International Electronic Journal of Pure and Applied Mathematics

Volume 8 No. 3 2014, 123-132
ISSN: 1314-0744
url: http://www.e.ijpam.eu
doi: http://dx.doi.org/10.12732/iejpam.v8i3.4

TWISTED KLOOSTERMAN SUM OVER NORM GROUP

S. Sergeev
I.I. Mechnikov National University
Odessa, UKRAINE

1. Introduction

In 1948, as a consequene of his resolution of the Riemann hypothesis for zeta-function of curve over finite field, A. Weil [6] established the following celebrated character sum estimates associated to additive and multiplicative characters

$$\left|\sum_{x\in\mathbb{F}_q}\chi(g(x))\phi(f(x))\right|\leq(m+n-1)\sqrt{q}$$

where $\mathbb{F}_q$ be a finite field of characteristic p and cardinality q; $g(u)$ be a nonzero rational function over k, $f(u)$ be a polynomial over k of degree n, χ be a multiplicative character of $\mathbb{F}_q^*$ of order d, m the total degree of the places ν in supp f such the order of g at ν is not a multiple of d (suppose $m>0$), ϕ be a non-trivial additive character of $\mathbb{F}_q$.

This result of Weil standed foundation for the construction non-trivial estimates of various exponential sums, particularly twisted Kloosterman sums.

Since the Kloosterman sums are importance not only in analytic number theory but its applications (for example, in cryptography or theory of coding) at the present time the varians generalisations of the Kloosterman sums are studying.

In 2006 W.-C.W. Li [1] investigated mixed exponential sum with additive and multiplicative characters in a quadratic extension $\mathbb{F}_q^*$ of finite field $\mathbb{F}_q$.He obtained

Received: June 2, 2014

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 8, No. 3 (2014)

also the "root bound"

$$\left| \sum_{\substack{x \in \mathbb{F}^*_{q^2} \\ N(x)=1}} \chi(x)\phi(f(Tr(\gamma x))) \right| \leq 2n\sqrt{q}$$

where $N(x)$ and $Tr(x)$ denote the norm and trace of x from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ (respectively); $f(n)$ be a polynomial over $\mathbb{F}_{q^2}$ of degree n prime to p, and χ and ϕ respectively are multiplicative and non-trivial additive characters over $\mathbb{F}^*_{q^2}$ and $\mathbb{F}_{q^2}$.

In present paper we will obtain non-trivial estimates for the generalized twister Kloosterman sums over $\mathbb{Z}[i]$:

$$K_\chi(\alpha, \beta; E_m) := \sum_{\substack{x_1, x_2 \in E^*_m \\ x_1 x_2 \equiv 1 (mod \mathrm{p}^m)}} \chi(x_1) e^{\pi i Tr\left(\frac{\alpha x_1 + \beta x_2}{\mathrm{p}^m}\right)}$$

S. Sergeev and P. Varbanets [2] study the sum $K_\chi(\alpha, \beta; E_m)$ with the principal character $\chi mod \mathrm{p}^m$ and P. Varbanets and S. Varbanets [4] investigated similar sum with polynomials as arguments of additive and multiplicative characters.

2. Notation and Preliminary Results

Before studying such sums, we standardize some notation to be used throughout this paper.

Lower case Roman (or Greek, respectively) letters usually denote rational (or Gaussian, respectively) integers; in particular, m, n, k are positive integers and p is always a rational prime $\mathrm{p} \equiv 3(mod 4)$. We also define a "norm" on $\mathbb{Q}(i)$ into $\mathbb{Q}$ by $N(\alpha) = |\alpha|^2$ and trace α as $Tr(\alpha)$.

