of γ; (α,β,γ) denotes the greatest common divisor of α, β, γ.

We consider two type of general Kloosterman sums over $\mathbb{Z}[i]$

$$K(\alpha,\beta;k;\gamma,\psi)=\sum_{x\in R^*(\gamma,i)}\psi(x)\exp\left(\pi i\,\mathrm{Sp}\frac{\alpha x^k+\beta {x'}^k}{\gamma}\right),$$

where α, β, $\gamma\in\mathbb{Z}[i]$, ψ is multiplicative character modulo γ,

$$\widetilde{K}(\alpha,\beta;h,q;k)=\sum_{\substack{x,y\in R^*(q,i)\\ N(xy)\equiv h\,(\mathrm{mod}\,q)}} e_q\left(\frac{1}{2}\,\mathrm{Sp}(\alpha x^k+\beta y^k)\right),$$

where $\alpha,\,\beta\in\mathbb{Z}[i]$, $h,q\in\mathbb{N}$, $(h,q)=1$.

We call $K(\alpha,\beta;k;\gamma,\psi)$ the general power Kloosterman sum and $\widetilde{K}(\alpha,\beta;h,q;k)$ call the norm Kloosterman sum.

Our aim is to obtain non trivial estimations for $K(\alpha,\beta;k;\gamma;\psi)$ and $\widetilde{K}(\alpha,\beta;h,q;k)$.

2. Auxiliary results. For the proofs of our main results some Lemmas are need.

Lemma 2.1. *Let $\mathfrak{p}$ be a Gaussian prime "odd" number,*

$$\alpha_1,\ldots,\alpha_k\in\mathbb{Z}[i],\qquad (\alpha_2,\mathfrak{p})=\ldots=(\alpha_k,\mathfrak{p})=1;\quad \nu_3,\nu_4,\ldots,\nu_k\ge 2,$$

are natural numbers.

Then for every natural $n\ge 2$ we have

$$\left|\sum_{\xi(\mathrm{mod}\,\mathfrak{p}^n)}\exp\left(2\pi i\,\mathrm{Sp}\left(\frac{\alpha_1\xi+\alpha_2\mathfrak{p}\xi^2+\alpha_3\mathfrak{p}^{\nu_3}\xi^3+\ldots+\alpha_k\mathfrak{p}^{\nu_k}\xi^k}{\mathfrak{p}^n}\right)\right)\right|=$$

$$=\begin{cases}0 & \textit{if}\quad (\alpha_1,\mathfrak{p})=1),\\ N(\mathfrak{p})^{\frac{n+1}{2}} & \textit{if}\quad \alpha_1\equiv 0\,(\mathrm{mod}\,\mathfrak{p}).\end{cases}\tag{2.1}$$

Lemma 2.2. *Let $\mathfrak{p}=1+i$ be a Gaussian "even" number and let $\alpha_j\in\mathbb{Z}[i]$, $j=1,2,\ldots,k$; $(\alpha_2,\mathfrak{p})=\ldots=(\alpha_k,\mathfrak{p})=1$.*

Then for any natural numbers $\nu_j\ge 2$, $j=2,3,\ldots,k$, and any $n\ge 2$ the following estimate:

$$\left|\sum_{\xi(\mathrm{mod}\,\mathfrak{p}^n)}\exp\left(2\pi i\,\mathrm{Sp}\left(\frac{\alpha_1\xi+\alpha_2\mathfrak{p}\xi^2+\alpha_3\mathfrak{p}^{\nu_3}\xi^3+\ldots+\alpha_k\mathfrak{p}^{\nu_k}\xi^k}{\mathfrak{p}^n}\right)\right)\right|\le\delta\cdot 2^{n+1},$$

holds, where

$$\delta=\begin{cases}0 & \textit{if}\quad \alpha_1\not\equiv 0\,(\mathrm{mod}\,\mathfrak{p}^2),\\ 2 & \textit{if}\quad \alpha_1\equiv 0\,(\mathrm{mod}\,\mathfrak{p}^2).\end{cases}$$

The assertion of these lemmas are the consequences of the estimates of complete linear sum and Gauss'sum to which we can reduced the primary sums.

Lemma 2.3. *Let **p** be a prime number, $A\in\mathbb{Z}$, $(A,p)=1$, $f(x)\in\mathbb{Z}[x]$,*

$$f(x)=a_1x+a_2x^2+p^{\lambda_3}a_3x^3+\ldots+p^{\lambda_k}a_kx^k,$$

$(a_i,p)=1$, $i=2,3,\ldots,k$; $\lambda_j>0$, $j=3,\ldots,k$.

Then for any $n\in\mathbb{N}$ the equality

$$S:=\sum_{x(\mathrm{mod}\,p^n)}e_{p^n}(Af(x))=\varepsilon(n)p^{\frac{n}{2}}e_{p^n}\big(AF(a_1,\ldots,a_n)\big)$$

holds, where $F(x_1,\ldots,x_n)\in\mathbb{Z}[x_1,\ldots,x_n]$,

$$\varepsilon(n)=\begin{cases}1 & \textit{if}\quad n\quad \textit{is even},\\ \left(\dfrac{A}{p}\right)\cdot(i)^{\left(\frac{p-1}{2}\right)^2} & \textit{if}\quad n\quad \textit{is odd},\end{cases}\qquad \left(\frac{A}{p}\right)\quad \textit{is a symbol of Legendry.}$$

Proof. We set $x=y+p^{n-1}z$, $y\,(\mathrm{mod}\,p^{n-1})$, $z\,(\mathrm{mod}\,p)$. Then we have

$$\sum_{x\,(\mathrm{mod}\,p^n)}e_{p^n}(Af(x))=\sum_{y\,(\mathrm{mod}\,p^{n-1})}\sum_{z\,(\mathrm{mod}\,p)}e_{p^n}\Big(A(f(y)+p^{n-1}zf'(y)\Big).$$

The sum over z gives zero if $f'(y) \not\equiv 0 \pmod{p}$. But we have $f'(y) \equiv a_1 + 2a_2 y \pmod{p}$. Let y_0 be a root of congruence $a_1 + 2a_2 y \equiv 0 \pmod{p}$. Then

$$S = e_{p^n}(Af(y_0)) \sum_{y \,(\mathrm{mod}\, p^{n-1})} e_{p^n}\Big(A(f(y_0+py) - f(y_0))\Big) =$$

$$= e_{p^n}\big(Af(y_0)\big) \sum_{y \,(\mathrm{mod}\, p^{n-1})} e_{p^{n-2}}\big(Ag(y)\big) =$$

$$= pe_{p^n}\big(Af(y_0)\big) \sum_{y \,(\mathrm{mod}\, p^{n-2})} e_{p^{n-2}}\big(Ag(y)\big),$$

where

$$g(y) = \frac{f(y_0+py) - f(y_0)}{p^2} = b_1 y + b_2 y^2 + p^{\mu_3} b_3 y^3 + \ldots + p^{\mu_k} b_k y^k,$$

moreover $b_1, \ldots, b_k$ are linear functions of $a_1, \ldots, a_k$ with the coefficients which depends on y_0, and $b_2 \equiv a_2 \pmod{p}$, $(b_j, p) = 1$, $\mu_j \geq 1$, $j = 3, \ldots, k$. Thus $g(y)$ is a polynomial such sort as $f(y)$.

These consideration we continue further. Then for $n \equiv 1 \pmod{2}$ we obtain

$$S = p^{\frac{n}{2}} e^{2\pi i A\left[\frac{f(y_0)}{p^n} + \frac{g(y_1)}{p^{n-2}} + \ldots\right]},$$

and for n is even

$$S = p^{\frac{n-1}{2}} e^{2\pi i A\left[\frac{f(y_0)}{p^n} + \frac{g(y_1)}{p^{n-2}} + \ldots\right]} \sum_{x \,(\mathrm{mod}\, p)} e_p^{(A(cx + a_2 x^2))} =$$

$$= \left(\frac{A}{p}\right) i^{(\frac{p-1}{2})^2} e^{2\pi i A\left[\frac{f(y_0)}{p^n} + \frac{g(y_1)}{p^{n-2}} + \ldots - \frac{(2'c)^2}{p}\right]}.$$

The lemma is proved.

Lemma 2.4. *Let p be a prime number, $p \equiv 3 \pmod{4}$ and let E_ℓ be a set of residue classes $\mathrm{mod}\, p^\ell$ of the ring $\mathbb{Z}[i]$, which has norms congruous modulo p^ℓ with ± 1. Then E_ℓ is a cyclical group of order $2(p+1)p^{\ell-1}$.*

Proof. From an equality $N(\alpha\beta) = N(\alpha)N(\beta)$ follows that E_ℓ is a subgroup of the group of residue classes modulo p^ℓ in $\mathbb{Z}[i]$.

At first let $\ell = 1$. Then the residue classes modulo p^ℓ organizes a field $\mathbb{F}_{p^2}$. Let g_0 be a generative element of multiplicative group of this field. We denote

$$g_0^u = x(u) + iy(u), \tag{2.2}$$

where $x(u), y(u) \in \mathbb{F}_p$ and i is an element of field $\mathbb{F}_{p^2}$ such that $i^2 = -1$. The residue classes $\mathrm{mod}\, p$ for which norms $\equiv \pm 1 \pmod{p}$ be characterized by a condition

$$x^2 + y^2 = \pm 1 \quad (\text{in } \mathbb{F}_p).$$

Now from (2.2) we have

$$g_0^{pu} = x(u) - iy(u).$$

Hence an element g_0^u has a norm $\equiv \pm 1 \pmod{p}$ iff $g_0^{(p+1)u} = \pm 1$, i.e., iff $\frac{p-1}{2} |_u$.

Denote $u = \frac{p-1}{2} t$, $t = 0, 1, \ldots, 2p+1$, and set $g_0^{\frac{p-1}{2}} = g$. The classes g^t, $t = 0, 1, \ldots, 2p+1$, are just those and only those which have a norm $\equiv \pm 1 \pmod{p}$.

Let $f = g + p\lambda$, $\lambda \in \mathbb{Z}[i]$. Then

$$f^p = g^p + p\lambda_1, \quad \lambda_1 \in \mathbb{Z}[i],$$

$$f^{p+1} \equiv g^{p+1} + pg^p\lambda_1 \,(\mathrm{mod}\, p^2),$$
$$f^{2(p+1)} \equiv g^{2(p+1)} + 2pg^{p+1}\lambda_1 \,(\mathrm{mod}\, p^2).$$

Let $g^{2(p+1)} = 1 + pg_1$. We have

$$f^{2(p+1)} - 1 \equiv p(g_1 + 2g^{p+1}\lambda_1) \,(\mathrm{mod}\, p^2).$$

Always we can take λ so

$$f^{2(p+1)} = 1 + ph, \qquad h \in \mathbb{Z}[i], \quad (h, p) = 1.$$

Thus we can account that a generative element g of the group E_ℓ had selected so $g^{2(p+1)} - 1 \not\equiv 0 \,(\mathrm{mod}\, p^2)$. Now we easily get

$$g^{2(p+1)p^{\ell-1}} \equiv 1 \,(\mathrm{mod}\, p^\ell), \qquad g^k \not\equiv 1 \,(\mathrm{mod}\, p^\ell), \quad 0 < k < 2(p+1)p^{\ell-1},$$

for every $\ell = 1, 2, \ldots$. We must show also that for every $\ell = 1, 2, \ldots$ there exists g_ℓ such that $g_\ell \equiv g \,(\mathrm{mod}\, p^\ell)$ and $N(g_\ell) \equiv -1 \,(\mathrm{mod}\, p^\ell)$.

