© Algebra and Discrete Mathematics RESEARCH ARTICLE
Volume **35** (2023). Number 2, pp. 251–270
DOI:10.12958/adm2048

The Kloosterman sums on the ellipse

S. Varbanets and Y. Vorobyov

Communicated by Yu. A. Drozd

Abstract. The main point of our research is to obtain the estimates for Kloosterman sums $\widetilde{K}(\alpha,\beta;h,q;k)$ considered on the ellipse bound for the case of the integer rational module q and for some natural number k with conditions $(\alpha,q)=(\beta,q)=1$ on the integer numbers of imaginary quadratic field. These estimates can be used to construct the asymptotic formulas for the sum of divisors function $\tau_\ell(\alpha)$ for $\ell=2,3,\ldots$ over the ring of integer elements of imaginary quadratic field in arithmetic progression.

The classical Kloosterman sums were being introduced in 1926 by work of [6] to study the representations of natural numbers by the binary quadratical forms. The Kloosterman sum is an exponential sum over the reduced residue system modulo q:

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

here x' denotes the multiplicative inverse for x modulo $\mod q$, i.e. $xx'\equiv 1 \pmod q$.

Over the following years the Kloosterman sums have been found its application on the different problems of asymptotic number theory and first of all on the distribution problems of the values of divisor functions $\tau(n)$ on arithmetic progressions.

2020 MSC: 11L05, 11L07, 11T23.

Key words and phrases: exponential sums, Kloosterman sums, asymptotic formulas, imaginary quadratic field.

The most complexity in construction the estimations of Kloosterman sums is represented by the case $q = p, p$ be a prime number. In 1948 A. Weill [11] proved the Riemann hypothesis on algebraic curves that leads to construction the best possible estimation

$$K(a, b\,; q) \ll p^{\frac{1}{2}}. \tag{2}$$

The Kloosterman sums play the essential role in the spectral theory of Riemann zeta-function devised by Yu. Motohashi (see [8]).

The renewed impetus of resolving the difficult problems of asymptotic number theory give the works of N.V. Kuznetsov[7] and R. Bruggeman[3] devoted to estimates of the sum of Kloosterman sums. Afterwards there are occured the generalizations of classical Kloosterman sums. For example, U. Zhanbyrbaeva[12] has studied the Kloosterman sums over the ring of Gaussian integers $\mathbb{Z}[\theta]$ and resolved the distribution problem of divisor function of the Gaussian integers in arithmetic progression. In the work [4] there have been investigated the Kloosterman sums over the entirely real number fields. In 2003 R. Bruggeman and Yu. Motohashi [2] obtained an analogue of Kuznetsov formula for the sum of Kloosterman sums over the ring of Gaussian integers. The geometry of Gaussian integers is richer that the geometry of integer rational numbers. In the work [10] there was considered the norm Kloosterman sum over the ring $\mathbb{Z}[\theta]$ that has no analogous rational case.

We use the following notations:

- $\alpha, \beta, \gamma, \ldots$ be the integer numbers from $\mathbb{Q}(\sqrt{-d})$;
- $\wp$ – Gaussian prime number;
- $Sp(\alpha)$ be the trace of α from $\mathbb{Q}(i)$ to $\mathbb{Q}$, i.e. $Sp(\alpha) = 2Re\,\alpha$;
- $N(\alpha) = |\alpha|^2$ be the norm of α;
- G_γ (respectively, G^*_γ) – complete (respectively, reduced) residue system modulo $\mod \gamma$ in $\mathbb{Q}(\sqrt{-d})$;
- the notation $\sum\limits_{S(C)}$ means that the summation goes over the condition C, and besides the condition C describing separately;
- $e_q(z) := e^{2\pi i \frac{z}{q}}, \quad \exp(x) := e^x$;
- $(a, b, \ldots, c)$ be the greater common divisor of $a, b, \ldots, c$ in $\mathbb{Z}$ or in $\mathbb{Z}[\sqrt{-d}]$ (that is usually follows from context);
- the Vinogradov symbol "$\ll$" means the same as Landau symbol "O";
- φ (respectively, $\widetilde{\varphi}$) be the Euler totient function in $\mathbb{N}$ (or, respectively, in $\mathbb{Z}[\theta]$, where $\theta = \sqrt{-d}$);

- and further instead $\sqrt{-d}$ we will use whenever it is the letter θ.

Now let $\alpha, \beta \in \mathbb{Z}[\theta]$, $h \in \mathbb{Z}$, $q \in \mathbb{N}$, $q > 1$, $(h, q) = 1$. Let us assume

$$\widetilde{K}(\alpha, \beta; h, q) := \sum_{\substack{x,y (\mathrm{mod}\, q) \\ N(xy) \equiv h (\mathrm{mod}\, q)}} e_q\left(\frac{1}{2} Sp(\alpha x + \beta y)\right) \qquad (3)$$

and call it the Kloosterman sum over the ellipse $u^2 + dv^2 \equiv 1 \pmod{p^m}$.

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

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

$$= \widetilde{K}(\alpha q_2, \beta q_2; h, q_1) \cdot \widetilde{K}(\alpha q_1, \beta q_1; h, q_2).$$

(here q'_2 be the inversive to q_2 modulo q_1 and q'_1 be the inversive to q_1 modulo q_2).

Therefore, we will consider only the case $q = p^n$, p be the prime rational number, $n \in \mathbb{N}$.

Denote $m_\alpha = \max\limits_{\alpha \equiv 0 (\mathrm{mod}\, p^m)} \{m : \ m \leqslant \nu_p(q)\}$ (i.e. m_α be the maximal exponent of p that is not more than $\nu_p(q)$ and such that $\alpha \equiv 0 \pmod{p^m}$).