For the sake of convenience, we denote by G the set of the Gaussian integers. Let $\mathbb{Z}_q$ (or G_q) denote the ring of the residue classes modulo q, and $\mathbb{Z}^*_q$ (or G^*_q) denote the multiplicative group in $\mathbb{Z}_q$ (or G_q). If $x \in G^*_q$ we write x^{-1} for the multiplicative inverse of $x mod q$, i.e. x^{-1} is any Gaussian integer satisfying $xx^{-1} \equiv 1(mod q)$. As usual, $gcd(a, b)$ or (a, b) stand for the greatest common divisor of a and b (or respecctively,α and $\beta \in G$). Through $\mathbb{Z}[x]$ (or $G[x]$) we denote the polynomial ring over $\mathbb{Z}$ (or G). For $a \in \mathbb{Z}$ (or $\alpha \in G$) stand $\nu_\mathrm{p}(a)$ (or $\nu_\mathrm{p}(\alpha)$) if $\mathrm{p}^{\nu_\mathrm{p}(a)} | a, \mathrm{p}^{\nu_\mathrm{p}(a)+1} \not| a$. Moreover, $\sum\limits_{S(c)}$ means the summation under the condition C, which describes additionaly. For $\alpha \in G_{\mathrm{p}^m}$ denote $ord\alpha$ the order α in G_{p^m}. Finally, we put $e_q(t) = e^{2\pi i \frac{t}{q}}$.

Before starting out study of $K_\chi(\alpha,\beta;E_m)$ several lemmas will be used in sequal.

It well-known that for $\mathrm{p}\equiv 3(mod4)$ the ring of residue classes modulo p over G finite field $\mathbb{F}_{\mathrm{p}^2}$, and thus the group G^*_{p} is a cyclic group of order p^2-1.

Next, we denote by E_m the following subgroups in $G^*_{\mathrm{p}^m}$

$$E_m := \left\{x\in G^*_{\mathrm{p}^m} : N(x)\equiv \pm 1(mod\mathrm{p}^m)\right\}$$

$$E^+_m := \left\{x\in G^*_{\mathrm{p}^m} : N(x)\equiv 1(mod\mathrm{p}^m)\right\}$$

The subgroup E^+_m we call the norm group in $G^*_{\mathrm{p}^m}$

Lemma 1. *[5] Let us $u+iv\in E_m$ be a generatring element of E_m. The $ord(u+iv)=|E_m|=2(\mathrm{p}+1)\mathrm{p}^{\mathrm{m}-1}$ and*

$$(u+iv)^{2(\mathrm{p}+1)} = 1+\mathrm{p}^2x_0+i\mathrm{p}y_0,$$

$$x_0+2y_0\equiv 1(mod\mathrm{p}), (x_0,\mathrm{p})=(y_0,\mathrm{p})=1$$

and also for any $t=4,5,\ldots$ we have modulo p^m

$$\begin{array}{l} Re(u+iv)^{2(\mathrm{p}+1)t}\equiv A_0+A_1t+A_2t^2+\cdots+A_{m-1}t^{m-1}\\ Re(u+iv)^{2(\mathrm{p}+1)t}\equiv B_0+B_1t+B_2t^2+\cdots+B_{m-1}t^{m-1}\end{array} \tag{1}$$

where

$$\begin{cases} A_0\equiv 1(mod\mathrm{p}^4), B_0\equiv 0(mod\mathrm{p}^4)\\ A_1\equiv \mathrm{p}^2x_0+\frac{1}{2}\mathrm{p}^2y_0^2\equiv 0(mod\mathrm{p}^3), B_1\equiv \mathrm{p}y_0(mod\mathrm{p}^3)\\ A_2\equiv -\frac{1}{2}\mathrm{p}^2y_0^2(mod\mathrm{p}^3), B_2\equiv 0(mod\mathrm{p}^3)\\ A_j\equiv B_j\equiv 0(mod\mathrm{p}^3), j=3,4,\ldots,m-1\end{cases} \tag{2}$$

Denote

$$\begin{array}{l}(u+iv)^k = u(k)+iv(k), 0\le k\le 2\mathrm{p}+1,\\ (u+iv)^{2(\mathrm{p}+1)t+k}\equiv \sum\limits_{j=0}^{m-1}\left(A_j(k)+iB_j(k)\right)t^j(mod\mathrm{p}^m)\end{array}$$