For $\ell = 1$ we proved already.

Let $\ell = 2$. If $g = x + iy$ then

$$x^2 + y^2 = -1 + \lambda p,$$
$$g^{2(p+1)} = 1 + p(h_1 + ih_2), \quad (h_1 + ih_2, p) = 1, \quad h_1, h_2 \in \mathbb{Z}.$$

We have for $k = k_1 + ik_2$, k_1, $k_2 \in \mathbb{Z}$:

$$N(x + iy + p(k_1 + ik_2)) = -1 + \lambda p + p(2xk_1 + 2yk_2) + p^2(k_1^2 + k_2^2) \equiv$$
$$\equiv -1 + p(\lambda + 2xk_1 + 2yk_2) \,(\mathrm{mod}\, p^2),$$
$$(x + iy + p(k_1 + k_2))^{2(p+1)p} \equiv$$
$$\equiv (x + iy)^{2(p+1)p} + 2p^2(x + iy)^{2(p+1)p-1}(k_1 + ik_2) \,(\mathrm{mod}\, p^3).$$

Hence,

$$((x + iy) + p(k_1 + ik_2))^{2(p+1)p}\lambda + 2xk_1 + 2yk_2 \equiv 0 \,(\mathrm{mod}\, p^2),$$

here $h^{(1)}$ and α are the Gaussian integers and co-prome numbers with p.

Next, the congruence $-h^{(1)} \equiv \alpha(k_1 + ik_2) \,(\mathrm{mod}\, p)$ holds only for one assembly of (k_1^0, k_2^0) by modulo p. Therefore, if we take $k_1 \not\equiv k_1^0 \,(\mathrm{mod}\, p)$ and define k_2 from the congruence

$$\lambda + 2xk_1 + 2yk_2 \equiv 0 \,(\mathrm{mod}\, p^2),$$

then we obtain that $f = x + iy + p(k_1 + ik_2)$ has a norm $\equiv -1 \,(\mathrm{mod}\, p^2)$. Moreover, f belongs to an exponent $2(p+1)p$ by modulo p^2 and $f^{2(p+1)p} = 1 + Hp^2$, $(H, p) = 1$, i.e., $f \in E_2$ and f belongs to an exponent $2(p+1)p^{\ell-1}$ by modulo p^ℓ for every $\ell = 2, 3, \ldots$.

Now we note that the $g_3 = f + p^2(m_1 + im_2)$ satisfies by the condition $g_3^{2(p+1)p} = 1 + H_1p^2$, $(H_1, p) = 1$, for any m_1, $m_2 \in \mathbb{Z}$. We take m_1, $m_1 \in \mathbb{Z}$, such that

$$\lambda_2 + 2f_1m_1 + 2f_2m_2 \equiv 0 \,(\mathrm{mod}\, p),$$

where $\lambda = \dfrac{N(f) - (-1)}{p^2} = \dfrac{N(f) + 1}{p^2}$, $f = f_1 + if_2$.

Then $g_3 = f + p^2(m_1 + im_2)$ is a generative element of the group E_3.

Next, by induction. If we defined already $g_{\ell-1}$ then a generative element of E_ℓ will be

$$g_\ell = g_{\ell-1} + p^{\ell-1}(m_1 + im_2),$$

where m_1, m_2 define from a congruence

$$\lambda_{\ell-1} + 2g'_{\ell-1}m_1 + 2g''_{\ell-1}m_2 \equiv 0 \pmod{p}$$

$\Big($here $\lambda_{\ell-1} = \dfrac{N(g_{\ell-1})+1}{p^{\ell-1}}$, $g_{\ell-1} = g'_{\ell-1} + ig''_{\ell-1}$, $g'_{\ell-1}, g''_{\ell-1} \in \mathbb{Z}\Big)$.

The lemma is proved.

Lemma 2.5. *Let p be prime number, $p \equiv 3 \pmod 4$, $\ell \in \mathbb{N}$. Then every residue $x+iy$ a reduced residue system* $\bmod p^\ell$ *of the ring of the Gaussian integers has unique representation in form*

$$x + iy \equiv g^c(u+iv)^d \pmod{p^\ell},$$

$$c = 0, 1, \ldots, (p-1)p^{\ell-1} - 1, \quad d = 0, 1, \ldots, (p+1)p^{\ell-1} - 1, \tag{2.3}$$

where g is a primitive root modulo p^ℓ in $\mathbb{Z}$, $u+iv$ is a generative element of E_ℓ.

Proof. Let $\overline{\varphi}(\alpha)$ denote the Euler function on $\mathbb{Z}[i]$. Then for $p \equiv 3 \pmod 4$ we have

$$\overline{\varphi}(p^\ell) = N(p^\ell)\left(1 - \frac{1}{N(p)}\right) = p^{2(\ell-1)}(p^2-1).$$

In the relation (2.3) we have $p^{2(\ell-1)}(p^2-1)$ the formally distinguishable expressions of form $g^c(u+iv)^d$. As for any c and d we have $(g^c(u+iv)^d, p) = 1$ then for the proof of the assertion of lemma sufficiently to show that the expression (2.3) are pairwise disjoint $\bmod p^\ell$ for different assemblies of (c,d).

Let us assume

$$g^{c_1}(u+iv)^{d_1} \equiv g^{c_2}(u+iv)^{d_2} \pmod{p^\ell}, \quad c_1 \geq c_2.$$

Then we have

$$g^{c_1-c_2} \equiv (u+iv)^{d_2-d_1} \pmod{p^\ell} \quad \text{if} \quad d_2 \geq d_1$$

or

$$g^{c_1-c_2}(u+iv)^{d_1-d_2} \equiv 1 \pmod{p^\ell} \quad \text{if} \quad d_2 < d_1.$$

And now take account that the sets $\{g^\ell\}$ and $\{(u+iv)^d\}$ has only one common element (it is 1) modulo p^ℓ we obtain all once $c_1 = c_2$, $d_1 = d_2$.

The lemma is proved.

Corollary. *All reduced classes $x+iy$ modulo p^ℓ, $p \equiv 3 \pmod 4$ which has equal norms modulo p^ℓ we can write in form*

$$x + iy \equiv g^c(u+iv)^{2d},$$

$$d = 0, 1, \ldots, p^{\ell-1}(p+1) - 1 \quad \textit{if} \quad N(x+iy) \equiv g^{2c} \pmod{p^\ell},$$

$$(x+iy) \equiv g^c(u+iv)^{2d+1},$$

$$d = 0, 1, \ldots, p^{\ell-1}(p+1) - 1 \quad \textit{if} \quad N(x+iy) \equiv -g^{2c} \pmod{p^\ell}$$

$\Big($*here* $0 \leq c \leq \dfrac{p-1}{2}p^{\ell-1} - 1\Big)$.

Let p be a prime number, $p \equiv 1 \pmod 4$. Then in the ring $\mathbb{Z}[i]$ we have $p = \mathfrak{p}\cdot\overline{\mathfrak{p}}$, where $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are the complex-conjugate Gaussian prime numbers ($\overline{\mathfrak{p}} \neq \pm\mathfrak{p}, \quad \pm i\mathfrak{p}$). Well-known that $\{a+bi \,|\, a,\ b = 0, 1, \ldots, p^\ell - 1\}$ is a complete residue system $\bmod p^\ell$. Similarly, for $p = 2$ we have $2 = -i(1+i)^2$ and $\{a+bi \,|\, a, b = 0, 1, \ldots, 2^\ell - 1\}$ is a complete system $\bmod \mathfrak{p}^\ell$, $\mathfrak{p} = 1+i$ in $\mathbb{Z}[i]$.

3. General Kloosterman sum $K(\alpha,\beta;k;\gamma)$. We consider the sum $K(\alpha,\beta;k;\gamma)$ defining in Introduction for the trivial character ψ_0:

$$K(\alpha,\beta;k;\gamma,\psi_0) = K(\alpha,\beta;k;\gamma) = \sum_{(U)} \exp\left(\pi i \,\mathrm{Sp}\frac{\alpha x^k + \beta x'^k}{\gamma}\right), \qquad (3.1)$$

where $U = \big\{(x,x') \in \mathbb{Z}[i]^2 \big| x,\ x' \,(\mathrm{mod}\,\gamma),\ xx' \equiv 1\,(\mathrm{mod}\,\gamma)\big\}$. Obviously, we have

$$K(\alpha,\beta;k;\gamma) = K(\alpha\gamma_2',\beta\gamma_2';k;\gamma_1)K(\alpha\gamma_1',\beta\gamma_1';k;\gamma_2) \quad \text{if} \quad \gamma=\gamma_1\gamma_2,\ (\gamma_1,\gamma_2),$$

where $\gamma_1\gamma_1' \equiv 1\,(\mathrm{mod}\,\gamma_2)$, $\gamma_2\gamma_2' \equiv 1\,(\mathrm{mod}\,\gamma_1)$.

Thus we can therefore assume, without loss of generality, that $\gamma = \mathfrak{p}^n$, $\mathfrak{p}$ is a Gaussian prime number.

In part 1 we had obtained a description of a reduced residue system $\mathrm{mod}\,\mathfrak{p}^n$, $\mathfrak{p} = p \equiv \equiv 3\,(\mathrm{mod}\,4)$. For $\mathfrak{p} \in \mathbb{Z}[i]$, $N(\mathfrak{p}) = p \equiv 1\,(\mathrm{mod}\,4)$, a reduced residue system $\mathrm{mod}\,\mathfrak{p}^n$ has a form

$$\big\{a \in \mathbb{Z}\big| 1 \geq a \geq p^n - 1,\ (a,p) = 1\big\},$$

and for Gaussian prime "even" number $\mathfrak{p} = 1+i$

$$\Big\{a + bi \big| a,b \in \{0,1,\ldots,2^n-1\},\ a \equiv 1\,(\mathrm{mod}\,2),\ b \equiv 0\,(\mathrm{mod}\,2)\Big\}.$$

Theorem 3.1. *Let $\mathfrak{p}$ be Gaussian prime number, $N(\mathfrak{p}) = p \equiv 1\,(\mathrm{mod}\,4)$ and let $d = (k, p-1)$. Then*

$$\big|K(\alpha,\beta;k;\mathfrak{p})\big| \leq 2dN((\alpha,\beta,\mathfrak{p}))^{\frac12} N(\mathfrak{p})^{\frac12}. \qquad (3.2)$$

Proof. If $(\alpha,\beta,\mathfrak{p}) = \mathfrak{p}$ then our assertion is clear. Let $(\alpha,\beta,\mathfrak{p}) = 1$. By a description of a reduced residue system $\mathrm{mod}\,\mathfrak{p}^n$ we can suppose that $\alpha = a$, $\beta = b$, $a,\ b \in \mathbb{Z}$, $\mathfrak{p} = c_1 + ic_2$, $c_1,\ c_2 \in \mathbb{Z}$, $(c_1,p) = (c_2,p) = 1$.