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

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

with absolute constant in symbol " $\ll$ ".

Proof. First of all let assume that $n = 1$. The case $m_\alpha = m_\beta = 1$ is a trivial. So we will suppose that $m_\alpha = 0$ or $m_\beta = 0$. And further let say $\alpha = a_1 + i a_2$, $\beta = b_1 + i b_2$, and then $(a_1, a_2, b_1, b_2) = 1$.

For the factorable p we have

$$\widetilde{K}(\alpha, \beta; h, p) = \sum_{(U)} e_p(a_1 x_1 - \varepsilon_0 a_2 x_2 + b_1 y_1 - \varepsilon_0 b_2 y_2), \qquad (4)$$

where

$$U = \left\{ \begin{matrix} x_1, x_2, y_1, y_2 \in \{0, 1, \ldots, p-1\}, \\ (x_1^2 + d \cdot x_2^2)(y_1^2 + d \cdot y_2^2) \equiv h \pmod{p} \end{matrix} \right\},$$

$$\varepsilon_0^2 \equiv -d \pmod{p^m}$$

We will suppose that $(d, p) = 1$.

The sum $\widetilde{K}(\alpha, \beta; h, p)$ we call the norm Kloosterman sum over the ring $\mathbb{Z}[\theta]$.

Let ε_0 be the solution of congruence $x^2 \equiv -d(\bmod p)$. This congruence has the solution because $-d$ is the quadratic residue modulo p.

Further let assume

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

Now from (4) we obtain

$$\widetilde{K}(\alpha, \beta; h, p) = \sum_{(U)} e_p(A_1 u_1 + A_2 u_2 + B_1 v_1 + B_2 v_2),$$

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

E. Bombieri[1] proved that the last sum can be estimated as $\ll p^{\frac{3}{2}}$.

If p be irreducible then the same estimate be valid for the sum (4)(the proof is analogous).

Now let $n \geqslant 2$. It is enough for us to consider only the case $(p^{m_\alpha}, p^{m_\beta}, p^n) = 1$. In such case just although one of numbers a_1, a_2, b_1, b_2 is not divided by p (here $\alpha = a_1 + \theta a_2$, $\beta = b_1 + \theta b_2$).

Then we infer

$$\begin{aligned} &\widetilde{K}(\alpha, \beta; h, p^n) = \\ &= \sum_{x,y \in G_{p^n}} \frac{1}{p^n} \sum_{k=0}^{p^n-1} e_{p^n}(k(N(x)N(y) - h) + \Re(\alpha x) + \Re(\beta y)) = \\ &= \frac{1}{p^n} \sum_{S(C)} e_{p^n}(k(d \cdot (x_1^2 + x_2^2)(y_1^2 + y_2^2) - h) + \\ &\qquad + a_1 x_1 - a_2 x_2 + d b_1 y_1 - d b_2 y_2), \end{aligned} \tag{5}$$

where

$$C := \{k(\bmod p^n); x_1, x_2(\bmod p^n); y_1, y_2(\bmod p^n); x_1, x_2, y_1, y_2 \in \mathbb{Z}_{p^n}\}$$

Just although the one of sum over x_1, x_2, y_1, y_2 is equal to 0, if $(k, p) = p$ (by rational analogue of the completed exponential sum of linear function).

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

$$\widetilde{K}(\alpha, \beta; h, p^n) =$$

$$= \frac{1}{p^n} \sum_{S(C)} e_p^n(-kh) e_{p^n}(kdN(x)(y_1^2 + y_2^2) + \Re(\alpha x) + db_1 y_1 - db_2 y_2) =$$

$$= \frac{1}{p^n} \sum_{k \in \mathbb{Z}_{p^n}^*} e_{p^n}(-kh) \left(\sum_{\substack{x \in \mathbb{G}_{p^n} \\ (N(x),p)=1}} + \sum_{\substack{x \in \mathbb{G}_{p^n} \\ x (\bmod p^n) \\ N(x) \equiv 0 \pmod p}} \right) = \sum\nolimits_1 + \sum\nolimits_2 . \tag{6}$$

where $C := \left\{ k \in \mathbb{Z}_{p^n}^*,\ x \in \mathbb{G}_{p^n},\ y_1, y_2 \in \mathbb{Z}_{p^n} \right\}$,

Let $N(x)'$ and k' be the solutions of congruence

$$N(x)u \equiv 1 (\bmod p^n),\ ku \equiv 1 (\bmod p^n),$$

respectively.

Then

$$\left| \sum\nolimits_1 \right| = \left| \sum_{k \in \mathbb{Z}_{p^n}^*} e_{p^n}(-kh) \times \right. \tag{7}$$

$$\left. \times \sum_{x \in \mathbb{G}_{p^n}} e_{p^n}(4' N(x)' k' (b_1^2 + b_2^2) + a_1 x_1 - a_2 x_2) \right| .$$

We assume

$$x_1 = x_1^0 + p^m z_1,\ x_2 = x_2^0 + p^m z_2,$$

$$0 \leqslant x_1^0, x_2^0 \leqslant p^m - 1,\ 0 \leqslant z_1, z_2 \leqslant p^{n-m} - 1,\ m = \left[\tfrac{n+1}{2} \right] .$$

It is clear that

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

And hence

$$|\textstyle\sum_1| = \left| \sum_{k \in \mathbb{Z}_{p^n}^*} e_{p^n}(-kh) \times \right.$$

$$\times \sum_{\substack{x_1^0, x_2^0 (\bmod p^n) \\ ({x_1^0}^2 + {x_2^0}^2, p) = 1}} e_{p^n}(4' k' ({x_1^0}^2 + {x_2^0}^2)' \cdot (b_1^2 + b_2^2) + a_1 x_1^0 - a_2 x_2^0) \times$$

$$\left. \times \sum\nolimits_{z_1, z_2 (\bmod p^{n-m})} e_{p^{n-m}}((A_1 + a_1) z_1 + (A_2 + a_2) z_2) \right| ,$$

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

The summation over z_1, z_2 gives zero if the congruence

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

or the equivalent congruence

$$a_2 x_1^0 + a_1 x_2^0 \equiv 0 (\operatorname{mod} p^{n-m}),\ 2x_2^0 \equiv -a_1 (x_1^{0\,2} + x_2^{0\,2})^2 (\operatorname{mod} p^{n-m})$$

are violated.