It is clear

$$\begin{array}{l}A_j(k)=A_ju(k)-B_jv(k)\\ B_j(k)=A_jv(k)+B_ju(k)\end{array}$$

Thus from Lemma 1 we have

Corollary. *For* $k = 1, 2, \dots, 2\mathrm{p}+1$ *we have*

$$u(k) \equiv u(-k), v(k) \equiv -v(-k)(mod\mathrm{p}^m),$$

$$(u(k),\mathrm{p}) \equiv (v(k),\mathrm{p}) \equiv 1 \text{ if } k \equiv 0 \left(mod\tfrac{\mathrm{p}+1}{2}\right),$$

$$u(0) = 1, v(0) = 0, (u(\mathrm{p}+1),\mathrm{p}) = 1, \mathrm{p}||v(\mathrm{p}+1),$$

$$u(k) \equiv 0(mod\mathrm{p}), (v(k),\mathrm{p}) = 1 \text{ if } k = \tfrac{\mathrm{p}+1}{2} or \tfrac{3(\mathrm{p}+1)}{2}$$

Moreover, for $k \not\equiv 0 \left(mod\frac{\mathrm{p}+1}{2}\right)$

$$A_0(k) = u(k), B_0(k) = v(k)(mod\mathrm{p}),$$
$$p||A_1(k), p||B_1(k), p^2||A_2(k), p^2||B_2(k);$$

and

$$A_1(0) \equiv 0(mod\mathrm{p}^4), B_1(0) \equiv \mathrm{p}y_0(mod\mathrm{p}^4), \mathrm{p}^2||A_2(0), B_2(0) \equiv (mod\mathrm{p}^3),$$

$$(A_0(\mathrm{p}+1),\mathrm{p}) = 1, \mathrm{p}||B_0(\mathrm{p}+1), \mathrm{p}^2||A_1(\mathrm{p}+1), \mathrm{p}||B_1(\mathrm{p}+1)$$

$$\mathrm{p}^2||A_2(\mathrm{p}+1), B_2(\mathrm{p}+1) \equiv 0(mod\mathrm{p}^3);$$

$$A_0(k) \equiv 0, B_0(k) \equiv 0(mod\mathrm{p}),$$

$$\mathrm{p}||A_1(k), \mathrm{p}^2||B_1(k), \mathrm{p}^2||A_2(k), B_2(k) \equiv 0(mod\mathrm{p}^3) \text{ if } k = \tfrac{\mathrm{p}+1}{2} \text{ or } \tfrac{3(\mathrm{p}+1)}{2}$$

$$A_j(k) \equiv B_j(k) \equiv 0(mod\mathrm{p}^3), k = 0, 1, \dots, 2\mathrm{p}+1, j \geq 3.$$

The proof of this Corollary is a simple exercise (in view the congruences $(u + iv)^{2(\mathrm{p}+1)} = 1 + \mathrm{p}^2 x_0 + iy_0, (x_0,\mathrm{p}) = (y_0,\mathrm{p}) = 1, 2x_0 + y_0^2 \equiv 0(mod\mathrm{p}), u^2 + v^2 \equiv -1(mod\mathrm{p}^m)$), and we omit.

Lemma 2. *[5] Let* $f(x)$ *and* $g(x)$ *be polynomials over* G*,*

$$f(x) = A_1x + A_2x^2 + \cdots + A_rx^r$$
$$g(x) = B_1x + B_2x^2 + \cdots + B_sx^s$$