Thus we have

$$K(\alpha,\beta;k;\mathfrak{p}) = \sum_{u \in R^*(p)} e_p\left(\frac12 \mathrm{Sp}\Big(a(c_1 - ic_2)u^k + b(c_1 - ic_2)u'^k\Big)\right) =$$

$$= \sum_{u \in R^*(p)} e_p\big(ac_1u^k + bc_1u'^k\big).$$

The last sum was estimated in [10] but we shall give a calculation in order to make more pricise an estimation.

We define

$$\mathfrak{I}_k(a) := \#\big\{x \in \mathbb{Z}\big| 0 \geq x \geq p-1,\ x^k \equiv a\,(\mathrm{mod}\,p)\big\}.$$

It is clear that

$$\mathfrak{I}_k(a) = \begin{cases} d & \text{if} \quad d \big| \mathrm{ind}\,a \\ 0 & \text{otherwise} \end{cases} = \sum_{t=0}^{d-1} e^{2\pi i}\frac{t\,\mathrm{ind}\,a}{d}.$$

(Here $\mathrm{ind}\,a$ denote an index of integer a, $(a,p) = 1$, by a radix of some primitive root modulo p.)

Then we obtain

$$|K(\alpha,\beta;k;\mathfrak{p})| = \left|\sum_{u\in R^*(p)} \Im_k(u)e_p(au+bu')\right| \le$$

$$\le \sum_{t=0}^{d-1}\left|\sum_{u\in R^*(p)} e_d(t\,\mathrm{ind}\,u)e_p(au+bu')\right| \le 2dp^{\frac12}. \tag{3.3}$$

Here we take into account that an inner sum is classical Kloosterman sum weighting by a character and hence estimates as $2p^{\frac12}$ (see Perel'muter [17], Williams [18]).

The theorem is proved.

Theorem 3.2. *Let* $p\equiv 3\,(\mathrm{mod}\,4)$, $k\in\mathbb{N}$, $d=(k,p^2-1)$. *Then*

$$\big|K(\alpha,\beta;k;p)\big| \le 2d\,N\big((\alpha,\beta,p)\big)^{\frac12}\,N(p)^{\frac12}. \tag{3.4}$$

Proof. The residue classes $\mathrm{mod}\,p$ in the ring $\mathbb{Z}[i]$ organizes a field $\mathbb{F}_{p^2}$. Hence, $\sigma_2(x)=x+x^p$. But we observed that $\overline{x}\equiv x^p\,(\mathrm{mod}\,p)$ for $x\in\mathbb{Z}[i]$. Thus

$$\mathrm{Sp}(x)=x+\overline{x}\equiv x+x^p\equiv\sigma_2(x)\,(\mathrm{mod}\,p).$$

Hence,

$$K(\alpha,\beta;k;p)=\sum_{x\in R^*(p)} e_p\left(\frac12\,\mathrm{Sp}(\alpha x^k+\beta\overline{x}^k)\right)=\sum_{x\in\mathbb{F}^*_{p^2}} e_p\left(\sigma_2\big(2'\alpha x^k+2'\beta x'^k\big)\right),$$

where $2\cdot 2'\equiv 1\,(\mathrm{mod}\,p)$.

Let g denote a primitive element of the field $\mathbb{F}_{p^2}$, $\mathrm{ind}_g\,x=\mathrm{ind}\,x$ for $x\in\mathbb{F}_{p^2}$ and let $\Im(u)$ is a number solutions of equation $x^k=u$ in $\mathbb{F}_{p^2}$. It follows that

$$|K(\alpha,\beta;k;p)| = \left|\sum_{t=0}^{d-1}\sum_{x\in\mathbb{F}^*_{p^2}} e^{2\pi i\frac{t\,\mathrm{ind}\,x}{d}}\,e_p\big(\sigma_2(2'\alpha x+2'\beta x')\big)\right| \le$$

$$\le \left|\sum_{x\in\mathbb{F}^*_{p^2}} e_p\big(\sigma_2(2'\alpha x+2'\beta x')\big)\right| + \left|\sum_{t=1}^{d-1}\sum_{x\in\mathbb{F}^*_{p^2}} \psi_t(x)e_p\big(\sigma_2(2'\alpha x+2'\beta x')\big)\right|,$$

where $\psi_t(x)=e_d(t\,\mathrm{ind}\,x)$ is a multiplicative character of the field $\mathbb{F}_{p^2}$.

Again using the estimations of the Kloosterman sums with a character of a finite field we obtain finally

$$\big|K(\alpha,\beta;k;p)\big| \le 2dN\big((\alpha,\beta,p)\big)^{\frac12}N(p)^{\frac12}.$$

The theorem is proved.

For $\mathfrak{p}=1+i$ we have trivially $\big|K(\alpha,\beta;k;p)\big|=1$.

Now for $\gamma=\mathfrak{p}^n$ we make a substitute $x\,(\mathrm{mod}\,\mathfrak{p}^n)=y+\mathfrak{p}^n z$, where $y\,(\mathrm{mod}\,\mathfrak{p}^n)$, $z\,(\mathrm{mod}\,\mathfrak{p}^{n-m})$, $m=\left[\dfrac{n+1}{2}\right]$, and then using the standard technique, we easily obtain the following theorem.

Theorem 3.3. *Let* $\gamma=(1+i)^{n_0}\prod_{\substack{i=1\\ N(\mathfrak{p}_i)\equiv 1(4)}}^{s}\mathfrak{p}_i^{n_i}\prod_{\substack{j=1\\ p_j\equiv 3(4)}}^{t}p_j^{n_j}$. *Then*

$$\big|K(\alpha,\beta;k;\gamma)\big| \le 2D\sqrt{N((\alpha,\beta,\gamma))}N(\gamma)^{\frac12}, \tag{3.5}$$

where $D=\prod_{i=1}^{s}(k,p_j-1)\prod_{j=1}^{t}(k,p_j^2-1)$.

Now we consider a nontrivial multiplicative character ψ of the field $\mathbb{F}_q$, $q = p^r$, $r \in \mathbb{N}$, p be a prime number, α, $\beta \in \mathbb{F}_q$ and $\alpha \neq 0$ or $\beta \neq 0$. We define the general power Kloosterman sum with a character ψ

$$K(\alpha, \beta; k; q, \psi) := \sum_{x \in \mathbb{F}_q^*} \psi(x) e_p\big(\sigma_2(\alpha x^k + \beta {x'}^k)\big). \tag{3.6}$$

Let $d = (k, q-1)$, $\psi(x) = e^{2\pi i \frac{h \operatorname{ind} x}{q-1}}$, where $\operatorname{ind} x$ take in regard to a some primitive element for $\mathbb{F}_q$. We have two probable cases: $d \not| h$ and $d \big| h$.

We shall prove that $K(\alpha, \beta; k; q, \psi) = 0$ in first case. We have for $\beta \neq 0$:

$$\sum_{\alpha \in \mathbb{F}_q} \big|K(\alpha, \beta; k; q, \psi)\big|^2 =$$

$$= \sum_{\alpha \in \mathbb{F}_q} \sum_{\substack{x, y \in \mathbb{F}_q^* \\ xx' = yy' = 1}} \psi(x)\psi(y') e_p\Big(\sigma_2(\alpha(x^k - y^k) + \beta({x'}^k - {y'}^k))\Big) =$$

$$= \sum_{x \in \mathbb{F}_q^*} \psi(x) \sum_{y \in \mathbb{F}_q^*} e_p\Big(\sigma_2(\beta {y'}^k (x^k - 1))\Big) \sum_{\alpha \in \mathbb{F}_q} e_p\Big(\sigma_2(\alpha y^k (x^k - 1))\Big) =$$

$$= q \sum_{y \in \mathbb{F}_q^*} \sum_{\substack{x \in \mathbb{F}_q^* \\ x^k = 1}} \psi(x) e_p\Big(\sigma_2(\beta {y'}^k (x^k - 1))\Big) = q(q-1) \sum_{\substack{x \in \mathbb{F}_q^* \\ x^k = 1}} \psi(x). \tag{3.7}$$

In the last sum the summation runs over $x \in \mathbb{F}_q^*$ for which $k \operatorname{ind} x \equiv 0 \,(\operatorname{mod}\,(q-1))$, i.e., $\operatorname{ind} x = \dfrac{q-1}{d} s$, $s = 0, 1, \ldots, d-1$, and thus

$$\sum_{\alpha} \big|K(\alpha, \beta; k; q, \psi)\big|^2 = q(q-1) \sum_{s=0}^{d-1} e^{2\pi i \frac{hs}{d}} = 0 \quad \text{if} \quad h \not\equiv 0 \,(\operatorname{mod} d).$$

If $d \big| h$ we have $\psi(x) = e_{q-1}(h_1 d \operatorname{ind} x) = e_{q-1}(h_1 \operatorname{ind} x^d)$. Hence, setting $k_1 = \dfrac{k}{d}$, $h_1 = \dfrac{h}{d}$, $\psi_1^d = \psi$, we obtain

$$K(\alpha, \beta; k; q, \psi) = \sum_{x \in \mathbb{F}_q^*} \psi_1(x^d) e_p\Big(\sigma_2(\alpha (x^d)^{k_1} + \beta ({x'}^d)^{k_1})\Big) =$$

$$= \sum_{x \in \mathbb{F}_q^*} \Im_d(x) \psi_1(x) e_p\Big(\sigma_2(\alpha x^{k_1} + \beta {x'}^{k_1})\Big) =$$

$$= \sum_{s=0}^{d-1} \sum_{x \in \mathbb{F}_q^*} e_d(s \operatorname{ind} x) e_{q-1}(h_1 \operatorname{ind} x) e_p\big(\sigma_2(\alpha x^{k_1} + \beta {x'}^{k_1})\big) =$$

$$= \sum_{s=0}^{d-1} \sum_{x \in \mathbb{F}_q^*} \psi_2(x) e_p\big(\sigma_2(\alpha x^{k_1} + \beta {x'}^{k_1})\big), \tag{3.8}$$

where $\psi_2(x) = e_{q-1}(h_2 \operatorname{ind} x)$, $h_2 = \dfrac{s(q-1) + h}{d}$.