This congruence system has at most three solutions modulo p^{n-m}, and so at most $3p^{m-(n-m)}$ solutions modulo p^m.

Hence,

$$\left|\sum\nolimits_1\right| = \left| p^{2(n-m)} \sum_{S(C)} e_{p^n}(a_1 x_1^0 - a_2 x_1^0) \sum_{k \in \mathbb{G}^*_{p^n}} (kh + k'B) \right| \leqslant 8p^{\frac{3}{2}n}, \quad (8)$$

where

$$C = \left\{ x_1^0, x_2^0 (\operatorname{mod} p^m) \;\middle|\; \begin{array}{l} a_2 x_1^0 \equiv -a_1 x_2^0 (\operatorname{mod} p^{n-m}), \\ \\ 2x_1^0 \equiv -a_1 (x_1^{0\,2} + x_2^{0\,2})^2 (\operatorname{mod} p^{n-m}) \end{array} \right\}.$$

Finally, if $N(x) \equiv 0 (\operatorname{mod} p)$ then $\sum_2 = 0$ by the rational analogue of completed esponential sum of lenear function. $\square$

For natural $k > 1$ we assume

$$\widetilde{K}(\alpha, \beta; h, q; k) := \sum_{\substack{x, y \in \mathbb{G}_q \\ N(xy) \equiv h (\operatorname{mod} q)}} e_q\left(\frac{1}{2} Sp(\alpha x^k + \beta y^k)\right). \quad (9)$$

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

The method of investigation the sum $\widetilde{K}(\alpha, \beta; h, q; k)$ shows that it is enough to consider the case $q = p^n$, p be a prime. First of all, we will assume that p be irreducible.

Theorem 2. *Let p be irreducible, $h \in \mathbb{Z}$, $(h, p) = 1$, $k \in \mathbb{N}$, $t = (k, p-1)$. Then for any of integer numbers α, β, $(\alpha, \beta, p) = 1$ over the ring $\mathbb{Z}[\theta]$ the following estimate*

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

holds.

Proof. Let $k = dk_1$, $(k_1, \frac{p-1}{t}) = 1$. We have

$$\sum_{\substack{x,y\in\mathbb{G}_p \\ N(xy)\equiv h(\bmod p)}} e_p(\tfrac{1}{2}Sp(\alpha(x^{k_1})^t + \beta(y^{k_1})^t)) =$$

$$= \sum_{\substack{x,y\in\mathbb{G}_p \\ N(x^{k_1}y^{k_1})\equiv h^{k_1}(\bmod p)}} e_p(\tfrac{1}{2}Sp(\alpha(x^{k_1})^t + \beta(y^{k_1})^t)) =$$

$$= \sum_{\substack{x,y\in\mathbb{G}_p \\ N(xy)\equiv h^{k_1}(\bmod p)}} e_p(\tfrac{1}{2}Sp(\alpha x^t + \beta y^t)) = \widetilde{K}(\alpha, \beta; h^{k_1}, p; t).$$

By virtue of the fact that for any multiplicative character χ over the field $\mathbb{F}_{p^2}$ we have

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

$$= \sum_{x,y\in\mathbb{F}^*_{p^2}} \chi(N(x)N(y))e_p(\tfrac{1}{2}Sp(\alpha x^t))e_p(\tfrac{1}{2}Sp(\beta y^t)) = \tag{10}$$

$$= (\sum_{x\in\mathbb{F}^*_{p^2}} \chi(N(x)e_p(\tfrac{1}{2}Sp(\alpha x^t))))(\sum_{y\in\mathbb{F}^*_{p^2}} \chi(N(y))e_p(\tfrac{1}{2}Sp(\beta y^t))),$$

The sums in righthand of (10) can be estimated as $(t-1)N(p)^{\frac{1}{2}}$ (because of this is generalized Gaussian sums).

So we obtain

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

The application of Plancherel theorem gives

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

Now, similar to the work of Bombieri[1], we infer that the weight of characteristic roots associating with $\widetilde{K}(\alpha, \beta; h, p; t)$ be no more than 3 if $(t-1)^4 < p$. Then using the results of Bombieri[1] and Deligne[5] we find

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

Further, for $x = x_1 + \theta x_2,\ x_1, x_2 \in \mathbb{Z}$, we have $x_1 - i\theta x_2 \equiv (x_1 + \theta x_2)^p (\bmod p)$ and then $N(x) \equiv x^{p+1} (\bmod p)$.