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 8, No. 3 (2014)

and, moreover, let

$$\begin{array}{l} 0 \le \nu_{\mathrm{p}}(A_2) < \nu_{\mathrm{p}}(A_j), j \ge 3, \\ (B_1, \mathrm{p}) = 1, \nu_{\mathrm{p}}(B_j) \ge 1, j = 2, 3, \ldots \\ \left| \sum_{x \in G_{\mathrm{p}^m}} e_{\mathrm{p}^m} \left(Re\left(f(x)\right)\right) \right| \le \\ \le \begin{cases} 0 & \text{if } \nu_{\mathrm{p}}(A_1) < \nu_{\mathrm{p}}(A_2), \\ 2^{\frac{m}{2}} \mathrm{p}^{m + \frac{1}{2}\nu_{\mathrm{p}}(A_2)} & \text{if } \nu_{\mathrm{p}}(A_2) < m, \nu_{\mathrm{p}}(A_1) > \nu_{\mathrm{p}}(A_2), \\ \mathrm{p}^m & \text{if } \nu_{\mathrm{p}}(A_2) \ge m \end{cases} \end{array} \tag{3}$$

$$\left| \sum_{x \in G^*_{\mathrm{p}^m}} e_{\mathrm{p}^m} \left(Re(f(x) + g(x^{-1})) \right) \right| \le 2 I_0^{\frac{m}{2}} \mathrm{p}^m, \tag{4}$$

where I_0 *is the number of solutions of the congruence* $A_1 U^2 \equiv 0 (mod \mathrm{p})$ *over* G^*_{p}.

Remark. The estimate (3) in the rational case take a form

$$\left| \sum_{x \in \mathbb{Z}_{\mathrm{p}^m}} e_{\mathrm{p}^m} \left(f(x) \right) \right| \le \begin{cases} 0 & \text{if } \nu_{\mathrm{p}}(A_1) < \nu_{\mathrm{p}}(A_2), \\ 2^{\frac{m}{2}} \mathrm{p}^{m + \nu_2(A_2)} & \text{if } \nu_{\mathrm{p}}(A_1) \ge \nu_{\mathrm{p}}(A_2) \end{cases} \tag{3'}$$

3. Twisted Exponential Sum over E_m^+

So we consider the following sum

$$K_\chi(\alpha, \beta; E_m^*) := \sum_{\substack{x, y \in E_m^+ \\ xy \equiv 1 (mod \mathrm{p}^m)}} \chi(x) e_{\mathrm{p}^m}(Tr(\alpha x + \beta y))$$

Let us $(\alpha, \beta, \mathrm{p}) = 1$ (general case easy reduce to this case). Note that for $\alpha \notin E_m^+, \beta \notin E_m^+$ the equality $K_\chi(\alpha, \beta; E_m^+) = \overline{\chi}(\alpha) K(1, \alpha\beta; E_m^+)$ can be violated.

We will distinguish two cases: $m = 1$ and $m > 1$.

First lef us $m = 1$. By Hilbert theorem every element y with norm one from normal extension K of the field P can be prescribe in the form

$$y = \frac{\sigma(z)}{z}, z \in K$$

where σ be a generating automorphism of Gaious group of K over P. Moreover, z is defined uniquely accurate to factor from P.

In our case $P = \mathbb{Z}_{\mathrm{p}}, K = G, [K : P] = 2$, and for $a + bi \in G$, we have

$$\sigma(a + bi) \equiv (a + bi)^{\mathrm{p}} \equiv a - bi (mod \mathrm{p})$$

Only two elements ± 1 is an element from $\mathbb{Z}_{\rm p}$ with norm equal $1(mod{\rm p})$. Thus for $a+bi \in G, a+bi \notin \mathbb{Z}$ we have $b \not\equiv (mod{\rm p})$, and then every element from $G_{\rm p} n \mathbb{Z}_{\rm p}$ with norm $\equiv 1(mod{\rm p})$ uniquely write in the form

$$y = \pm i, y = \frac{a-i}{a+i} \text{ or } y = i\frac{a-i}{a+i}, a \in \mathbb{Z}_{\rm p}$$

Hence, we obtain the description of elements from E_1^*

$$E_1 = \left\{ \pm 1, \pm i, \frac{a-i}{a+i}, i\frac{a-i}{a+i} : a = 1, \ldots, {\rm p}-1 \right\}$$