So then we diminished the exponent k in d-time if $d > 1$. But if $d = 1$ then clearly that

$$K_k(\alpha,\beta;q) = \sum_{x\in\mathbb{F}_q^*} e_{q-1}\big(hk' \operatorname{ind} x^k\big) e_p\big(\sigma_2(\alpha x^{k_1} + \beta {x'}^{k_1})\big) =$$

$$= \sum_{x\in\mathbb{F}_q^*} e_{q-1}(hk' \operatorname{ind} x) e_p\big(\sigma_2(\alpha x + \beta x')\big) = K_1(\alpha,\beta;q;\psi_3),$$

where $kk' \equiv 1 \,(\operatorname{mod}(q-1))$, $\psi_3 = \psi^{k'}$.

The sum $K_1(\alpha,\beta;q,\psi_3)$ is the Kloosterman sum over $\mathbb{F}_q$ weighting by a multiplicative character ψ_3 of the field $\mathbb{F}_q$ and has a estimation as $2q^{\frac{1}{2}}$ if $\beta \neq 0$ (see Perel'muter [17]). The relation (3.8) show that if $(k_1, q-1) = 1$ then

$$\big|K_k(\alpha,\beta;q,\psi)\big| \le 2dq^{\frac{1}{2}}.$$

If $(k_1, q-1) = d_1 > 1$ we again consider two cases

$$(h_1, d_1) = d_1 \quad \text{or} \quad (h_2, d_1) < d_1.$$

But if $(h_2, d_1) < d_1$ we have $K(\alpha,\beta;k;q,\psi) = 0$.

The case $h_2 \vdots d_1$ can execute only for those s, $0 \le s \le d-1$, for which $h_2 \equiv \equiv 0 \,(\operatorname{mod} d_1)$, i.e., s must satisfy the congruence

$$s\frac{q-1}{d} + \frac{h}{d} \equiv 0 \,(\operatorname{mod} d_1).$$

But $\left(d_1, \dfrac{q-1}{d}\right) = 1$ since $d_1 \big| k_1$ and $\left(k_1, \dfrac{q-1}{d}\right) = 1$.

It follows that we have only one value s modulo d_1, and hence, at most $\left[\dfrac{d}{d_1}\right] + 1$ the value of s among $0 \le s \le d-1$, for which $h_2 \vdots d_1$. We apply this reduction and through $\nu(k)$ steps we obtain the estimation

$$\big|K_k(\alpha,\beta;q,\psi)\big| \le 2^{\nu(k)+1} k q^{\frac{1}{2}},$$

where $\nu(k)$ denote the number a prime divisors of k.

And so we proved the following theorem.

Theorem 3.4. *Let α, $\beta \in \mathbb{F}_q$ and though one of element α or β is not equal to zero. Then for any multiplicative character ψ of field $\mathbb{F}_q$ the estimation*

$$\big|K_\psi(\alpha,\beta;q;k)\big| \le 2kq^{\frac{1}{2}}$$

holds.

Corollary. *Let $\mathfrak{p}$ be a Gaussian prime number and let χ is a multiplicative character of a field of the residue classes* $\operatorname{mod}\mathfrak{p}$. *Then*

$$\left|\sum_{x\,(\operatorname{mod}\mathfrak{p})}{}' \chi(x) \exp \pi i \operatorname{Sp}\left(\frac{\alpha x^k + \beta {x'}^k}{\mathfrak{p}}\right)\right| \le 2^{\nu(k)+1} k N(\mathfrak{p})^{\frac{1}{2}} N((\alpha,\beta,\mathfrak{p}))^{\frac{1}{2}}.$$

4. General Kloosterman sums over norm. Let α, $\beta \in \mathbb{Z}[i]$, $h \in \mathbb{Z}$, $q \in \mathbb{N}$, $q > 1$, $(h,q) = 1$. We set

$$\widetilde{K}(\alpha,\beta;h,q) := \sum_{\substack{x,y\,(\operatorname{mod} q)\\ N(xy)\equiv h\,(\operatorname{mod} q)}} e_q\left(\frac{1}{2}\operatorname{Sp}(\alpha x + \beta y)\right) \tag{4.1}$$

and call the norm Kloosterman sum in $\mathbb{Z}[i]$.

For $q = q_1q_2$, $(q_1, q_2) = 1$ we have

$$\widetilde{K}(\alpha, \beta; h, q) = \widetilde{K}(\alpha, \beta; hq''_2, q_1)\widetilde{K}(\alpha, \beta; hq''_1, q_2) =$$
$$= \widetilde{K}(\alpha q_2, \beta q_2; h, q_1)\widetilde{K}(\alpha q_1, \beta q_1; h, q_2).$$

Thus we shall consider only case $q = p^n$, p is prime rational number, $n \in \mathbb{N}$. We denote $m_\alpha = \max_{m \geq n} \{\alpha \equiv 0 \,(\mathrm{mod}\, p^m)\}$.

Theorem 4.1. *Let* $(h, p) = 1$. *Then*

$$\widetilde{K}(\alpha, \beta; h, p^n) \ll (p^{m_\alpha}, p^{m_\beta}, p^n)^{\frac{1}{2}} p^{\frac{3n}{2}} \tag{4.2}$$

with an absolute constant in symbol “$\ll$”.

Proof. At first let $n = 1$. The case $m_\alpha = m_\beta = 1$ is a trivial. Thus we shall suppose that $m_\alpha = 0$ or $m_\beta = 0$. We set $\alpha = a_1 + ia_2$, $\beta = b_1 + ib_2$ and, hence, $(a_1, a_2, b_1, b_2) = 1$.

For $p \equiv 1 \,(\mathrm{mod}\, 4)$ we have

$$\widetilde{K}(\alpha, \beta; h, p) = \sum_{(U)} e_p(a_1x_1 - a_2x_2 + b_1y_1 - b_2y_2), \tag{4.3}$$

where $U = \big\{x_1, x_2, y_1, y_2 \in \{0, 1, \ldots, p-1\},\ (x_1^2 + x_2^2)(y_1^2 + y_2^2) \equiv h \,(\mathrm{mod}\, p)\big\}$. Let ε_0 is a solution of congruence $x^2 \equiv -1 \,(\mathrm{mod}\, p)$.

We set

$$u_1 = x_1 + \varepsilon_0 x_2, \qquad u_2 = x_1 - \varepsilon_0 x_2, \qquad v_1 = y_1 + \varepsilon_0 y_2, \qquad v_2 = y_1 - \varepsilon_0 y_2.$$

Now by (4.3) we obtain

$$\widetilde{K}(\alpha, \beta; h, p) = \sum_{(U)} e_p(A_1u_1 + A_2u_2 + B_1v_1 + B_2v_2),$$

where $U = \big\{u_1, u_2, v_1, v_2 \in \{0, 1, \ldots, p-1\},\ u_1u_2v_1v_2 \equiv h \,(\mathrm{mod}\, p)\big\}$.

E. Bombieri [14] proved that the last sum can be estimated as $\ll p^{\frac{3}{2}}$. If $p \equiv 3 \,(\mathrm{mod}\, 4)$ then the such estimation holds for the sum (4.3) (the proof is analogous).

The case $p = 2$ is a trivial.

Now, let $n \geq 2$. It is enough to consider only the case $(p^{m_\alpha}, p^{m_\beta}, p^n) = 1$. In this case though one of number a_1, a_2, b_1, b_2 does not divide on p (here $\alpha = a_1 + ia_2$, $\beta = b_1 + ib_2$). We have

$$\widetilde{K}(\alpha, \beta; h, p^n) =$$
$$= \sum_{x, y \,(\mathrm{mod}\, p^n)} \frac{1}{p^n} \sum_{k=0}^{p^n-1} e_{p^n}\Big(k(N(x)N(y) - h) + \Re(\alpha x) + \Re(\beta y)\Big) =$$
$$= \frac{1}{p^n} \sum_{U} e_{p^n}\Big(k((x_1^2 + x_2^2)(y_1^2 + y_2^2) - h) + a_1x_1 - a_2x_2 + b_1y_1 - b_2y_2\Big), \tag{4.4}$$

where $U := \big\{k \,(\mathrm{mod}\, p^n);\ x_1, x_2 \,(\mathrm{mod}\, p^n);\ y_1, y_2 \,(\mathrm{mod}\, p^n)\big\}$.

Though one out of sums over x_1, x_2, y_1, y_2 is equal 0 if $(k, p) = p$ (by a rational analogue of Lemma 2.1).

Thus, supposing $(a_1, a_2, p) = 1$, we have

$$\widetilde{K}(\alpha,\beta;h,p^n)=$$
$$=\frac{1}{p^n}\sum_U e_p^n(-kh)e_{p^n}\Big(kN(x)(y_1^2+y_2^2)+\Re(\alpha x)+b_1y_1-b_2y_2\Big)=$$
$$=\frac{1}{p^n}\sum_{k\,(\mathrm{mod}\,p^n)}{}^{*}\; e_{p^n}(-kh)\left(\sum_{\substack{x\,(\mathrm{mod}\,p^n)\\(N(x),p)=1}}+\sum_{\substack{x\,(\mathrm{mod}\,p^n)\\N(x)\vdots p}}\right)=\sum_1+\sum_2, \tag{4.5}$$

say, where $U:=\big\{k\in R^*(p^n),\ x\in R(p^n,i),\ y_1,\ y_2\in R(p^n)\big\}$. Let $N(x)'$ and k' are the solutions of the congruences

$$N(x)u\equiv 1\,(\mathrm{mod}\,p^n),\qquad ku\equiv 1\,(\mathrm{mod}\,p^n),$$

accordingly. Then

$$\Big|\sum\nolimits_1\Big|=\left|\sum_{k\,(\mathrm{mod}\,p^n)}{}^{*}\; e_{p^n}(-kh)\sum_{x\,(\mathrm{mod}\,p^n)} e_{p^n}\Big(4'N(x)'k'(b_1^2+b_2^2)+a_1x_1-a_2x_2\Big)\right|. \tag{4.6}$$

We set

$$x_1=x_1^0+p^mz_1,\qquad x_2=x_2^0+p^mz_2,$$
$$0\le x_1^0,x_2^0\le p^m-1,\quad 0\le z_1,z_2\le p^{n-m}-1,\quad m=\left[\frac{n+1}{2}\right].$$

It is obvious

$$N(x)'=\big({x_1^0}^2+{x_2^0}^2\big)'\Big(1-2p^m({x_1^0}^2+{x_2^0}^2)'(x_1^0z_2+x_2^0z_1)\Big)$$

and consequently

$$\Big|\sum\nolimits_1\Big|=\Bigg|\sum_{k\,(\mathrm{mod}\,p^n)}{}^{*}\; e_{p^n}(-kh)\,\times$$
$$\times\sum_{\substack{x_1^0,x_2^0\,(\mathrm{mod}\,p^n)\\({x_1^0}^2+{x_2^0}^2,\,p)=1}} e_{p^n}\Big(4'k'({x_1^0}^2+{x_2^0}^2)'(b_1^2+b_2^2)+a_1x_1^0-a_2x_2^0\Big)\times$$
$$\times\sum_{z_1,z_2\,(\mathrm{mod}\,p^{n-m})} e_{p^{n-m}}\big((A_1+a_1)z_1+(A_2+a_2)z_2\big)\Bigg|,$$

where $A_1=2\big(({x_1^0}^2+{x_2^0}^2)'\big)^2x_2^0$, $A_2=2\big(({x_1^0}^2+{x_2^0}^2)'\big)^2x_1^0$.