Hence,

$$\sum_{\substack{x,y \in \mathbb{G}_p \\ N(xy) \equiv h (\bmod p)}} e_p(\tfrac{1}{2} Sp(\alpha x^t + \beta y^t)) =$$

$$= \sum_{\substack{x,y \in \mathbb{G}_p \\ (xy)^{p+1} \equiv h (\bmod p)}} e_p(\tfrac{1}{2} Sp(\alpha x^t + \beta y^t)) = \tag{11}$$

$$= \sum_{\substack{\varepsilon \in \mathbb{G}_p \\ \varepsilon^{p+1} \equiv h (\bmod p)}} \sum_{x (\bmod p)} e_p(\tfrac{1}{2} Sp(\alpha x^t + \beta y^t)).$$

The congruence $z^{p+1} \equiv h (\bmod p)$ has the exactly 2 solutions $\bmod p$ if h be the quadratic residue. The inner sum at the righthand of (11) estimates as $\leqslant 2dp$. This finalize the proof of theorem. □

Now, let $q = p^n$, p be irreducible, $n \geqslant 2$. We will use the description of elements with norm 1 of reduced residue system $\bmod p^n$. They form a group that we describe through E_m.
Further we will need to use the following statement.

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

$$(1 + p^k u)^t \equiv 1 + p^k a_1 t + p^{2k} a_2 t^2 + p^{\lambda_3} a_3 t^3 + \cdots + p^{\lambda_n} a_n t^n (\bmod p^n),$$

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

Proof. From the relation

$$\begin{pmatrix} t \\ m \end{pmatrix} = \frac{1}{m!}(t^m - \frac{m(m-1)}{2} t^{m-1} + \cdots + (-1)^{m-1}(m-1)! \cdot t)$$

and the upper bound of exponent with that the number p falls into $m!$, we obtain

$$(1 + p^k u)^t \equiv 1 + p^k a_1 t + p^{2k} a_2 t^2 + p^{\lambda_3} a_3 t^3 + \cdots + p^{\lambda_n} a_n t^n (\bmod p^n),$$

where $(a_i, p) = 1$, $i = 1, \ldots, n$; $\lambda_j > (k - \frac{1}{p-1}) \cdot j > 2k$ for $j = 3, 4, \ldots$. □

Therefore, it is obvious that the generating element $u+\sqrt{-d}v$ of the group E_1 may be taken as it will be the generating element of group E_ℓ for any fixed ℓ, $\ell=2,3,\dots$. Let $\ell=\max(5,n)$. We have

$$N((u+\sqrt{-d}v))^2 \equiv 1 (\operatorname{mod} p^\ell)$$

$$(u+\sqrt{-d}v)^{2(p+1)} = 1 + p(x_0+\sqrt{-d}y_0),\ (x_0+\sqrt{-d}y_0,p)=1.$$

Then

$$N(1+px_0+\sqrt{-d}py_0) \equiv 1+2px_0+p^2x_0^2+p^2dy_0^2 \equiv 1 (\operatorname{mod} p^\ell).$$

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

$$(u+\sqrt{-d}v)^{2(p+1)} \equiv 1+p^2x_0+\sqrt{-d}py_0,\ (x_0,p)=(y_0,p)=1.$$

Now applying previous lemma we easy obtain

$$\begin{aligned} &\Re((u+\sqrt{-d}v)^{2(p+1)t}) \equiv \\ &\quad \equiv A_0 + A_1t + A_2t^2 + \dots + A_{n-1}t^{n-1} (\operatorname{mod} p^n), \\ &\Im((u+\sqrt{-d}v)^{2(p+1)t}) \equiv \\ &\quad \equiv B_0 + B_1t + B_2t^2 + \dots + B_{n-1}t^{n-1} (\operatorname{mod} p^n), \end{aligned} \tag{12}$$

where

$$A_0 \equiv 1 (\operatorname{mod} p),\ B_0 \equiv 0 (\operatorname{mod} p),$$

$$A_1 \equiv p^2x_0 + 2'dy_0^2p^2 (\operatorname{mod} p^3),\ \text{i.e. } A_1 \equiv 0 (\operatorname{mod} p^3),$$

$$A_2 \equiv -2'y_0^2p^2 (\operatorname{mod} p^3),\ \text{i.e. } A_2 = p^2A_2',\ (A_2',p)=1,$$

$$B_1 \equiv py_0 (\operatorname{mod} p^3),\ \text{i.e. } B_1 = pB_1',\ (B_1',p)=1,$$

$$B_2 \equiv A_3 \equiv B_3 \equiv \dots \equiv A_{n-1} \equiv B_{n-1} \equiv 0 (\operatorname{mod} p^3).$$

Let assume

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

and define

$$(u+\sqrt{-d}v)^z = u(z) + \sqrt{-d}v(z),\ z=0,1,\dots,2p+1.$$

Then

$$(u+\sqrt{-d}v)^{\beta}=(u+\sqrt{-d}v)^{2(p+1)t}\cdot(u(z)+\sqrt{-d}v(z)).$$

And therefore, we have

$$\Re\{(u+\sqrt{-d}v)^{2(p+1)t+z}\}\equiv$$
$$\equiv A_0(z)+A_1(z)t+\cdots+A_{n-1}(z)t^{n-1}\,(\mathrm{mod}\,p^n), \tag{13}$$

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

Now define for which values of z the congruence $v(z)\equiv 0(\mathrm{mod}\,p)$ holds.

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

Then

$$(u+\sqrt{-d}v)^{z}=u(z)+\sqrt{-d}pv_0(z)$$

$$(u+\sqrt{-d}v)^{z(p-1)p^{n-k}}\equiv(u(z))^{(p-1)p^{n-k}}\,(\mathrm{mod}\,p^n).$$

The sequences $\{(u+\sqrt{-d}v)^{2\beta}\}$ and $\{g^{\alpha}\}$ can have two common elements modulo p: 1 or -1. Then

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

The congruence $(u(z))^{(p-1)p^{n-k}}\equiv -1(\mathrm{mod}\,p^n)$ impossible because otherwise we would be 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,

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

$$z(p-1)p^{n-k}\equiv 0(m_0d\,2(p+1)p^{n-1}).$$

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

$$p\|A_1(z),\ A_i(z)\equiv 0(\mathrm{mod}\,p^2),\qquad i=2,\ldots,n-1 \text{ if } z\neq 0, z\neq p+1;$$

$$A_1(0)=A_1(p+1)\equiv 0(\mathrm{mod}\,p^2),\quad p^2\|A_2(0)\ p^2\|A_2(p+1),$$

$$A_j(0)\equiv A_j(p+1)\equiv 0(\mathrm{mod}\,p^3),\quad j=3,4,\ldots,n-1.$$

We use below the following lemma.