Taking into account that $\frac{a-i}{a+i} = 1 - 2i\frac{1}{a+i}$, we obtain

$$\begin{aligned} \sum_{\substack{x,y \in E_1 \\ xy \equiv 1(mod{\rm p})}} \chi(x) e_{\rm p}(Tr(\alpha x + \beta y)) &= \sum_{a \in \mathbb{Z}_{\rm p}^*} \chi\left(1 - 2i\tfrac{1}{a+i}\right) e_{\rm p}(R_1(a)) + \\ &+ \sum_{a \in \mathbb{Z}_{\rm p}^*} \chi\left(1 + 2i\tfrac{1}{a+i}\right) e_{\rm p}(R_2(a)) + \\ &+ O(1), \end{aligned}$$

where $R_1(u), R_2(u)$ are rational functions over $\mathbb{Z}_{\rm p}$.

Now for a principal character χ_0 by [6], the last two sums estimate as $\leq 2\sqrt{\rm p}$. Hence we obtain

$$\left| \sum_{\substack{x,y \in E_1 \\ xy \equiv 1(mod{\rm p})}} \chi_0(x) e_{\rm p}(Tr(\alpha x + \beta y)) \right| \leq 6\sqrt{\rm p} \tag{5}$$

If χ is a non-principal character then multiplicative character $mod{\rm p}$ over $G_{\rm p}^*$ can replace by additive character of the field $G_{\rm p}$ and we again obtained analogous estimate (for a detail see [1]).

$$\left| \sum_{\substack{x,y \in E_1 \\ xy \equiv 1(mod{\rm p})}} \chi(x) e_{\rm p}(Tr(\alpha x + \beta y)) \right| \leq 6\sqrt{\rm p}$$

For $m > 1$ by Lemma 1 we will use the following representations for $x, y \in E_m$

$$
\begin{aligned}
&x = (u+iv)^{2(\mathrm{p}+1)t+k} \equiv \sum_{j=0}^{m-1} \left(A_j(k) + iB_j(k)\right) t^j (mod \mathrm{p}^m) \\
&y = (u+iv)^{-2(\mathrm{p}+1)t-k} \equiv \sum_{j=0}^{m-1} \left(A_j(-k) + iB_j(-k)\right) (-1)^j t^j (mod \mathrm{p}^m), \\
&t \in \mathbb{Z}_{\mathrm{p}^{m-1}}, k \in \{0, 1, \ldots, 2(\mathrm{p}+1)-1\}
\end{aligned}
\tag{6}
$$

By Lemma 1 we have

$$
\begin{aligned}
A_j(k) &= A_j u(k) - B_j v(k) \\
B_k(-k) &= -A_j v(k) + B_j u(k)
\end{aligned}
$$

Moreover,

$$A_0(k) \equiv u(k), B_0(k) \equiv v(k) (mod \mathrm{p}), \text{ if } k \neq \tfrac{\mathrm{p}+1}{2} \text{ and } \tfrac{3(\mathrm{p}+1)}{2}$$

$$A_0(k) \equiv 0, B_0(k) \not\equiv 0 (mod \mathrm{p}), \text{ if } k = \tfrac{\mathrm{p}+1}{2} \text{ or } \tfrac{3(\mathrm{p}+1)}{2}$$

Hence, for any k we have

$$\chi(x) = \chi(A_0(k) + iB_0(k)) \cdot \chi\left(1 + \mathrm{p} \sum_{j=0}^{m-1} \left(A'_j(k) + iB'_j(k)\right) t^j\right) \tag{7}$$

where $A'_j(k)\frac{1}{\mathrm{p}} = A_j(k), B'_j(k) = \frac{1}{\mathrm{p}} B_j(k)$