The summation over z_1, z_2 gives zero if the congruences

$$A_1+a_1\equiv 0\,(\mathrm{mod}\,p^{n-m}),\qquad A_2-a_2\equiv 0\,(\mathrm{mod}\,p^{n-m})$$

or the equivalent congruences

$$a_2x_1^0+a_1x_2^0\equiv 0\,(\mathrm{mod}\,p^{n-m}),\qquad 2x_2^0\equiv -a_1({x_1^0}^2+{x_2^0}^2)^2\,(\mathrm{mod}\,p^{n-m})$$

are disturbs.

This system of the congruences has at most three solutions modulo p^{n-m}, and therefore at most $3p^{m-(n-m)}$ solutions modulo p^m.

Hence,

$$\left|\sum\nolimits_1\right| = \left|p^{2(n-m)} \sum_{(U)} e_{p^n}(a_1x_1^0 - a_2x_1^0) \sum\nolimits^*_{k\,(\mathrm{mod}\,p^n)} (kh + k'B)\right| \le 8p^{\frac{3}{2}n}, \qquad (4.7)$$

where

$$U = \Big\{x_1^0, x_2^0\,(\mathrm{mod}\,p^m)\Big| a_2x_1^0 \equiv -a_1x_2^0\,(\mathrm{mod}\,p^{n-m}),$$

$$2x_1^0 \equiv -a_1\Big({x_1^0}^2 + {x_2^0}^2\Big)^2\,(\mathrm{mod}\,p^{n-m})\Big\}.$$

At last, if $N(x) \equiv 0\,(\mathrm{mod}\,p)$ then $\sum\nolimits_2 = 0$ by Lemma 2.1.

The theorem is proved.

For natural $k > 1$ we set

$$\widetilde{K}(\alpha, \beta; h, q; k) := \sum_{\substack{x,y\,(\mathrm{mod}\,q)\\ N(xy)\equiv h\,(\mathrm{mod}\,q)}} e_q\left(\frac{1}{2}\,\mathrm{Sp}(\alpha x^k + \beta y^k)\right). \qquad (4.8)$$

It is obvious that $\widetilde{K}(\alpha, \beta; h, q; 1) = \widetilde{K}(\alpha, \beta; h, q)$.

The method of investigation of the sum $\widetilde{K}(\alpha, \beta; h, q; k)$ towards suffices to consider the case $q = p^n$, p be a prime. At first we shall account that $p \equiv 3\,(\mathrm{mod}\,4)$.

Theorem 4.2. *Let* $p \equiv 3\,(\mathrm{mod}\,4)$, $h \in \mathbb{Z}$, $(h, p) = 1$, $k \in \mathbb{N}$, $d = (k, p-1)$. *Then for any Gaussian integers* α, β, $(\alpha, \beta, p) = 1$ *the estimation*

$$\left|\widetilde{K}(\alpha, \beta; h, p; k)\right| \ll \begin{cases} d^2p^{\frac{3}{2}} & \text{if} \quad d - 1 \le \sqrt[4]{p}, \\ dp^2 & \text{if} \quad d \ge \sqrt[4]{p} + 1 \end{cases}$$

holds.

Proof. Let $k = dk_1$, $\left(k_1, \dfrac{p-1}{d}\right) = 1$. We have

$$\sum_{\substack{x,y\,(\mathrm{mod}\,p)\\ N(xy)\equiv h\,(\mathrm{mod}\,p)}} e_p\left(\frac{1}{2}\,\mathrm{Sp}(\alpha(x^{k_1})^d + \beta(y^{k_1})^d)\right) =$$

$$= \sum_{\substack{x,y\,(\mathrm{mod}\,p)\\ N(x^{k_1}y^{k_1})\equiv h^{k_1}\,(\mathrm{mod}\,p)}} e_p\left(\frac{1}{2}\,\mathrm{Sp}(\alpha(x^{k_1})^d + \beta(y^{k_1})^d)\right) =$$

$$= \sum_{\substack{x,y\,(\mathrm{mod}\,p)\\ N(xy)\equiv h^{k_1}\,(\mathrm{mod}\,p)}} e_p\left(\frac{1}{2}\,\mathrm{Sp}(\alpha x^d + \beta y^d)\right) = \widetilde{K}(\alpha, \beta; h^{k_1}, p; d).$$

Now, for any multiplicative character χ of field $\mathbb{F}_{p^2}$ we have

$$\sum_{h\in\mathbb{F}^*_{p^2}} \chi(h)\widetilde{K}(\alpha, \beta; h, p; d) =$$

$$= \sum_{x,y\in\mathbb{F}^*_{p^2}} \chi\big(N(x)N(y)\big)e_p\left(\frac{1}{2}\,\mathrm{Sp}(\alpha x^d)\right)e_p\left(\frac{1}{2}\,\mathrm{Sp}(\beta y^d)\right) =$$

$$= \left(\sum_{x\in\mathbb{F}^*_{p^2}} \chi\left(N(x)e_p\left(\frac{1}{2}\,\mathrm{Sp}(\alpha x^d)\right)\right)\right)\left(\sum_{y\in\mathbb{F}^*_{p^2}} \chi\big(N(y)\big)e_p\left(\frac{1}{2}\,\mathrm{Sp}(\beta y^d)\right)\right), \qquad (4.9)$$

and moreover the sums on the right of (4.9) can be estimate as $(d-1)N(p)^{\frac{1}{2}}$ (see [17]). Thus we obtain

$$\left|\sum_{h\in\mathbb{F}^*_{p^2}} \chi(h)\widetilde{K}(\alpha,\beta;h,p;d)\right| \le (d-1)^2p^2.$$

The application of the Plansherel theorem give

$$\sum_{h\in\mathbb{F}^*_{p^2}} |K(\alpha,\beta;h,p;d)|^2 \le (d-1)^4p^4.$$

Now similarly as in the Bombieri work [14] we conclude that the weights of characteristic roots associating with $\widetilde{K}(\alpha,\beta;h,p;d)$ are at most 3 if $(d-1)^4 < p$. Hence, using the results of Bombieri [14] and Deligne [13] we infer

$$\widetilde{K}(\alpha,\beta;h,p;d) \ll (d-1)^2p^2 \ll d^2p^2 \quad \text{if} \quad d-1 < \sqrt[4]{p}.$$

Further, for $x = x_1 + ix_2$, $x_1, x_2 \in \mathbb{Z}$, we have $x_1 - ix_2 \equiv (x_1+ix_2)^p \pmod p$ and thus $N(x) \equiv x^{p+1} \pmod p$. Hence,

$$\sum_{\substack{x,y \pmod p \\ N(xy)\equiv h \pmod p}} e_p\left(\frac{1}{2}\operatorname{Sp}(\alpha x^d + \beta y^d)\right) =$$

$$= \sum_{\substack{x,y \pmod p \\ (xy)^{p+1}\equiv h \pmod p}} e_p\left(\frac{1}{2}\operatorname{Sp}(\alpha x^d + \beta y^d)\right) =$$

$$= \sum_{\substack{\varepsilon \pmod p \\ \varepsilon^{p+1}\equiv h \pmod p}} \sum_{x \pmod p} e_p\left(\frac{1}{2}\operatorname{Sp}(\alpha x^d + \beta y^d)\right). \tag{4.10}$$

The congruence $z^{p+1} \equiv h \pmod p$ has exactly $p+1$ solutions $\bmod p$. The inner sum in the right in (4.10) estimates as $\le 2dp$. This completes the proof of the theorem.

Now, let $q = p^n$, $p \equiv 3 \pmod 4$, $n \ge 2$. We shall use the description of a reduced residue system $\bmod p^n$ (see Lemma 2.5).

In farther the following assertion are need.

Lemma 4.1. *Let n, $k \in \mathbb{N}$, $p \ge 3$ be a prime, $u \in \mathbb{Z}$, $(p,u) = 1$. Then for any natural t we have*

$$(1+p^ku)^t \equiv 1 + p^ka_1t + p^{2k}a_2t^2 + p^{\lambda_3}a_3t^3 + \ldots + p^{\lambda_n}a_nt^n \pmod{p^n},$$

moreover $(a_i,p) = 1$, $i = 1,\ldots,n$, $\lambda_j > 2k$, $j = 3,\ldots,n$.

Proof. By the relation

$$\binom{t}{m} = \frac{1}{m!}\left(t^m - \frac{m(m-1)}{2}t^{m-1} + \ldots + (-1)^{m-1}(m-1)!\cdot t\right)$$

and upper estimation of an exponent with which p enters in $m!$ we obtain

$$(1+p^ku)^t \equiv 1 + p^ka_1t + p^{2k}a_2t^2 + p^{\lambda_3}a_3t^3 + \ldots + p^{\lambda_n}a_nt^n \pmod{p^n},$$

where $(a_i,p) = 1$, $i = 1,\ldots,n$, $\lambda_j > \left(k - \dfrac{1}{p-1}\right)j > 2k$ for $j = 3,4,\ldots.$

The lemma is proved.