Lemma (Generalized Gauss sum)**.** *Let $\mathfrak{p}$ be the prime odd number from imaginary quadratic field, $m \geqslant 1$ be the natural, $\alpha_1, \alpha_2, \ldots, \alpha_n \in G$, $(\alpha_2, \mathfrak{p}) = 1$. Then for any natural $k \geqslant 2$ we have*

$$\left| \sum_{\omega \in G_{\mathfrak{p}^m}} \exp\left(\pi i Sp\left(\frac{\alpha_1\omega + \mathfrak{p}\alpha_2\omega^2 + \mathfrak{p}^3\alpha_3\omega^3 + \cdots + \mathfrak{p}^k\alpha_k\omega^k}{\mathfrak{p}^m}\right)\right)\right| =$$

$$= \begin{cases} 0, & \text{if } \ (\alpha_1, \mathfrak{p}) = 1 \pmod{\mathfrak{p}}, \\ (N(\mathfrak{p}))^{\frac{m+1}{2}}, & \text{if } \ \alpha_1 \equiv 0 \pmod{\mathfrak{p}}. \end{cases}$$

Now we can prove the following statement.

Theorem 3. *Let p be a prime irreducible number, $h \in \mathbb{Z}$, $(h,p) = 1$, $k > 1$ be the natural, a, b are integer numbers in $\mathbb{Z}[\theta]$, $(a,p) = (b,p) = 1$. Then for $n \geqslant 2$*

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

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

Proof. Applying lemma about the structure of group $G^*_{p^n}$, we can write a, b in form

$$a = g^{\alpha'_0}(u+\theta v)^{\beta'_0}, \ b = g^{\alpha''_0}(u+\theta v)^{\beta''_0}.$$

where g be the primitive root $\bmod\, p^n$ in $\mathbb{Z}$, $u + \theta v$ be the generative element of group E_n.

Then we obtain

$$\widetilde{K}(a,b;h,p^n;k) =$$

$$= \sum_{\substack{x,y \in \mathbb{G}_{p^n} \\ N(x)N(y) \equiv h \pmod{p^n}}} e_{p^n}\left(g^{\alpha'_0}\Re((u+\theta v)^{\beta'_0}x^k) + g^{\alpha''_0}\Re((u+\theta v)^{\beta''_0}y^k)\right). \tag{14}$$

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

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

The sum over $x \in \mathbb{G}_{p^n}$ in (14) we will split in two parts, $\sum = \sum_1 + \sum_2$. In the sum $\sum_1$ we put such $x \in \mathbb{G}_{p^n}$, for which

$$N(x) \equiv g^{2\alpha_1} \pmod{p^n},$$

and in the sum $\sum_2$ will falling such $x \in \mathbb{G}_{p^n}$, for which

$$N(x) \equiv -g^{2\alpha_1} (\operatorname{mod} p^n).$$

For both cases we have that α_1 runs over all values $0, 1, \ldots, \frac{p-1}{2} p^{n-1} - 1$.

Hence,

$$\widetilde{K}(a, b; h, p^n; k) = \sum\nolimits_1 + \sum\nolimits_2 \tag{15}$$

For x from $\sum_1$ we have

$$x \equiv g^{\alpha_1} (u + \theta v)^{2\beta_1} (\operatorname{mod} p^n),$$

$$\alpha_1 = 0, 1, \ldots, \tfrac{1}{2}(p-1)p^{n-1} - 1; \;\; \beta_1 = 0, 1, \ldots, (p+1)p^{n-1} - 1.$$

It means that

$$\Re((u + \theta v)^{\beta_0'} x^k) \equiv g^{k\alpha_1} \Re((u + \theta v)^{2k\beta_1 + \beta_0'}) (\operatorname{mod} p^n).$$

From condition $N(x)N(y) \equiv h (\operatorname{mod} p^n)$ it follows that

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

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

And so we have

$$\sum\nolimits_1 = \sum_{(\alpha_1)} \sum_{(\beta_1)} \sum_{(\beta_2)} e_{p^n}(\mathfrak{U}), \tag{16}$$

where

$$(\mathfrak{U}) = (g^{\alpha_0' + \alpha_1 k} \Re((u + \theta v)^{2k\beta_1 + \beta_0'}) + g^{\alpha_0'' + \alpha_2 k} \Re((u + \theta v)^{2k\beta_2 + \beta_0'' + \delta k}))$$

here (α_1) means that α_1 runs over all values $0, 1, \ldots, \frac{1}{2}(p-1)p^{n-1} - 1$; (β_i) run over all $0, 1, \ldots, (p+1)p^{n-1} - 1$, $(i = 1, 2)$; and, moreover, $\delta = 0$ if $h \equiv g^{2\alpha_0} (\operatorname{mod} p^n)$ and $\delta = 1$ if $h \equiv -g^{2\alpha_0} (\operatorname{mod} p^n)$.