We will use the following analogue of Postnikov's lemma

Lemma 3. *([3], Lemma 1) Let $\mathrm{p} \equiv 3(mod 4)$ be a prime, $n \geq 2$ be a positive integer. There exists a polynomial $F(u)$ with the coefficients from G*

$$F(u) = u + a_2 u^2 + \ldots + a_{N-1} u^{N-1}, N < 2n,$$

such that, for any character of the subgroup $U_n \subset G^*_{\mathrm{p}^n}$, $U_n = \left\{1 + \mathrm{p}u : u \in G_{\mathrm{p}^{n-1}}\right\}$ we have

$$\chi(1 + \mathrm{p}u) = e_{\mathrm{p}^{n-1}}(Tr(\Lambda F(u)))$$

where $\Lambda \in G_{\mathrm{p}^{n-1}}$ depends only χ, and the coefficients a_k satisfy the condition $a_k \equiv (-1)^k \frac{\mathrm{p}^{k-1}}{k} (mod \mathrm{p}^n)$, and hence,

$$\nu_{\mathrm{p}}(a_k) \geq k - \nu_{\mathrm{p}}(k) - 1, k = 2, 3, \ldots$$

Remark. This Lemma shows that any non-trivial character modulo p^n of subgroup U_n can replace on additive character modulo p^{n-1}.

Now we are able to prove the main assertion this paper.

Theorem. *Let* p *be a prime number,* $\mathrm{p} \equiv 3(mod4), \alpha, \beta \in G, (\alpha, \beta, \mathrm{p}) = 1$, *and let* χ *be a character modulo* $\mathrm{p}^m, m \geq 1$, *of the group* G_{p^m}*. Then the following estimate*

$$K_\chi(\alpha, \beta, E_m) << \begin{cases} \mathrm{p}^{\frac{m}{2}} & \text{if } \chi \text{ is a primitive character,} \\ \mathrm{p}^{\frac{m+1}{2}} & \text{if } \chi \text{ is a non-primitive character.} \end{cases}$$

Proof. The case $m = 1$ was proved above. Let us $m > 1$. On account (7), we have

$$\alpha x + \beta y = \sum_{j=0}^{m-1} X_j(k) t^j, \tag{8}$$

where

$$\begin{aligned} X_1(k) &\equiv \alpha(A_1(k) + iB_1(k)) - \beta(A_1(-k) + iB_1(-k)) \equiv \\ &\equiv (-\alpha y_0 v(k) + \beta y_0 u(k)) + i\mathrm{p}(-\alpha y_0 v(k) - \beta y_0 u(k)) \equiv \\ &\equiv \mathrm{p} y_0(-\alpha y_0 v(k)(1+i) - \beta u(k)(1+i))(mod\mathrm{p}^3), \end{aligned} \tag{9}$$

$$\begin{aligned} X_2(k) &\equiv \alpha(A_2(k) - iB_2(k)) + \beta(A_2(-k) + iB_2(-k)) \equiv \\ &\equiv -\tfrac{1}{2}\mathrm{p}^2 y_0^2((\alpha u(k) - \beta u(k)) + i(-\alpha v(k) - \beta v(k))) \equiv \\ &\equiv -\tfrac{1}{2}\mathrm{p}^2 y_0^2(\alpha(u(k) - iv(k)) - \beta(u(k) + iv(k))) \equiv \\ &\equiv -\tfrac{1}{2}\mathrm{p}^2 y_0^2((\alpha - \beta)u(k) - i(\alpha + \beta)v(k))(modo\mathrm{p}^3), \\ X_j(k) &\equiv 0(mod\mathrm{p}^3), j \geq 3 \\ y_0 &= y_0(k) := A_0(k) + iB_0(k) \equiv u(k) + iv(k) \end{aligned} \tag{10}$$

Moreover, we have

$$\chi(x) = \chi(y_0(k))\chi(1 + \mathrm{p}x_1),$$

where $x_1 = \frac{y_0^{-1}(k)}{\mathrm{p}} \sum_{j=1}^{m-1} (A_j(k) + iB_j(k))\, t^j \in G_{\mathrm{p}^{m-1}}$ for $t \in \mathbb{Z}_{\mathrm{p}^{m-1}}$ $y_0^{-1}(k)$ denotes that $y_0(k) y_o^{-1}(k) \equiv 1(mod\mathrm{p}^m)$.