From the proof of Lemma 2.3 it is obvious that a generative element $u+iv$ of the group E_1 can be take that it is a generative element of the group E_ℓ for any fixed ℓ, $\ell=2,3,\ldots$. Let $\ell=\max(5,n)$. We have

$$N((u+iv))^2 \equiv 1 \,(\mathrm{mod}\, p^\ell),$$
$$(u+iv)^{2(p+1)} = 1+p(x_0+iy_0), \quad (x_0+iy_0,p)=1.$$

Thus

$$N(1+px_0+ipy_0) \equiv 1+2px_0+p^2x_0^2+p^2y_0^2 \equiv 1 \,(\mathrm{mod}\, p^\ell).$$

Hence, $2px_0 \equiv 0 \,(\mathrm{mod}\, p^2)$, $x_0 = px_0'$, $(y_0,p)=1$. So,

$$(u+iv)^{2(p+1)} \equiv 1+p^2x_0+ipy_0, \quad (x_0,p)=(y_0,p)=1.$$

Now, applying the previous lemma we easy obtain

$$\begin{aligned}\Re((u+iv)^{2(p+1)t}) &\equiv A_0+A_1t+A_2t^2+\ldots+A_{n-1}t^{n-1} \,(\mathrm{mod}\, p^n),\\ \Im((u+iv)^{2(p+1)t}) &\equiv B_0+B_1t+B_2t^2+\ldots+B_{n-1}t^{n-1} \,(\mathrm{mod}\, p^n),\end{aligned} \tag{4.11}$$

where

$$A_0 \equiv 1 \,(\mathrm{mod}\, p), \qquad B_0 \equiv 0 \,(\mathrm{mod}\, p),$$
$$A_1 \equiv p^2x_0 + 2'y_0^2p^2 \,(\mathrm{mod}\, p^3), \quad \text{i.e.,} \quad A_1 \equiv 0 \,(\mathrm{mod}\, p^3),$$
$$A_2 \equiv -2'y_0^2p^2 \,(\mathrm{mod}\, p^3), \quad \text{i.e.,} \quad A_2 = p^2A_2', \quad (A_2',p)=1,$$
$$B_1 \equiv py_0 \,(\mathrm{mod}\, p^3), \quad \text{i.e.,} \quad B_1 \equiv pB_1', \quad (B_1',p)=1,$$
$$B_2 \equiv A_3 \equiv B_3 \equiv \ldots \equiv A_{n-1} \equiv B_{n-1} \equiv 0 \,(\mathrm{mod}\, p^3).$$

We set

$$\beta = 2(p+1)t+z, \quad 0 \le t \le p^{n-1}-1, \quad 0 \le z \le 2p+1,$$

and denote

$$(u+iv)^z = u(z)+iv(z), \quad z=0,1,\ldots,2p+1.$$

Then

$$(u+iv)^\beta = (u+iv)^{2(p+1)t}(u(z)+iv(z)).$$

And hence, we have

$$\Re\big\{(u+iv)^{2(p+1)t+z}\big\} \equiv A_0(z)+A_1(z)t+\ldots+A_{n-1}(z)t^{n-1} \ (\mathrm{mod}\, p^n), \tag{4.12}$$

where $A_i(z) = A_iu(z) - B_iv(z)$.

We clear up for which values z the congruence $v(z) \equiv 0 \,(\mathrm{mod}\, p)$ holds.

Let $v(z) = pv_0(z)$, $v_0(z) \equiv 0 \,(\mathrm{mod}\, p^k)$, $k \ge 0$. Then

$$(u+iv)^z = u(z)+ipv_0(z),$$
$$(u+iv)^{z(p-1)p^{n-k}} \equiv (u(z))^{(p-1)p^{n-k}} \ (\mathrm{mod}\, p^n).$$

The sequences $\big\{(u+iv)^{2\beta}\big\}$ and $\{g^\alpha\}$ can have only two common elements modulo p: 1 or -1. Thus

$$(u(z))^{(p-1)p^{n-k}} \equiv \pm 1 \ (\mathrm{mod}\, p^n).$$

The congruence $(u(z))^{(p-1)p^{n-k}} \equiv -1 \,(\mathrm{mod}\, p^n)$ is impossible, so the other way we have $(-1)^{p^{k-1}} \equiv (u(z))^{(p+1)p^{n-1}} \equiv 1 \,(\mathrm{mod}\, p^n)$, i.e., $-1 \equiv 1 \,(\mathrm{mod}\, p)$. Hence

$$(u(z))^{(p-1)p^{n-k}} \equiv 1 \pmod{p^n},$$
$$z(p-1)p^{n-k} \equiv 0 \left(\operatorname{mod} 2(p+1)p^{n-1}\right).$$

Since, $(p-1, p+1) = 2$, then $z \equiv 0 \left(\operatorname{mod}(p+1)p^{k-1}\right)$. Whence it follows that from $p \| v(z)$ we have $z = p+1$ and from $p^2 | v(z)$ follows $z = 0$. So we have

$$p \| A_1(z), \quad A_i(z) \equiv 0 \pmod{p^2}, \quad i = 2, \ldots, n-1, \quad \text{if} \quad z \neq 0, z \neq p+1,$$
$$A_1(0) = A_1(p+1) \equiv 0 \pmod{p^2}, \quad p^2 \| A_2(0), \quad p^2 \| A_2(p+1),$$
$$A_j(0) \equiv A_j(p+1) \equiv 0 \pmod{p^3}, \quad j = 3, 4, \ldots, n-1.$$

We are now in position to prove the following assertion.

Theorem 4.3. *Let p be a prime number,* $p \equiv 3 \pmod 4$, $h \in \mathbb{Z}$, $(h,p) = 1$, $k > 1$ *is a natural,* a, b *are the Gaussian integer,* $(a,p) = (b,p) = 1$. *Then for* $n \geq 2$

$$\left| \widetilde{K}(a, b; h, p^n; k) \right| \leq 2p^{\frac{3}{2}n+m} \log p^n, \tag{4.13}$$

where m *such that* $p^m \| k$.

Proof. Applying Lemma 2.5, we can write a, b in the form

$$a = g^{\alpha_0'}(u+iv)^{\beta_0'}, \quad b = g^{\alpha_0''}(u+iv)^{\beta_0''},$$

where g is a primitive root $\operatorname{mod} p^n$ in $\mathbb{Z}$, $u + iv$ is a generative element of the group E_n. Then we obtain

$$\widetilde{K}(a, b; h, p^n; k) =$$
$$= \sum_{\substack{x,y \pmod{p^n} \\ N(x)N(y) \equiv h \pmod{p^n}}} e_{p^n}\left(g^{\alpha_0'} \Re((u+iv)^{\beta_0'} x^k) + g^{\alpha_0''} \Re((u+iv)^{\beta_0''} y^k) \right). \tag{4.14}$$

Let $h \equiv g^{\alpha} \, (\text{mod} p^n)$. Then $h \equiv \pm g^{2\alpha_0} \pmod{p^n}$, where

$$2\alpha_0 = \begin{cases} \alpha & \text{if} \quad \alpha \quad \text{is even,} \\ \alpha + \dfrac{p-1}{2} p^{n-1} & \text{if} \quad \alpha \quad \text{is odd.} \end{cases}$$

The sum over $x \pmod{p^n}$ in (4.14) we split into two pairs, $\sum = \sum_1 + \sum_2$.

In sum over $\sum_1$ we take these $x \pmod{p^n}$ for which $N(x) \equiv g^{2\alpha_1} \pmod{p^n}$, and in $\sum_2$ come upon these $x \pmod{p^n}$ for which $N(x) \equiv -g^{2\alpha_1} \pmod{p^n}$. In both cases α_1 runs the values $0, 1, \ldots, \dfrac{p-1}{2} p^{n-1} - 1$. So

$$\widetilde{K}(a, b; h, p^n; k) = \sum\nolimits_1 + \sum\nolimits_2. \tag{4.15}$$

For x from $\sum_1$ we have

$$x \equiv g^{\alpha_1}(u+iv)^{2\beta_1} \pmod{p^n},$$
$$\alpha_1 = 0, 1, \ldots, \frac{1}{2}(p-1)p^{n-1} - 1, \quad \beta_1 = 0, 1, \ldots, (p+1)p^{n-1} - 1.$$

Hence,

$$\Re\left((u+iv)^{\beta_0'} x^k\right) \equiv g^{k\alpha_1} \Re\left((u+iv)^{2k\beta_1 + \beta_0'}\right) \pmod{p^n}.$$

From the condition $N(x)N(y) \equiv h \pmod{p^n}$ it follows

$$N(y) \equiv \pm g^{2\alpha_2} \pmod{p^n},$$

where $\alpha_2 = \alpha_0 + \big((p-1)p^{n-1} - 1\big)\alpha_1$.

And thus we have

$$\sum\nolimits_1 = \sum_{(\alpha_1)} \sum_{(\beta_1)} \sum_{(\beta_2)} e_{p^n} \Big(g^{\alpha_0' + \alpha_1 k} \Re\big((u+iv)^{2k\beta_1 + \beta_0'}\big) + \\ + g^{\alpha_0'' + \alpha_2 k} \Re\big((u+iv)^{2k\beta_2 + \beta_0'' + \delta k}\big) \Big), \tag{4.16}$$

here (α_1) denotes that α_1 runs the value $0, 1, \ldots, \frac{1}{2}(p-1)p^{n-1} - 1$; (β_i) runs the value $0, 1, \ldots, (p+1)p^{n-1} - 1$, $i = 1, 2$; furthermore, $\delta = 0$ if $h \equiv g^{2\alpha_0} \pmod{p^n}$ and $\delta = 1$ if $h \equiv -g^{2\alpha_0} \pmod{p^n}$.

Similarly,

$$\sum\nolimits_2 = \sum_{(\alpha_1)} \sum_{(\beta_1)} \sum_{(\beta_2)} e_{p^n} \Big(g^{\alpha_0' + \alpha_1 k} \Re\big((u+iv)^{2k\beta_1 + \beta_0' + 1}\big) + \\ + g^{\alpha_0'' + \alpha_2 k} \Re\big((u+iv)^{2k\beta_2 + \beta_0'' + \delta k}\big) \Big). \tag{4.17}$$

Again we have

$$\beta_i = (p+1)t_i + z_i, \quad t_i \pmod{p^{n-1}}, \quad z_i = 0, 1, \ldots, p, \quad i = 1, 2.$$

Then

$$k\beta_i = 2(p+1)kt_i + kz_i, \quad i = 1, 2.$$

Now by (4.12), (4.13) and Lemma 2.1, it follows that the sums over t_i are equal zero if the congruences

$$\begin{gathered} \beta_0' + 2kz_1 \equiv 0 \pmod{(p+1)}, \\ \beta_0'' + 2kz_2 + k\delta \equiv 0 \pmod{(p+1)} \quad \text{for a sum} \quad \sum\nolimits_1, \\ \beta_0' + 2kz_1 + 1 \equiv 0 \pmod{(p+1)}, \\ \beta_0'' + 2kz_2 + k\delta \equiv 0 \pmod{(p+1)} \quad \text{for a sum} \quad \sum\nolimits_2, \end{gathered} \tag{4.18}$$

are disturb.

Consequently one from the sums $\sum_1$ or $\sum_2$ is equal always zero.

The congruences (4.18) can be true only for $(k, p+1)^2$ pairs of the value (z_1, z_2). Let $\mathfrak{B}$ be set of these values (z_1, z_2).