Similarly,

$$\sum\nolimits_2 = \sum_{(\alpha_1)} \sum_{(\beta_1)} \sum_{(\beta_2)} e_{p^n}(\mathfrak{V}) \tag{17}$$

where

$$(\mathfrak{V}) = (g^{\alpha_0' + \alpha_1 k} \Re((u + iv)^{2k\beta_1 + \beta_0' + 1}) + g^{\alpha_0'' + \alpha_2 k} \Re((u + \theta v)^{2k\beta_2 + \beta_0'' + \delta k})).$$

Let assume again

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

Then

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

Now from (13)-(14) and Lemma 1.1 it follows that the sums over t_i are equal to zero if the congruences

$$\begin{aligned} &\beta_0' + 2kz_1 \equiv 0(\mathrm{mod}(p+1)),\\ &\beta_0'' + 2kz_2 + k\delta \equiv 0(\mathrm{mod}(p+1)) \text{ for the sum} \textstyle\sum_1,\\ \\ &\beta_0' + 2kz_1 + 1 \equiv 0(\mathrm{mod}(p+1)),\\ &\beta_0'' + 2kz_2 + k\delta \equiv 0(\mathrm{mod}(p+1)) \text{ for the sum} \textstyle\sum_2, \end{aligned} \tag{18}$$

are violated.

Therefore, the one from sums $\sum_1$ or $\sum_2$ is always equal to zero. The relations (18) can be hold only for $(k, p+1)^2$ pairs of values (z_1, z_2). Let $\mathfrak{B}$ be the set of such values (z_1, z_2).

From (13)-(14) we obtain

$$\widetilde{K}(a, b; h, p^n; k) = \sum_{(\alpha_1)} e_{p^n}(N_0 g^{\alpha_1} + M_0 g^{\alpha_2}) \times$$

$$\times \sum_{(z_1,z_2)\in\mathfrak{B}} \ \sum_{t_1,t_2 (\mathrm{mod}\, p^{n-1})} e_{p^{n-2}}(F_1(kt_1) g^{\alpha_1} + F_2(kt_2) g^{\alpha_2}),$$

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

The sums over t_1, t_2 are calculated similarly. Let $k = p^m k_1$, $(k_1, p) = 1$. Let split the sum over t_i by the blocks with length of p^{n-2-2m}(if $2m < n-2$). Then, applying the lemma above, we obtain

$$\widetilde{K}(a, b; h, p^n; k) = p^{n+2m} \sum_{(\alpha_1)} e_{p^n}(N_1 g^{\alpha_1} + N_2 g^{\alpha_2}), \tag{19}$$

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

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

The sum in righthand of (19) is an incomplete Kloosterman sum. By selection of primitive root g we have

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

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

$$\alpha_1 = (p-1)t + z,$$

$$t = 0, 1, \ldots, \tfrac{1}{2}(p^{n-1} - 1),\ z = 0, 1, \ldots, p-2.$$

Then

$$g^{\alpha_1} = g^z(1 + a_1pt + a_2p^2t^2 + a_3p^{\lambda_3}t^3 + \cdots) \pmod{p^n},$$

$$a_1 \equiv -u_1,\ a_2 \equiv -2'u^2 \pmod p,\ \lambda_j \geqslant 3.$$

Similarly, we have

$$g^{\lambda_2} \equiv g^{\alpha_0}g'^{\alpha_1} \equiv g^{\alpha_0}g'^{z}(1 + b_1pt + b_2p^2t^2 + b_3p^{\mu_3}t^3 + \cdots) \pmod{p^n}$$

$$b_1 \equiv -u_1,\ b_2 \equiv -2'u^2 \pmod p,\ \mu_j \geqslant 3.$$

Therefore,

$$N_1g^{\alpha_1} + N_2g^{\alpha_2} \equiv c_0 + c_1pt + c_2p^2t^2 + c_3p^{\nu_3}t^3 + \cdots \pmod{p^n},$$

where $c_i = g^z a_i N_1 + g^{\alpha_0}g'^z b_i N_2,\ (i = 1, 2)$.
By virtue of $(N_1, p) = (N_2, p) = 1$ it easy to see that two congruences

$$c_1 \equiv 0 \pmod p, \qquad c_2 \equiv 0 \pmod p$$

can not be hold at once.

But from $c_1 \equiv 0 \pmod p$ it follows that $g^{2z} \equiv g^{\alpha_0}N_2N_1' \pmod p$. It is possible only for single value of z. Denote this value as z_0.

Then from (19) we get

$$\widetilde{K}(a, b; h, p^n; k) = p^{n+2m}\times$$

$$\times\Bigg(\sum_{\substack{z=0\\ z\neq z_0}}^{p-2}\ \sum_{t=0}^{\frac12(p^{n-1}-1)} e^{2\pi i\frac{c_0}{p^n}} \cdot e_p^{n-1}\big(c_1t + c_2pt^2 + c_3p^{\nu_3-1}t^3 + \cdots\big) + \qquad (20)$$

$$+\sum_{t=0}^{\frac12(p^{n-1}-1)} e^{2\pi i\frac{c_0'}{p^n}} \cdot e_{p^{n-2}}\big(c_1't + c_2't^2 + c_3'p^{\nu_3-2}t^3 + \cdots\big)\Bigg),$$

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

The sums over t are incomplete rational sums, which estimates we obtaining in help with the estimates of complete exponential sums.