Hence, by Lemma 3, we obtain

$$\chi(x) = \chi(x_1(k)) e_{\mathrm{p}^{m-1}}(Tr(\Lambda F(x_1)))$$

where Λ be defined by the character χ and

$$F(x_1) \equiv x_1 - \frac{1}{2}\mathrm{p}x_1^2 + \frac{1}{6}\mathrm{p}^2 x_1^3 + \ldots (mod\mathrm{p}^m) \tag{11}$$

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 8, No. 3 (2014)

So by (8)-(11) we deduce

$$|K_\chi(\alpha,\beta;E_m)| = \left|\sum_{k=0}^{2p+1}\chi(y_0(k))e_{p^m}\sum_{t\in\mathbb{Z}_{p^{m-1}}} e_{p^{m-1}}\left(Tr\left(\sum_{j=1}^{m-1}Y_j(k)t^j\right)\right)\right| \tag{12}$$

where

$$\begin{aligned} Y_j(k) \quad &\equiv \quad \tfrac{\Lambda}{p}X_j(k) + \Lambda\tfrac{y_0^{-1}(k)}{p}\Big(A_j(k)+iB_j(k)+\Lambda\tfrac{2y_0^{-1}(k)}{p^2}\cdot \\ &\cdot \sum_{l_1+l_2=j}(A_{l_1}(k)+iB_{l_1}(k))\cdot(A_{l_2}(k)+iB_{l_2}(k))\Big)\,(mod p^3) \end{aligned} \tag{13}$$

From (13) we see that the exponential sum on the right-hand side in (13) can be estimated by Lemma 1. For this purpose we consider coefficients $Y_1(k)$ and $Y_2(k)$. We have modulo p^2

$$\begin{aligned} Y_1(k) \quad &\equiv \quad \tfrac{1}{p}X_1(k) + \Lambda\tfrac{y_0^{-1}(k)}{p}(A_1(k)+iB_1(k)) \\ Y_2(k) \quad &\equiv \quad \tfrac{1}{p}X_2(k) + \Lambda\tfrac{y_0^{-1}(k)}{p}(A_2(k)+iB_2(k)) + \\ &+\Lambda\tfrac{2y_0^{-1}(k)}{p^2}(A_1(k)+iB_1(k))^2 \end{aligned} \tag{14}$$

Obviously, $Re(Y_2(k)) \not\equiv 0(mod p)$ only if $Re(\Lambda(A_1(k)+iB_1(k))^2) \not\equiv 0(mod p)$ and then Lemma 1 gives

$$|K_\chi(\alpha,\beta;E_m)| \le 2p^{\frac{m-1}{2}}\cdot 2p \le 4p^{\frac{m+1}{2}} \tag{15}$$

For $Re(\Lambda(A_1(k)+iB_i(k))^2) \equiv 0(mod p)$ we can be handled similarly [2] that there is at most $O(1)$ values of k such that $Re(X_1(k)) \equiv 0(mod p)$. Thus in that case

$$|K_\chi(\alpha,\beta;E_m)| << p^{\frac{m}{2}}. \tag{16}$$

Hence, we proved theorem.

References

[1] W.-C.W.Li, Character sums over norm group, Finite fields and their Application, 12 (2006), 1-15, DOI 10.1016/j.ffa.2004.06.006.

[2] Sergeev S., Varnabets P, Exponential sums over norm group (to appear in iauliaii Math., Semin).

[3] Varbanets P. and Varbanets S., Twisted Kloosterman sum $\mathbb{Z}[i]$, Ukr, Math, Jorn., 66 (5) (2014), 609-618.

[4] Varbanets P., Varbanets S., Generalized twisted exponential sum, Siauliai Math. Semin., 8 (16) (2013), 267-279.

[5] Varbanets S., General Kloosterman sums over ring of Gaussian integers, Ukr. Math. Jorn., 59 (9), 2007, 1179-2000, DOI 10.1007/s11253-007-0090-4.

[6] Weil A., On some exponential sums, Proc. Nat. Acad. Sci. USA, 34 (1948), 204-207, DOI 10.1073/pnas.34.5.204.