By (4.12) – (4.14) we obtain

$$\widetilde{K}(a, b; h, p^n; k) = \sum_{(\alpha_1)} e_{p^n} (N_0 g^{\alpha_1} + M_0 g^{\alpha_2}) \times \\ \times \sum_{(z_1, z_2) \in \mathfrak{B}} \; \sum_{t_1, t_2 \pmod{p^{n-1}}} e_{p^{n-2}} \big(F_1(kt_1) g^{\alpha_1} + F_2(kt_2) g^{\alpha_2} \big),$$

where $F_i(t) = c_1^{(i)} t + c_2^{(i)} t^2 + p^{\lambda_3} c_3^{(i)} t^3 + \ldots + p^{\lambda_\ell} c_\ell^{(i)} t^\ell$, $(c_2^{(i)}, p) = (c_3^{(i)}, p) = \ldots = 1$, $\lambda_j > 0$ for $j \geq 3$, $(N_0, p) = (M_0, p) = 1$.

The sums over t_1, t_2 calculates equally. Let $k = p^m k_1$, $(k_1, p) = 1$. We break the sum over t_i into blocks of the length p^{n-2-2m} (if $2m < n - 2$). Then applying Lemma 2.3, we obtain

$$\widetilde{K}(a,b;h,p^n;k) = p^{n+2m}\sum_{(\alpha_1)} e_{p^n}(N_1g^{\alpha_1}+N_2g^{\alpha_2}), \tag{4.19}$$

where $(N_1,p)=(N_2,p)=1$.

From the definition α_2 follows $g^{\alpha_2}\equiv g^{\alpha_0}(g')^{\alpha_1}\,(\mathrm{mod}\,p^n)$.

The sum on the right in (4.19) is the incomplete Kloosterman sum. By a choice of a primitive root g we have

$$g^{p-1}=1+pu, \quad (u,p)=1.$$

Then ${g'}^{p-1}=1-pu_1, (u_1,p)=1, u\equiv u_1\,(\mathrm{mod}\,p)$. We set

$$\alpha_1=(p-1)t+z,$$
$$t=0,1,\ldots,\frac{1}{2}(p^{n-1}-1), \quad z=0,1,\ldots,p-2.$$

Thus

$$g^{\alpha_1}=g^z(1+a_1pt+a_2p^2t^2+a_3p^{\lambda_3}t^3+\ldots)\,(\mathrm{mod}\,p^n),$$
$$a_1\equiv -u_1, \qquad a_2\equiv -2'u^2\,(\mathrm{mod}\,p), \quad \lambda_j\ge 3.$$

Similarly

$$g^{\lambda_2}\equiv g^{\alpha_0}{g'}^{\alpha_1}\equiv g^{\alpha_0}{g'}^{z}(1+b_1pt+b_2p^2t^2+b_3p^{\mu_3}t^3+\ldots)\,(\mathrm{mod}\,p^n),$$
$$b_1\equiv -u_1, \qquad b_2\equiv -2'u^2\,(\mathrm{mod}\,p), \quad \mu_j\ge 3.$$

Hence,

$$N_1g^{\alpha_1}+N_2g^{\alpha_2}\equiv c_0+c_1pt+c_2p^2t^2+c_3p^{\nu_3}t^3+\ldots \quad (\mathrm{mod}\,p^n),$$

where $c_i=g^za_iN_1+g^{\alpha_0}{g'}^{z}b_iN_2$, $i=1,2$.

Since $(N_1,p)=(N_2,p)=1$ it easy observe that two congruence

$$c_1\equiv 0\,(\mathrm{mod}\,p), \quad c_2\equiv 0\,(\mathrm{mod}\,p)$$

cannot realize simultaneously.

But from $c_1\equiv 0\,(\mathrm{mod}\,p)$ follows $g^{2z}\equiv g^{\alpha_0}N_2N_1'\,(\mathrm{mod}\,p)$. It is possible only one value z. Let's designate this value through z_0.

Thus from (4.19) we infer

$$\widetilde{K}(a,b;h,p^n;k) =$$
$$= p^{n+2m}\left(\sum_{\substack{z=0\\ z\ne z_0}}^{p-2}\ \sum_{t=0}^{\frac12(p^{n-1}-1)} e^{2\pi i\frac{c_0}{p^n}}e_p^{n-1}\big(c_1t+c_2pt^2+c_3p^{\nu_3-1}t^3+\ldots\big)+\right.$$
$$\left.+\sum_{t=0}^{\frac12(p^{n-1}-1)} e^{2\pi i\frac{c_0'}{p^n}}e_{p^{n-2}}\big(c_1't+c_2't^2+c_3'p^{\nu_3-2}t^3+\ldots\big)\right), \tag{4.20}$$

where $(c_1,p)=(c_2',p)=1$.

The sums over t are the incomplete rational sums, their estimations we obtain by way of estimations complete exponent sums.

We have for an arbitrary polynomial $\Phi(t)\in\mathbb{Z}[t]$:

$$\left|\sum_{t=0}^{T}e^{2\pi i\frac{\Phi(t)}{q}}-\frac{T}{q}\sum_{t=0}^{q-1}e^{2\pi i\frac{\Phi(t)}{q}}\right|\le\sum_{r=1}^{q}\frac{1}{\min(r,q-r+1)}\left|\sum_{t=0}^{q-1}e^{2\pi i\frac{\Phi(t)-t}{q}}\right|. \tag{4.21}$$

Now, if $\Phi(t) = c_1 t + c_2 p t^2 + c_3 p^{\nu_3 - 1} t^3 + \ldots$, $(c_1, p) = 1$, $q = p^{n-1}$, then the complete sums in (4.21) are equal to zero for all r except the case $r \equiv c_1 \pmod p$. In this special case we have $\Psi(t) = c_1' t + c_2' t^2 + c_3' p^{\nu_3 - 1} t^3 + \ldots$, $(c_2', p) = 1$, $q = p^{n-2}$, and than a complete sum estimates by a value $2p^{\frac{n-2}{2}}$.

Hence,

$$\left|\widetilde{K}(a, b; h, p^n; k)\right| \le p^{n+m} \left[\sum_{\substack{z=0 \\ z \ne z_0}}^{p-2} \frac{1}{|c_1(z)|} + \sum_{r=1}^{p^n} \frac{1}{kp} p^{\frac{n-2}{2}} + p p^{\frac{n-2}{2}} \right].$$

At last, we take account that for the distinct values z we have the distinct values $c_1(z) \pmod p$, and thus we obtain

$$\left|\widetilde{K}(a, b; h, p^n; k)\right| \le p^{\frac{3}{2}n+m} \left(\log p + \frac{\log p^n}{p} \right).$$

If $2m > n - 2$ then the assertion of theorem is trivial.

The theorem is proved.

We go towards a estimation of the norm Kloosterman sum $\widetilde{K}(a, b; h, p^n; k)$ for the case $p \equiv 1 \pmod 4$, $k \ge 2$, $(a, p) = (b, p) = 1$. For $p \equiv 1 \pmod 4$ we have $p = \mathfrak{p}\overline{\mathfrak{p}}$, where $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are the complex conjugate Gaussian prime number. Then the reduced residue system $\bmod p^n$ can write as

$$x = g^{\ell_1} \overline{\mathfrak{p}}^n + g^{\ell_2} \mathfrak{p}^n, \quad 0 \le \ell_1, \quad \ell_2 \le (p-1)p^{n-1} - 1,$$

where g is a primitive root $\bmod p^n$ such that

$$g^{p-1} = 1 + pH, \quad H \in \mathbb{Z}, \quad (H, p) = 1.$$

Thus

$$N(x) = x\overline{x} = g^{2\ell_1} p^n + g^{\ell_2} p^n + g^{\ell_1+\ell_2} \overline{\mathfrak{p}}^{2n} + g^{\ell_1+\ell_2} \mathfrak{p}^{2n} \equiv$$
$$\equiv g^{\ell_1+\ell_2} Sp(\mathfrak{p}^{2n}) \pmod{p^n}. \tag{4.22}$$

Therefore, if $\mathfrak{p} = c + id$ then $(c, p) = (d, p) = 1$, and by the induction we easily obtain

$$\mathfrak{p}^{2n} \equiv c_n + id_n, \quad n = 1, 2, \ldots,$$

where

$$c_n \equiv \begin{cases} (-1)^{n-1} \cdot 2^m \cdot c \cdot d^{2(m-1)} \pmod p, \\ (-1)^m \cdot 2^{m+2} \cdot d^{2m}, \end{cases}$$

$$d_n \equiv \begin{cases} (-1)^{2m-1} \cdot 2^m \cdot d^{2m-1} \pmod p \quad \text{if} \quad n = 2m-1, \\ (-1)^{m-1} \cdot 2^{m+2} \cdot c \cdot d^{2m-1} \pmod p \quad \text{if} \quad n = 2m. \end{cases}$$

Hence, for $p \equiv 1 \pmod 4$ we have

$$\widetilde{K}(a, b; h, p^n; k) = \sum_{(U)} e_{p^n}(A(g^{\ell_1' k} + g^{\ell_2' k}) + B(g^{\ell_1'' k} + g^{\ell_2'' k})) =$$
$$= \sum_{(U')} e_{p^n}\Big(A(x_1^k + x_2^k) + B(y_1^k + y_2^k)\Big), \tag{4.23}$$

where

$$U := \left\{ \ell_1', \ell_2', \ell_1'', \ell_2'' \pmod{(p-1)p^{n-1}} \middle| g^{\ell_1' + \ell_2' + \ell_1'' + \ell_2''} \equiv H \pmod{p^n} \right\},$$

$$U' := \left\{x_1, x_2, y_1, y_2 \,(\operatorname{mod} p^n) \middle| x_1x_2y_1y_2 \equiv H \,(\operatorname{mod} p^n)\right\},$$
$$A, B, \in \mathbb{Z}, \quad (A,p) = (B,p) = 1.$$

Theorem 4.4. *Let $p \equiv 1 \,(\operatorname{mod} 4)$ is a prime number and let $a, b \in \mathbb{Z}[i]$, $(a,p) = (b,p) = 1$. Then*

$$\left|\widetilde{K}(a,b;h,p;k)\right| \ll \begin{cases} d^2 p^{\frac{3}{2}} & \text{if} \quad (d-1)^4 < p, \\ d^4 p^2 & \text{if} \quad (d-1)^4 \geq p, \end{cases}$$

where $d = (k, p-1)$.

Proof. With out loss of generality, we can suppose a, $b \in \mathbb{Z}$.