For arbitrary polynomial $\Phi(t) \in \mathbb{Z}[t]$ we have

$$\left|\sum_{t=0}^{T} e^{2\pi i\frac{\Phi(t)}{q}} - \frac{T}{q}\sum_{t=0}^{q-1} e^{2\pi i\frac{\Phi(t)}{q}}\right| \leqslant \qquad (21)$$

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

Now if $\Phi(t) = c_1 t + c_2 p t^2 + c_3 p^{\nu_3 - 1} t^3 + \cdots$, $(c_1, p) = 1$, $q = p^{n-1}$ then the complete sums in (21) are equal to zero for all r except the case $r \equiv c_1 (\bmod p)$. In this special case we have $\Psi(t) = c_1' t + c_2' t^2 + c_3' p^{\nu_3 - 1} t^3 + \cdots$, $(c_2', p) = 1$, $q = p^{n-2}$ and then the complete sum is estimated as $2p^{\frac{n-2}{2}}$.

Hence,

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

Finally, taking into account that for different values z we have different values for $c_1(z) (\bmod p)$ and then we obtain

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

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

From now we continue with the estimating of Kloosterman sum $\widetilde{K}(a, b; h, p^n; k)$ on the ellipse bound for the case of factorable p and for $k \geqslant 2$, $(a, p) = (b, p) = 1$.

In this case we have $p = \mathfrak{p}\overline{\mathfrak{p}}$, where $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are the complex-conjugate prime numbers over $\mathbb{Z}[\theta]$. Then the reduced residue system $\bmod p^n$ can be rewrite as

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

where g be the primitive root $\bmod p^n$ such that

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

Therefore

$$N(x) = x \cdot \overline{x} =$$

$$= g^{2\ell_1} p^n + g^{\ell_2} p^n + g^{\ell_1 + \ell_2} \overline{\mathfrak{p}}^{2n} + g^{\ell_1 + \ell_2} \mathfrak{p}^{2n} \equiv \tag{22}$$

$$\equiv g^{\ell_1 + \ell_2} Sp(\mathfrak{p}^{2n}) (\bmod p^n).$$

Moreover, if $\mathfrak{p} = a_0 + \theta b_0$ then $(a_0, p) = (b_0, p) = 1$ and by induction we easy obtain

$$\mathfrak{p}^{2n} \equiv a_n + \theta b_n, \; n = 1, 2, \ldots,$$

where

$$a_n \equiv \begin{cases} (-1)^{n-1} \cdot 2^m \cdot a_0 \cdot {b_0}^{2(m-1)} (\operatorname{mod} p) & \text{if} \quad n = 2m-1, \\ (-1)^m \cdot 2^{m+2} \cdot d^{2m} & \text{if} \quad n = 2m \end{cases}$$

$$b_n \equiv \begin{cases} (-1)^{2m-1} \cdot 2^m \cdot {b_0}^{2m-1} (\operatorname{mod} p) & \text{if} \quad n = 2m-1, \\ (-1)^{m-1} \cdot 2^{m+2} \cdot a_0 \cdot {b_0}^{2m-1} (\operatorname{mod} p) & \text{if} \quad n = 2m \end{cases}$$

From here for the factorable p we have

$$\begin{aligned} &\widetilde{K}(a, b; h, p^n; k) = \\ &= \sum_{(U)} e_{p^n}(A(g^{\ell_1' k} + g^{\ell_2' k}) + B(g^{\ell_1'' k} + g^{\ell_2'' k})) = \\ &= \sum_{(U')} e_{p^n}(A(x_1^k + x_2^k) + B(y_1^k + y_2^k)), \end{aligned} \tag{23}$$

where

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

$$U' := \left\{ x_1, x_2, y_1, y_2 (\operatorname{mod} p^n) \middle| x_1 x_2 y_1 y_2 \equiv H (\operatorname{mod} p^n) \right\},$$

$$A, B, \in \mathbb{Z},\ (A, p) = (B, p) = 1.$$

Theorem 4. *Let p be factorable prime number and let $a, b \in \mathbb{Z}[\theta]$, $(a, p) = (b, p) = 1$. Then*

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

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

Proof. Without loss of generality we can suppose that $a, b \in \mathbb{Z}$.

In virtue of (23) and by an analogue of the case of irreducible p we obtain

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

Now, for $(d-1)^4 < p$ we obtain by an analogue of the case with irreducible p

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

$$= \left(\sum_{x\in\mathbb{F}_p^*}\chi(x)e_p(Ax^d)\right)^2\left(\sum_{y\in\mathbb{F}_p^*}\chi(y)e_p(By^d)\right)^2.$$

From here,

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

Then

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

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

Let G be the group of multiplicative characters of field $\mathbb{F}_p$. For $\chi\in G$ we have
$\chi(x) = e_{p-1}(\nu\cdot ind\,x)$ with some $\nu\in\mathbb{F}_p$. Then using the assertion of theorem about estimate of exponential sum of Gauss type, we obtain the following relation

$$\widetilde{K}(a,b;h,p;d) =$$

$$= \tfrac{1}{p-1}\sum_{\chi\in G}\overline{\chi}(H)\sum_{s_1,\ldots,s_4=0}^{d-1}\overline{\chi}(A^2B^2)\times$$

$$\times\, e_d((s_1+s_2)ind\,A + (s_3+s_4)ind\,B)\times$$

$$\times\sum_{x_1,\ldots,x_4\in\mathbb{F}_p^*} e_d(s_1 ind\,x_1 + \cdots + s_4 ind\,x_4)\times$$

$$\times\,\chi(x_1,\ldots,x_4)e_p(x_1+\cdots+x_4) =$$

$$= \tfrac{1}{p-1}\sum_{\nu\in\mathbb{F}_p}\sum_{s_1,\ldots,s_4=0}^{d-1} e_{p-1}(\nu\cdot ind\,H)e_{p-1}(F_1(\nu,s))\times$$

$$\times\sum_{x_1,\ldots,x_4\in\mathbb{F}_p^*} e_{p-1}(F_2(\nu,s,x))e_p(x_1+\cdots+x_4).$$

where

$$F_1(\nu,s) := (2\nu + (s_1+s_2)\tfrac{p-1}{d})ind\,A + (2\nu + (s_3+s_4)\tfrac{p-1}{d})ind\,B$$

$$F_2(\nu,s,x) := (s_1\tfrac{p-1}{d}+\nu)ind\,x_1 + \cdots + (s_4\tfrac{p-1}{d}+\nu)ind\,x_4.$$