By (4.23) and similarly as in the case $p \equiv 3 \,(\operatorname{mod} 4)$ we obtain

$$\widetilde{K}(a,b;h,p;k) = \sum_{\substack{x_2, x_2, y_1, y_2 \in \mathbb{F}^*_{\scriptscriptstyle |} \\ x_1,x_2,y_1,y_2 \equiv H_1^k}} e_p\Big(A(x_1^d + x_2^d) + B(y_1^d + y_2^d)\Big).$$

Now, for $(d-1)^4 < p$ we obtain by analogy with the case $p \equiv 3 \,(\operatorname{mod} 4)$

$$\sum_{h \in \mathbb{F}_p^*} \chi(h) \widetilde{K}(\alpha, \beta; h, p; d) = \left(\sum_{x \in \mathbb{F}_p^*} \chi(x) e_p(Ax^d)\right)^2 \left(\sum_{y \in \mathbb{F}_p^*} \chi(y) e_p(By^d)\right)^2.$$

Hence,

$$\sum \left|\widetilde{k}(\alpha, \beta; h, p; d)\right|^2 \leq (d-1)^4 p^4 \quad \text{if} \quad (d-1)^4 < p.$$

Then

$$\widetilde{K}(a,b;h,p;k) \ll d^2 p^{\frac{3}{2}} \quad \text{if} \quad (d-1)^4 < p.$$

Let $(d-1)^4 \geq p$. Denote through g a primitive element of field $\mathbb{F}_p$ and let $x = g^{\operatorname{ind} x}$ for $x \in \mathbb{F}_p^*$.

Let G is a group of multiplicative characters of $\mathbb{F}_p$. For $\chi \in G$ we have $\chi(x) = e_{p-1}(\nu \operatorname{ind} x)$ with some $\nu \in \mathbb{F}_p$. Then using the arguments from Theorem 4.1, we can obtain on a routine way the following relation:

$$\widetilde{K}(a,b;h,p;d) =$$
$$= \frac{1}{p-1} \sum_{\chi \in G} \overline{\chi}(H) \sum_{s_1,\ldots,s_4=0}^{d-1} \overline{\chi}(A^2B^2) e_d\Big((s_1+s_2)\operatorname{ind} A + (s_3+s_4)\operatorname{ind} B\Big) \times$$
$$\times \sum_{x_1,\ldots,x_4 \in \mathbb{F}_p^*} e_d(s_1 \operatorname{ind} x_1 + \ldots + s_4 \operatorname{ind} x_4) \chi(x_1,\ldots,x_4) e_p(x_1 + \ldots + x_4) =$$
$$= \frac{1}{p-1} \sum_{\nu \in \mathbb{F}_p} \sum_{s_1,\ldots,s_4=0}^{d-1} e_{p-1}(\nu \operatorname{ind} H) e_{p-1}(F_1(\nu, s)) \times$$
$$\times \sum_{x_1,\ldots,x_4 \in \mathbb{F}_p^*} e_{p-1}(F_2(\nu,s,x)) e_p(x_1 + \ldots + x_4),$$

where

$$F_1(\nu, s) := \left(2\nu + (s_1+s_2)\frac{p-1}{d}\right)\operatorname{ind} A + \left(2\nu + (s_3+s_4)\frac{p-1}{d}\right)\operatorname{ind} B,$$
$$F_2(\nu, s, x) := \left(s_1\frac{p-1}{d} + \nu\right)\operatorname{ind} x_1 + \ldots + \left(s_4\frac{p-1}{d} + \nu\right)\operatorname{ind} x_4.$$

The last sum over $x_1, \ldots, x_4$ is the product of the Gauss sums of field $\mathbb{F}_p$. And hence,

$$\left|\widetilde{K}(a, b; h, p; k)\right| \leq d^4 p^2.$$

The theorem is proved.

If $n \geq 2$ we can use the description of solution of the congruence $x_1,\ x_2,\ x_3,\ x_4 \equiv H \,(\operatorname{mod} p^n)$:

$$x_i = y_i + p^m z_i, \quad y_i \,(\operatorname{mod} p^m), \quad z_i \,(\operatorname{mod} p^{n-m}),$$
$$(y_i, p) = 1, \quad i = 1, 2, 3; \quad m = \left[\frac{n+1}{2}\right], \tag{4.24}$$
$$x_4 = H y_1' y_2' y_3' \left(1 - p^m y_1' z_1 - p^m y_2' z_2 - p^m y_3' z_3\right), \quad y_i y_i' \equiv 1 \,(\operatorname{mod} p^m).$$

Theorem 4.5. *Let* $p \equiv 1 \,(\operatorname{mod} 4)$ *be a prime number,* $n \in \mathbb{N}$, $n \geq 2$; $h \in \mathbb{Z}$, $(h, p) = 1$; $a, b \in \mathbb{Z}[i]$, $(a, p) = (b, p) = 1$. *Then*

$$\left|\widetilde{K}(a, b; h, p^n; k)\right| \ll \begin{cases} d^4 p^{\frac{3}{2}n} & \text{if} \quad (d-1)^4 < p, \\ d^4 p^{n+m} & \text{if} \quad (d-1)^4 \geq p, \end{cases}$$

where $m = \left[\dfrac{n+1}{2}\right]$.

Proof. By (4.23), (4.24) we have

$$\widetilde{K}(a, b; h, p^n; k) = \sum_{y_1, y_2, y_3 \in R^*(p^m)} e_{p^n}\left(f(y_1, y_2, y_3)\right) \times$$
$$\times \sum_{z_1, z_2, z_3 \,(\operatorname{mod} p^{n-m})} e_{p^{n-m}}(F(z_1, z_2, z_3)), \tag{4.25}$$

where

$$f(y_1, y_2, y_3) = A y_1^k + a y_2^k + B y_3^k + B H {y_1'}^k {y_2'}^k {y_3'}^k,$$
$$F(z_1, z_2, z_3) = k\Bigg[\Big(A y_1^{k-1} - B {y_1'}^{k+1} {y_2'}^k {y_3'}^k\Big) z_1 +$$
$$+ \Big(A y_2^{k-1} - B(y_1^{k+1} y_2^k y_3^k)'\Big) z_2 + \Big(A y_3^{k-1} - B(y_1^k y_2^k y_3^{k+1})'\Big) z_3\Bigg].$$

Let $(k, p^{n-m}) = p^\ell$. Then we obtain from (4.25)

$$\widetilde{K}(a, b; h, p^n; k) = p^{3(n-m)} \sum_{(U)} e_{p^n}(f(y_1, y_2, y_3)),$$

where $U := \Big\{y_1,\ y_2,\ y_3 \,(\operatorname{mod} p^m) \Big| (y_i,\ p) = 1,\ i = 1,\ 2,\ 3;\ y_1^k \equiv {y_2}^k \equiv {y_3}^k \,(\operatorname{mod} p^{n-m-\ell}),\ y_1^{4k} \equiv BA' \,(\operatorname{mod} p^{n-m-\ell})\Big\}$.

Now, for $n = 2m$ we estimate the sum $\sum_{(U)}$ by the number triples $(y_1, y_2, y_3) \in U$, and for $n = 2m - 1$ we take into account also the Theorem 2.4. Hence, we have finally

$$\left|\widetilde{K}(a, b; h, p^n; k)\right| \ll \begin{cases} d^4 p^{\frac{3}{2}n} & \text{if} \quad (d-1)^4 < p, \\ d^4 p^{n+m} & \text{if} \quad (d-1)^4 \geq p. \end{cases}$$

The theorem is proved.

Collection our previous estimations from the Theorems 4.2 – 4.5 we get the following theorem.

Theorem 4.6. *Let* α, $\beta \in \mathbb{Z}[i]$ *and let* $h, q, k, n \in \mathbb{N}$, $k \geq 2$, $(k, q) = (h, q) = 1$. *Then for* $(\alpha, q) = (\beta, q) = 1$ *we have*

$$\widetilde{K}(\alpha, \beta; h, q; k) \ll D(k, q) q^{\frac{3}{2}},$$

where

$$D(k, q) = \prod_{\substack{p \mid q \\ p \equiv 1(q)}} d^6(k, p) \prod_{\substack{p^n \| q \\ p \equiv 3(q)}} d^3(k, p) \log p^n,$$

$$d(k, p) = (k, p - 1).$$

We must note that the norm Kloosterman sum $\widetilde{K}(\alpha, \beta; h, q; k)$ has not an analogue in the ring $\mathbb{Z}$.

1. *Kloosterman H. D.* On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$ // Acta math. – 1926. – **49**. – P. 407 – 464.
2. *Davenport H.* On certain exponential sums // I. reine und angew. Math. – 1933. – **169**. – S. 158 – 176.
3. *Weil A.* On some exponential sums // Proc. Nat. Acad. Sci. USA. – 1948. – **34**. – P. 204 – 207.
4. *Kyznetsov N. V.* Petterson conjecture for forms of weight zero and the conjecture Linnik // A mimeographed. – Khabarovsk, 1977. – Preprint 2 (in Russian).
5. *Kyznetsov N. V.* Petterson conjecture for forms of weight zero and the conjecture Linnik, Sums of Kloosterman sums // Mat. sb. – 1980. – **3**. – P. 334 – 383 (in Russian).
6. *Bruggeman R. W.* Fourier coefficients of cusp forms // Invent. math. – 1978. – **445**. – P. 1 – 18.
7. *Deshouillers I.-M., Iwaniec H.* Kloosterman sums and Fourier coefficients of cusp forms // Ibid. – 1982. – **70**. – P. 219 – 288.
8. *Proskurin N. V.* On general Kloosterman sums. – Leningrad, 1980. – (Preprint / LOMI; R-3) (in Russian).
9. *Yi. Yuan, Zhang Wenpeng.* On the generalization of a problem of D. H. Lehmer // Kyushu J. Math. – 2002. – **56**. – P. 235 – 241.
10. *Kanemitsu S., Tanigawa Y., Yi. Yuan, Zhang Wenpeng.* On general Kloosterman sums // Anna. Univ. sci. Budapest. Sec. comp. – 2003. – **22**. – P. 151 – 160.
11. *Mordell L. Y.* On a special polynomial congruence and exponential sums // Calcutta Math. Soc. Golden Iub. – 1963. – Pt 1. – P. 29 – 32.
12. *Dwork B.* On the zeta function of a hypersurface. III // Ann. Math. – 1966. – **83**. – P. 457 – 579.
13. *Deligne P.* La conjecture de Weill. I, II // Publ. Math. IHES. – 1974. – **43**. – P. 273 – 307; 1980. – **52**. – P. 137 – 252.
14. *Bombieri E.* On exponential sums in finite fields. II // Invent. math. – 1978. – **47**, Fasc. 1. – P. 29 – 39.
15. *Deligne P.* Applications de la formula des traces aux sommes trigonometriques // Cohomologie Etale: Lect. Notes Math. – Berlin etc.: Springer, 1977. – **569**. – P. 168 – 232.
16. *Zanbyrbaeva U. B.* Asymptotic problems of number theory in sectorial regions: Dissertation. – Odessa, 1993.
17. *Perel'muter G. I.* On some sums with characters // Uspechi Mat. Nauk. – 1963. – **18**, № 2. – P. 143 – 149 (in Russian).
18. *Williams K. S.* A class of character sums // J. London Math. Soc. – 1971. – **3**, № 2. – P. 61 – 72.

Received 17.02.2006