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

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

□

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

$$\begin{array}{l} x_i = y_i + p^m z_i,\\ y_i(\operatorname{mod} p^m),\\ z_i(\operatorname{mod} p^{n-m}),\\ (y_i,p)=1,\\ i=1,2,3;\ m=\left[\frac{n+1}{2}\right]\\ x_4 = Hy_1'y_2'y_3'(1-p^my_1'z_1-p^my_2'z_2-p^my_3'z_3),\\ y_iy_i' \equiv 1(\operatorname{mod} p^m).\end{array} \tag{24}$$

Theorem 5. *Let p be the irreducible prime number in the ring $\mathbb{Z}[\theta]$, $n\in\mathbb{N}$, $n\geqslant 2$; $h\in\mathbb{Z}$, $(h,p)=1$; $a,b\in\mathbb{Z}[\theta]$, $(a,p)=(b,p)=1$. Then*

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

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

Proof. From (23)-(24) we have

$$\begin{aligned}&\widetilde{K}(a,b;h,p^n;k) =\\ &= \sum_{y_1,y_2,y_3\in\mathbb{Z}^*_{p^m}} e_{p^n}(f(y_1,y_2,y_3))\times\\ &\times \sum_{z_1,z_2,z_3(\operatorname{mod} p^{n-m})} e_{p^{n-m}}(F(z_1,z_2,z_3)),\end{aligned} \tag{25}$$

where

$$f(y_1, y_2, y_3) = Ay_1^k + ay_2^k + By_3^k + BH{y'_1}^k {y'_2}^k {y'_3}^k,$$

$$F(z_1, z_2, z_3) = k\Big[(Ay_1^{k-1} - B{y'_1}^{k+1}{y'_2}^k{y'_3}^k)z_1 +$$

$$+ (Ay_2^{k-1} - B(y_1^{k+1}y_2^k y_3^k)')z_2 + (Ay_3^{k-1} - B(y_1^k y_2^k y_3^{k+1})')z_3\Big].$$

Let $(k, p^{n-m}) = p^\ell$. Then from (25) we obtain

$$\widetilde{K}(a, b; h, p^n; k) = p^{3(n-m)} \sum_{S(C)} e_{p^n}(f(y_1, y_2, y_3)), \tag{26}$$

where

$$C := \left\{ y_1, y_2, y_3 (\operatorname{mod} p^m) \;\middle|\; \begin{array}{l} (y_i, p) = 1,\ i = 1, 2, 3; \\ y_1^k \equiv {y_2}^k \equiv {y_3}^k (\operatorname{mod} p^{n-m-\ell}), \\ y_1^{4k} \equiv BA' (\operatorname{mod} p^{n-m-\ell}) \end{array} \right\}.$$

Now, for $n = 2m$ we estimate the sum $\sum\limits_{S(U)}$ by the number of triples $(y_1, y_2, y_3) \in C$, and for $n = 2m - 1$ we get

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

In case of even n we have the similar estimate. □

Collecting previous estimates of theorems 2-5, we obtain

Theorem. *Let $\alpha, \beta \in \mathbb{Z}[\theta]$ and let $h, q, k, n \in \mathbb{N}$, $k \geqslant 2$, $(k, q) = (h, q) = 1$. 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

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

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

We have to note that the Kloosterman sum on the ellipse $\widetilde{K}(\alpha, \beta; h, q; k)$ has no an analogue in the ring $\mathbb{Z}$.

In help with obtained estimates of Kloosterman sums on the ellipse it can be constructed the asymptotic formulas for the divisors sum $\tau_k(\alpha)$, $k = 2, 3, \ldots$, $\alpha\mathbb{Z}[\theta]$ (see, for example, [9]).

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] Bruggeman R.,Fourier Coefficients of Automorphic Forms // Lecture Notes in Math., Springer Verlag, Berlin, 1981. – pp.865.

[4] Bruggeman R.W., Fourier coefficients of cusp forms, // Invent. Math..-1978.-Vol. 445.-P. 1-18.

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

[6] Kloosterman H., On the representatin of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$ // Acta Math.- 49(1926).-p. 407-464.

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

[8] Motohashi Y., Spectral Theory of the Riemann zeta-function // Cambridge: Cambridge Univ, 1997.

[9] Antonina Radova, Sergey Varbanets On exponential sums involving the divisor function over $\mathbb{Z}[i]$ // Annales Univ. Sci. Budapest., Sect. Comp. – 2017. – V. 46. – pp.235–246.

[10] O. Savastru, S. Varbanets, Norm Kloosterman sums over $\mathbb{Z}[i]$ // Algebra and Discrete Mathematics. – 2011. – Volume 11(2) . – pp.82–91.

[11] Weill A., On some exponential sums // Proc. Nat. Acad. Sci. USA.- 34(1948).- p.204-207.

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

CONTACT INFORMATION

Sergey Varbanets Odessa I.I. Mechnikov National University, str. Dvoryanskaya 2, 65086 Odessa, Ukraine
E-Mail(s): svarbanets@onu.edu.ua

Yakov Vorobyov Izmail State University of Humanities, str. Repina 12, 68601 Izmail, Ukraine
E-Mail(s): yashavoro@gmail.com

Received by the editors: 14.12.2022.